УДК 336.7

Чернишов Микита Олександрович
аспірант кафедри фінансів та бізнес-консалтингу
Київського національного університету технологій та дизайну
Chernyshov Mykyta
Postgraduate of the Department of Finance and Business Consulting
Kyiv National University of Technologies and Design
ORCID: 0009-0000-3825-133X

Науковий керівник:
Левченко Валентина Петрівна
доктор економічних наук, професор,
професор кафедри фінансів та бізнес-консалтингу
Київський національний університет технологій та дизайну

DOI: 10.25313/2520-2294-2024-5-9943

ОСОБЛИВОСТІ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ АКЦІОНЕРНОГО ТОВАРИСТВА «ДЕРЖАВНИЙ ОЩАДНИЙ БАНК УКРАЇНИ»

FEATURES OF THE SECURITY MANAGEMENT SYSTEM OF THE JOINT STOCK COMPANY STATE SAVINGS BANK OF UKRAINE

Анотація. *Вступ. Банківська система є однією з важливих складових сучасної ринкової економіки. Її основу складають банківські установи, які володіють певним комплексом засобів впливу на фінансову, інвестиційну, виробничу та інші сфери економіки. У контексті зростаючої відкритості економік держав та їх послідовної інтеграції у світове господарство, забезпечення безпеки банківської системи стає актуальним завданням. Це обумовлено впливом зовнішнього середовища, яке сьогодні характеризується елементами поглиблення фінансової кризи, а також внутрішнього середовища, зокрема посиленням конкуренції та консолідації банківського бізнесу. Вплив внутрішнього середовища передбачає виникнення загроз, які ускладнюють процес реалізації стратегічних напрямків розвитку банків з точки зору прибутковості та мінімізації ризиків. Тому проблема забезпечення безпеки банківської діяльності є досить актуальною і повинна розглядатися як системоутворюючий елемент фінансової стійкості банківської системи.*

Мета. Метою дослідження є аналіз особливостей системи управління безпекою банку АТ «Ощадбанк» з метою визначення її відповідності вимогам нормативно-правової бази України, оцінки стану та ефективності функціонування, розробки рекомендацій щодо її вдосконалення.

Матеріали і методи. У ході дослідження використовувалися наступні джерела і методи: 1) офіційні документи та нормативно-правові акти, що регулюють безпеку банківської діяльності; 2) наукові праці вітчизняних та зарубіжних авторів, що стосуються інформаційної, фінансової, фізичної та кібербезпеки банків.

У процесі дослідження використано наступні наукові методи: теоретичне узагальнення та групування (для опису складових безпеки банку, включаючи фізичну, фінансову, інформаційну та кібербезпеку); формалізація, аналіз і синтез (для вивчення фінансових особливостей діяльності АТ «Ощадбанк»); логічне узагальнення отриманих результатів (формулювання висновків).

Результати. У статті досліджено особливості системи управління безпекою акціонерного товариства «Державний ощадний банк України» (АТ «Ощадбанк»). Здійснено аналіз нормативно-правової бази України, яка регулює питання безпеки банків, а також оцінку стану та ефективності функціонування системи управління безпекою АТ «Ощадбанк».

Основні теми, що розглядаються в статті, включають роль управління безпекою в забезпеченні фінансової стійкості банку, ідентифікацію та аналіз потенційних загроз, методи виявлення та мінімізації ризиків, а також ефективність заходів безпеки в контексті досягнення стратегічних цілей банку.

Дослідження показало, що система управління безпекою АТ «Ощадбанк» відповідає вимогам нормативно-правової бази України. Банк приділяє особливу увагу захисту критичної інформаційної інфраструктури, до якої відносяться інформаційні системи, що забезпечують основні операційні процеси банку. Банк активно впроваджує передові технології інформаційної безпеки, такі як хмарне зберігання даних, штучний інтелект та машинне навчання.

Стаття є актуальним доповненням до розуміння проблем безпеки в банківському секторі та може бути корисною для фахівців у галузі фінансів, а також для управлінців та регуляторів, які вивчають і вдосконалюють практики управління безпекою в банківській сфері.

