МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Кафедра банківської справи

Допущено до захисту
Завідувач кафедри _____Л. В. Жердецька
“_____” _____ 2024 року

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття освітнього ступеня бакалавра зі спеціальності 072 «Фінанси, банківська справа та страхування» за освітньо-професійною програмою «Міжнародний банківський бізнес» на тему:
«Організаційно - методичні засади інформаційної безпеки банку в умовах невизначеності»

Виконавець:
студент 4 курсу, групи 3 ФФБС
ГОЛИКОВ Андрій Олександрович
_____
Науковий керівник:
К.е.н., доцент кафедри банківського справи
СЕРГЄЄВА Олена Степанівна
_____

ОДЕСА – 2024

АНОТАЦІЯ

Голиков А.О.. «Організаційно - методичні засади інформаційної безпеки банку в умовах невизначеності»

Кваліфікаційна робота на здобуття освітнього ступеня бакалавра зі спеціальності «Фінанси, банківська справа та страхування» – Одеський національний економічний університет. – Одеса, 2024.

У роботі визначаються теоретичні аспекти обґрунтування поняття «інформаційна безпека банку»: наукові підходи, функції, напрями, розглянуто характеристики чинників та загроз, які мають вплив на інформаційну безпеку банку, проведена оцінка дотримання інформаційної безпеки АТ «А – БАНК» за напрями «інформаційне поле», «інформаційні ресурси» та «інформаційна інфраструктура» за 2020 – 2024 рр. на початок періоду, розглянуто світові виклики, які вимушують банки удосконалювати свою інформаційну безпеку та надані рекомендації щодо підвищення інформаційної безпеки банків України в умовах діючого воєнного стану

За результатами зроблені висновки щодо удосконалення інформаційної безпеки банків України в умовах діючого воєнного стану, а тощо удосконалення системи контроля банків, через підвищення ролі контролінгу, через формування в працівниках банків професійної досконалості щодо прийняття правильних рішень та мінімізації операційних ризиків.

Результати кваліфікаційної роботи отримано з урахуванням сукупності загальнонаукових і спеціальних методів дослідження, а саме: абстрактно-логічний, аналітичний, графічний, аналізу та синтезу, економіко-статистичний. структурно-динамічного аналізу, порівняльного аналізу.

Ключові слова: банк, інформаційна безпека, загрози, ризик, цифровізація.

ANNOTATION

GOLYKOV A.O. « Organizationally - methodical principles of bank information security in conditions of uncertainty»

Qualification work for a bachelor's degree in Finance, banking and insurance – Odesa National Economic University. – Odesa, 2024.

The work defines the theoretical aspects of the justification of the concept of "bank information security": scientific approaches, functions, directions, the characteristics of factors and threats that have an impact on the bank's information security are considered, an assessment of compliance with information security of JSC "A - BANK" in the directions of "information field ", "information resources" and "information infrastructure" for 2020 - 2024 at the beginning of the period, global challenges that force banks to improve their information security were considered, and recommendations were given to improve the information security of Ukrainian banks in the current state of war

Based on the results, conclusions were drawn regarding the improvement of the information security of Ukrainian banks in the conditions of the current state of war, as well as the improvement of the bank control system, through increasing the role of controlling, through the formation of professional excellence in bank employees regarding making the right decisions and minimizing operational risks.

The results of the qualification work were obtained taking into account a set of general scientific and special research methods, namely: abstract-logical, analytical, graphic, analysis and synthesis, economic-statistical. structural and dynamic analysis, comparative analysis.

Keywords: bank, information security, threats, risk, digitalization.

ЗМІСТ

ВСТУП

Стрімкий розвиток інформаційних технологій, розширення глобального інформаційного середовища, широке застосування засобів обміну інформацією, всеохоплююча комп'ютеризація всіх сфер життєдіяльності зумовлюють актуальність дослідження питань безпеки інформаційної інфраструктури. Забезпечення ефективного захисту інформації є надзвичайно актуальним і для установ банківської сфери, де щоденно оброблюється великий обсяг інформації різного рівня конфіденційності.

На сьогодні банки відіграють надважливу роль у забезпеченні сталого розвитку економіки, адже саме вони є тими фінансовими посередниками, що забезпечують постачання ліквідності на фінансовий ринок та забезпечують кредитування реального сектору економіки. Банки належать до об'єктів критичної інфраструктури, що є стратегічно важливими для функціонування економіки та безпеки держави. Однією з нових загроз втрати стійкості банків в умовах переходу на шостий технологічний уклад та пов'язаного з цим застосування технологій Індустрії 4.0, таких як штучний інтелект, «хмарні» та «туманні» обчислення, IoT / IIoT, Big Data, Blockchain, VR / AR є кіберзагрози, ландшафт яких постійно трансформується та оновлюється. Зважаючи на це, банки мають формувати комплекс заходів, інструментів та механізмів для забезпечення інформаційної безпеки, кіберстійкості як здатності протистояти зовнішнім та внутрішнім загрозам, спричинених кіберризиками, адаптуватися до них та / або відновлюватися після них.

Вивченням питанням безпеки банків займалися такі науковці як М. Зубок М., Баранівський О., Букін С., Бланк І., Вовчак О., П. Гайдуцький П., Геєць В., Гіжевський В., Гриценко Р., Криклій О., Коваленко В. Проте питання розробки ефективної системи забезпечення банківської інформаційної безпеки ще потребують подальшого вивчення.

Визначені проблеми підвищують актуальність дослідження в напряму рекомендацій щодо удосконалення інформаційної безпеки банків в умовах невизначеності та кіберзагроз.

Метою кваліфікаційної роботи є теоретичне узагальнення, яке полягає у розгляді поняття «інформаційна безпека банку» та запропонуванні рекомендацій щодо підвищення її в умовах невизначеності (воєнного стану).

Для досягнення мети в роботі було поставлено наступні задачі:

- обґрунтувати поняття «інформаційна безпека» через визначення наукових підходів, функцій, видів та напрямів;
- надати характеристику загроз, що впливають на інформаційну безпеку банків та визначити правове регулювання, яке регламентує дотримання інформаційної безпеки в банках;
- провести оцінку діяльності АТ «А – БАНК» в українському інформаційному полі;
- проаналізувати дотримання безпеки інформаційних ресурсів АТ «А – БАНК»;
- оцінити дотримання безпеки інформаційної інфраструктури АТ «А – БАНК
- ознайомитися зі світовими викликами, які впливають на інформаційну безпеку банків;
- надати рекомендації щодо підвищення інформаційної безпеки банків України та АТ «А - БАНК» в умовах діючого воєнного стану.

Об'єктом дослідження є процес організації та дотримання інформаційної безпеки в Акціонерне товариство «АКЦЕНТ-БАНК» (далі АТ «А – БАНК»).

Предметом дослідження є теоретико-методичні засади організації процесів організація та дотримання інформаційної безпеки банку в умовах невизначеності.

Методи дослідження. Теоретичною основою кваліфікаційної роботи є положення економічної теорії банківської справи та фінансового

менеджменту, дослідження вітчизняних науковців з питань організації та забезпечення інформаційної безпеки в банках. Результати кваліфікаційної роботи отримано з урахуванням сукупності загальнонаукових і спеціальних методів дослідження, а саме: системний – для визначення економічної сутності поняття «інформаційна безпека банку», джерел, особливостей та чинників його виникнення; угруповань і класифікацій – для систематизації чинників, які впливають на інформаційну безпеку; економіко-математичні методи – для аналізу впливу чинників на формування прибутку банку, які впливають на розмір його економічного результату; порівняльного – співставлення результатів діяльності АТ «А – БАНК» на 01.01.2020 – 2024 рр., дослідженню діючих інструментів та впровадження нових технологій щодо підвищення інформаційної безпеки банків в умовах цифровізації.

Інформаційну базу дослідження становили дослідження українських науковців, Закони та Постанова НБУ, офіційні відкриті статистичні бази Державної служби статистики України, Міністерства фінансів України, аналітичні матеріали Національного банку України, фінансова звітність АТ «А-БАНК», розрахунки автора.

Апробація результатів дослідження. По темі кваліфікаційної роботи була прийнята участь у VII Міжнародної науково-практичної Інтернет-конференції «ФІНАНСИ, БАНКІВСЬКА СИСТЕМА ТА СТРАХУВАННЯ В УКРАЇНІ: СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ В КРИЗОВІЙ ЕКОНОМІЦІ» м. Дніпро, 4-5.03.2024 р. та опубліковані тези на тему «Удосконалення механізму фінансової стійкості банків в умовах воєнного стану».

Кваліфікаційна робота бакалавра складається зі вступу, трьох розділів, висновків, списку використаних джерел (73 найменування). Загальний обсяг роботи становить 96 сторінок. Основний зміст викладено на 82 сторінках. Робота містить 20 таблиць, 26 рисунка, 4 додатки.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

1.1. Економічне обґрунтування поняття «інформаційної безпеки банку»: наукові підходи, функції, принципи та напрями

Сучасний світ вступив в період динамічних інноваційних змін, що відображається насамперед у процесах глобалізації, що охоплюють всі сфери життя суспільства, насамперед банківську сферу. У зв'язку зі зазначеними процесами банки відчувають певний тиск та піддаються додатковим загрозам, які змушують їх коригувати політику в галузі управління та розвитку. Нові умови діяльності вимагають не тільки активного використання традиційних банківських рішень, а й впровадження передових досягнень науки і техніки, реалізованих в різних напрямах використання інформаційного забезпечення.

Як вказують більша частина економічних джерел цифрова (інформаційна) економіка (англ. Digital economy) «це тип економіки, де ключовими факторами та засобами виробництва є цифрові дані (бінарні, інформаційні тощо) та мережеві транзакції, а також їх використання як ресурсу, що дає змогу істотно збільшити ефективність та продуктивність діяльності та цінність для отриманих продуктів та послуг» [1]. Цифрову економіку також іноді називають інформаційною економікою, інтернет-економікою, новою економікою, або веб-економікою.

Впродовж більш десятиріччя український бізнес знаходиться в трансформації до цифровізації усіх бізнес-процесів, що спонукає банки з класичним веденням бізнесу вкладати великі суми в сучасні інформаційні технології як для підвищення конкурентоспроможності самого банку, для залучення нових клієнтів та привабливості діючих. Економічна користь інформаційно-технологічних нововведень на результативність банку можливо розглядати з двох боків, як суттєве скорочення операційних витрат, так зниження вартості одержаної інформації.

Однак, сучасна діяльність банків на пряму пов’язується «з забезпеченням кіберстійкості банків на сучасному етапі розвитку цифрової економіки країни, зважаючи на негативний фінансовий та нефінансовий вплив кібератак на банківську систему та економіку країни в цілому» [2].

З цього приводу фокусуючи увагу на нових викликах цифрової сучасності банкам необхідно перебудовувати та модернізувати свої ІТ-інфраструктури, а як слід необхідності формування та постійного удосконалення інформаційної безпеки самого банку.

Для визначення терміну «інформаційна безпека банку» логічно з початку розглянути цілком визначення поняття «безпека банку» та її складових.

На думку вченого Зубка М.І. з яким ми повністю погоджуємось, «безпека банку – стан стійкої життєдіяльності, за якого забезпечується реалізація основних інтересів і пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування. Основна мета безпеки банку - виключити можливість нанесення йому збитків або упущення вигоди та забезпечити ефективну його діяльність і якісну реалізацію всіх операцій та угод» [3].

Автори «Енциклопедія банківської справи» визначають безпеку банків як «систему заходів, яка забезпечує захищеність інтересів власників, клієнтів, працівників і керівництво банку від зовнішніх та внутрішніх загроз» [4].

Авторка Коваленко В.В. трактує «систему безпеки банківської діяльності можна визначити як організовану сукупність спеціальних органів, коштів, методів і заходів, що забезпечують захист діяльності від впливу внутрішніх та зовнішніх загроз» [5].

На думку Барановського О.І. «банківська безпека це сукупність умов, за яких потенційно небезпечні для фінансового стану комерційного банку дії чи обставини, попереджені чи зведені до такого рівня, за якого вони не здатні завдавати шкоди встановленому порядку функціонування банку» [6]. При цьому автор надає головне значення фінансової безпеки банку.

Узагальнюючи наукові підходи авторів щодо визначення поняття «безпека банку» можемо зазначити, що це комплексний процес захисту діяльності банків у всіх напрямах.

Можемо зазначати, що «актуальність забезпечення фінансової стійкості банків України в умовах війни набуває великого значення з погляду забезпечення їх життєдіяльності, здатності виконувати фінансові зобов'язання та відновлення економічного стану країни в післякризовий період» [7], а безпека банків створює усі умови для реалізації цієї стратегічної мети.

З приводу цього, розглянемо складові банківської безпеки, які представлені на рис. 1.1.

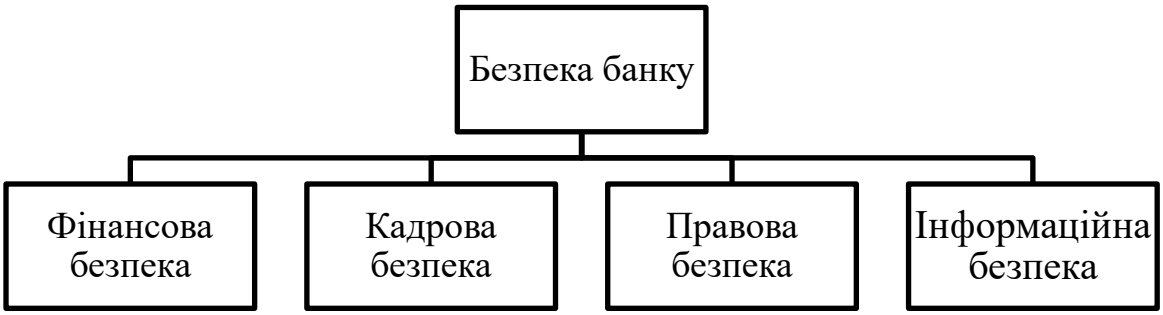

Рис. 1.1 Складові банківської безпеки

Джерело: складено автором за матеріалами [8]

З наведеного рис. 1.1 наочно видно, що тісний взаємозв'язок усіх складових надає повну безпеку діяльності банку. Практичний досвід діяльності банків показує, що головна помилка банків є в зосередженні уваги організації безпеки окремо по кожному з напрямів діяльності банків, що на нашу думку є не вірним.

Як зазначає науковиця Яременко С. М. «разом з тим, дослідження ролі, місця, видів безпеки у захисті інтересів банків показує, що банківська безпека має концентрувати свої зусилля насамперед навколо забезпечення саме фінансової безпеки банків та інформаційної безпеки, створюючи умови для формування високого рівня стійкості банків до впливу загроз, підтримання

ними своєї ліквідності та платоспроможності, у тому числі й під дією різного роду дестабілізуючих факторів» [9].

Отже, оскільки сучасні банки максимально працюють в інформаційному просторі, основою для банківської безпеки є інформаційна безпека як окремого банку, так цілком для усієї банківської системи України при взаємодії між усіма учасниками фінансового ринку.

В процесі дослідження важливе місце займає розкриття змісту досліджуваних понять. З нашої точки зору, можна погодитися з визначенням «інформаційна безпека банку», яке надано Світлічною В.Ю. а саме: «це стан інформаційної інфраструктури банку, за якого забезпечуються умови стабільного функціонування, максимізації прибутку, оптимального використання ресурсів банку, а також забезпечення захищеності клієнтів, співробітників і керівництва банку від зовнішніх і внутрішніх загроз» [10].

Слід зауважити, що організація інформаційної безпеки банків повинно забезпечуватись на основі інформації, яка в першу чергу пов’язана зі зовнішніми та внутрішніми джерелами (табл. 1.1).

Таблиця 1.1

Структура зовнішніх і внутрішніх джерел інформації, необхідної для організації інформаційної безпеки банків

Зовнішні джерела	Внутрішні джерела
Аналіз макроекономічного середовища: прогноз розвитку економіки; ділова активність у сфері послуг; політика уряду; міжнародні аспекти.	Аналіз змін активів та пасивів банків: обсяги операцій і ціни на активи та пасиви (абсолютні показники і спред); зростання активів та пасивів за період; порівняння основних показників зростання цін з фінансовими планами та бюджетом, даними за попередні періоди; тенденції у зміні показників

	Продовження табл. 1.1
Оцінка стану фінансових ринків: процентні ставки, обмінні курси і ціни на акції; оцінка ситуації на вторинному ринку боргових інструментів, емітованих банком і основними конкурентами; розподіл кредитного ризику на вторинному ринку; інновації та інституційні зміни.	Оцінка відповідності вимогам НБУ щодо: достатності капіталу; ліквідності; розподілу активів та пасивів за строками погашення; розміру валютної позиції; внутрішнім вимогам, встановленим у політиці банків.
	Аналіз валютної позиції: поточний стан; аналіз чутливості валютної позиції до валютних курсів; очікувана зміна валютної позиції з урахуванням передбачуваного зростання операцій; коригування позиції для захисту від зміни валютних курсів; варіанти закриття позицій за різних сценаріїв зміни валютних курсів
Регулювання, оподаткування та облік: очікувані зміни у регулюванні та їх вплив на управління активами та пасивами банків; оцінка витрат, викликаних передбачуваними змінами в регулюванні, оподаткуванні та обліку; оцінка ступеня захисту від несприятливих змін.	Аналіз позиції по процентному ризику: поточний стан; аналіз чутливості поточної позиції до змін процентних ставок; очікувана зміна позиції з урахуванням передбачуваного зростання операцій; коригування позиції для захисту від зміни процентних ставок; варіанти закриття нейтральних позицій за різних сценаріїв зміни процентних ставок

Джерело: складно автором за матеріалами [12]

Для повного розуміння поняття «інформаційна безпека банку» пропонуємо розглянути базові елементи з яких вона складається.

Як бачимо з рис. 1.2 поняття «інформаційна безпека» це важлива складова успішної діяльності будь-якого банку, формується з певних базових елементів таких як мета, завдання, суб’єктів та об’єктів.

Потрібно звернути увагу на функції інформаційної безпеки як сукупність заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації та інформаційних ресурсів. Функції інформаційної безпеки можуть бути класифіковані за різними критеріями, наприклад, за метою, за об’єктом захисту, за рівнем реалізації тощо. Надалі, пропонуємо розгляд функцій, які виконує категорія «інформаційна безпека банку» (рис. 1.3).

Рис. 1.2 Базові елементи інформаційної безпеки банків

Джерело: складено автором за матеріалами [11]

Як бачимо з рис. 1.3 до основних функцій інформаційної безпеки банків належать:

- превентивна (запобігання попередженням безпеки);
- детективна (виявлення порушень безпеки);
- реактивна (відновлення нормального функціонування після порушень безпеки);
- коректива (усунення причин та наслідків порушень безпеки).

Принципів інформаційної безпеки.

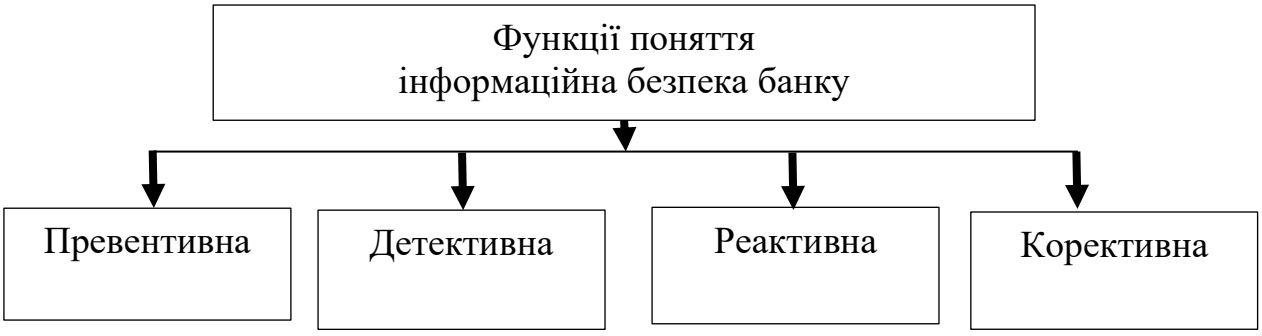

Рис. 1.3 Функції поняття «інформаційна безпека банків»

Джерело: авторська розробка

Визначення функцій інформаційної безпеки банків дає змогу надати нам розуміння принципів інформаційної безпеки – це сукупність правил, норм і вимог, які спрямовані на забезпечення конфіденційності, цілісності та доступності банківської інформації. Ці принципи базуються на міжнародних стандартах і рекомендаціях з питань інформаційної безпеки, а також на вимогах національного законодавства. Принципи інформаційної безпеки банків мають бути враховані при розробці, впровадженні та підтримці банківських інформаційних систем, а також при взаємодії з клієнтами, партнерами та органами контроля.

Отже, є всі підстави визначити, що в організації інформаційної безпеки сучасного банку необхідно відокремлювати наступні напрями (табл. 1.2).

Таблиця 1.2

Напрями забезпечення інформаційною безпекою та їх вплив на діяльність банків

Напрям	Об’єкт (суб’єкт) захисту	Канали загроз	Результативність впливу на інформ безпеку
Безпека «інформаційне поле»	Розповсюдження недостовірної інформації про діяльність банку (розповсюджується конкурентами, колишніми	- інтриги; - ажіотаж; - мозаїка подій; - провокація; - інсинуація	Бездоганна ділова репутація банку

	співробітниками, ЗМІ, у тому числі у мережі Інтернет, шахрайські веб-сайти), що несе репутаційний ризик		
Безпека інформаційних ресурсів	Інформаційні ресурси, які напряму чи опосередковано пов'язані як зі суб'єктами банку, так із об'єктами інформації про діяльність банку	- інформація з обмеженим доступом (комерційна таємниця; - персональні дані клієнтів та співробітників	Захист інформаційних ресурсів від навмисного та незаконного розголошення та використання конфіденційної інформації, мінімізація операційного ризику
Безпека інформаційної інфраструктури	Якість програмно-технологічних комплексів, комп'ютерного обладнання, ефективна СУІБ (система управлінням інформаційною системою банком)	- конфігурація та недосконаліть тестування та оцінка безпеки; - збій програмного та апаратного забезпечення; - коди програмно-технічних комплексів; - вразливості(ОСБД, телекомунікаційних технологій та протоколів); - зовнішні кібератаки	Забезпечення цілісності та доступності інформації в поєднанні з її безпекою, кібербезпекою, мінімізація операційного ризику

Джерело: складено автором за матеріалами [10]

Отже, наведемо характеристику кожному напряму, але розуміємо, що тільки сукупність цих напрямів формує багаторівневу інформаційну безпеку банків.