Перспективи. Перспективи дослідження включають ряд напрямків, які можуть бути досліджені та розвинуті для збільшення розуміння та ефективності управління безпекою в банку. Оскільки кіберзагрози стають все більш серйозним викликом для банків, наступні дослідження будуть спрямовуватися на аналіз сучасних тенденцій кібербезпеки та розробку стратегій захисту від кібератак, що будуть вивчати роль новітніх технологій, таких як штучний інтелект, блокчейн тощо, у забезпеченні безпеки банківських операцій та захисті інформації. Також у подальших дослідженнях розглядатимуться ефективні методи підвищення свідомості персоналу банку щодо безпеки та навчання їх діяти в умовах загроз.

Ключові слова: *банк, фінансова безпека, аналіз, система управління безпекою, інформаційна безпека, кібербезпека, цифровізація, технології, стратегії, ліквідність.*

Summary. *Introduction. The banking system is one of the important components of the modern market economy. Its basis consists of banking institutions that possess a certain set of means of influencing the financial, investment, production and other spheres of the economy. In the context of the growing openness of the economies of states and their consistent integration into the world economy, ensuring the security of the banking system is becoming an urgent task. This is due to the influence of the external environment, which today is characterized by elements of the deepening of the financial crisis, as well as the internal environment, in particular, the strengthening of competition and consolidation of the banking business. The influence of the internal environment implies the emergence of threats that complicate the process of implementing the strategic directions development of the banks from the point of view of profitability and risk minimization. Therefore, the problem of ensuring the security of banking activity is quite urgent and should be considered as a system-forming element of the financial stability of the banking system.*

Purpose. The purpose of the study is analyze the features of the security management system of the bank JSC "Oschadbank" in order to determine its compliance with the requirements of the regulatory and legal framework of Ukraine, assess the state and effectiveness of its functioning, and develop recommendations for improvement.

Materials and methods. During the research, the following sources and methods were used: 1) official documents and legal acts regulating the security of banking activity; 2) scientific works of domestic and foreign authors related to information, financial, physical and cyber security of banks.

The following scientific methods were used in the research process: theoretical generalization and grouping (to describe the components of bank security, including physical, financial, information and cyber security); formalization, analysis and synthesis (for the study of financial features of JSC "Oschadbank"); logical generalization of the obtained results (formulation of conclusions).

Results. The article examines the features of the security management system of the Joint Stock Company State Savings Bank of Ukraine (JSC "Oschadbank"). An analysis of the legal framework of Ukraine, which regulates the issue of bank security, was carried out, as well as an assessment of the state and effectiveness of the security management system of JSC "Oschadbank".

The main topics discussed in the article include the role of security management in ensuring the financial stability of the bank, identification and analysis of potential threats, methods of identifying and minimizing risks, as well as the effectiveness of security measures in the context of achieving the bank's strategic goals.

The study showed that the security management system of JSC "Oschadbank" meets the requirements of the regulatory and legal framework of Ukraine. The bank pays special attention to the protection of critical information infrastructure, which includes information systems that support the bank's main operational processes. The bank actively implements advanced information security technologies, such as cloud data storage, artificial intelligence and machine learning.

The article is a timely addition to the understanding of security issues in the banking sector and can be useful for financial professionals, as well as for managers and regulators who study and improve security management practices in the banking sector.

Discussion. Research perspectives include a number of areas that can be explored and developed to increase the understanding and effectiveness of bank security management. As cyber threats become an increasingly serious challenge for banks, the focus will be on the analysis of current cyber security trends and the development of strategies to protect against cyber attacks, exploring the role of the latest technologies such as artificial intelligence and blockchain in ensuring the security of banking operations and protecting information. Further studies will also consider effective methods of raising the awareness of bank personnel regarding security and training them to act in the face of threats.

Key words: *bank, financial security, analysis, security management system, information security, cyber security, digitalization, technologies, strategies, liquidity.*

Постановка проблеми. Банки є важливими фінансовими установами, які зберігають та обробляють великі обсяги грошових коштів та цінної інформації. Управління безпекою в банку стає все

більш важливим аспектом в умовах зростаючих загроз та складних викликів, з якими стикаються фінансові установи сьогодні. Необхідність впровадження системи управління безпекою банку є визнаною не лише з погляду захисту фінансових активів та конфіденційної інформації, але і як стратегічна необхідність для збереження довіри клієнтів, стійкості фінансової системи та забезпечення ефективності банківської діяльності.

Аналіз останніх досліджень і публікацій. Сутність поняття «безпека» в контексті управління банками розглядало багато науковців. У контексті діяльності публічних або приватних організацій поняття «безпека» в наш час може тлумачитися двома способами: як стан або сприйняття, і як процес зменшення ризиків і захисту або створення стійкості в умовах можливих загрозливих сценаріїв [1, с. 157–174]. Безпеку, що тлумачиться як стан або сприйняття, можна тлумачити в залежності від різних «ситуаційних факторів» і, зокрема для осіб, між різними місцями та часом доби, також враховуючи, що такі сприйняття можуть бути відкориговані прийняттям заходів ситуативного запобігання злочинності [2, с. 9–20; 3, с. 93–104] або ступенем знайомства з ризиком [4, p. 142]. На рівні організації, ради директорів великих компаній звертають увагу на ризики безпеки, оскільки вони також сприймаються як причина розриву в міжнародному бізнесі [5, с. 237–244; 6, с. 79–97; 7, с. 425–442]; тоді як в залежності від області функціонування, сприйняття може відрізнятися всередині самої організації [8].

Розуміння безпеки як процесу (на додаток до регулярного управління операційними ризиками, які спеціально породжуються людьми в організаціях), активно співпрацює у зборі та аналізі розвідувальної інформації, отриманої вищим керівництвом для стратегічного прийняття рішень [9], а також у комплексному кризовому управлінні [4, с. 142] під час стикання з серйозними руйнівними подіями (глобальними пандеміями, природними лихами, масштабними кібератаками тощо).

Щодо вітчизняних науковців, то можна навести думку автора Кришталь Г., який у своїй роботі пропонує власне розуміння поняття «фінансова безпека банківської системи в умовах цифровізації та воєнного стану в країні», яке враховує процеси цифровізації у фінансовій сфері. Це означає, що визначення даного поняття не тільки враховує традиційні аспекти безпеки, але й розглядає нові вимоги та можливості, що виникають зі зростанням використання сучасних технологій [10, с. 39–47]. Дослідження Москвіна Б. [11] та Коробцової Д. [12] аналізують проблеми фінансової безпеки банківської системи в найважливіший період для України — в період воєнного стану. Роботи вчених, таких як Мушенюк І. [13], Бондаренко А. [14], Варналій З. та Мехед А. [15], зосереджують увагу на аспектах цієї трансформації та розробляють наукові підходи до забезпечення фінансової стійкості банків у цифровому середовищі.

Забезпечення безпеки у банківській сфері стикається з низкою невирішених питань, які потребують ретельної уваги та подальших досліджень для гарантування ефективного функціонування фінансових установ. Насамперед стрімкий розвиток технологій та зростання кіберзлочинності створюють нові загрози для кібербезпеки банківських систем. Недостатній захист від кібератак може призвести до значних фінансових втрат та підірвати довіру клієнтів. Крім того, внутрішнє шахрайство та корупція в банках залишаються серйозними проблемами, оскільки відсутність ефективної системи контролю та нагляду може спричинити внутрішні збитки та порушення етичних норм. Нарешті, мінливе середовище ставить під загрозу фінансову стабільність банків, що може призвести до втрати довіри клієнтів та, в кінцевому підсумку, банкрутства установи.

Метою статті є аналіз особливостей системи управління безпекою банку АТ «Ощадбанк» з метою визначення її відповідності вимогам нормативно-правової бази України, оцінки стану та ефективності функціонування, розробки рекомендацій щодо вдосконалення..

Матеріали і методи. У ході дослідження використовувалися наступні джерела і методи: 1) офіційні документи та нормативно-правові акти, що регулюють безпеку банківської діяльності; 2) наукові праці вітчизняних та зарубіжних авторів, що стосуються інформаційної, фінансової, фізичної та кібербезпеки банків.

У процесі дослідження використано наступні наукові методи: теоретичне узагальнення та групування (для опису складових безпеки банку, включаючи фізичну, фінансову, інформаційну та кібербезпеку); формалізація, аналіз і синтез (для вивчення фінансових особливостей діяльності АТ «Ощадбанк»); логічне узагальнення отриманих результатів (формулювання висновків).