1. Напрям «Безпека «інформаційне поле»» банку сприяє підвищенню довіри клієнтів, партнерів та регулятору до банку, зменшенню ризиків втрати або пошкодження інформації, попередженню фінансових збитків та репутаційних ризиків. Міністерство юстиції України, визначає, що «недостовірною вважається інформація, яка не відповідає дійсності або

викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені)» [15].

2. Напрям «Безпека інформаційних ресурсів» реалізується через дотримання банківської таємниці. Згідно ЗУ «Про банки та банківську діяльність» [13] «банківська інформація є інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку» [13]. Своєю чергою банки зобов'язані через персонал та технічні засоби банку забезпечити банківську таємницю через:

– «обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю;

– організації спеціального діловодства з документами, що містять банківську таємницю;

– застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

– застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом» [14].

3. Напрям «Безпека інформаційної інфраструктури» є важливою необхідною складовою успішної діяльності банку, яка містить в себе всі системи, мережі, бази даних, програмне забезпечення та апаратне обладнання, які забезпечують обробку, зберігання, передачу та захист інформації. Безпека інформаційної інфраструктури банку вимагає застосування комплексу заходів, таких як криптографічний захист даних, аутентифікація користувачів, контроль доступу, моніторинг та аудит подій, резервне копіювання та відновлення даних, антивірусний захист, захист від зламу та вторгнення тощо.

Узагальнюючи зазначене вище, нами можемо сформувати визначення системи управління інформаційною безпекою, як «забезпечення захисту конфіденційності, цілісності та доступності інформаційних активів. Вона

складається з безлічі різних процесів, кожен з яких спрямований на обробку певних загроз» [7]. Це визначення нам дає нам привод для ствердження, що процес управління інформаційною безпекою складним, а управління інформаційною безпекою є постійним процесом і може застосовуватися до стандарту СОУ Н НБУ 65.1 СУІБ 1.0: 2010 PVPD, який представлено на рис. 1.4.

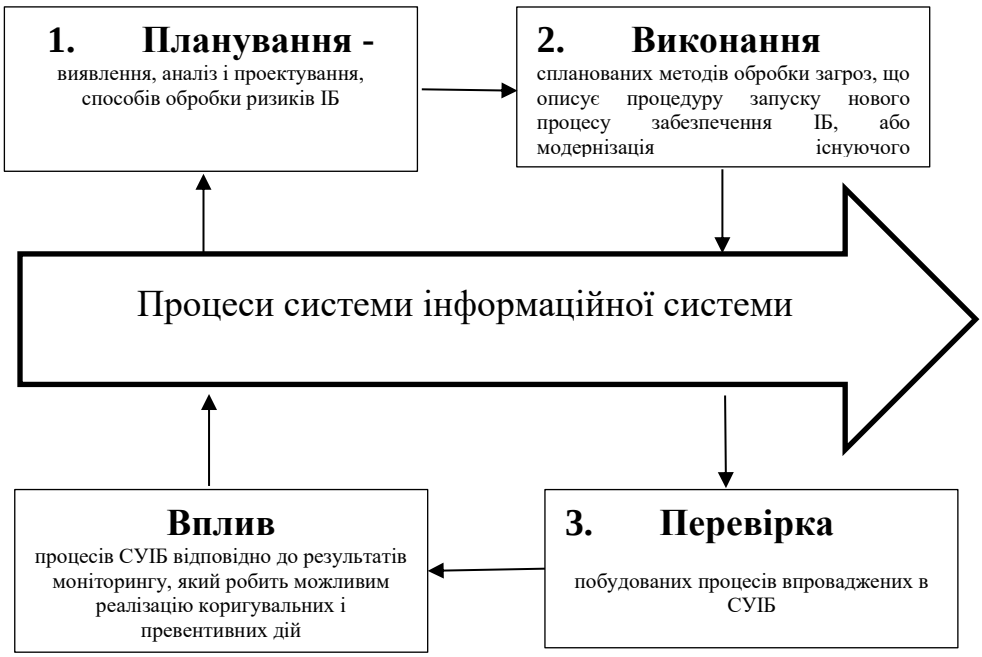

Рис. 1.4 Структура системи управління інформаційної безпеки [СОУ Н НБУ 65.1 СУІБ 1.0:2010].

Джерело: складено автором за матеріалами [7]

В практичній діяльності банків, технологічні процеси мають відображення в внутрішньому документів самого банку «Політика управління інформаційною безпекою», який складено на основі державних законодавчих нормативних документів.

Підсумовуючи все сказане, відзначимо, що для забезпечення надійного захисту даних клієнтів та партнерів, банк повинен використовувати сучасні технології, дотримуватися стандартів та регуляторних вимог, а також проводити регулярні аудити та перевірки. Банк також повинен нести відповідальність за підвищення обізнаності своїх співробітників та клієнтів

щодо загроз інформаційної безпеки та способів їх запобігання. В епоху цифрової економіки ці умови повинні бути одними з обов'язкових частин діяльності будь-якого сучасного банку, а захист конфіденційності як головний напрям.

1.2 Правове забезпечення, що регламентує дотримання інформаційної безпеки в банках

В сучасному світі для усіх суб'єктів фінансового ринку існують як зовнішні, так й внутрішні загрози, вплив яких може суттєво завдати шкоди для їх діяльності.

Сучасна діяльність банків пов'язана з невизначеністю, ризиками та кібератаками, тому можливо стверджувати, що усі чинники, які мають вплив на діяльність банків відображаються в фінансовому результаті банку, в першу чергу через дотримання інформаційною безпеки.

Сьогодні не можливо відокремлювати терміни «інформаційна безпека» та «кібербезпека», яка визначається як «кібербезпека банків, це трансформація інформаційної безпеки, яка спрямована на діджиталізовану середу функціонування банків», тому термін «кібербезпека має на увазі не тільки сам по собі захист інформації, а й захист всієї системи в інформаційному полі, в IT-полі в цілому» [16].

Взаємозв'язок понять "кіберзагроза", "кібербезпека", "кіберризик" і "кіберстійкість" представлено на рис. 1.5.

Розглянувши в підпункті 1.1 економічне обґрунтування «інформаційна безпека банку» пропонуємо надалі розглянути чинники впливу, загрози, шо впливають на інформаційну безпеку та можливі ризики, які можуть виникнути при її не дотриманні.

Рис. 1.5 Взаємозв'язок понять "кіберзагроза", "кібербезпека", "кіберризик" та "кіберстійкість"

Джерело: складено автором за матеріалами [58]

Розглянувши підходи науковців щодо визначення чинників впливу на банківську безпеку, під якими слід розуміти «явища чи процеси діяльності банків та / або зовнішні та внутрішні чинники, що призводять до зміни кількісних та / або якісних параметрів діяльності банків» [17], зазначимо, що не можливо відокремлювати загальну безпеку банку та інформаційну безпеку.

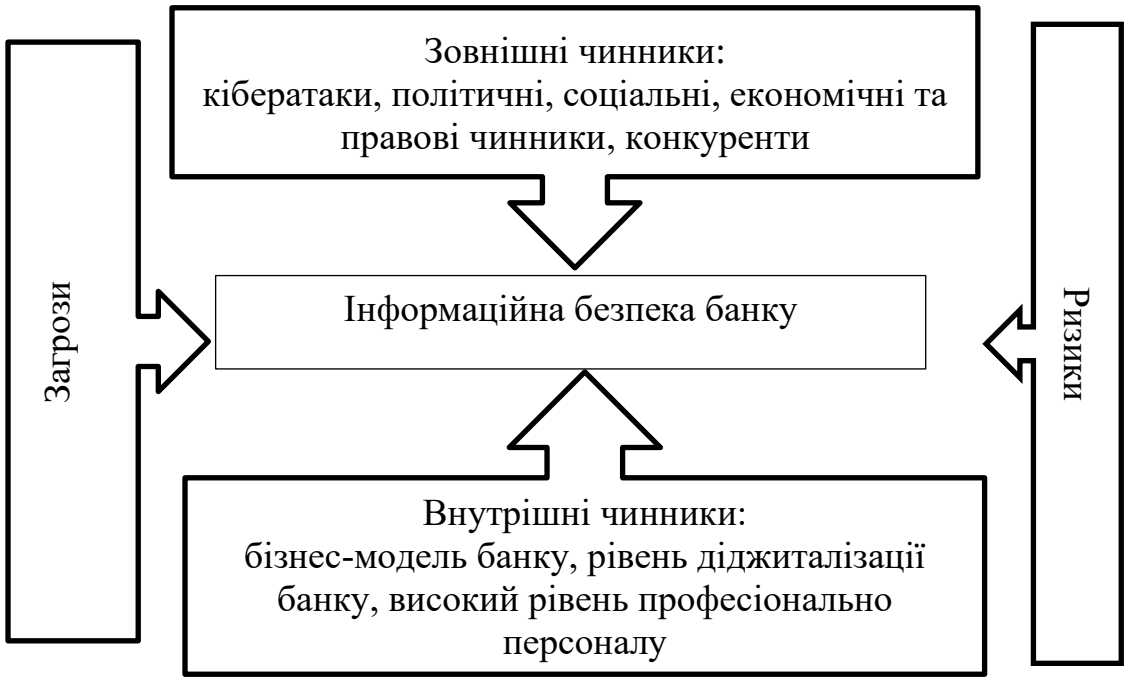

Рис. 1.6 Чинники впливу на інформаційну безпеку банку

Джерело: складено автором за матеріалами [17]

З рис. 1.6 наочно бачимо, що як зовнішні, так й внутрішні чинники мають достатній вплив діяльність банків, через недотримання інформаційної безпеки.

Ми погоджуємось, з автором Крупка І., який наголошує, «що зміни внутрішнього і зовнішнього середовища діяльності банківського сектору зумовлюють появу різноманітних загроз, які, зазвичай, мають фінансово-економічний характер» [18].

Зазначимо, що багато наукової дискусії стосовно прийняття понять «ризик» та «загроза» як розглядають ці дві категорії як синоніми. Ми не погоджуємось з цим твердженням, аргументуючи це тим, що прояв загрози може сприяти несприятливим обставинам, провокуючи ризик, що може дестабілізувати діяльність банку, але при ефективному ризико-орієнтованому підходу та впровадженні дій з боку як керівництва, так й самих співробітників цей ризик може бути мінімізовано чи знизити ступінь ризику до допустимого.

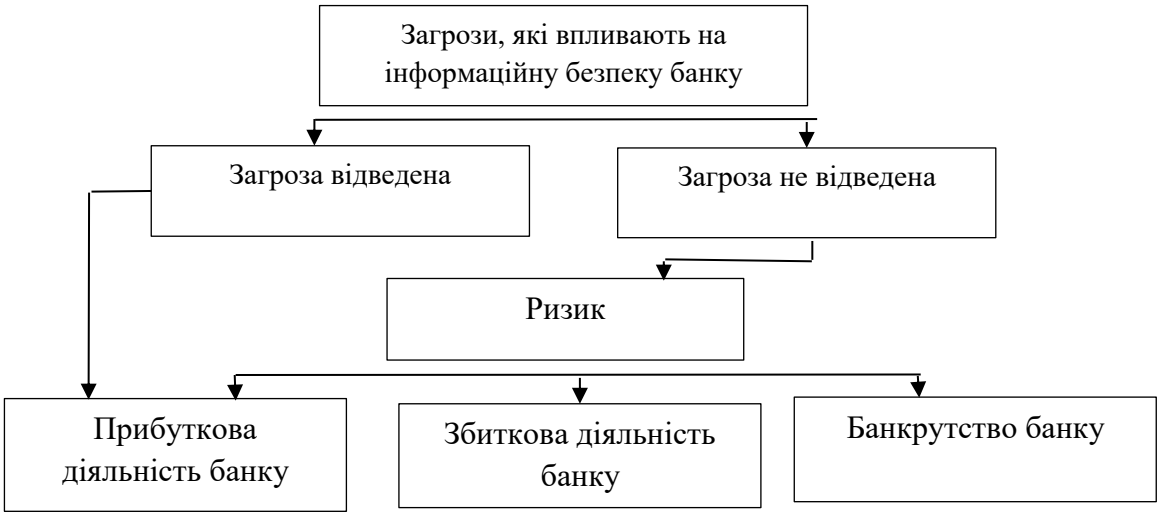

Рис. 1.7 Взаємодія загроз та ризиків в процесі забезпечення інформаційної безпеки банку

Джерело: складено автором за матеріалами [17]

Як свідчать дані рис 1.7, загрози, які можуть завдати інформаційної небезпеки банку можуть нанести банку як фінансових збитків, так й

нефінансового (втрата довіри клієнтів, контрагентів та ключових співробітників та ін.) в результаті чого може довести банк до збанкрутування.

Наступним етапом нашого дослідження пропонуємо розглянути ризики, які можуть виникати під впливом випадкових чи навмисних загроз на інформаційну безпеку банк.

До видів загроз інформаційної безпеки банків пропонуємо відносити наступні, при цьому об'єднуючи їх у дві групи випадкові та навмисні (рис. 1.8)..

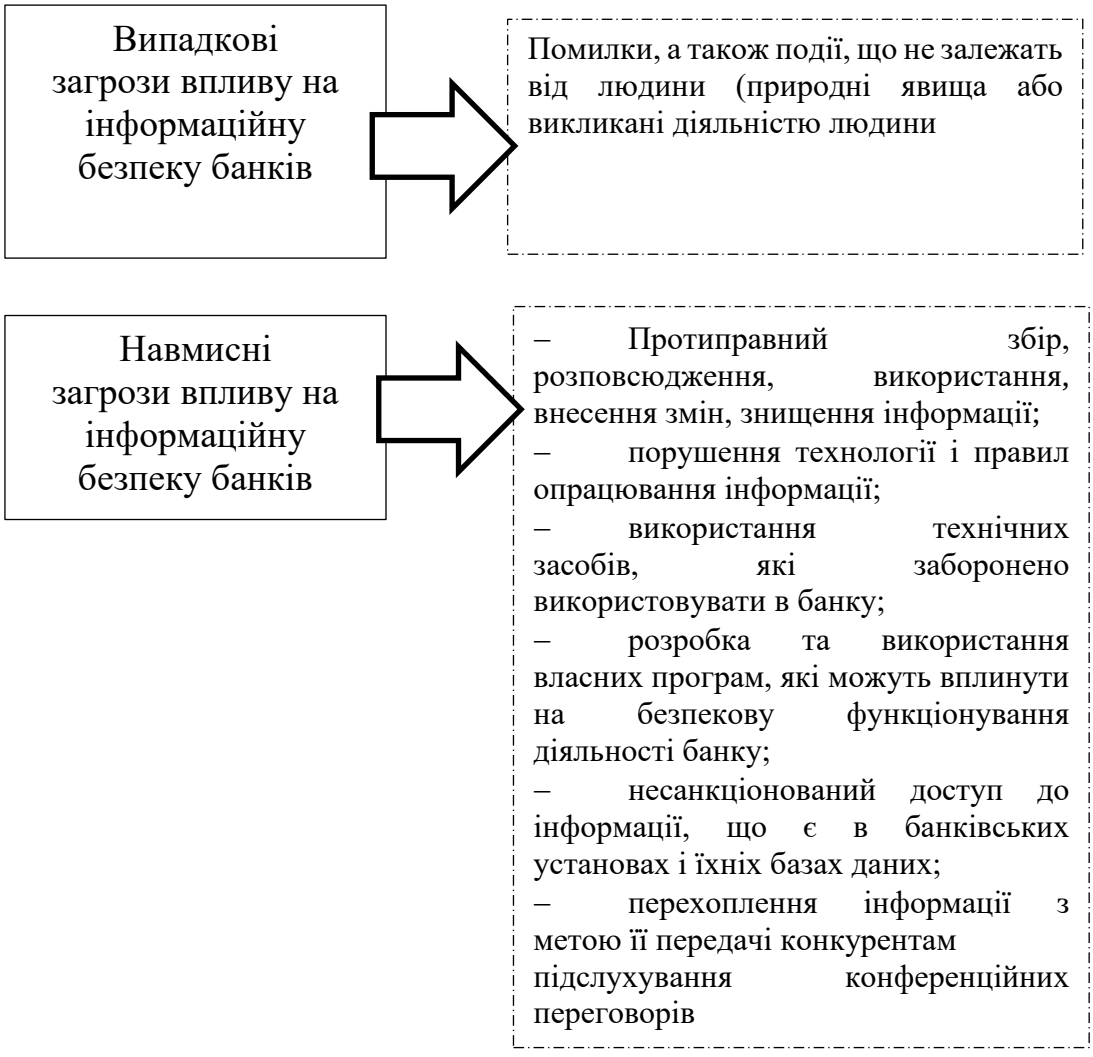

Рис. 1.8 Види загроз впливу на інформаційну безпеку банків

Джерело: складено автором за матеріалами [19]

При цьому визначимо, що до випадкових загроз впливу на інформаційну безпеку банку можемо віднести надмірна балакучість, недбалість,

неуважність, відсутність мотивації співробітників банків, конфлікти, недотримання корпоративної етики, до навмисних загроз – осмислене здійснення промислового шпигунства з метою передачі даних банкам конкурентам.

Виходячи з того, що загрози, які можуть впливати на інформаційну безпеку банку можуть провокувати інформаційні ризики в банках, які можна розглядати як можливість втрати або пошкодження інформації, яка є цінним ресурсом для банківської діяльності. Інформаційні ризики можуть виникати через зовнішні або внутрішні чинники, такі як кібератаки, помилки персоналу, недостатня захищеність систем, порушення нормативних вимог тощо. Інформаційні ризики можуть призвести до фінансових збитків, репутаційних ризиків, судових позовів, штрафів або санкцій. Для запобігання та мінімізації інформаційних ризиків банки повинні мати ефективну систему управління інформаційною безпекою, яка включає ідентифікацію, оцінку, контроль та моніторинг інформаційних ризиків, а також заходи щодо їх локалізації та ліквідації у разі їх виникнення. Узагальнюючи це ми можемо виділити три інформаційних ризики (рис. 1.9).

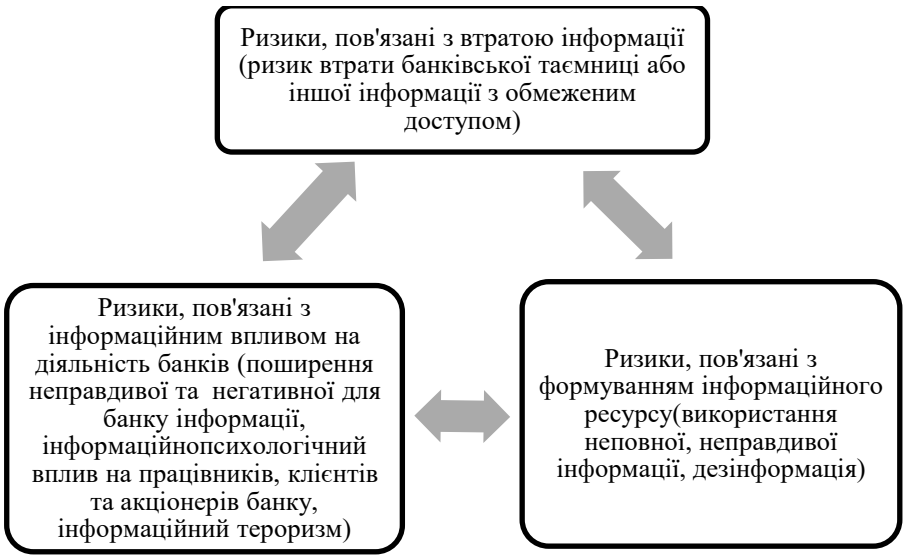

Рис. 1.9 Інформаційні ризики банку залежно від походження

Джерело: складено автором за матеріалами [10, 20]

Виходячи з наведеного рис. 1.9, можна стверджувати, що інформаційне середовище, в якому функціонують банки України є нестійким та мінливим, тому забезпечення ефективності інформаційної безпеки вимагає постійного удосконалення розробки чинних механізмів з урахуванням усього спектру ризиків як зовнішнього, так і внутрішнього походження. З цього приводу ми можемо визначити, один зі значущих ризиків це операційний ризик, який пов'язано з усіма напрямами діяльності банку, що своєю чергою підвищує роль інформаційної безпеки.

Як визначається в «Положенні про організацію системи управління ризиками в банках України та банківських групах» «операційний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі систем банку або внаслідок впливу зовнішніх факторів. Операційний ризик уключає юридичний ризик, однак має виключати ризик репутації та стратегічний ризик» [21].

За визначенням авторки Сергєєвої О.С. «використання цифрових технологій у банківській діяльності дозволить банкам поліпшити якість і прибутковість не лише від надання банківських послуг, а й від підвищення ефективності супутніх процесів, таких як управління персоналом, аналітична діяльність, забезпечення безпеки інформації тощо. Але, як слід, останнім часом спостерігається зростання операційного ризику та його матеріалізація у значних втратах, що пов'язано також зі впровадженням складних інноваційних систем дистанційного банкінгу» [22]. Прояв якого є у «результаті недоліків та помилок у ході здійснення внутрішніх процесів у банку, допущених зі збоку працівників, через інформаційні системи, а також зовнішніх подій» [67].

Статистичні дані, щодо виникнення операційного ризику представлені на рис. 1.10.

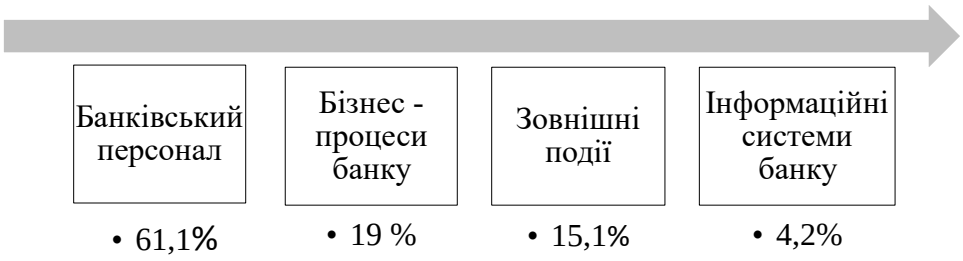

Рис. 1.10 Чинники, які впливають на виникнення операційного ризику

Джерело: складено автором за матеріалами [23]

Як свідчать дані, наведені на рис. 1.10 ризикованість діяльності банківського персоналу складає 61.1%, бізнес – процеси та зовнішні події 19% та 15,1% відповідно, а інформаційні системи банку складають не більш 4%. Тому на сьогодні актуальним є питання у підготовки високопрофесійних працівників банків, що несе за собою підвищення інформаційної безпеки банків.