Виклад основного матеріалу. Безпеку банків можна описати як складне комплексне утворення, яке включає декілька складових (рис. 1).

Всі складові безпеки банків тісно пов'язані між собою. Наприклад, фізична безпека забезпечує захист інформаційних систем банку, які є частиною його інформаційної інфраструктури. А організаційна безпека визначає правила і процедури, які повинні дотримуватися співробітники банку, в тому числі в частині інформаційної безпеки.

Розглянемо складові безпеки для АТ «Ощадбанк». АТ «Ощадбанк» — найбільший державний банк України, заснований у 1999 році. Він є універсальним банком, який пропонує широкий спектр фінансових послуг для фізичних осіб, малого та середнього бізнесу (МСБ), а також

корпоративних клієнтів. Провівши аналіз кількості підрозділів банку (див. рис. 2), можна помітити, що їх кількість постійно зменшується. Це стало результатом двох чинників: по-перше, значна частина відділень АТ «Ощадбанк» залишилась на тимчасово окупованих територіях України та в Криму, а по-друге, керівництво банку оптимізує свою мережу та закриває нерентабельні відділення.

Розглянемо структуру активів та пасивів банку на рис. 3–4.

Щоб прокоментувати, зміни у структурі активів банку, наведемо таблицю 1 з даними до рисунку 3.

Загальна сума активів банку зростала протягом досліджуваного періоду. У 2021 році вона незначно збільшилася порівняно з 2020 роком (на 1,17 млрд. грн або 0,5%), а у 2022 році спостерігалося більш суттєве зростання — на 35,35 млрд. грн (14,9%) порівняно з 2021 роком. Кредити юридичним особам демонстрували стабільне зростання: з 54,31 млрд. грн у 2020 році до 71,74 млрд. грн у 2022 році, що свідчить про розширення кредитування корпоративного сектору. Динаміка кредитів фізичним особам була нестабільною: у 2021 році спостерігалося різке зростання на 52,8% порівняно з 2020 роком, але у 2022 році обсяг кредитів фізичним особам знизився на 15,8% порівняно з 2021 роком. Грошові кошти та їх еквіваленти зменшилися у 2021 році на 19,4% порівняно з 2020 роком, але у 2022 році знову зросли на 32,3% порівняно з 2021 роком, що може свідчити