Отже, діяльність банків під впливом інформаційної небезпеки невід'ємно пов'язана з прийняттям рішень щодо управління ним та як слід передбачає застосування заходів та прийняття рішень щодо забезпечення дотримання певних норм інформаційної безпеки (ризик-апетиту банку), пом'якшення та мінімізації його.

Як ми вже зазначали, що організація та дотримання інформаційної безпеки в банках стосується кожної ланки банківського бізнесу, що вимагає від банків дотримування механізму підтримки нормативно-законодавчими актами держави та їх організації та регулювання, в особах Верховної Ради, Кабінет Міністрів та НБУ, а їх реалізація, повинна гармонійно вписується в стратегію корпоративного управління банками.

Законодавство щодо організації та регулювання безпекової діяльності банків України складається із сукупності правових актів різної юридичної чинності. За напрямом щодо правового впливу, можемо розглядати міжнародні правові акти та стандарти [24 – 28], національне законодавство й

Положення НБУ [13,21,29 – 44] та внутрішні документи спеціальної дії, що мають метою забезпечити безпеку діяльності банків.

Не можна заперечувати той факт, що впровадження НБУ реформ в банківському секторі з початку 2015 р, створили умови для оздоровлення та підвищення показників діяльності банків України протягом до 24 лютого 2022 р., а протягом двох років повномасштабної війни надали удосконаленню нормативної бази.

Повний перелік нормативно-правового забезпечення, яке стосується організації інформаційної безпеки банків представлено в Додатку А. Ми зупинимось, на наш погляд, на головний із них.

Серед міжнародних стандартів щодо діяльності банків слід віднести стандарт ISO 27001 «Інформаційна безпека, кібербезпека та захист конфіденційності». Серед якісних характеристик, слід зазначити, що цей стандарт є «всесвітньо визнаним для систем управління інформаційною безпекою (ISMS). У ньому викладаються вимоги до створення, впровадження, обслуговування і постійного вдосконалення системи управління інформаційною безпекою організації» [28]. Пропонуємо в табл. 1.3 розглянути основні переваги цього стандарту.

Таблиця 1.3

Характеристика стандарту ISO 27001
«Інформаційна безпека, кібербезпека та захист конфіденційності»

Особливості	Переваги	Принципи	Контролінг
ISO 27001 є міжнародно визнаний стандарт для систем управління інформаційною безпекою (ISMS), розроблений Міжнародною організацією по стандартизації (ISO)	Глобальне визнання	Оцінка ризиків	Внутрішні Аудитори
	Всеосяжна Рамкова програма	Обробка ризиків	Зовнішні Аудитори
	Підхід, заснований на оцінці ризику	Контекстуальний підхід	Аудитори Органи з сертифікації
	Вимоги до відповідності	Цикл PDCA (Плануй-Роби-Перевіряй-Дій)	
	Бізнес-Вимоги	Лідерство і Цілеспрямованість	
	Постійне Вдосконалення	Процесно-комплексний підхід	
		Документування та прийняття рішень, заснованих на факт. даних	

Джерело: складено автором за матеріалами [28]

Отже, як бачимо з даних табл. 1.3 дотримання цього стандарту пропонує українським банкам «систематичний і структурований підхід до управління інформаційними активами організації та їх захисту, включаючи чутливу і конфіденційну інформацію. Вона включає в себе процес управління ризиками, який допомагає організаціям виявляти, оцінювати та усувати ризики інформаційної безпеки. Стандарт також містить вимоги до встановлення політик, процедур, засобів контролю та інших заходів щодо зниження ризиків і захисту інформації від несанкціонованого доступу, розкриття, зміни, знищення і переривання роботи» [28].

Постанова НБУ № 267 [39] чітко прописує вимоги щодо організації інформаційної безпеки банків, визначаючи, що «автоматизовані системи оброблення інформації повинні мати вбудовану систему захисту інформації, яку неможливо відключити або здійснити оброблення інформації, минаючи її» [39].

Метою впровадження Постанови НБУ № 95 [40] є «удосконалення вимог до захисту інформації в інформаційних системах банків з урахуванням актуальних кіберзагроз, установлення вимог щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків» [40]. Документом визначено принципи управління ІБ, термінологія, яка стосується нових технологічних загроз, упровадження систему управління інформаційною безпекою (СУІБ) та вимог до неї. Надані рекомендації щодо впровадження банками внутрішнього документу «Політика інформаційної безпеки», впровадження підрозділу з інформаційної безпеки.

Епоха цифровізації, перехід банків на діджитал-процеси сприяло появи банківського законодавства пов’язаного з забезпеченням кібербезпеки в банках. Спочатку з’являється ЗУ [41], який відображає правові та організаційні засади захисту усіх суб’єктів України у кіберпросторі, «основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та

громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» [41].

Продовженням, через місяць виходить Положення НБУ № 178 [42], яке визначило норми щодо організації й забезпечення кіберзахисту в банках України за такими напрямами: «основні засади функціонування системи кіберзахисту, принципи забезпечення інформаційного обміну між Центром кіберзахисту НБУ і банками України, вимоги щодо заходів із забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури, вимоги щодо проведення незалежного аудиту інформаційної безпеки банків» [42].

В ході дослідження ми визначили, що порушення ІБ може відбуватися не тільки від зломів інформаційних систем банку, а й за порушення певних вимог дотримання ІБ співробітниками банків, тому керівництву необхідно приділяти увагу Постанові НБУ [45], яка «регламентує принципи щодо ефективного корпоративного управління та функціонування системи внутрішнього контролю» [45]. Документ пропонує розділити систему внутрішнього контролю (СВК) на п'ять компонентів за наступними напрямами, це контрольне середовище, головним аспектом є забезпечення розвитку культури контролю в банку, управління ризиками, контрольна діяльність, контроль за інформаційними потоками та комунікаціями та моніторинг ефективності СВК.

Проведене дослідження показало, що система інформаційної банку має вирішувати, окрім головного свого завдання – формування системного підходу до забезпечення інформаційної безпеки, ще й завдання концентрації та маневрування силами і засобами згідно із визначеними цілями й завданнями з урахуванням змін у характері та інтенсивності загроз, що виникають.

Узагальнююче зазначене, вважаємо, що перехід до цифрової економіки сьогодення вимагає від банків перетворюватися на сучасний цифровий банкінг, що несе за собою з одного боку – підвищення його конкурентоспроможності, але з іншого боку, від банку, який використовує

інноваційні цифрові технології, вимагається дотримання високих стандартів до забезпечення інформаційної безпеки.

Висновок до розділу 1

Ефективна та безризикова діяльність банків залежить від зваженої політики управління інформаційною безпекою банків яка є базисом довгострокової фінансової стійкості усіх банків.

За результатами написання розділу 1 можемо зробити наступні висновки.

1. Проведено аналіз поняття «інформаційна безпека банку» та визначено, що це поняття рекомендовано розглядати як стан інформаційної інфраструктури банку, за якого забезпечуються умови стабільного функціонування, максимізації прибутку, оптимального використання ресурсів банку, а також забезпечення захищеності клієнтів, співробітників і керівництва банку від зовнішніх і внутрішніх загроз.

2. Визначені базові елементи інформаційної безпеки банків, такі як мета, завдання, суб'єкт, об'єкт. Визначення функцій інформаційної безпеки: превентивна, детективна, реактивна, коректива.

3. З'ясовано, що в організації інформаційної безпеки сучасного банку необхідно відокремлювати наступні напрями безпеки як інформаційне поле, інформаційні ресурси, інформаційна інфраструктура.

4. У роботі запропоновано визначати, що система управління інформаційною безпекою це забезпечення захисту конфіденційності, цілісності та доступності інформаційних активів. Вона складається з безлічі різних процесів, кожен з яких спрямований на обробку певних загроз.

5. Проведена характеристика чинників впливу на інформаційну безпеку банку, які пропонується розглядати як зовнішні чинники: кібератаки,

політичні, соціальні, економічні та правові чинники, конкуренти та внутрішні чинники: бізнес-модель банку, рівень діджиталізації, високий рівень професіонально персоналу. Завдяки чому, було визначено види загроз інформаційної безпеки банків, які запропоновано розглядати як випадкові та навмисні.

6. За результатами здійсненого аналізу чинного законодавства України можна зробити висновок, що нормативно – правові норми, які регулюють діяльність банків, постійно удосконалюються та адаптуються в залежно від політичних та економічних умов в яких функціонує країна.

РОЗДІЛ 2
ОЦІНКА ДІЯЛЬНОСТІ БАНКУ В ІНФОРМАЦІЙНО - ЦИФРОВОМУ ПРОСТОРІ

2.1 Оцінка діяльності АТ «А–БАНК» в українському інформаційному полі

Діяльність банків в інформаційному полі є ключовим аспектом сучасної банківської системи. Сучасні технологічні банки сьогодні використовують різноманітні інформаційні технології для забезпечення безпеки транзакцій, управління ризиками, а також для покращення якості обслуговування клієнтів. Банки активно працюють над створенням ефективних каналів комунікації з клієнтами через інтернет-банкінг, мобільні додатки та соціальні мережі, що дозволяє їм оперативно реагувати на запити клієнтів та надавати актуальну інформацію про продукти та послуги. Окрім того, використання великих даних й аналітики допомагає банкам краще розуміти потреби своїх клієнтів і пропонувати персоналізовані фінансові рішення.

Слід зазначити, що відповідно до Закону України «Про доступ до публічної інформації» [46] «право на доступ до публічної інформації гарантується зокрема обов'язком розпорядників інформації оприлюднювати інформацію, крім випадків, передбачених законом» [46], при тому надається уточнення «інформація про організаційну структуру, усі без винятку нормативно-правові акти, система обліку публічної інформації, інформація про діяльність суб'єктів владних повноважень та інше» [46]. На основі цього можемо зазначити, що прозоре розміщення та розповсюдження публічної діяльності АТ «А – БАНК» повність відповідає законодавчим вимогам.

АТ «А – БАНК» — універсальний комерційний банк, який пропонує повний спектр сучасних фінансових послуг як фізичним, так і юридичним особам. Основним напрямом розвитку якого є здійснення роздрібних банківських операцій. АТ «А – БАНК» працює в Україні з 1992 року. Спочатку

банк мав назву «Київприватбанк», потім – «Український кредитний банк». З березня 2007 року банк перейменували «Акцент-Банк» або ж АТ «А – БАНК» [47].

Не можливо, не відділити місце АТ «А – БАНК» в діяльності банківської системи країни через щорічне визначення НБУ його як системно важливим банком України. Цей факт вимагає від банку виконання підвищених вимог до інформаційної безпеки в банку.

Бізнес – модель діяльності АТ «А – БАНК» вже протягом багато років направлена на роздрібний бізнес, не зважаючи на пандемію COVID-19 та понад двох років повномасштабної війни в Україні. Банк й надалі підтримує прагнення населення зберігати кошти у надійному банку, займається впровадженням змін заради покращення клієнтського досвіду, розвиває новітні канали обслуговування і комунікації з клієнтами.

Регіональний розвиток АТ «А – БАНК» фокусується насамперед на збільшенні присутності у великих регіонах (Дніпро, Одеса, Київ, Львів, Харків тощо) з одночасним утриманням лідерських позицій на південному сході України. На 01.01.2024 р. Кількість підрозділів АТ «А – БАНК» складає 201 відділення, динаміку підрозділів АТ «А – БАНК» представлено на рис. 2.1 та у розрізі за регіонами на 01.01.2024 р. представлено на рис. 2.2.

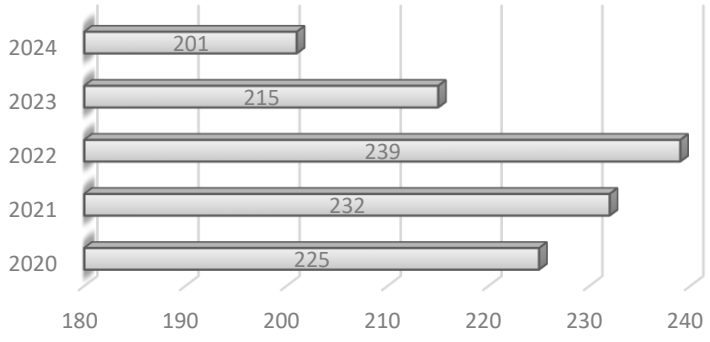

Рис. 2.1 Динаміка кількості підрозділів АТ «А – БАНК» за період 2020 – 2024 рр., на початок періоду

Джерело: складено автором з використанням матеріалів [48]

Наочно бачимо з рис. 2. 1, що до 01.01.2022 р. АТ «А – БАНК» мав за мету збільшення своїх підрозділів та починаючи з початку 2020 року їх кількість зросла на 14 одиниць, але вже за результатами 2022 року, ця кількість зменшилась на 24 одиниці, а на початок 2024 року, ще на 14 одиниці та склала 201 підрозділ, це зрозуміло або основна діяльність АТ «А – БАНК» розташована на південному сході України (рис. 2.2).

Рис. 2.2 Кількість діючих підрозділів АТ «А – БАНК» у розрізі України станом на 01.01. 2024 р.

Джерело: складено автором за матеріалами [48]

Проведемо оцінку основних фінансових показників діяльності АТ «А – БАНК» в розрізі найбільш значущих складових які впливають на формування прибуткового результату.

Для можливості функціонувати банку на фінансовому ринку та зберігати свою стійкість банку за необхідним є формування, поповнення ресурсної бази та як слід дотримування нормативів НБУ.

Дані табл. 2.1 наочно відображають, що статутний капітал АТ «А – БАНК» за аналізований період збільшився до 1514594 тис. грн., практично у 3 рази, це відбулось за рахунок власних коштів акціонерів банків та капіталізації за рахунок прибутку, в результаті чого збільшився загальний показник

власного капіталу АТ «А – БАНК» з 292 162 тис. грн. до 2 9997309 тис. грн., що практично у 10 разів.

Таблиця 2.1

Структура та динаміка капіталу АТ «А – БАНК»
за 2020 – 2024 рр., на початок періоду, тис. грн.

Роки	Статутний капітал	Резервні та інші фонди банку	Резерви переоцінки	Нерозподілений прибуток (непокритий збиток)	Усього власного капіталу
2020	502 240	91 522	35 057	292 162	292 162
2021	778 472	104 328	48 384	303 371	1 234 595
2022	1 054 704	127 834	46 828	804 162	804 162
2023	1 054 704	172 107	63 526	503 281	2 418 459
2024	1 514 505	172 107	80 474	1 065 183	2 997 309

Джерело: складено автором з використанням матеріалів [49]

Оскільки функцією любого банку є мобілізація грошових коштів, основним показником є аналіз зобов'язань банку.

Таблиця 2.2

Структура та динаміка зобов'язань АТ «А – БАНК»
за 2020 – 2024 рр., на початок періоду, тис. грн.

Роки	Кошти банків	Кошти клієнтів	Зобов'язання щодо поточного податку на прибуток	Відстрочені податкові зобов'язання	Резерви за зобов'язаннями	Інші фінансові зобов'язання	Інші зобов'язання	Усього зобов'язань
2020	11 143	5 167 804	-	6 781	13 405	173 319	139 461	5 511 914
2021	49 766	7 588 332	33 345	11 011	17 265	124 434	167 141	7 991 294
2022	90 812	11 533 922	82 673	11 357	16 288	227 658	216 634	12 179 344
2023	252 177	14 579 786	19 883	14 055	12 576	327 441	162 351	15 368 269
2024	91 217	20 359 333	789	19 958	26 309	766 088	404 747	21 668 440

Джерело: складено автором з використанням матеріалів [49]

Данні табл. 2.2 наочно показують, що за основними статтями зобов'язань як кошти банків та кошти клієнтів за аналізований період АТ «А – БАНК» відображав постійне зростання, за виключенням 2022 року для

коштів банків, своєю чергою кошти клієнтів мали постійну тенденцію до зростання та за 5 років виросли з 5 167 804 тис.грн. до 20 359 333 тис.грн, тому як результат усіх зобов'язання АТ «А – БАНК» теж збільшились та склав на 01.01.2024 р. 21 668 440 тис. грн., рис. 2.3 наочно відображає питому вагу в загальних пасивах банків власного капіталу та коштів клієнтів.

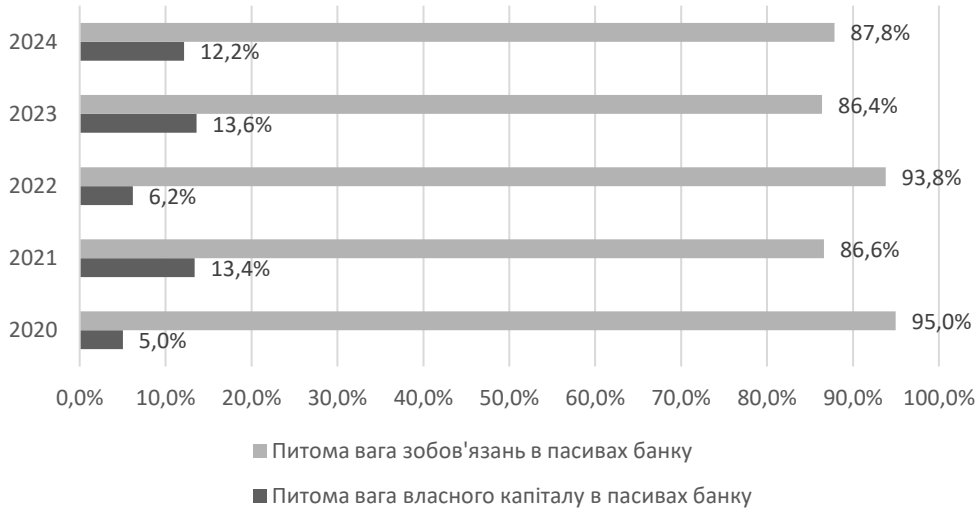

Рис. 2.3 Динаміка часток зобов'язань та власного капіталу в пасивах АТ «А – БАНК» за період 2020 – 2024 рр., на початок періоду, тис. грн., %

Джерело: складено та розраховано автором за матеріалами [49]

З рис. 2.3 можемо зробити висновок, що на 01.01.2020 рік АТ «А – БАНК» не дотримувався співвідношення капітал/зобов'язання, що порушувало фінансову безпеку банку, але починаючи з 2021 року ці пропорції вирівнялись, та з початку 2023 року дорівнюють вимогам НБУ.

Оцінка усіх пасивів АТ «А – БАНК» дає змогу зробити висновок, що управління фінансовими ресурсами Банку відбувається з дотриманням банківського законодавства.

В таблиці 2.3 розглянемо склад та структуру активів АТ «А – БАНК» за період 2020 – 2024 рр. на початок періоду.

Таблиця 2.3

Склад та структуру активів АТ «А – БАНК»
за період 2020 – 2024 рр. на початок періоду, тис. грн.

№	Показники	на 01.01									
		2020		2021		2022		2023		2024	
		тис.грн.	%	тис.грн.	%	тис. грн.	%	тис. грн.	%	тис.грн.	%
1.	Високоліквідні активи	231 270	2,8%	344 573	3,2%	856 856	5,4%	1 841 859	8,3%	2 289 583	8,1%
2.	Кредитний портфель	4 868 112	59,3%	7 190 533	66,1%	9 501 507	59,6%	6 220 966	28,2%	9 346 122	33,2%
2.1.1.	*у т.ч. кредити та заборгованість юридичних осіб*	311 194	3,8%	1 025 988	9,4%	1 648 047	10,3%	1 407 845	6,4%	1 440 893	5,1%
2.1.2.	*у т.ч. кредити та заборгованість фізичних осіб*	4 556 917	55,6%	6 164 546	56,7%	7 853 460	49,2%	4 813 120	21,8%	7 905 229	28,1%
3.	Інвестиційний портфель	270 382	3,3%	594 931	5,5%	2 332 286	14,6%	6 255 999	28,3%	9230605	32,8%
4.	Основні засоби та нематеріальні активи	236 713	2,9%	413 732	3,8%	431 810	2,7%	413 256	1,9%	418 342	1,5%
5.	Інші активи	141 936	1,7%	62 671	0,6%	56 981	0,4%	38 417	0,2%	105 617	0,4%
6.	Усього активів	8 203 238	100,0%	10 878 823	100,0%	15 951 075	100,0%	22 072 445	100,0%	28 162 093	100,0%

Джерело: складено та розраховано автором за матеріалами [49]

З таблиці 2.3 наочно видно, що в розрізі активів АТ «А – БАНК» ситуація суттєво покращилась, за аналізований період загальні активи АТ «А – БАНК» збільшились на 19 958 855 тис. грн. чи на 243%.

Показник «Високоліквідні активи» зросли з 231270 тис. грн. до 2289583 тис. грн на 01.01.2024 р.

Показник «Кредитний портфель» за аналізований період збільшився на 4 478 011 тис. грн. та склав 9 346122 тис. грн. чи 33,2% загальних активів Банку.

Починаючи з 2021 року різко збільшується показник «Інвестиційний портфель», який на 01.01.2024 р. складає 32,8 % усіх активів АТ «А – БАНК».

АТ «А – БАНК» дотримується нормативів ліквідності, встановлених НБУ. Для покращення контролю за нормативом ліквідності було встановлено внутрішні нормативи ліквідності, показники яких відстежуються щоденно та презентуються на кожному засіданні КУАП. У разі необхідності, банк здійснює стрес-тестування для значень показників ліквідності та досліджує можливий вплив зміни певних внутрішніх та зовнішніх чинників.

Розрахунок нормативів ліквідності представлено у таблиці 2.4.

Таблиця 2.4

Нормативи ліквідності банку АТ «А – БАНК»
за період 2020 – 2024 рр., на початок період. %

Показники	Нормативне значення, %	Станом на 01.01.				
		2020	2021	2022	2023	2024
«Норматив короткострокової ліквідності» Н6	Не менше 60%	86,32	83,31	90,15	-	338,05
Коефіцієнт LCR	Не менше 100%	202,82	142,41	240,74	242,0378	271,23

Джерело: складено автором за матеріалами [50,51]

Норматив короткострокової ліквідності Н6 встановлюється для контроля за здатністю банку виконувати прийняті ним короткострокові (≤ 1 року) зобов'язання за рахунок ліквідних активів. Норматив Н6 мав такі показники: на 01.01.2020 рік – 86,32%, 2021 рік – 83,31% та 2022 рік – 90.15% АТ «А – БАНК» дотримується нормативного значення НБУ.