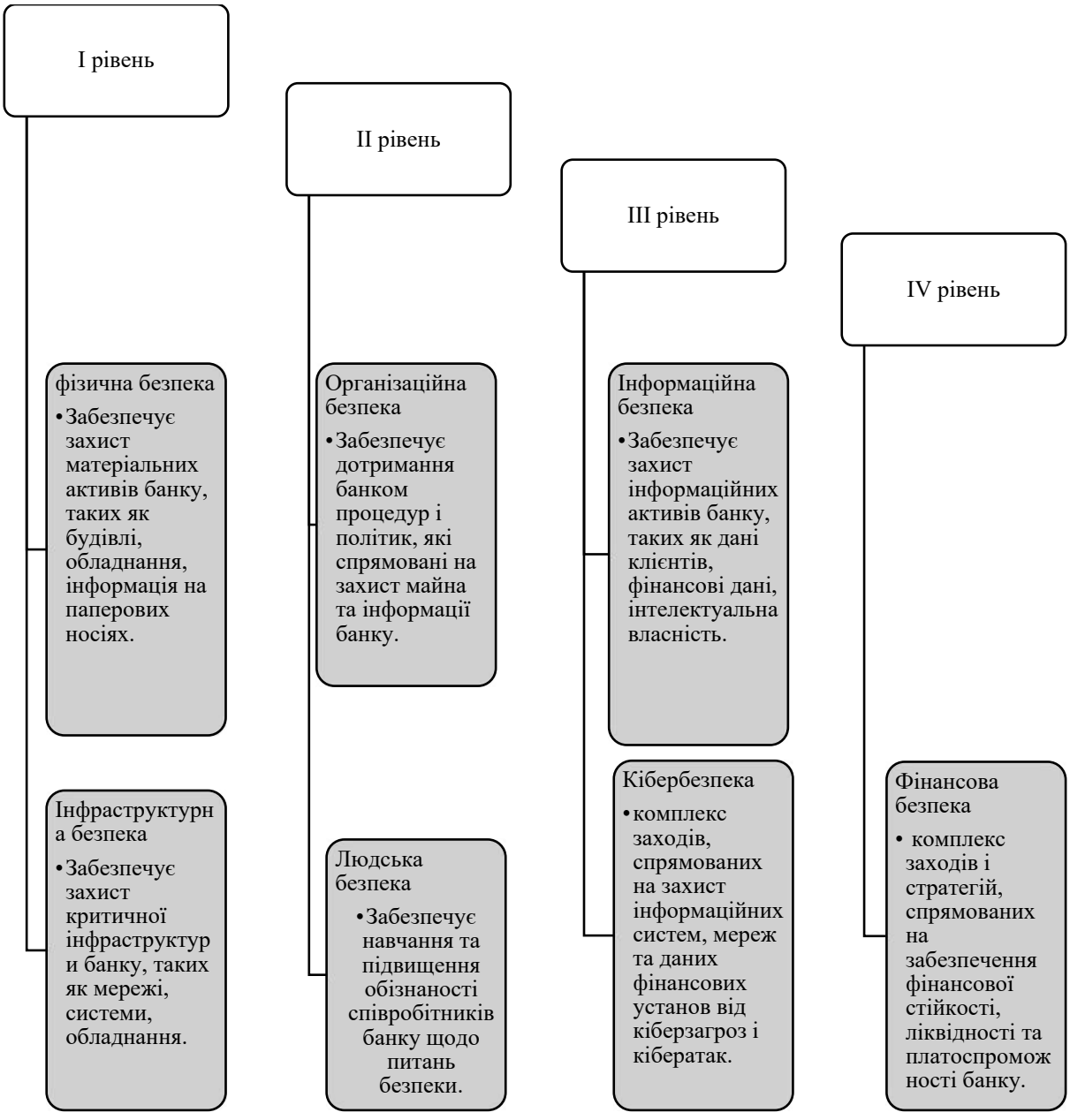

Рис. **1.** Склад банківської безпеки як комплексного утворення

Джерело: розроблено автором

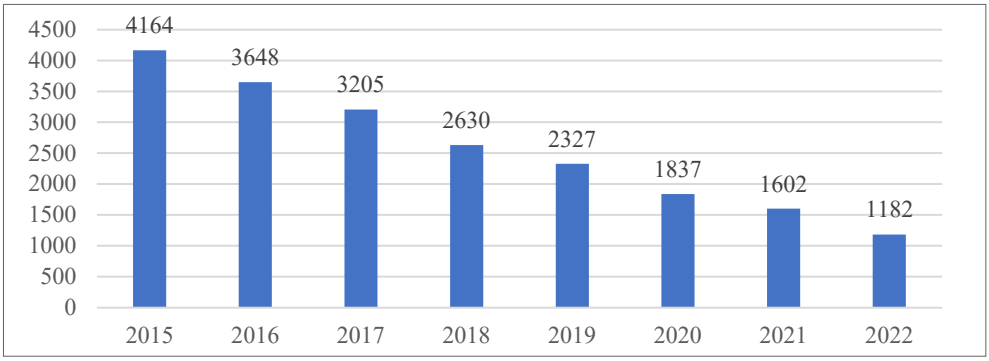

Рис. 2. Кількість підрозділів банку станом на кінець року
Джерело: розроблено автором на основі [16]

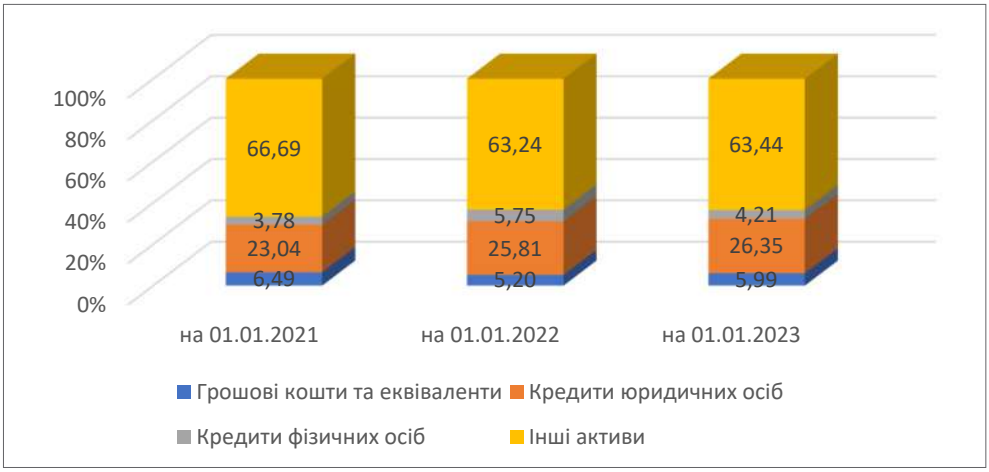

Рис. 3. Структура активів банку станом на кінець року
Джерело: розроблено автором на основі [16]

про нерівномірне управління ліквідністю банку. Загалом, дані свідчать про зростання активів банку, особливо за рахунок кредитування юридичних осіб, проте спостерігалася нестабільність у динаміці деяких активів, що може бути викликано різними факторами, включаючи економічну ситуацію та стратегію управління активами банку.

В структурі активів банку найбільшу частину займають кредити юридичним особам. Кредити юридичних осіб та фізичних осіб показали різні тенденції: кредити юридичних осіб постійно збільшувалися в структурі активів, тоді як кредити фізичних осіб спочатку зростали, а потім скоротилися. Загальна сума активів також зросла з часом.

Якщо розглядати пасиви АТ «Ощадбанк» (рис. 4), то в структурі пасивів кошти банків та депозити юридичних осіб зменшилися у період від 01.01.2021 до 01.01.2023 року відповідно з 1,92% до 0,98% та з 24,9% до 22,93%. Тоді як депозити фізичних осіб значно збільшилися з 53,29% до 61,25% з 01.01.2021 по 01.01.2023 року. Загальні зобов'язання збільшилися з часом. Власний капітал в структурі пасисів декілька зменшився, а саме з 9,33% на 01.01.2021 до 8,16% на 01.01.2023 року.

Розглянемо нормативи АТ «Ощадбанк» в порівнянні з нормативами за банківською системою в цілому (табл. 2).

Таблиця 1

Динаміка активів АТ «Ощадбанк» за 2020–2022 роки, *тис грн*

	2020	2021	2022
Грошові кошти та еквіваленти	15 294 209	12 326 181	16 303 348
Кредити юридичних осіб	54 311 100	61 133 592	71 740 948
Кредити фізичних осіб	8 914 977	13 620 493	11 474 646
Інші активи	157 195 552	149 807 436	172 719 852
Активи	235 715 838	236 887 702	272 238 794

Джерело: розроблено автором на основі [16; 17]

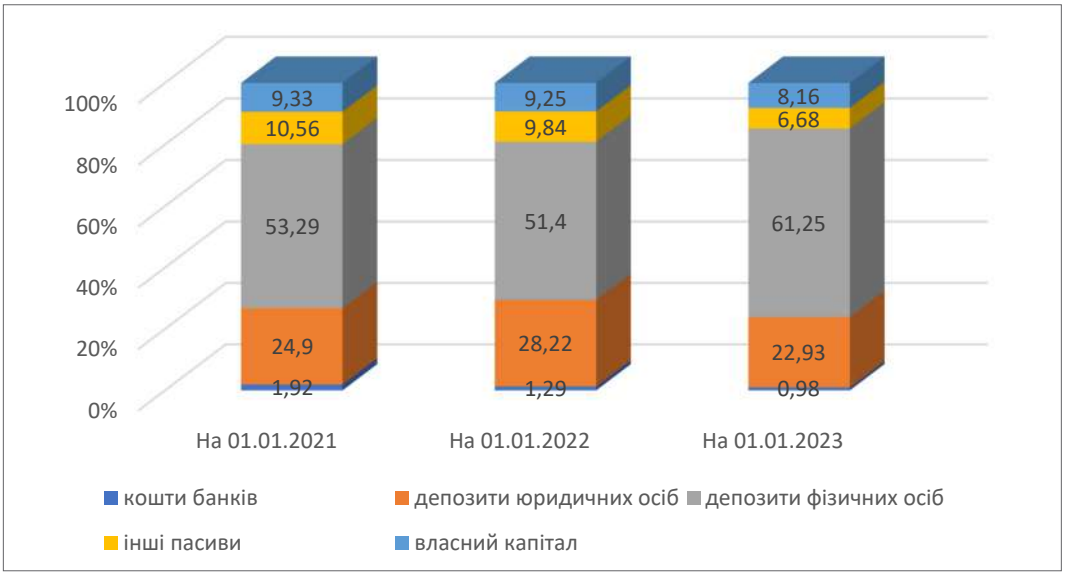

Рис. 4. Структура пасивів банку станом на кінець року
Джерело: розроблено автором на основі [16]