Виконання нормативу LCR в АТ «А – БАНК» виглядає наступним чином: на 01.01.2020 рік – 202,82%, 2021 рік – 142,41% та 2022 рік – 240,73%. Слід визначити, значення LCR за звітні роки перевищує норматив у 2,5 рази, але все ж дотримується нормативного значення НБУ, що означає захищеність клієнтів АТ «А – БАНК» та подальшу стабільну роботу банку на банківському ринку України.

Від організації та дотримання ефективної інформаційної безпеки за усіма напрямами діяльності банку напряму залежить його прибуткова діяльність. В сучасних умовах, коли країна пройшла пандемію COVID-19 та вже більше, як два роки знаходиться у повномасштабній війні, спостерігається негативна динаміка у всіх напрямах економіки, у тому числі й фінансовому секторі. Тому перед банківськими установами постає завдання як збереження філіальної мережі й клієнтської бази, підтримання банківського бізнесу на плаву та отримання прибутковості.

Проведемо оцінку складових прибутку АТ «А – БАНК» в табл. 2.5.

Таблиця 2.5

Динаміка складових прибутку АТ «А – БАНК»

за період 2020 – 2024 рр., на початок періоду, тис. грн.

Складові прибутку	2020	2021	2022	2023	2024
Чистий процентний дохід	1 443 185	1 821 455	2 458 825	2 685 868	2705 540
Чистий комісійний дохід	286 403	346 797	537 650	505 445	543 409
Резерв під зменшення корисності кредитів	632 321	740 259	656 369	586 988	757 620
Дохід/Витрати з податку на прибуток	312 211	368 059	978 167	259 153	707 832
Усього чистий прибуток/збиток	254 801	299 738	800 013	202 637	561 312

Джерело: складено автором за матеріалами [47,49]

Зазначимо, що до основних джерел банківського прибутку, відповідно до таблиці, можна віднести: чистий процентний дохід (ЧПД) та чистий комісійний дохід (ЧКМ).

Більшу частину займає ЧПД АТ «А – БАНК» на 01.01.2020 року він склав 1 443 185 тис. грн., на 01.01.2021 року – 1 821 455 тис. грн., на 01.01.2022 року, ми бачимо, що ЧПД зріс та склав – 12458825 тис. грн., за 2022 та 2023 рр. надглядається збільшення ЧПД та на 01.01.2024 р. Він склав 2705540 тис. грн., це пов’язано, в перш, від збільшення високоліквідних активів АТ «А – БАНК».

ЧКД АТ «А – БАНК» за аналізований період теж мав тенденції до постійного зростання, що пов’язане з отриманням дохідності від надання банківських послуг. ЧКД мав наступні показники: на початок 2020 року – 286 403 тис. грн, на початок 2021 року – 346797 тис. грн., та на початок 2022 року – 537650 тис. грн., на початок 2023 року цей показник знизився до 505445 тис. грн., але вже на 01.01.2024 р. мав тенденцію до зростання та склав 543409

тис.грн. За досліджуваний період ЧКД АТ «А – БАНК» збільшився практично у двічі.

Таким чином, ми можемо зазначити, що за аналізований період прибуткова діяльність АТ «А – БАНК» пов’язані зі зваженою політикою управління активами та пасивами, професіоналізмом персоналу та якісно організованою інформаційною безпекою банку.

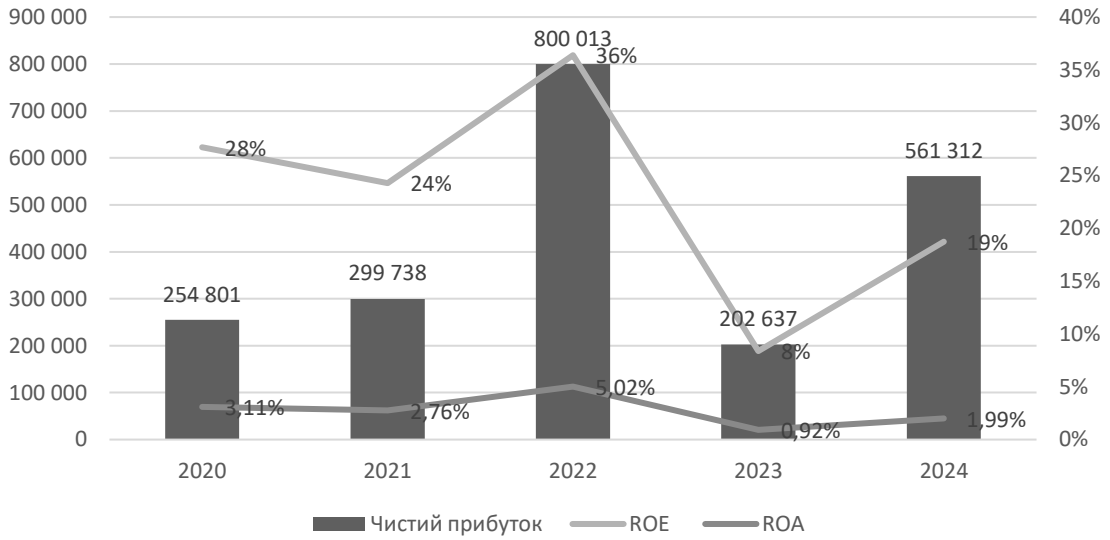

Рис. 2.4 Динаміка показників прибутковості АТ «АТ – БАНК» за 2020 – 2024 рр, на початок періоду, тис. грн., %

Джерело: складено автором за матеріалами [47,49]

Розглядаючи прибутковість АТ «А – БАНК», зазначимо, що за звітний період спостерігається позитивна динаміка до збільшення розміру прибутку, отриманого АТ «А – БАНК» в процесі здійснення своєї діяльності, попри умов воєнного стану в якому перебуває Україна. На початку аналізованого періоду АТ «А – БАНК» отримав прибуток у розмірі 254 801 тис. грн., на початок 2021 року 299738 тис. грн., на початок 2022 року АТ «А – БАНК» збільшив прибутковість практично в чотири рази або 800 013 тис. грн, за перший воєнний рік, на 01.01.2023 р, АТ «А – БАНК» відзвітував про отримання прибутку 202 637 тис. грн, а вже на 01.01.2024 р. АТ «А – БАНК» 561 312 тис. грн.

Показник рентабельність капіталу банку(ROE) АТ «А – БАНК» має тенденцію до зростання, вони складають на початок 2020 року – 28%, на початок 2021 року – 24%, на початок 2022 року вже 36%, але на початок 2023 показник знизився за об'єктивними причинами до рівня 8%, але вже на початок 2024 року підвищився до рівня 19%.

Рекомендоване значення показника рентабельність активів банку (ROA) складає ≥ 1%, протягом аналізованого періоду АТ «А – БАНК» не дотримувався рекомендованого значення: у 2020 році показник склав 3,1%, а у 2021 році – 2,76%, на початок 2022 року вже 5,02%., також на початок 2023 року показник ROA знизився до рівня 0,92%, але вже на початок 2024 року підвищився до рівня 1.99%. Позитивна динаміка свідчить про збільшення ефективності внутрішньої політики банку з управління активами й пасивами та демонструє покращення ефективності роботи керівництва банку.

Проведене дослідження показало, що на сьогоднішній день репутація банків - це прозорість їх діяльності, висока адаптивність та стійкість до викликів, безперебійність роботи тощо. Завдяки їй, тобто репутації, банки отримують: збільшення довіри клієнтів (нарощення клієнтської бази), забезпечення доступу до фінансових ресурсів від інвесторів, партнерів; крім того досягається зменшення витрат на приваблення нових клієнтів тощо

Аналіз публічної фінансової інформації про діяльність АТ «А – БАНК» дає змогу зробити висновок, що банк виконує усі вимоги щодо діяльності банків на території України та дотримується усіх правових актів щодо розміщення інформації..

Протягом діяльності АТ «А – БАНК» не потрапляв під інформаційні атаки з боку конкурентів, персоналу, клієнтів, на офіційному сайті банку постійно оновлюється інформація. В інформаційне українське середовище не потрапляла негативна інформація про його діяльність. АТ «А – БАНК» цінує та береже свою репутацію, взаємовідносини з клієнтами та свій персонал, що має відображення в фінансових результатах діяльності банку.

2.2 Оцінка дотримання безпеки інформаційних ресурсів АТ «А – БАНК»

Безпека інформаційних ресурсів банку є критично важливою для забезпечення стабільності та надійності банківських операцій. Законом України «Про інформацію» визначено, «що за режимом доступу інформація поділяється на відкриту та з обмеженим доступом, а остання — на конфіденційну й таємну» [34]. Для банку конференційна інформація розглядається як дані, які перебувають у володінні та користуванні самого банку та може поширюватися відповідно до передбачених умов. Оскільки діяльність банку напряму пов’язана з обслуговування клієнтів, саме ця інформація є банківською та комерційною таємницею. ЗУ ««Про банки і банківську діяльність» [13] визначає, що «банківська таємниця — це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою для банка у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту» [13].

Діяльність банку напряму пов’язана з інтересами клієнтів та є повністю конференційною, де банк своєю чергою повинен відповідати за забезпечення рівня таємності. Об’єктивно, правом клієнта є очікування, що банк повинен піклуватися про їхні інтереси, інакше він ризикує своєю репутацією з усіма наслідками, що випливають звідси.

Згідно з ЗУ [38] про фінансовий моніторинг, банки почали дуже прискіпливо перевіряти своїх клієнтів. Ідентифікація та верифікація клієнтів банку є ключовими елементами безпеки інформаційних ресурсів. Це допомагає забезпечити безпеку фінансовим операціям, які виконуються легітимними особами та зменшують ризик шахрайства. НБУ посилює контроль за кіберзахистом та інформаційною безпекою банків, що включає як виїзні перевірки, так безвиїзний нагляд. Банки зобов’язані проводити

самооцінку стану інформаційної безпеки та кіберзахисту, складати та подавати щорічний звіт з питань оцінювання ризиків. Для підвищення рівня безпеки, банки використовують сучасні інструменти, такі як Система BankID НБУ, кваліфікований електронний підпис для верифікації ідентифікаційних даних клієнта. Це дозволяє банкам ефективно управляти ризиками інформаційної безпеки та кіберризиками, забезпечуючи надійну систему внутрішнього контролю.

Отже, для банку головною задачею є встановлення межі щодо інформації з обмеженим доступом, розповсюдження якої несе загрози як самого банку, так й для його клієнтів.

Дотримання безпеки інформаційних ресурсів, пропонуємо розглянути діяльність АТ «А – БАНК» через обслуговування клієнтів, як з боку залучення коштів (поточні, строкові), так і в напряму кредитування.

Таблиця 2.6

Динаміка коштів клієнтів АТ «А – БАНК» з поділом на суб'єктів господарювання, небанківських фінансових установ та клієнтів – фізичних осіб за 2020 – 2024 рр., на початок періоду, тис. грн.

Роки	Кошти банків	Кошти клієнтів	у тому числі кошти суб'єктів господарювання та небанківських фінансових установ	у тому числі кошти на вимогу	у тому числі кошти фізичних осіб	у тому числі кошти на вимогу	Усього зобов'язань
2020	11 143	5 167 804	680 191	281 479	4 487 613	448 221	5 511 914
2021	49 766	7 588 332	1 244 181	525 737	6 344 151	726 653	7 991 294
2022	90 812	11 533 922	2 359 230	1 726 065	9 174 692	1 247 986	12 179 344
2023	252 177	14 579 786	2 725 964	1 827 287	11 853 822	3 366 703	15 368 269
2024	91 217	20 359 333	4 678 965	3 512 625	15 680 367	5 431 796	21 668 440

Джерело: складено автором за матеріалами [49]

Дані, представлені в табл. 2.6 свідчать, що АТ «А – БАНК» за п'ять років активно залучав кошти як від банківських установ, так від клієнтів юридичних та фізичних осіб.

Збільшення усіх показників підтверджує, що протягом досліджуваного періоду до АТ «А – БАНК» дотримується усіх норм безпеки інформаційних ресурсів, завдяки чому має високу довіру з боку клієнтів, що відображається в щорічному збільшенню клієнтської бази. Кошти населення традиційно є джерелом фондування для банків, але водночас цей ресурс має високу чутливість до стану операційного середовища та може призвести до значних відтоків в разі дестабілізації на ринку («набіги на банки»).

АТ «А – БАНК» [47] позиціонує себе лідером в роздрібному сегменті банківського обслуговування вже протягом п’яти років.

У таблиці 2.7 наведено аналіз складу депозитного портфеля фізичних осіб АТ «А – БАНК».

Таблиця 2.7

Структура депозитного портфеля фізичних осіб АТ «А – БАНК»
за 2020 – 2024 рр., на початок періоду, тис. грн.

Показники	01.01.2020	01.01.2021	01.01.2022	01.01.2023	01.01.2024
Кошти фізичних осіб	3 908 781	6 344 151	9 174 692	11 853 822	15 680 367
В національній валюті	3 460 560	5 372 751	7 657 970	7 851 061	11 058 722
В іноземній валюті	448 221	971 400	1 516 723	4 002 762	4 621 645
Кошти на вимогу	448 221	726 653	1 247 986	3 366 703	5 431 796
В національній валюті	374 778	608 182	1 048 463	2 211 202	3 058 579
В іноземній валюті	73 443	118 471	199 522	1 155 501	2 373 217
Кошти на строкових рахунках	3 460 560	5 617 498	7 926 707	8 487 120	10 248 571
В національній валюті	3 085 782	4 764 569	6 609 506	6 275 918	7 189 992
В іноземній валюті	374 778	852 929	1 317 200	2 211 202	3 058 579
Зобов’язання	4 855 695	7 991 294	12 179 344	15 368 269	21 668 440

Джерело: складено автором за матеріалами [49]

Як бачимо з табл. 2.7 діяльність АТ «А – БАНК» в напряму обслуговування поточних та строкових рахунків фізичних осіб за п’ять років мала тенденцію до постійного зростання, як в національній, так і в іноземній валюті. За два роки повномасштабного вторгнення кошти фізичних осіб виросли на 6 505 675 тис. грн., я яких кошти на вимогу на 4 183 810 тис. грн., строкові вклади на 2 321 865 тис. грн. В загальній сумі зобов’язань АТ «А –

БАНК» у впродовж 2019 та 2020 років обслуговування фізичних осіб займало практично 80% усіх зобов'язань банку, то вже починаючи з 2021 року АТ «А – БАНК» зменшує цей показник до рівня 75%, а на 01.01.2024 р. до 72%, це визначає, що АТ «А – БАНК» почав активно займатися обслуговування юридичних осіб.

Проведемо аналіз депозитного портфеля юридичних осіб АТ «А – БАНК» за період 2020 – 2024 рр. на початок періоду.

Таблиця 2.8

Структура депозитного портфеля юридичних осіб АТ «А – БАНК» за 2020 – 2024 рр. на початок періоду, тис. грн.

Показники	2020	2021	2022	2023	2024
Кошти юридичних осіб	680 191	1 244 181	2 359 230	2 725 964	4 678 965
В національній валюті	611 869	961 654	1 906 188	2 384 594	4 393 276
В іноземній валюті	68 322	282 526	453 042	341 369	285 689
Кошти на вимогу	281 479	525 737	1 726 065	1 827 287	3 512 625
В національній валюті	214 533	278 291	1 275 861	1 485 991	3 228 265
В іноземній валюті	66 946	247 446	453 042	341 296	284 360
Кошти на строкових рахунках	398 712	718 443	633 165	898 676	1 166 340
В національній валюті	184 179	683 364	630 327	898 603	1 165 011
В іноземній валюті	214 533	35 080	0	73	1 329
Зобов'язання	4 855 695	7 991 294	12 179 344	15 368 269	21 668 440

Джерело: складено автором за матеріалами [49]

Як бачимо з табл. 2.8 діяльність АТ «А – БАНК» в напряму депозитних операцій юридичних осіб в загальній сумі зобов'язань АТ «А – БАНК» за досліджуваний період 01.01.2020 на початок 01.01.2024 збільшились з 14% до 21%, це збільшення відображає, що АТ «А – БАНК» за останні роки активно почав займається обслуговування юридичних осіб.

Починаючи з 2021 року АТ «А – БАНК» збільшив кошти юридичних осіб з 680 191 тис. грн. до 1 244 181 тис. грн., а вже на початок 2024 року цей показник склав 4 678 965 тис. грн., за весь період на 3 998 774 тис. грн, з яких переважно відкриті в національній валюті.

Отже, з точки погляду, формування ресурсів АТ «А – БАНК» позитивним є сталість надходження на рахунки клієнтів, попри невизначеність

та загрози операційного середовища.

Оцінка якості кредитної діяльності кожного банку є невід'ємною складовою, оскільки кредитна діяльність є основною для більшості банків та вона дуже чутлива до різних макроекономічних та мікроекономічних факторів, тобто розуміння її стану дає банку певну інформацію для прийняття стратегічно важливих рішень. В основу формування кредитної політики закладено принципи професіоналізму співробітників, зваженої оцінки кредитного ризику й щільну співпрацю з клієнтом-позичальником

Кредитна діяльність банку є дуже ризиковою та вимагає як акціонерів, керівників та співробітників чітко механізму щодо усіх етапів кредитування від надання до погашення. Кожний етап окремо забезпечує вирішення певних приватних завдань, а сукупності досягається головна мета кредитних операцій – їх надійність та прибутковість для банку. Особливо важливим етапом є оцінка кредитоспроможності клієнта, яка спрямована на виявлення об'єктивних результатів і тенденцій у його діяльності про те, щоб попередити чи мінімізувати негативні для банку наслідки видачі цьому клієнту позички. У кожному окремому випадку банк визначає ступінь ризику, який він готовий взяти на себе, і розмір кредиту, який може бути наданий. Протягом усього терміну кредитування з боку банку відбувається кредитний моніторинг, який відображає систему спостережень за станом кредитного портфеля банку, включаючи аналіз, оцінку та прогноз виконання умов кредиту, зумовлених договорами, метою кредитного моніторингу – забезпечити погашення у строк основного боргу та сплату відсотків за позикою.

Таким чином, організація кредитного процесу банку має бути зорієнтована на максимально повне задоволення потреб позичальників у необхідних кредитних продуктах, збільшення обсягів одержуваного прибутку позичальників, банків та грошових оборотів від кредитних операцій,

покращення якості кредитного портфеля за суворого дотримання вимог кредитної політики банку та чинного законодавства України.

На рис. 2.5 наведено аналіз складу кредитного портфелю АТ «А – БАНК» за клієнтами фізичними та юридичними особами.

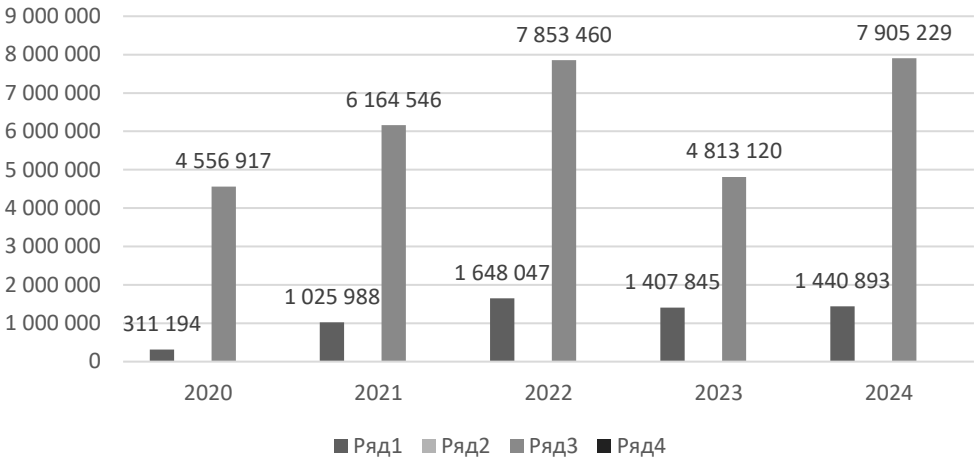

Рис. 2.5 Динаміка обсягів наданих кредитів юридичним та фізичним особами АТ «А – БАНК» за 2020 – 2024 рр. на початок періоду, тис. грн.

Джерело: складено автором за матеріалами [49]

Як ми бачимо з рис. 2.5, на початок 2020 р сума наданих кредитів юридичним особам АТ «А – БАНК» становила 311 194 тис. грн, на початок 2021 року збільшилось до 1 025 988 тис. грн., а на початок 01.01.2022 р. зросла до 1 648 047 тис.грн., за 2022 перший воєнний рік знизились до 1 407 845 тис. грн, але вже за 2023 другий воєнний рік відбувається несуттєве збільшення до 1 440893 тис.грн.

Інші ситуація з обсягами наданих кредитів фізичним особами, як бачимо з рис. 2.5 за 2019, 2020, 2021 рр. відбувається щорічне зростання, за 2022 рік зниження, а вже на результатами 2023 року кредитний портфель фізичних осіб склав 7 905 229 тис. грн, та перевищив показник довоєнного 2021 року.

Проведемо аналіз складу кредитного портфеля АТ «А – БАНК» за галузями та напрямами (табл. 2.9), який засновано на даних публічної фінансової звітності банку згідно МСФЗ, а саме: активу балансу та 10 примітки до фінансової звітності було проведено аналіз складу кредитного портфелю.

Таблиця 2.9

Структура кредитного портфеля АТ «А – БАНК» за галузями економіки за 2020 – 2024 рр. на початок періоду, тис. грн., %

Показники	2020		2021		2022		2023	
	тис. грн.	%	тис. грн.	%	тис. грн.	%	тис. грн.	%
Кредити фізичним особам	6300055	95,12%	7901815	91,22%	9 771 163	92,95%	8 738 511	92,64%
Сільське господарство, ліспопромисловий і деревоообробний комплекс	55591	0,84%	279999	3,23%	219 793	2,09%	281 093	2,98%
Торгівля	139083	2,10%	179948	2,08%	242979	2,31%	217940	2,31%
Виробництво	13596	0,21%	36066	0,42%	95330	0,91%	68456	0,73%
Гірничо-добувна промисловість/металургія	93055	1,40%	95475	1,10%	53113	0,51%	61510	0,65%
Будівництво	--	-	-	-	22301	0,21%	21943	0,23%
Енергетика	15122	0,23%	6633	0,08%	68797	0,65%	504	0,01%
Надання інформаційних послуг	3739	0,06%	20436	0,24%	-	-	-	-
Інше	8054	0,12%	35538	0,41%	38378	0,37%	42443	0,45%
Всього коштів клієнтів	6623226	100,00%	8661979	100%	10511854	100%	9 432	100%

Джерело: складено та розраховано автором за матеріалами [49,50,51]

Провівши аналіз кредитного портфеля АТ «А – БАНК» за галузями та напрямами за 2020 – 2024 рр. на початок періоду, можемо зробити висновки за звітний період АТ «А – БАНК» зберігав такі ж пропорції кредитного портфеля з невеликими змінами, насамперед пов’язаними впливом пандемії COVID 19, через яку мав негативний вплив на функціонуванні клієнтів АТ «А – БАНК». Несуттєві зміни відбулися в інших напрямах, таких як виробництво, торгівля, гірничо-добувна промисловість/металургія, але основними клієнтами для отримання кредитування залишаються клієнти – фізичні особи, кредитний портфель яких складає 92,64%.

Як свідчать дані табл. 2.10 основа структури кредитного портфелю АТ «А – БАНК» складається з «Кредити фізичним особам» де основні частки складають «Кредитні карти» та «Споживчі кредити фізичним особам». За аналізований період усі показники збільшувались за виключенням 2022 року.

Таблиця 2.10

Структура кредитного портфеля АТ «А – БАНК» за класами кредитів фізичних та юридичних осіб за 2020 – 2024 рр. на початок періоду, тис. грн.

Вид кредиту	2020	2021	2022	2023
Кредити фізичним особам	6300055	7901815	9771163	8738511
Кредитні карти	3236008	4206983	5154549	5183273
Споживчі кредити фізичним особам	2465349	2877784	330603	2282935
Автокредитування фізичних осіб	322823	316877	212109	148705
Фінансовий лізинг фізичним особам	27583	201866	444760	323821
Іпотечне кредитування фізичних осіб	133516	84045	71771	100853
Інші кредити фізичним особам	114778	214260	557370	698924
Кредити юридичним особам	322171	660164	740691	693889
Усього кредитів та заборгованості клієнтів	6622226	8561979	10511854	9432400

Джерело: розроблено автором за матеріалами [49,50,51]

Провівши аналіз кредитного портфеля АТ «А – БАНК» можна побачити, що пріоритетним напрямком в кредитній політиці є співпраця АТ «А – БАНК» з фізичними особами, частка кредитів та заборгованостей яких в кредитному портфелі значно перевищує частку кредитів та заборгованостей юридичних осіб. Але, можна побачити позитивну динаміку в обсягах кредитування АТ «А – БАНК» юридичних осіб. Крім того, слід відзначити, що за категоріями якостей більша частка кредитного портфеля визначається як без ризику, але, з іншого боку, згідно з проведеним аналізом, бачимо, що в АТ «А – БАНК» є проблеми з формування резервів за кредитним портфелем, що є негативною характеристикою і передбачає перегляд АТ «А – БАНК» його кредитної політики щодо формування резервів за кредитним портфелем.

Розглянемо ситуацію з розподілом кредитів за фізичними та юридичними особами в національній та іноземній валютах, та розмір

кредитного ризику за цими операціями.

В умовах цифровізації використання банківських карток є самим розповсюдженим засобом платежу, що надає можливість клієнтам доступ до максимальної кількості послуг банків, «однак, зростання використання банківських платіжних карток призвело до збільшення кількості кіберзлочинності, яка пов’язана з операціями з цими картками, що негативно впливає на фінансову безпеку банків та як слід, на їх прибутковість» [52].

Сучасну діяльність кожного банку не можливо розглядати» без участі у системах грошових переказів, АТ «А – БАНК» є учасником міжнародних платіжних систем VISA, Mastercard, Western Union Network, IntelExpress, Welsend та національної платіжної системи «ПРОСТІР» [47].

Для залучення клієнтів та підвищення своєї конкурентоспроможності, банки постійно впроваджують нові карткові продукти з різними умовами видачі та користування. АТ «А – БАНК» позиціонує себе впродовж декілька років як один із лідерів за кількістю електронних платіжних засобів.

«В умовах цифрової економіки банківські платіжні карти є одним з найсучасніших та найпоширеніших засобів безготівкових розрахунків, що забезпечують доступ клієнтів до різноманітних фінансових послуг та товарів» [52]. Суттєвою загрозою для банку є інформаційні загрози як зовнішнього, так і внутрішнього характеру, що своєю чергою негативно впливає діяльність банку. «Банки стають все більш уразливими перед кіберзлочинцями, які використовують різні методи та техніки для здобуття карткових даних та незаконного доступу до рахунків користувачів».

Управління інформаційними ризиками при обслуговуванні банками платіжних карток є одним із ключових аспектів забезпечення інформаційної безпеки, це включає захист від шахрайства, забезпечення конфіденційності даних клієнтів та зниження ризиків пов’язаних з електронним банкінгом.

Таблиця 2.11

Дані про кількість електронних платіжних засобів та платіжних пристроїв АТ «А – БАНК» за 2020 – 2024 рр. на початок періоду,

Роки	Кількість (штук, одиниць)							
	електронних платіжних засобів, термін дії яких не закінчився (в обігу)	електронних платіжних засобів, за якими протягом звітнього періоду (листопад) була здійснена хоча б одна видаткова транзакція	платіжних терміналів					Кількість пунктів продажу товарів/наданих послуг, одиниць
			загальна	торгово-вельних	із них без-контакт-них	надавача платіжних послуг	із них без-контакт-них	
2020	1 703 787	439 830	24	0	0	24	0	0
2021	1 575 677	526 377	24	0	0	24	0	0
2022	2 269 328	709 536	1 527	1 269	1 269	258	0	1 902
2023	3 720 635	719 630	2 020	1 816	1 816	204	0	5 041
2023	5 681 197	1 175 077	6 118	5 924	5 924	194	0	14 558

Джерело: складено автором за матеріалами [7]

Як наочно видно з табл. 2.11 АТ «А – БАНК» за п’ять років збільшив кількість електронних платіжних засобів на 3 977 410 штук, загальних платіжних терміналів на 6 094 штук, починаючи з 01.01.2020 року їх кількість складала 24 штуки, але вже на 01.01.2024 рік - 6 118 штук. Для захисту клієнтських даних АТ «А – БАНК» застосовує передові технології, такі як шифрування та двофакторна аутентифікація, та володіє власною системою антифроду для моніторингу та блокування підозрілих транзакцій. Ці заходи та інші викликали зростання довіри до банка, що відображається у збільшенні обсягу коштів клієнтів.

Для підвищення інформаційної безпеки банкам в напряму банківських карт рекомендовано дотримуватись методичних рекомендації НБУ, які включають кращі міжнародні практики та підходи для ефективного управління цими ризиками. Основні ризики, з якими можуть зіткнутися банки та їх клієнти, включають шахрайство з платіжними картками, ризик

ліквідності, операційні ризики, стратегічні ризики, репутаційні та юридичні ризики. Захист від цих ризиків вимагає комплексного підходу, включаючи технічні заходи, такі як криптування даних та безпечні комунікаційні протоколи, а також організаційні заходи, як от навчання персоналу та розробка внутрішніх політик і процедур. Важливо, щоб банки постійно оновлювали свої системи безпеки, щоб відповідати зростаючим вимогам та новим викликам у сфері інформаційних технологій.

Підсумовуючи можемо зазначити, що дотримання ефективної інформаційної безпеки в напряму безпеки інформаційних ресурсів дозволяє на ранніх стадіях визначати проблемні місця в діяльності банку та забезпечує захищеність фінансових інтересів банку, його клієнтів і акціонерів.

2.3 Оцінка дотримання безпеки інформаційної інфраструктури АТ «А – БАНК»

Сучасний технологічний банк займає ключові позиції у сучасному фінансовому світі, де інновації та цифровізація стають вирішальними факторами конкурентоспроможності.

В Україні, щорічна премія FinAwards визначає найбільш технологічні банки, які впроваджують новітні розробки для оптимізації процесів та підвищення якості обслуговування клієнтів. За 2023 рік АТ КБ «ПриватБанк», який посів перше місце у номінації, запровадив ряд проєктів, таких як систему SmartID для електронного підпису та FacePay24 для оплати покупок за допомогою розпізнавання обличчя. Ці та інші інновації дозволяють клієнтам банків здійснювати фінансові операції з великою зручністю та безпекою. Водночас, банки, такі як АТ «Ощадбанк», АТ «А – БАНК» та інші також зробили значний внесок у цифрову трансформацію, реалізувавши функції, які спрощують взаємодію з клієнтами та розширюють можливості онлайн-

сервісів. Така трансформація не лише підвищує ефективність банківських операцій, але й відкриває нові горизонти для розвитку фінансових послуг.

Протягом понад 10 років банки вже сформували моделі онлайнового банківського бізнесу, які представлені на рис 2.6.

Рис. 2.6 Моделі онлайнового банківського бізнесу

Джерело: складено автором за матеріалами [54]

На сьогоднішній день найбільш поширеними є перші три моделі. Інтернет-підрозділ зазвичай використовується для операцій на внутрішньому фінансовому ринку, а Інтернет-банк – для виходу за кордон(в першу чергу на ринки країн, що розвиваються), оскільки саме він забезпечує необхідну для зарубіжної діяльності гнучкість у використанні фінансових інструментів, встановленні тарифів й відборі клієнтів.

Зазначимо, що сучасна сфера інформаційних технологій, яка пов'язана з банками, характеризується ступенем високої невизначеності. Це пов'язане з технологічною основою всіх основних напрямків діяльності банку. Розглядаючи банк як інформаційний об’єкт, можемо визначити, що це єдина система компонентів, пов’язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну.

Організація дотримання інформаційної безпеки АТ «А – БАНК» регулюється державними нормативними актами, які ми розглядали в підрозділі 1.1 та внутрішнім документом Політика інформаційної безпеки АТ «А – БАНК» [53]. Процеси забезпечення інформаційної безпеки банку описані,

формально визначені та затверджені у реєстрі бізнес-процесів та внутрішніх нормативних документах. Організація будь-якого бізнес-процесу, що автоматизується й має оброблятись в інформаційній системі, або внесення змін в наявні процеси здійснюється з урахуванням вимог забезпечення інформаційної безпеки банку (рис. 2.7).

Рис. 2.7 Етапи побудови процесів захисту інформаційної системи АТ «А – БАНК»

Джерело: складено автором за матеріалами [40]

Отже, з рис. 2.7 бачимо, що базисом для дотримання інформаційної безпеки банку первинним є захист його інформаційної (технологічної) інфраструктури. В Банку контролюється ефективність впроваджених заходів та засобів забезпечення інформаційної безпеки в інформаційних системах, визначено перелік усіх бізнес-процесів та інформаційних ресурсів, які забезпечують їх функціонування.

Розглядаючи об’єкти, які складають основу інформаційної інфраструктури банку їх можливо поділити за двома напрямами це: програмне забезпечення, до якого відносять прикладне, системне, сервісне та програмне забезпечення (власне чи ліцензоване), яке використовується у Банку співробітниками, системами для роботи та взаємодії з клієнтами та іншими зовнішніми системами. В умовах цифровізації програмне забезпечення банку є ключовим елементом сучасної банківської індустрії, яке дозволяє банкам ефективно управляти різноманітними фінансовими операціями та надавати високоякісні послуги своїм клієнтам. ПЗ містить в себе системи ідентифікацій клієнтів, обробки платежів, кредитування, управління активами та пасивами, а також інструменти для аналітики та звітності. Сучасні банківські програмні рішення пропонують гнучкість та масштабність, що дозволяє банкам адаптуватися до змінних вимог ринку та впроваджувати інноваційні продукти та послуги.

Сучасними прикладами програмних забезпечень є продукт компанії CS, який пропонує комплексні програмні рішення для оцінки знецінення активів, автоматизації кредитних рішень, інтернет-банкінгу, а також управління бізнес-процесами. Інші платформи, такі як Square, надають інструменти для обробки платежів, які підходять як для електронної комерції, так і для фізичних компаній. Важливою перевагою сучасного банківського програмного забезпечення є його здатність інтегруватися з різними платіжними системами та підтримувати міжнародні транзакції, що є невід’ємною частиною глобалізованого фінансового світу.

Другим напрямом інформаційної інфраструктури банку є сервісні ресурси банку, до яких відносять обчислювальні та комунікаційні сервіси, доступ до мережі Інтернет, електронну пошту, телефонний зв’язок, систему сигналізації, відео та звуко-моніторинг, при взаємодії з якими, за умовами недотримання норм інформаційної безпеки можливість загроз може бути дуже великою.

Цифровізація банківських процесів та підвищений рівень кібератак спонукає банки постійно удосконалювати інформаційну інфраструктуру, щоб не допустити відставання від новітніх безпекових технологій. Сучасна філософія цифрового бізнесу це інвестиції в безпеку повинні відповідати реальному ризику, а не залежати від фінансових результатів діяльності.

Для мінімізації інформаційних ризиків, завдяки Постанові НБУ № 95 «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [40] банки використовують наступні засоби безпеки:

- захист від зловмисного коду;
- заходи безпеки при використанні електронної пошти;
- контроль доступу до інформаційних систем банку;
- заходи безпеки в мережі банку;
- криптографічний захист інформації.

«У разі застосування криптографічного захисту банк зобов'язаний використовувати криптографічні алгоритми, такі як асиметричні алгоритми та симетричне шифрування» [40].

Сучасністю для банків України стало використання хмарних технологій, особливо в умовах воєнного стану, що дозволяє банкам підтримувати стабільність та доступність своїх послуг. Згідно з регуляціями НБУ, банки мають можливість використовувати хмарні сервіси для надання банківських послуг та процесингу операцій з електронними платіжними засобами, використовуючи обладнання, розташоване в країнах ЄС, Великобританії, США та Канади. Це не тільки забезпечує безперебійну роботу в складних умовах, але й відкриває шлях до модернізації банківської системи, збільшення ефективності та оптимізації витрат, «під час оброблення банківських операцій та персональних даних клієнтів із застосуванням хмарних сервісів можна використовувати: вітчизняні засоби криптографічного захисту інформації, засоби, що відповідають вимогам законодавства держави, на території якої розташовано обладнання для надання хмарних сервісів» [55].

Сучасні автоматизовані системи банків забезпечують ефективність, безпеку та високий рівень обслуговування клієнтів. Вони містять в собі різноманітні рішення, починаючи від Core-banking систем, які є основою для проведення всіх банківських операцій, до інтегрованих платформ для інтернет-банкінгу, що дозволяють клієнтам керувати своїми фінансами онлайн. Завдяки автоматизації, банки можуть пропонувати персоналізовані фінансові продукти, підвищувати рівень захисту від шахрайських дій та фінансових злочинів, а також покращувати банківську звітність та аналітику. Цифрова трансформація у банкінгу є одним з найбільших викликів сучасності, але вона необхідна для забезпечення конкурентоспроможності та відповідності сучасним вимогам клієнтів. Системи, такі як АБС БАРС, АБС Б2, та Оракл ФлексКуб, є прикладами високотехнологічних рішень, які допомагають банкам оптимізувати їхні процеси та підвищити конкурентоспроможність.

Розглянемо одні з найпопулярніших автоматизованих систем, які використовують в банках України, в тому числі й в АТ «А – БАНК» для банківських установ є ProFIX, Scrooge, Б2, Oracle FLEXCUBE, BIS GRANT та інші.

Отже, використання автоматизованих банківських систем відіграють важливу роль у цифровізації банківської діяльності, сприяючи підвищенню ефективності, зниженню витрат та покращенню обслуговування клієнтів. Вони дозволяють банкам швидко адаптуватися до змін на ринку, впроваджувати інноваційні фінансові продукти та послуги, а також забезпечують високий рівень безпеки та конфіденційності даних.

Таблиця 2.12

Порівняльна характеристика найпопулярніших автоматизованих систем для банків

Назва автоматизованої банківської систем	Переваги	Користувачі
ProFIX	Спроектована з урахуванням особливостей функціонування бухгалтерії банку, зокрема використовує банківський план рахунків, допомагає в формуванні банківської звітності, підтримує інтеграцію з будь-якою АБС та забезпечує необхідний для банку рівень відмовостійкості ІБ	Клієнти є 250 банків у більш ніж 40 країнах світу АТ «Ощадбанк», АТ «Райффайзен Банк», АТ «Південний»
Scrooge	Комплексна система для автоматизації операційної, облікової і управ. діяльності кредитної установи з розгалуженою мережею відділень, що забезпечує інтегроване управ ресурсами банку та його ефект. діял.	ПрАТ «Банк Фамільний», АТ «А - Банк», АТ «ПУМБ», АТ «Універсал банк»
Master	Програма поєднує в собі не тільки ПЗ для обліку, а ще й має функціонал CPM-системи	Міністерстві фінансів України, Державній митній службі України, Міністерстві освіти і науки України, АТ «Укргазбанк»
Call Center XRM Banking	Повна автоматизація системи виплат вкладникам ліквідованих банків Можливість реалізації модуля «soft-collection», який передбачає автоматизацію процедур дистанційної роботи з позичальником щодо запобігання простроченої заборгованості або автоматизувати логістику та обслуговування POS-терміналів і банкоматів	Усі українські банки
«Клієнт – банк»	Дозволяє виконувати різні операції з рахунком та дистанційно взаємодіяти з банком, в тому числі обмінюватися листами та документами через захищені канали зв’язку мережі Інтернет. Цей інструмент допомагає спростити та автоматизувати процеси обліку фінансових транзакцій, переглядати стан рахунків, оперативно отримувати банківські виписки, формувати звіти та реєстри	Усі українські банки

Джерело: складено автором за матеріалами [55]

Одним із сучасних показників інформаційної інфраструктури банку є запровадження мобільного додатку, що дає можливість для банків покращувати комунікацію з клієнтами, збільшувати лояльність та відгуки, просувати свої продукти та послуги, а також аналізувати потреби та поведінку споживачів. Мобільні додатки банків значно спростили повсякденне управління фінансами для клієнтів, надаючи можливість здійснювати платежі, перевіряти баланси та управляти рахунками з будь-якого місця та в будь-який час.

Згідно з дослідженнями, до весни 2023 року, близько 78% клієнтів вже використовують мобільні додатки для банківських операцій, що свідчить про швидке прийняття цифрових технологій серед населення.

Для дотримання безпеки мобільних додатків банків рекомендовано встановлювати надійні паролі, використовувати двофакторну аутентифікацію та завантажувати додатки лише з офіційних магазинів додатків. Регулярне оновлення програмного забезпечення та використання надійного антивірусного захисту також можуть значно знизити ризики безпеки. У разі втрати або крадіжки пристрою, користувачам рекомендовано необхідно негайно заблокувати доступ до банківських додатків та повідомити банк для запобігання несанкціонованого доступу. Крім того, уважне ставлення до повідомлень про шахрайство та надання особистої інформації може допомогти уникнути фінансових втрат.

З огляду на зростаючу кількість кібератак, таких як DDoS-атаки на українські банки, клієнтам банків важливо бути в курсі сучасних методів захисту та рекомендацій з кібербезпеки, порівняльна характеристика мобільних додатків провідних банків представлена на рис. 2.8.

До критеріїв оцінки мобільних додатків слід включати зручність для користувача, багатство функцій, необхідність вдаватися до допомоги десктопного додатка або оператора, популярність серед користувачів, рейтинги симпатій, ступінь захисту від злому, та доступність інформації про фінанси. Цифрові технології, такі як блокчейн та штучний інтелект,

відкривають нові можливості для розвитку банківської сфери, зокрема у сфері мобільного банкінгу та безготівкових розрахунків.

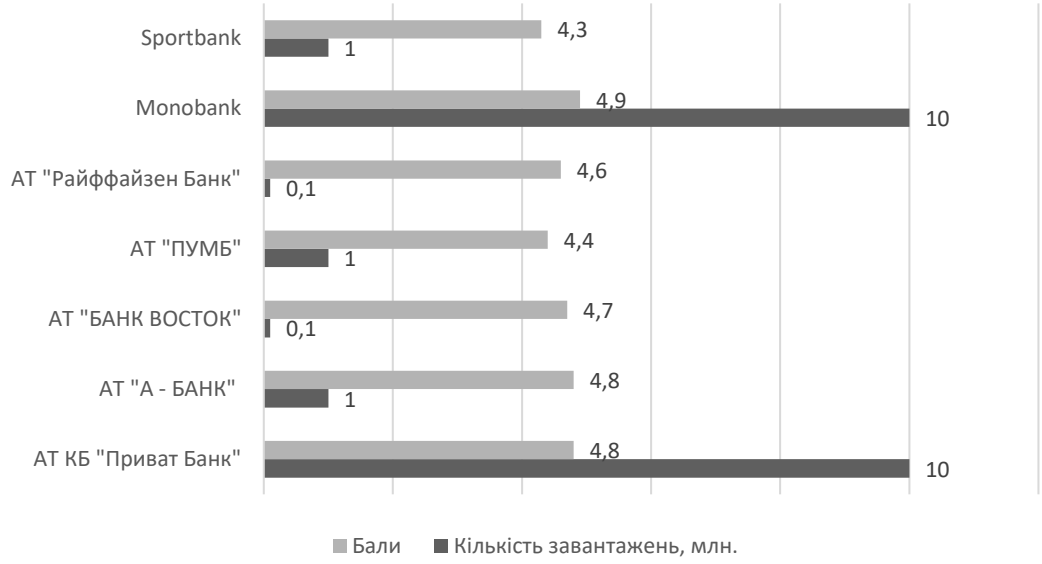

Рис. 2.8 Порівняльна характеристик мобільних додатків обраних банків на 01.01.2024 р.

Джерело: складено автором за матеріалами [56]

Сучасна інформаційна інфраструктура банку є обов'язковою необхідністю для забезпечення ефективності та безпеки банківських операцій, що містить в себе не лише апаратне та програмне забезпечення, а й комплексні системи кіберзахисту, які захищають дані клієнтів та фінансові операції від несанкціонованого доступу та інших кіберзагроз.

Використання сучасних інформаційних технологій дозволяє банкам не лише підвищувати рівень захисту інформації, але й оптимізувати внутрішні процеси, підвищуючи тим самим ефективність роботи банку. Таким чином, інформаційна інфраструктура є фундаментом для забезпечення стабільності, інноваційності та конкурентоспроможності банківського сектору.

Висновки до розділу 2

За результатами розділу 2 можемо надати наступні висновки:

1. Бізнес – модель діяльності АТ «А – БАНК» вже протягом багато років направлена на роздрібний бізнес, не зважаючи на пандемію COVID-19 та понад два роки повномасштабної війни в Україні, й надалі підтримує прагнення населення зберігати кошти у надійному банку, займається впровадженням змін заради покращення клієнтського досвіду, розвиває новітні канали обслуговування і комунікації з клієнтами. На 01.01.2024 р. діяльність АТ «А – БАНК» відбувається через 201 фізичне відділення, інтернет – банкінг та мобільний додаток.

2. Проведена оцінка основних фінансових показників діяльності АТ «А – БАНК» в розрізі найбільш значущих складових які впливають на формування прибуткового результату.

Статутний капітал АТ «А – БАНК» за аналізований період збільшився до 1514594 тис. грн., практично у 3 рази, це відбулось за рахунок власних коштів акціонерів банків та капіталізації за рахунок прибутку, в результаті чого збільшився загальний показник власного капіталу АТ «А – БАНК» з 292 162 тис. грн. до 2 9997309 тис. грн. практично у 10 разів.

Зобов’язання за аналізований період АТ «А – БАНК» відображав постійне зростання, за виключенням 2022 року для коштів банків, своєю чергою кошти клієнтів мали постійну тенденцію до зростання та за 5 років виросли з 5 167 804 тис.грн. до 20 359 333 тис.грн, тому як результат усіх зобов’язання АТ «А – БАНК» теж збільшились та склав на 01.01.2024 р. 21 668 440 тис. грн.

Активи АТ «А – БАНК» ситуація суттєво покращилась, за аналізований період загальні активи АТ «А – БАНК» збільшились на 19 958 855 тис. грн. чи на 243%.

За аналізований період АТ «А – БАНК» отримав прибуток у розмірі 254 801 тис. грн., на початок 2021 року 299738 тис. грн., на початок 2022 року АТ «А – БАНК» збільшив прибутковість практично в чотири рази або 800 013 тис. грн, за перший воєнний рік, на 01.01.2023 р, АТ «А – БАНК» відзвітував про отримання прибутку 202 637 тис. грн, а вже на 01.01.2024 р. АТ «А – БАНК» 561 312 тис. грн.

Визначено, що АТ «А – БАНК» за п’ять років активно залучав кошти як від банківських установ, так від клієнтів юридичних та фізичних осіб. Збільшення усіх показників підтверджує, що протягом досліджуваного періоду до АТ «А – БАНК» дотримується усіх норм безпеки щодо інформаційних ресурсів, завдяки має високу довіру з боку клієнтів, що відображається в щорічному збільшенню клієнтської бази.

В напряму обслуговування поточних та строкових рахунків фізичних осіб за п’ять років мала тенденцію до постійного зростання, як в національній, так і в іноземній валюті. За два роки повномасштабного вторгнення кошти фізичних осіб виросли на 6 505 675 тис. грн., я яких кошти на вимогу на 4 183 810 тис. грн., строкові вклади на 2 321 865 тис. грн. В загальній сумі зобов’язань АТ «А – БАНК» у впродовж 2019 та 2020 років обслуговування фізичних осіб займало практично 80% усіх зобов’язань банку, то вже починаючи з 2021 року АТ «А – БАНК» зменшує цей показник до рівня 75%, а на 01.01.2024 р. до 72%,

Оцінка кредитного портфеля АТ «А – БАНК» за клієнтами фізичними та юридичними особами показала, що по юридичним особам АТ «А – БАНК» відбувається несуттєве збільшення до 1 440893 тис. грн.

За обсягами наданих кредитів фізичних осіб відбувається щорічне зростання, за 2022 рік зниження, а вже за результатами 2023 року кредитний портфель фізичних осіб склав 7 905 229 тис. грн, та перевищив показник довоєнного 2021 року.

3. Оцінювання дотримання інформаційної безпеки в напряму безпеки інформаційних ресурсів АТ «А – БАНК» показало, що АТ «А – БАНК» вже

на ранніх стадіях інформаційної загрози визначає проблемні місця в діяльності б та забезпечує захищеність фінансових інтересів банку, його клієнтів і акціонерів.

4. Інформаційна інфраструктура є необхідною умовою в діяльності сучасних банків, оскільки вона забезпечує ефективне управління даними, оптимізацію процесів та підвищення безпеки. Інформаційні технології дозволяють банкам скорочувати витрати, підвищувати ефективність роботи, забезпечувати лояльність клієнтів та спрощувати надання послуг.

РОЗДІЛ 3 НАПРЯМИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВ УКРАЇНИ В УМОВАХ НЕВИЗНАЧЕНОСТІ

3.1 Світові виклики, що впливають на рівень інформаційної безпеки банків

У сучасному світі, де цифровізація проникає у всі сфери нашого життя, питання кіберзахисту банків набуває особливої актуальності. Досвід країн світу у сфері підвищення інформаційної безпеки банків відіграє важливу роль у формуванні ефективних стратегій захисту від кіберзагроз. З огляду на глобальний характер інтернету та транскордонну природу кібератак, банки по всьому світу співпрацюють та обмінюються кращими практиками для забезпечення високого рівня захисту своїх систем. «Упродовж останніх десятиліть відбувається постійне збільшення обсягів та розширення сфер використання цифрових технологій, поширення Інтернету речей, гібридних і віддалених форм роботи, розвиток соціальних мереж, підвищення рівня «цифрової залученості» населення тощо, що об’єктивно обумовлює виникнення кіберзагроз й наражає всіх учасників цифрових екосистем на кіберризики, які мають специфічні форми прояву та можуть негативно впливати на різноманітні сфери діяльності» [58].

Таблиця 3.1

Рейтинг вразливості діяльності до кіберзлочинів у світі

за період з 2018 по 2022 рр.

Сфера діяльності	Рік					Зміна, 2022/2018
	2018	2019	2020	2021	2022	
Фінансові послуги	19	17	23	22,4	18,9	0
Виробництво	10	8	17,7	23,2	24,8	+15
Енергетика	6	6	11,1	8,2	10,7	+5
Роздрібна торгівля	11	16	10,3	7,3	8,7	-2
Професійні послуги	12	10	8,7	12,7	14,6	+3
Охорона здоров’я	6	3	6,6	5,1	5,8	0
Медіа	8	10	5,7	2,5	0,5	-8
Транспорт	13	13	5,1	4	3,9	-9
Освіта	6	8	4	2,8	7,3	+1

Джерело: [59]

Як видно з табл. 3.1 «найбільший приріст зафіксовано по сфері виробництва, при цьому зменшився інтерес кіберзлочинців до транспортної галузі та медіа» [59]. Але, слід зазначити, що за останні роки фінансовий сектор має високий рівень вразливості до кіберзлочинів. Це пояснюється тим, що банки – це фактично «кровоносна система» національної економіки, через яку здійснюється обслуговування інтересів держави (виконання державного і місцевих бюджетів, отримання міжнародної допомоги, надання субсидій тощо), суб'єктів господарювання різних галузей економіки, а також громадян суспільства. З урахуванням цього, банки акумулюють значну за обсягом інформацію від своїх клієнтів. У разі порушення інформаційної безпеки фінансових установ конфіденційні дані можуть бути використані для здійснення протиправної діяльності або продані на темних веб-майданчиках, що може призвести до втрати ділової репутації як фінансових установ, так і їх клієнтів.

Таблиця 3.2

Основні суттєві події ризику банків світу 1991 – 2017 рр.

Рік	Назва банку	Назва ризику	Збитки, млрд. дол
1991	Bank of Credit and Commercial International	Приховування збитків	1,0
1995	Barings	Несанкціоновані операції з ф'ючерсними контрактами	1,0
2007	Societe Generale		7,0
2007	Northern Rock	Житлова криза	137,0
2009	HSBS	Відмивання грошей	1,9
2012	Rabobank, UBS, JPMorgan, Deutsche Bank та ін.	Махінації LIBOR	9,0
2012	Deutche Bank	«Fat fingers» операції	6,0
2015	Goldman Sachs	Неналежні операції	5,6
2016	Bangladesh Bank	Кібератаки	0,1
2016	Privatbank (Ukraine)	Шахрайство SWIFT	10,1
2017	Вплив вірусу Petya (у т.ч. 70% укр. банків)	Кібератака	8,0

Джерело: [60]

Як бачимо з табл. 3.2 за останні роки основними викликами для банків є загрози від кібератак.

На Всесвітньому економічному форумі 2024 у Давосі, який проводиться вже 54 раз поспіль, були визначені основні ризики на 2024 рік, такі як:

1. «Безпека і співпраця в сучасному розрізненому світі.
2. Забезпечення зростання і робочих місць в нову еру.
3. Штучний інтелект як рушійна сила економіки й суспільства.
4. Довгострокова стратегія для клімату, природи й енергії» [61].

Отже, бачимо, що дотримання та удосконалення безпеки є основним пріоритетом світового суспільства.

Причини, які провокують виникненню кіберризиків для банків представлено на рис. 3.1.

Рис. 3.1 Причини, які провокують виникненню кіберризиків для банків

Джерело: складено автором за матеріалами [58]

Як бачимо з рис. 3.1, що практично усі кіберризики на пряму, чи опосередковано пов'язані з недосконалістю, чи економії на інформаційній інфраструктурі, тому завданням управління кіберризиками повинно бути

направлена на зниження їх виникнення та мінімізації розмірів втрат, а заходи щодо підвищення ефективності управління повинні бути спрямовані на поліпшення техніко-технологічних характеристик інформаційно-комп'ютерних систем, обладнання, програмного забезпечення та вдосконалення управління банком.

Роль кіберстійкості банків полягає в забезпеченні досягнення банком своєї «місії та бізнес-цілей, які залежать від рівня надійності, функціонування та ефективності використання кіберресурсів» [58].

При умові таких викликів, на нашу думку, банкам необхідно на базовому рівні визначити універсальні міжнародні індикатори в забезпеченні кібербезпеки у вигляді єдиних стандартів доступу до даних, програмне забезпечення з вбудованими кодами.

Розглянемо досвід США щодо втрати від окремих видів кіберзлочинності за 2022 рік.

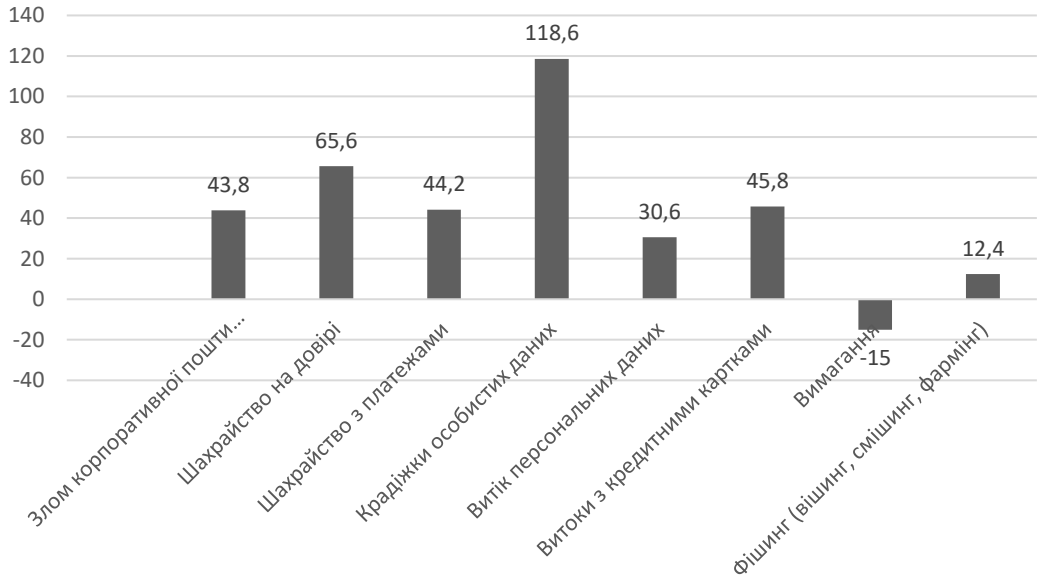

Рис. 3.2 Втрати від окремих видів кіберзлочинності в США за 2022 рік, %

Джерело: складено автором за матеріалами [58]

Як бачимо з рис. 3.2, що найуразливішою кіберзагрозою для банків та фінансових посередників, які здійснюють операції з грошима є крадіжка

особистих даних, які за рік зросла на 118% та навпаки вид кіберзлочинності «Вимагання» зменшився на 15%, що відображає рівень фінансової грамотності користувачів.

Ще одним із розповсюджених кіберзагроз як для України, так і для зарубіжних країн є несанкціонований доступ до даних банку через злом комп'ютерних мереж банку.

Найпоширенішим видом кіберзагроз є фішинг, виникнення якого відбувається через викрадення або пошкодження корпоративних і персональних даних, BEC/EAC-атаки.

Цікавим до аналізу є визначення джерел через які викрадаються персональні дані громадян США за 2022 рік.

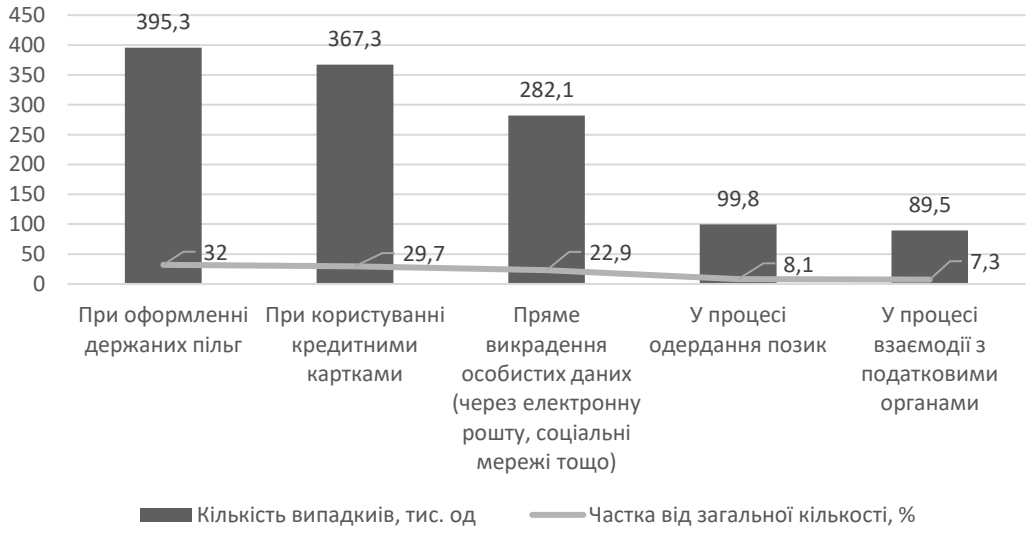

Рис. 3.3 Джерела викрадення персональних даних громадян США у 2022 році, тис. од., %

Джерело: складено автором за матеріалами [58]

З рис. 3.3 наочно бачимо, що найчастішим викраденням даних громадян відбувається через їхню необачність і довірливість при оформленні державних пільг (32 %), у процесі використання кредитних карток (29,7%), а також при користуванні електронною поштою й соціальними мережами (22,9%).

Соціальна інженерія складає значний ризик для інформаційної безпеки банків, оскільки вона експлуатує людський фактор, який часто є найслабшою

ланкою в системах безпеки. Цей метод маніпуляції людьми може включати різноманітні тактики, такі як фішинг, вішинг, смішинг, а також інші форми обману, щоб отримати доступ до конфіденційної інформації. Банки повинні постійно вдосконалювати свої стратегії інформаційної безпеки, щоб протистояти соціальній інженерії, включаючи навчання персоналу розпізнавати та реагувати на спроби шахрайства з використанням соціальної інженерії. Крім того, важливо розробляти комплексні системи захисту, які враховують не тільки технічні аспекти, але й психологічні особливості співробітників.

На жаль, за останні роки у світі рівень кіберзлочинності тільки зростає, що спонукає банки ще більш оптимізувати та удосконалювати свою інформаційну інфраструктуру (рис. 3.4).

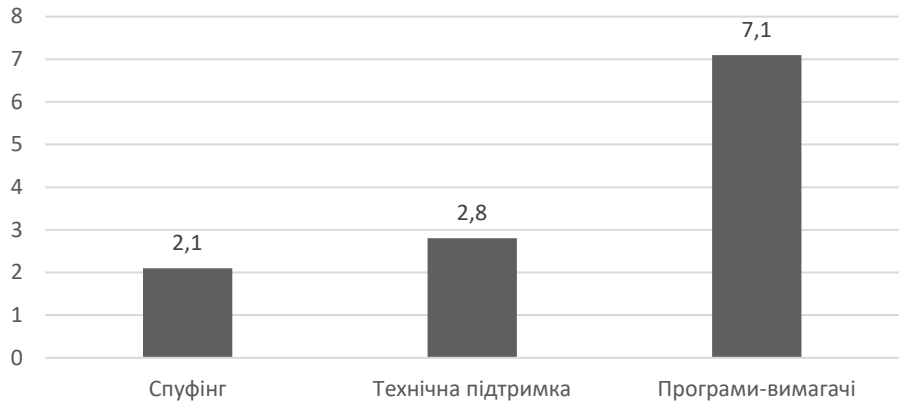

Рис. 3.4 Втрати від окремих видів кіберзлочинності в США за 2022 рік, разів

Джерело: складено автором за матеріалами [58]

Рис. 3.4 відображає зростання впливу кіберзагроз на програмне забезпечення.

Третій рік повномасштабної війни для банків України стала ще більш уразливими до кібератак. Державна служба спеціального, зв'язку та захисту інформації України, яка активно співпрацює з міжнародними організаціями для підвищення рівня кіберзахисту на національному рівні, проінформувала,

«що країна агресор щомісяця проводить від 102 до 293 кібератак» (рис. 3.5) [62].

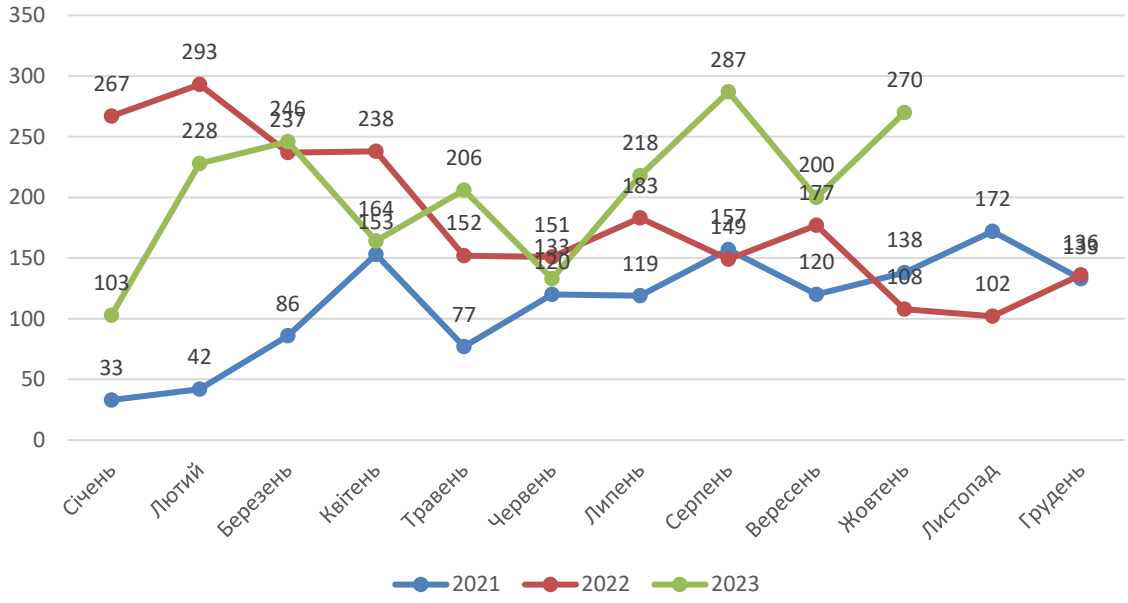

Рис. 3.5 Кількість кібератак на Україну за місяцями 2021 – 2023 (по жовтень), разів

Джерело: складено за матеріалами [63]

З рис. 3.5 наочно видно, що «хакери використовують різні підходи: від сканування IT - периметру до DDoS-атак – перевантаження сервісу запитами для того, щоб його «покласти». Під час однієї з DDoS-атак на «Укренерго» кількість запитів могла перевищувати 5 млн за декілька годин» [63].

При цьому самими вразливими секторами економіки, на які були здійснені кібератаки, це енергетичний сектор. сектор безпеки та оборони уряд і місцеві органи влади та фінансовий сектор. Кіберзагрози відбувались через несанкціонований збір інформації, впровадження шкідливого програмного коду, втручання або спроби втручання в ІК-системи та через порушення доступності мереж.

Останній масштабний збій через хакерську атаку був направлено на найбільшого мобільного оператора України «Київстар» наприкінці 2023 року, втрати були приблизно 40% інформаційної інфраструктури компанії.

З метою запобігань та уникнення впливу кіберзагроз банки повинні створювати комплекс взаємопов’язаних підсистем, таких як технічні, технологічні, організаційні, юридичні та управлінські на оперативному, тактичному та стратегічному рівнях

Таким чином, можемо зазначити, що міжнародний досвід у сфері інформаційної безпеки банків є надзвичайно цінним, оскільки він допомагає формувати ефективні механізми захисту, які можуть бути адаптовані до специфіки кожної країни, забезпечуючи таким чином стійкість фінансової системи перед викликами до кіберзагроз, які постійно еволюціонують. З іншого боку, міжнародний досвід також підкреслює важливість використання комплексного підходу до інформаційної безпеки, який охоплює моніторинг, аналіз, прогнозування ризиків, розробку стратегій та заходів щодо захисту від інформаційних загроз. Це дозволить банкам не лише реагувати на поточні виклики, а й прогнозувати майбутні загрози, адаптуючи свої системи захисту відповідно до змінюваних умов.

3.2 Напрями підвищення інформаційної безпеки в банках України

Стратегія кібербезпеки України на 2021-2025 роки визначає пріоритети та завдання для створення умов безпечного функціонування кіберпростору, враховуючи глобальні тренди та ризики, пов'язані з розвитком інформаційних технологій, що включає захист критичної інформаційної інфраструктури та протидію кіберзагрозам, які можуть вплинути на національну безпеку країни.

Виходячи з цих викликів, НБУ посилює контроль за виконанням банками заходів із забезпечення кіберзахисту та інформаційної безпеки, що є важливим кроком у зміцненні фінансової стабільності країни. Впровадження нових видів контролю, таких як виїзні перевірки та безвиїзний нагляд, дозволяє ефективніше протидіяти сучасним кіберзагрозам. Цифрові

технології, які активно використовуються в банківській сфері, вимагають відповідного рівня захисту, особливо в умовах воєнного часу, коли ризики кібератак зростають щодня. В цих умовах банки зобов'язані постійно проводити самооцінку стану інформаційної безпеки та кіберзахисту, що повинно сприяти підвищенню їхньої відповідальності та готовності до можливих кіберінцидентів.

З огляду на глобальні тенденції, українські банки продовжують розвивати цифрові канали обслуговування клієнтів, що вимагає постійного вдосконалення систем кіберзахисту для забезпечення безпеки транзакцій та даних користувачів.

Для стійкої діяльності банку під впливом воєнного стану, кіберзагроз можемо надати рекомендації, що дотримання наступних принципів рис. 3.7.

Як бачимо з рис. 3.6 до принципів планування реагування банків в умовах воєнних дій в країні в першу чергу необхідно дотримуватись інформаційної безпеки в повному обсязі, як фінансової, інформаційної так і кадрової. Цей принцип реагування повинен базуватися на зосередженні щодо продовження очікування невизначеності та підвищення кіберзагроз, що зможе забезпечити кіберстійкість банків та продовження адаптування банків до існуючих чинників в країні.

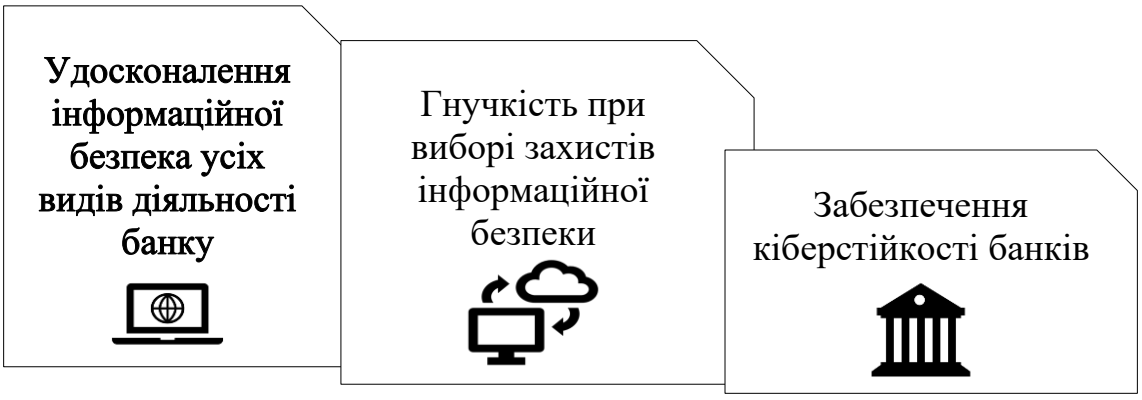

Рис. 3.6 Принципи планування реагування банків України впродовж воєнних дій в країні під впливом кіберзагроз

Джерело: авторська розробка

По-друге, необхідність керівництва пристосовувати та удосконалювати програмне забезпечення під впливом світових викликів та змінювати вектор діяльності банків з метою задоволення потреб клієнтів банків та фінансових цілей самих банків.

По-третє, необхідність забезпечення кіберстійкості банків. При цьому «…забезпечення кібербезпеки, в основному, орієнтоване на оцінку ймовірності виникнення інцидентів та запобігання можливих загроз безпеки, то забезпечення кіберстійкості спрямоване на збереження цільової поведінки та працездатності кіберсистем в умовах як відомих (приблизно 45 %), так і невідомих кібератак (решта 55 %)» [64].

У квітні 2024 р. НБУ відзвітувався, що «продовжує співпрацю з Міністерством фінансів Сполучених Штатів Америки у сфері забезпечення кібербезпеки в банківському та фінансовому секторах України» [65]. На основі цієї співпраці було підписано Меморандум «Про взаємодію та співробітництво у сфері кібербезпеки». «Метою цього документа є організація взаємодії між Національним банком України та Міністерством фінансів США для:

- реалізації механізмів обміну інформацією у сфері кібербезпеки та актуальних кіберзагроз;
- подальшого розвитку Центру кіберзахисту Національного банку (CSIRT-NBU);
- розроблення та реалізації заходів підтримки НБУ з питань кібербезпеки в банківському та фінансовому секторах України» [65].

Спираючись на основні принципи планування реагування банків України впродовж воєнних дій в країні під впливом кіберзагроз та реагуванням на них пропонуємо розглянути основні напрями щодо захисту банку як суб’єкту в реаліях сьогодення на рис 3.7.

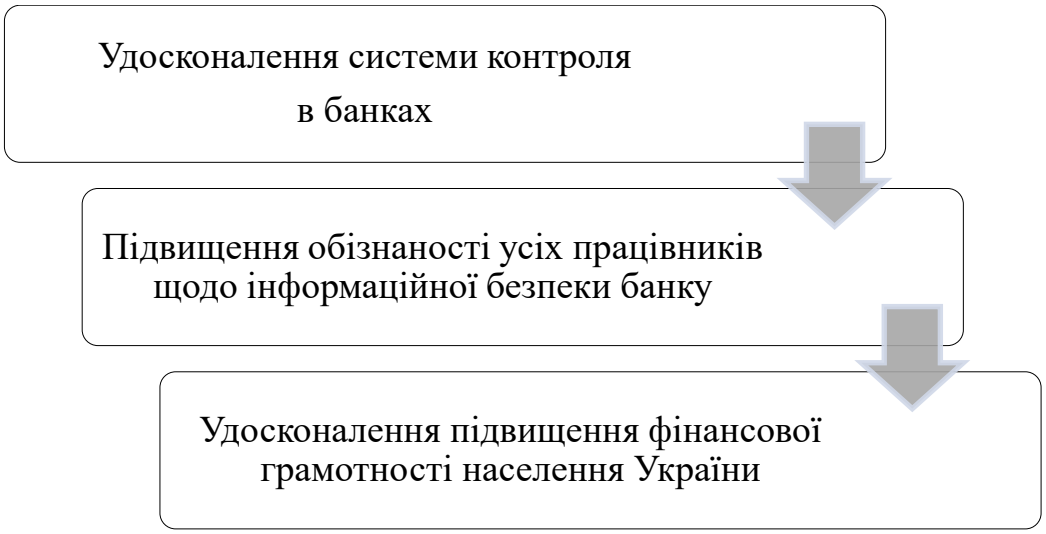

Рис. 3.7 Напрями щодо підвищення рівня інформаційної безпеки банків в реаліях сьогодення

Джерело: авторська розробка

Першим пріоритетом підвищення інформаційного захисту банків в умовах невизначеності є удосконалення системи управління в банках через підвищення ролі контролінгу в банках. Зазначимо, що сучасному етапі в кожній банківській установі створені програмно-технологічні елементи щодо відображення ризиків. Але, впровадження ефективної системи управління інформаційного захисту банком, яка зв'язує усі рівні управління від планування до регулювання є визначення ролі контролінгу в банку «який дозволяє інтегрувати на системній основі всі ключові аспекти управління грошовими потоками на базі чинної організаційної структури та інформаційного забезпечення та яка ефективно впливає на управління операційним ризиком в банках» [66]. Тому, логічно, розглядати діяльність банку через вплив як зовнішніх, так і внутрішніх інформаційних ризиків, які мають відображення в операційному ризику.

Вплив інформаційних ризиків, які мали прояв в операційному ризику банків в умовах війни наведені в таблиці 3.3.

Таблиця 3.3

Вплив інформаційних ризиків, які мали прояв в операційному ризику банків в умовах війни

Вид	Характеристика	Індикативні події втрат
Кібератаки	Втрати від призупинення діяльності банку через DdoS атаки, атаки на інформаційну інфраструктуру, зокрема за допомогою шкідливого програмного забезпечення	Безпека інформаційних систем
Зовнішнє шахрайство	Втрати від заволодіння обманним шляхом або незаконне відчуження коштів / майна або інша шкода, включно з кіберщахрайствами	Крадіжки / грабежі (відділення, ATM, APS). Втрата готівкових коштів
		Безпека інформаційних систем (злами, крадіжка інформації, фішингові посилання на вебсайти стилізовані під урядові портали та фіктивні посилання на соціальну допомогу від державних чи міжнародних організацій)
Відносини з персоналом і безпека робочого місця	Втрати, що випливають із діяльності банку, яка не відповідає стандартам та правилам безпеки персоналу	Витрати на забезпечення безпеки персоналу. Виплати персоналу. Фінансування евакуації. Організація нових робочих місць для внутрішньо переміщеного персоналу
Клієнти, продукти та бізнес-практика	Втрати, що випливають із ненавмисного невиконання функцій/ процедур або недбалого виконання зобов'язань перед клієнтами	Професійна невідповідність. Розкриття/несанкціоноване використання конфіденційної інформації. Неналежна ідентифікація клієнта.
Призупинення діяльності та відмова інформаційних систем	Втрати від подій, що сталися через збої/некоректну роботу інформаційних систем	Апаратні, програмні збої, збої телекомунікацій та допоміжних систем, які перешкоджають/ унеможливлюють діяльність банку
Виконання, доведення та менеджмент процесів	Втрати від подій, що сталися в результаті помилок обробки операцій/транзакцій, помилок управління процесами	Некоректне введення даних/ помилки завантаження. Недотримання строків. Некоректна робота системи.

Вид	Характеристика	Індикативні події втрат
		Проблеми в зберіганні та підтримці даних.
		Хибна робота, невиконання зобов'язань з незалежних причин контрагентів, продавців та постачальників ресурсів

Джерело: складено автором з використанням [68]

Виходячи із аналізу таблиці 3.3, ми можемо погодитися, що сьогодні конкурентоспроможний банк той, який надає максимум банківських послуг завдяки технологіям, що з одного боку несе для банку якість та прибутковість діяльності, але з іншого боку підвищує рівень операційного ризику та його відображення у банківських витратах. Тому, на нашу думку, для раціоналізації та ефективності банківських процесах та мінімізації операційних ризиків необхідно удосконалювати рівні інформаційної безпеки на кожному рівні.

Рекомендацією для АТ «А - БАНК» можемо запропонувати для підвищення інформаційної безпеки в напряму коригування оцінки кредитного, процентного ризиків, ризику втрат, ризику ліквідності, переглянути структуру активів і пасивів та організацію ризик-менеджменту, з урахуванням економічних змін сучасного часу та діджиталізації.

Другим пріоритетом є підвищення обізнаності щодо інформаційної безпеки банку усіх працівниках банку, які використовують інформаційні ресурси (комп'ютерне, телекомунікаційне і офісне обладнання) відповідно до посадових обов'язків. Працівникам рекомендовано виявляти, враховувати і реагувати на дійсні і ймовірні порушення інформаційної безпеки. Всі інциденти інформаційної безпеки банку повинні фіксуватися у журналі обліку інцидентів ІБ, з наступним врахуванням при розробці заходів захисту інформаційних активів.

Працівниками системи управління інформаційною безпекою через внутрішні нормативні документи доводяться до відома працівників Банку в

частині, що їх стосується. У Банку на регулярній основі забезпечується інформування та навчання працівників Банку з питань інформаційної безпеки.

З метою зниження інформаційних ризиків для працівників банків проводяться систематичні навчання нормам та заходам інформаційної безпеки.

В сучасних банках для підвищення інформаційної безпеки банку сформована «модель порушника» в якій покрокове описані дії порушників, які складаються з типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушники можуть бути зовнішні або внутрішні, залежно від рівня доступу до банківської інформації.

До внутрішніх порушників належать: працівники, користувачі інформаційної системи, які можуть завдавати навмисної чи ненавмисної шкоди інформаційним ресурсам; технічний персонал, який обслуговує будівлі, приміщення, технічні засоби які не є елементами Інформаційної системи (електрики, сантехніки, інженери, техніки).

До зовнішніх порушників відносяться сторонні особи, які знаходяться поза периметром інформаційно-телекомунікаційної системи Банку або її не авторизовані користувачі. Це означає, що вони не мають в ІКС Банку облікового запису і не мають повноважень працювати в даній системі.

Отже, зазначимо, що банківські порушники можуть мати значний вплив на інформаційну безпеку банків, оскільки їх дії можуть призвести до порушення законодавства у сфері фінансового моніторингу. Для інформаційної безпеки банків дуже високий ризик можуть нанести особи, які напряму пов’язані з повним доступом до програмного забезпечення банку, а тощо адміністратори ІС, працівники ДІБ, з боку зовнішніх порушників це хакери та агенти конкурентів та спецслужб.

Таблиця 3.4

Категорії порушників банків в залежності від поділу на внутрішні та зовнішні

№№	Визначення категорії	Тип порушника по відношенню до Банку	Рівень загрози
1.	Технічний персонал (електрики, прибиральники, тощо)	Внутрішній	Низький
2.	Персонал, що обслуговує технічні засоби ІС	Внутрішній	Високий
3.	Користувачі ІС	Внутрішній	Середній
4.	Адміністратори ІС, працівники ДІБ	Внутрішній	Дуже високий
5.	Керівники підрозділів з розширеними повноваженнями в тому числі в інформаційних системах	Внутрішній	Високий
6.	Клієнти, відвідувачі Банку	Зовнішній	Низький
7.	Представники обслуговуючих організацій (енергопостачання, газова служба, водопостачання, тощо)	Зовнішній	Низький
8.	Хакери	Зовнішній	Дуже високий
9.	Агенти конкурентів та спецслужб	Зовнішній	Дуже високий

Джерело: [53]

Слід зазначити, що особливої уваги повинні привертати об'єкти критичної інформаційної інфраструктури банку, до яких відносяться інформаційні системи, що безпосередньо забезпечують автоматизацію банківської діяльності (надання банківських послуг) та відповідають двом критеріям:

- порушення функціонування інформаційної системи внаслідок кіберінциденту, кібератаки може вплинути на стале функціонування Банку та безперервність надання Банком ОКІ відповідних послуг;
- якщо в Банку немає альтернативних за функціональними можливостями інформаційних систем для надання аналогічних відповідних послуг.

Рівні кваліфікації банківського порушника представлено на рис. 3.8.

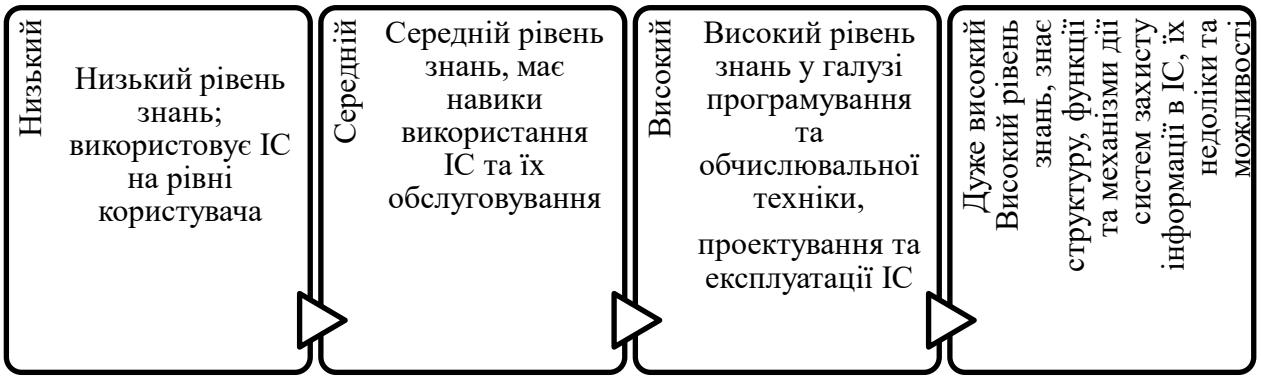

Рис 3.8 Рівні кваліфікації банківського порушника

Джерело: [53]

З рис. 3. 8 наочно бачимо, що на інформаційні ризики має вплив рівень знаннь щодо програмування та комп’.юерної інженерії персоналу банку.

Внутрішній документ «Політики інформаційної безпеки банку» [53] чітко визначає, що «усі працівники Банку, незалежно від займаної посади, персонально відповідають за дотриманням вимог ІБ відповідно до чинного законодавства України, вимог НБУ та внутрішніх нормативних документів. Керівники підрозділів Банку додатково є відповідальними за порушення вимог ІБ і неправомірні дії підлеглих їм працівників в межах обов’язків з контролю за підлеглими, згідно з посадовими інструкціями. Кожен працівник Банку забезпечує підтримку належного рівня інформаційної безпеки. Працівники усіх підрозділів Банку є відповідальними за виконання і за порушення вимог Політики інформаційної безпеки, законодавчих, регуляторних і внутрішньобанківських норм інформаційної безпеки. Усі працівники під час приймання на роботу повинні бути ознайомлені з Політикою інформаційної безпеки під підпис та надати зобов'язання про дотримання конфіденційності» [53].

Тому рекомендацією для АТ «А - БАНК» щодо удосконалення інформаційної безпеки банків з боку персоналу є вживання відповідних

заходів для запобігання таким порушенням, включаючи розробку ефективних систем фінансового моніторингу та управління ризиками.

Третім пріоритетом є підвищення рівня фінансової грамотності. Дотримання цього напряму сприяє формуванню здатності клієнтів розуміти та ефективно управляти фінансовими ризиками, а також підвищує їхню здатність до прийняття обґрунтованих фінансових рішень.

НБУ активно працює над підвищенням фінансової обізнаності громадян, проводячи заходи та розробляючи стратегії, спрямовані на збільшення фінансових знань серед населення. Це включає ініціативи, які охоплюють різні цільові аудиторії та містять в себе освітні програми, що дозволяють людям краще розуміти фінансові продукти та послуги. Також важливою є робота з молоддю, адже формування фінансової грамотності з раннього віку може мати довгостроковий позитивний вплив на економічне майбутнє країни. Враховуючи міжнародний досвід, Україна прагне досягти стандартів фінансової грамотності, що встановлені в країнах з розвиненою економікою, що своєю чергою, сприятиме зміцненню фінансової стабільності та безпеки на національному рівні.

Сучасні банки дуже активно беруть участь в цьому напряму, це реалізується через відображення на своїх сайтах умов дотримання безпеки при використанні банківських продуктів.

З аналізу сайтів банків категорії «Безпека» відображені основні, напрями: наявність внутрішнього документа «Політика інформаційної безпеки, загальні правила безпеки, правила безпеки фізичних осіб, правила безпеки в разі підозрілих дзвінків та смс. правила безпеки при користуванні мобільними застосунками та наявність гарячої лінії шахрайства. Усі аналізовані банки на своїх сайтах мають необхідну інформацію для свох існуючих та потенційних клієнтів щодо уникнення можливих загроз з боку шахраїв.

Таблиця 3.5

Порівняльна характеристика наявності інформації на сайтах АТ КБ "ПриватБанк", АТ "Райффайзен Банк", АТ "УКРСИББАНК", Акціонерний банк "Південний", АТ «А – БАНК» щодо дотримання інформаційної безпеки

Назва банку	АТ КБ «ПриватБанк»	АТ «Райффайзен Банк»	АТ «УКРСИББАНК»	Акціонерний банк «Південний»	АТ «А – БАНК»
Наявність документа	+	+	+	-	+
Загальні правила безпеки	-	+	+	+	+
Правила безпеки фізичних осіб	+	+	+	+	+
Правила безпеки в разі підозрілих дзвінків та смс	+	+	+	+	+
Правила безпеки при користуванні мобільними застосунками	-	+	+	+	+
Гаряча лінія шахрайства	+	+	+	-	+

Джерело: складено автором за матеріалами [69 - 73]

Отже, підвищення рівня безпеки в умовах цифровізації для населення є ключовим елементом стратегії забезпечення безпеки як окремого банку так стійкості банківської системи країни.

Враховуючи глобальний характер загроз від кіберзлочинів в області дистанційного банківського обслуговування, для підвищення ефективності інформаційної безпеки необхідно створити координуючий центр з вивчення нових способів розкрадання грошових коштів в умовах електронного банкінгу. Взаємодія у цієї галузі дозволить скоротити терміни проведення розслідувань правоохоронними органами та підвищити ефективність превентивних заходів з боку регулювальних і наглядових органів.

Результатом стане підвищення надійності та стабільності банківської системи України.

Висновки до розділу 3

За результатами розділу 3 можемо надати наступні висновки:

1. Розглянуто світові виклики одним із яких є безпека і співпраця в сучасному розрізненому світі та визначено, що за останні роки фінансовий сектор має дуже високий рівень вразливості до кіберзлочинів. Розглянутий досвід основних суттєвих подій ризику банків світу 1991 – 2017 рр, показує, що практично усі кіберризики на пряму, чи опосередковано пов'язані з недосконалістю, чи економії на інформаційній інфраструктурі, тому завданням управління кіберризиками повинно бути направлена на зниження їх виникнення та мінімізації розмірів втрат, а заходи щодо підвищення ефективності управління повинні бути спрямовані на поліпшення техніко-технологічних характеристик інформаційно-комп'ютерних систем, обладнання, програмного забезпечення та вдосконалення управління банком.

Найбільш розповсюдженими кіберзагрозами як для України, так і для зарубіжних країн є несанкціонований доступ до даних банку через злом комп'ютерних мереж банку. Найпоширенішим видом кіберзагроз є фішинг, виникнення якого відбувається через викрадення або пошкодження корпоративних і персональних даних, BEC/EAC-атаки.

2. Запропоновано про необхідність банкам на базовому рівні визначити універсальні міжнародні індикатори в забезпеченні кібербезпеки у вигляді єдиних стандартів доступу до даних, програмне забезпечення з вбудованими кодами.

3. Розглянуто досвід США в напряму впливу кібератак на фінансові установи та зазначено, що кожного року зростає вплив кіберзагроз на

програмне забезпечення, що спонукає банки ще більш оптимізувати та удосконалювати свою інформаційну інфраструктуру.

4. Надані рекомендації що використання принципів планування реагування банків України впродовж воєнних дій в країні, а тощо: удосконалення інформаційної безпеки усіх видів діяльності банку, гнучкості при виборі захистів інформаційної та забезпеченні кіберстійкості банків.

Надані пропозиції основних напрямів щодо підвищення інформаційної безпеки банків в реаліях сьогодення до яких слід віднести: удосконалення системи контролю банків, через підвищення ролі контролінгу, через формування в працівниках банків професійної досконалості щодо прийняття правильних рішень та удосконалення підвищення фінансової грамотності населення України.

ВИСНОВКИ

У кваліфікаційній роботі наведено теоретичне узагальнення, яке полягає у розгляді сутності «інформаційна безпека банку» та запропонуванні рекомендацій щодо її підвищення в умовах невизначеності (воєнного стану).

За результатами виконаної кваліфікаційної роботи можемо зробити наступні висновки:

1. Визначено теоретичний аспект щодо сутності поняття «інформаційна безпека банку», базові елементи та функції. Залежно від підходів організації інформаційної безпеки банків запропоновано розглядати наступні напрями безпеки як інформаційне поле, інформаційні ресурси, інформаційна інфраструктура, які наддадуть можливості безризикової діяльності банку.

2. Розглянуто загрози, які впливають на інформаційну безпеку банків України в умовах невизначеності та зазначено, що їх необхідно розглядати в тісному взаємозв'язку одних з другими. Інформаційна безпека банків регулюється нормативно - правовими актами, які забезпечують оперативний контроль, регулювання інформаційної безпеки та відбувається корегування тактичних та стратегічних цілей для досягнення стратегій банків.

3. За результатами оцінка діяльності АТ «А – БАНК» в українському інформаційному полі визначено, що АТ «А – БАНК» не потрапляв під інформаційні атаки з боку конкурентів, персоналу, клієнтів, на офіційному сайті банку постійно оновлюється інформація. В інформаційному середовищі відсутня негативна інформація про його діяльність.

4. Оцінювання дотримання безпеки інформаційних ресурсів діяльності АТ «А – БАНК» через обслуговування клієнтів, як з боку залучення коштів (поточні, строкові), так і в напряму кредитування показала, що АТ «А – БАНК» дотримується усіх норм безпеки інформаційних ресурсів, завдяки

чому має високу довіру з боку клієнтів, що відображається в щорічному збільшенню клієнтської бази.

5. З’ясовано, що основою для дотримання інформаційної безпеки банку первинним є захист його інформаційну (технологічну) інфраструктури. АТ «А – БАНК» контролює ефективність впроваджених заходів та засобів забезпечення інформаційної безпеки в інформаційних системах, які забезпечують їх функціонування.

6. Доведено, що міжнародний досвід підкреслює важливість комплексного підходу до інформаційної безпеки, який охоплює моніторинг, аналіз, прогнозування ризиків, розробку стратегій та заходів щодо захисту від інформаційних загроз. Це дозволяє банкам не лише реагувати на поточні виклики, а й прогнозувати майбутні загрози, адаптуючи свої системи захисту відповідно до змінюваних умов.

7. У роботі були надані рекомендації підвищення інформаційної безпеки банків України в умовах діючого воєнного стану та під впливом кіберзагроз через удосконалення системи контролю банків, через підвищення ролі фінансового контролінгу, через формування в працівниках банків професійної досконалості щодо прийняття правильних рішень та удосконалення підвищення фінансової грамотності населення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. УІМ: Україна 2030Е – країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#summary (дата звернення: 12.02.2024).

2. Кріклій О.А. Теорія та практика забезпечення кіберстійкості банків. URL: http://www.economy.nayka.com.ua/?op=1&z=8248 (дата звернення: 12.02.2024).

3. Зубок М.І. Безпека банківської діяльності. Навч. посібник. К.: КНЕУ, 2002. 190 с.

4. Арбузов С.Г., Колобов Ю.В., Міщенко В.І., Науменкова С.В. Банківська енциклопедія. Київ : Центр наукових досліджень НБУ : Знання, 2011. 504 с.

5. Коваленко В.В. Концептуальні основи формування системи безпеки банківської діяльності . Економічний часопис-XXI. 2013. № 1-2(1). С. 56-59. (дата звернення: 13.02.2024).

6. Барановський О.І. Безпека банківської сфери. *Вісник НБУ.* 2014. № 6. С. 20-27.

7. Голиков А. О., Сергєєва О. С. Удосконалення механізму фінансової стійкості банків в умовах воєнного стану. Фінанси, банківська система та страхування в Україні: стан, проблеми та перспективи розвитку в кризовій економіці: Матеріали VII Міжнародної науково-практичної Інтернет-конференції 4-5 березня 2024 р.: Дніпро : ДДАЕУ, 2024. С. 72 – 74.

8. Гіваргізов І.Г. Теоретико-методологічні засади стійкого розвитку банків. Збірник наукових праць. *Економічні науки.* 2017. № 13. С. 113–125.

9. Яременко С. М. , Забезпечення економічної безпеки діяльності банків : автореф. дис. канд. ек. наук : спец. 08.00.08 "Гроші, фінанси і кредит" / Київ, 2010. 289 с.

10. Світлична В.Ю. Забезпечення інформаційної безпеки банківських установ. Кримський економічний вісник. Науковий журнал. №1 (08) лютий 2014. Частина ІІ. Сімферополь, 2014. С.172-175.

11. Виклюк М. І. Складові безпеки банківської діяльності. *Науковий вісник НЛТУ України.* 2014. №24. С. 302–307.

12. Сергєєва О. С. Управління грошовими потоками банків : дис. канд. ек. наук : 08.00.08 / Одеса, 2015. 282 с.

13. Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121. URL: http://zakon.rada.gov.ua (дата звернення: 18.02.2024).

14. Офіційний сайт «WikiLegalAid» довідково-інформаційна платформа правових консультацій. URL: http://surl.li/avabc (дата звернення: 18.02.2024).

15. Офіційний сайт Міністерства юстиції. URL: https://minjust.gov.ua/m/vidpovidalnist-za-rozpovsyudjennya-nedostovirnoi-informatsii (дата звернення: 19.02.2024).

16. Інформаційна безпека і кібербезпека – в чому різниця? URL: https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/ (дата звернення: 01.03.2024).

17. Сучасні детермінанти управління банківськими ризиками: колективна монографія / За ред. В.В. Коваленко. Одеса, ОНЕУ, 2022. 331 с.

18. Крупка І.М. Фінансово-економічна безпека банківської системи України та перспективи розвитку національної економіки. *Бізнес Інформ.* 2012. № 6. С. 168-175.

19. Бєлоусова К.І., Бєлоус Я.І. Забезпечення інформаційної безпеки – реалізація стратегії банківської установи. *Науковий вісник ДУІКТ.* 2010. С.33-38.

20. Диба М.О. Інформаційні ризики в банківській діяльності. *Вісник НБУ.* 2007. С.28-35

21. Про організацію системи управління ризиками в банках України та банківських групах : Постанова НБУ від 11.06.2018 р. № 64. URL:

https://zakon.rada.gov.ua/laws/show/v0064500-18#Text (дата звернення: 04.03.2024).

22. Сергєєва О.С. Фінансовий контролінг в управлінні операційним ризиком в банках. *Науковий вісник Одеського національного економічного університету*. 2021, №11-12 (288-289). С. 75 – 81.

23. Примостка Л.О., Соколовська Н.С. *Економічна сутність та джерела виникнення операційного ризику в банках.* Науковий журнал. Острог: Вид-во НаУОА, грудень 2021. № 23(51). DOI: 10.25264/2311-5149-2021-23(51)-81-88.

24. Науменкова С. БАЗЕЛЬ I, II, III: Розвиток підходів для зміцнення регуляторної основи. URL: http://bulletin-econom.univ.kiev.ua/wp-content/uploads/2016/04/177_5.pdf (дата звернення: 04.03.2024).

25. Директива 2006/48/ЄС Європейського Парламенту та Ради про започаткування та здійснення діяльності кредитних установ (виправлене видання). URL: https://zakon.rada.gov.ua/laws/show/994_862 (дата звернення: 04.03.2024).

26. Sound Practices for the Management and Supervision of Operational Risk. URL: https://www.bis.org/publ/bcbs96.htm . (дата звернення: 04.03.2024).

27. Міжнародні стандарти управління ризиками. URL: https://fincontrolnew.com.ua/attachments/6d9e0ad2-134b-49ee-be78-fb6ab36b76f4_9.pdf (дата звернення: 05.03.2024).ISO/IEC 27001 – Інформаційна безпека, кібербезпека та захист конфіденційності. URL: https://cqr.company/ua/wiki/compliance/iso-iec-27001-information-security-cybersecurity-and-privacy-protection/

28. Цивільний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 06.03.2024).

29. Цивільний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 04.03.2024).

30. Стратегія розвитку фінансового сектору України. URL: https://bank.gov.ua/ua/news/all/strategiya-rozvitku-finansovogo-sektoru-ukrayini

31. Про схвалення Концепції забезпечення національної безпеки у фінансовій сфері. URL: https://zakon.rada.gov.ua/laws/show/569-2012-%D1%80#Text (дата звернення: 04.03.2024).

32. Про захист персональних даних : Закон України від 01.06.2010 р.№ 2297-VI .URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.03.2024).

33. Про інформацію : Закон України від 21.03.2023 р. № 3005-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.03.2024).

34. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 01.12.2022 р. № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 14.03.2024).

35. Про основи національної безпеки України : Закон України від 07.11.2017 р. № 2180-VIII. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 14.03.2024).

36. Про Національний банк України : Закон України № 679 від 20.05.1999 р.. URL: http://zakon.rada.gov.ua (дата звернення:14.03.2024).

37. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 17.10.2023 р. № 3419-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text (дата звернення: 14.03.2024).

38. Правила зберігання, захисту, використання та розкриття банківської таємниці : Постанова НБУ від 14.07.2006 р. № 267. URL: https://zakon.rada.gov.ua/laws/show/z0935-06#n18 (дата звернення: 14.03.2024).

39. Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова НБУ від 28.09.2017 р. № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 14.03.2024).

40. Про основні засади забезпечення кібербезпеки України : Закон України від 28.07.2022 р. № 2470-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.03.2024).

41. Про організацію кіберзахисту в банківській системі України : Постанова від 12.08.2022 р. № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (дата звернення: 15.03.2024).

42. Про затвердження Змін до Правил зберігання, захисту, використання та розкриття банківської таємниці : Постанова НБУ від 30.01.2020 р. № 13 . URL: https://zakon.rada.gov.ua/laws/show/v0013500-20#Text (дата звернення: 15.03.2024).

43. Деякі питання Національної програми інформатизації. Постанова КМ від 2 лютого 2024 р. № 119. URL: https://zakon.rada.gov.ua/laws/show/119-2024-%D0%BF#Text (дата звернення: 16.03.2024).

44. Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах : Постанова НБУ від 02.07.2019 р. № 88 . URL: https://zakon.rada.gov.ua/laws/show/v0088500-19#Text (дата звернення: 16.03.2024).

45. Про доступ до публічної інформації : Закон України від 2011 № 32. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 16.03.2024).

46. Офіційний сайт АТ «А – БАНК». URL: https://a-bank.com.ua/(дата звернення: 20.03.2024).

47. Кількість структурних підрозділів банків (у розрізі банків). URL: https://bank.gov.ua/ua/statistic/supervision-statist#5 (дата звернення: 20. 03.2024).

48. Основні показники діяльності банків України. URL: http://www.bank.gov.ua/control/uk/publish/article? art_id=36807 (дата звернення: 20.03.2024).

49. Річний консолідований звіт АТ «А - БАНК» за 2020 р. URL: https://a-bank.com.ua/about/general (дата звернення: 20.03.2024).

50. Річний консолідований звіт АТ «А - БАНК» pf 2022. URL: https://a-bank.com.ua/about/general./

51. Сергєєва О.С. Фінансова безпека банків на ринку платіжних карток України. *Науковий вісник Одеського національного економічного університету*. 2023, № 9 (310). С. 90– 97

52. Політика інформаційної безпеки АТ «А – БАНК». URL: https://a-bank.com.ua/security (дата звернення: 02.04.2024).

53. Вахнюк, С.В. Принципи фінансового стимулювання розвитку систем віддаленого банківського обслуговування. Проблеми і перспективи розвитку банківської системи України. 2004.Т.10. С. 186–191.

54. Банки можуть використовувати хмарні технології для надання послуг. URL: https://pravo.ua/banky-mozhut-vykorystovuvaty-khmarni-tekhnolohii-dlia-nadannia-posluh/ (дата звернення: 15.04.2024).

55. Радова Н.В., Плотнікова А.О. Вплив цифрової трансформації на бухгалтерський облік. *Науковий вісник Одеського національного економічного університе*т. 2023, № 11-12 (312-313). С. 141– 148.

56. Google Play Маркет. URL: https://play.google.com/store/apps?hl=uk&gl=US (дата звернення: 20.04.2024).

57. Міщенко В. Управління кібербезпекою в системі забезпечення національно укоріненої стійкості економічного розвитку. URL: DOI: https://doi.org/10.15407/etet2023.01.047 (дата звернення: 20.04.2024).

58. Кушнерьов О.С. Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки: дис. доктор філософії : 051 / Суми, 2023. 205 с.

59. Соколовська Н.С. Операційний ризик-менеджмент у банках: . дис. доктор філософії : 072 / Київ, 2022. 318 с.

60. Давосі стартував Всесвітній економічний форум. Цьогоріч його тема – «Відновлення довіри». Forbes зібрав основне з першого дня щорічної зустрічі. URL: https://forbes.ua/svit/vidnovlennya-dovirivsesvitniy-ekonomichniy-forum-u-davosi-pidsumki-pershogo-dnya-15012024-18511 (дата звернення: 22.04.2024).

61. Кількість кібератак в Україні зросла на 62% у 2023 році. URL: https://ain.ua/2024/01/12/kilkist-kiberatak-v-ukrayini-zrosla/ (дата звернення: 23.04.2024).

62. Як Україна протистоїть кібератакам на енергосистему. URL: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242 (дата звернення: 24.04.2024).

63. Петренко С. Киберустойчивость индустрии 4.0. The 2018 symposium on cybersecurity of the digital economy (CDE'18). Вторая международная научно-техническая конференция. 2018. С. 370-381.

64. Національний банк України та Міністерство фінансів США продовжать обмін досвідом у сфері кібербезпеки. URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-ukrayini-ta-ministerstvo-finansiv-ssha-prodovjat-obmin-dosvidom-u-sferi-kiberbezpeki (дата звернення: 29.04.2024).

65. Оптимізація моделей бізнесу державних банків в умовах посилення вимог до фінансової безпеки у 2022 році. URL: http://bulletin-econom.univ.kiev.ua/wp-content/uploads/2016/04/177_5.pdf (дата звернення: 29.04.2024).

66. Примостка Л.О., Соколовська Н.С. Економічна сутність та джерела виникнення операційного ризику в банках. Науковий журнал. Острог: Вид-во НаУОА, грудень 2021. № 23(51). DOI: 10.25264/2311-5149-2021-23(51)-81-88

67. Богун М. М. Управління фінансовою стійкістю банків як невід'ємною складової національної економіки України. Економіка та підприємництво. 2021. Вип. 46. С. 73–85.

68. Заходи безпеки при використанні банківських продуктів АТ КБ «ПриватБанк». URL: https://privatbank.ua/informational-security (дата звернення: 30.04.2024).

69. Заходи безпеки АТ «Райффайзен Банк». URL: https://raiffeisen.ua/data-protectionn/bezpeka-danykh (дата звернення: 30.04.2024).

70. Інформаційна безпека АТ «УКРСИББАНК». URL: https://ukrsibbank.com/about-bank/informational-security/(дата звернення: 30.04.2024).

71. Безпека обслуговування Акціонерний банк «Південний». URL: https://bank.com.ua/safety (дата звернення: 30.04.2024).

72. Правила безпеки АТ «А – БАНК». URL: https://a-bank.com.ua/security (дата звернення: 30.04.2024).

ДОДАТКИ

ДОДАТОК А

Міжнародні, національні нормативно- правові акти, які регламентують дотримання інформаційної безпеки в банках

Міжнародні нормативно- правові акти	Національні та внутрішні нормативно- правові акти
Базель 1, Базель 2, Базель 3 [24]	Цивільний кодекс України [29]
Директива 2006/48/ЄС Європейського Парламенту та Ради [25]	Цивільний процесуальний кодекс України
Документ «Комплексна практика управління та нагляду за управлінським ризиком» (Sound Practices for the Management and Supervision of Operational Risk) [26]	Кримінальний кодекс України [30]
Стандарт управління ризиками COSO ERM (Enterprise Risk Management Integrated Framework) [27]	Стратегія розвитку фінансового сектору України [31]
Стандарт ISO/IEC GUIDE 73:2002 «Управління ризиками» (Risk management); - стандарт ISO 31000:2009 «Управління ризиками [27]	Концепції забезпечення національної безпеки у фінансовій сфері [32]
Стандарт ISO 31000:2018 документ «Ризик-менеджмент – Методи ризик-менеджменту» [27]	Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [33]
Стандарт ISO 27001:2013 з інформаційної безпеки [28]	Закон України «Про інформацію» [34]
	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [35]
	Закон України «Про основи національної безпеки України» [36]
	Закон України «Про НБУ» [37]
	Закон України «Про банки та банківську діяльність» [13]

	Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [38]
	Закон України «Про основні засади забезпечення кібербезпеки» України» [41]
	Положення НБУ № 64 «Про організацію системи управління ризиками в банках України та банківських групах» [21]
	Постанова НБУ № 95 Положення «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [40]
	Положення НБУ № 178 «Про організацію кіберзахисту в банківській системі України» [42]
	Постанова НБУ№ 267 «Правила зберігання, захисту, використання та розкриття банківської таємниці» [39]
	Постанова НБУ № 98 «Про затвердження Змін до Правил зберігання, захисту, використання та розкриття банківської таємниці» [43]
	Постанова № 119 «Деякі питання Національної програми інформатизації» [44]
	Постанова НЮУ № 88 Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах

	Кодекс безпеки банку
	Політика інформаційної безпеку банку
	Корпоративний кодекс банку

ДОДАТОК Б

Карткові пропозиції АТ «А - БАНК» різних рівнів приватних карт

Назва картки	Умови оформлення	Пільговий період	Кредитний ліміт
Картка «Зелена»	Бескоштовне	До 62 днів	1000—200 000 ₴
Преміальна картка	До 20% кешбек на обрані категорії	До 62 днів	1000 - 500 000 ₴
Картка «Жовта»	Безкоштовне оформлення та облсуговування До 20% кешбек на обрані категорії	-	-
Картка «АТБ»	Бескоштовне	До 62 днів	1000—200 000 ₴
Картка «Вигода»	3,4% базова процентна ставка	До 62 днів	1000—200 000 ₴
Картка «Дитяча»	Безкоштовне оформлення, облсуговування та зарахування	-	-
Картка «єВідновлення»	Безкоштовне оформлення, облсуговування та зарахування	-	-
Картка «Українці Разом»	Бескоштовне	До 62 днів	1000—200 000 ₴
Картка «єПідтримка»	Безкоштовне оформлення, облсуговування та зарахування	-	-

ДОДАТОК В

Депозитні програми для фізичних осіб АТ «А - БАНК»

станом на 01.01. 2024 р.

Назва депозиту	Термін (місяців)	Умови вкладу	% гривня	% долар	% євро
Депозит «Online»	3	Максимальна сума поповнення в місяць за вкладами (окрім Online на 15 міс.) дорівнює стартовій сумі вкладу або сумі на дату лонгації, але не більше ніж 100 тис. грн (5 тис. дол. США / євро)	14,5		
	6		14,75		
	12		14,85		
	15		15		
Депозит «Стандарт Строковий»	1	Від 5 тис. діє ставка 2,1% в доларах США / 1,6% в євро на термін 6 міс. та 12 міс. При оформленні вкладу на 6 міс. у валюті доступна умова купівлі валюти за курсом НБУ, при цьому повернення вкладу та виплата процентів відбувається у кінці строку у національній валюті, на поточний рахунок Клієнта. Дострокове розірвання не передбачено	5	0,01	0,01
	3		14	0,01	0,01
	6		14,25	0,1	0,1
	12		14,35	0,1	0,1
Депозит «Стандарт»	3	Щомісячна виплата відсотків Можливість дострокового розірвання	9	0,01	0,01
	6		9,5	0,1	0,1
	12		10	0,1	0,1
Депозит «Скарбничка»	12	Різні способи поповнення рахунку: від надходжень на Ваші картки або витрат за ними, регулярний платіж	6	-	-
Депозит «А-Вклад»	12	Можливість знімати гроші з рахунку без комісії та зниження процентної ставки	0,1	0,01	0,01
Депозит «Рантьє»	3	*0,87 від ставки за депозитними сертифікатами НБУ на 3 міс. Без дострокового розірвання Поповнення без обмежень Мінімальна сума - 5 млн. грн.	16,53		
Вклад "До запитання"			0,01	0,01	0,01

ДОДАТОК Г

Банківські продукти для юридичних осіб

АТ «А - БАНК» станом на 01.01.2024 р.

Назва картки	Умови оформлення	Умови обслуговування	Додаткові опції
Рахунки ФОП Популярні сервіси для підприємців	Безкоштовно відкриття та обслуговування	Онлайн ваш рахунок у смартфоні	Бізнес-картка в комплекті
Рахунки ЮО Комплексне обслуговування бізнесу	Швидко відкриття рахунку за годину	Вигідно без комісії за обслуговування	Оптимально широка лінійка бізнес-послуг
Торговий еквайринг Сучасні рішення для карткових розрахунків у торгівлі та сфері послуг	Від 1.2% комісія за операції	Онлайн реєстрація торгової точки	Каса інтеграція з ПРРО
Зарплатний проєкт Зарплатні та інші виплати на картки працівників	Безкоштовно усі види виплат	Онлайн реєстрація та відкриття карток	Без комісій зняття готівки в Україні
Депозити Декілька видів депозитів з гнучкими умовами розміщення	Онлайн оформлення в клієнт-банку	UAH, USD, EUR валюта депозитів	Від одного дня строки розміщення
Приймання платежів Приймання платежів через каси банку та системи онлайн-обслуговування	Комфортні умови для ваших платників	Онлайн система обміну даними	201 відділень з якісним сервісом

Джерело: складено автором за матеріалами [1]