За даними таблиці 2, АТ «Ощадбанк» у 2023 році відповідав усім нормативам достатності капіталу, встановленим Національним банком України. Норматив достатності (адекватності) регулятивного капіталу (Н2) становив 16,57%, що перевищує встановлений норматив у 10%. Норматив достатності основного капіталу (Н3) становив 8,3%, що також перевищує встановлений норматив у 7%.

Однак, у порівнянні з банківською системою в цілому, АТ «Ощадбанк» має нижчі значення нормативів Н2 та Н3. Норматив Н2 у АТ «Ощадбанк» у 2023 році становив 16,57%, тоді як у банківській системі в цілому — 21,07%. Норматив Н3 у АТ «Ощадбанк» у 2023 році становив 8,3%, тоді як у банківській системі в цілому — 12,24%.

Незважаючи на зниження значень нормативів Н2 та Н3, АТ «Ощадбанк» у 2023 році відповідав усім нормативам достатності капіталу, встановленим Національним банком України. Це свідчить про те, що банк має достатній рівень капіталу для покриття своїх ризиків.

У дослідженні ми зупинимося на такому прийомі оцінки фінансової безпеки банку як інтегральному методі, який дає можливість представити фінансову безпеку банку як єдину кількісну узагальнену характеристику. При розрахунку інтегрального показника зазвичай використовується

Таблиця 2

Нормативи АТ «Ощадбанк» в порівнянні з нормативами за банківською системою в цілому

Показник	Норматив	2021		2022		2023	
		банк	В цілому за системою	банк	В цілому за системою	банк	В цілому за системою
Норматив достатності (адекватності) регулятивного капіталу (Н2)	>10%	15,48	18,01	14,48	19,68	16,57	21,07
Норматив достатності основного капіталу (Н3)	>7%	11,83	11,99	10,52	13,12	8,3	12,24
Норматив максимального розміру кредитного ризику на одного контрагента (Н7)	<25%	27,46	18,60	9,79	17,80	7,44	15,53
Норматив великих кредитних ризиків (Н8)	<800%	102,37	72,35	80,07	86,33	54,91	63,13
Норматив максимального розміру кредитного ризику за операціями з пов'язаними з банком особами (Н9)	не вище 5%	0,36	3,71	0,26	2,81	0,08	1,08

Джерело: розроблено автором на основі [16; 17]

ряд базових показників. Істотним недоліком даної методики є те, що вагові коефіцієнти, що враховуються при розрахунку інтегрального показника, визначаються експертним шляхом, що може суттєво впливати на результати оцінки.

Методика розрахунку, згідно з індикаторним підходом, складається з декількох етапів.

Перший етап включає вибір показників, що характеризують фінансову безпеку банку. На нашу думку, всі показники слід розділити на дві групи.

У першу групу входять показники, які характеризують зміну основних показників діяльності банківської установи порівняно зі зміною цих показників загалом за банківською системою України.

До таких показників відносяться:
– рентабельність власного капіталу;
– рентабельність активів.

Значення банківської системи України виступають як нормативи для цієї групи показників.

До другої групи входять обов'язкові нормативи для кредитних організацій, встановлені НБУ. Вони включають такі показники:
– норматив достатності (адекватності) регулятивного капіталу (Н2);
– норматив достатності основного капіталу (Н3);
– норматив максимального розміру кредитного ризику на одного контрагента (Н7);
– норматив великих кредитних ризиків (Н8);
– норматив максимального розміру кредитного ризику за операціями з пов'язаними з банком особами (Н9).

На другому етапі для кожного показника необхідно встановити нормативне значення.

Третій етап передбачає обчислення щодо відхилення фактичного показника від нормативного. Для цього використовуються наступні формули:

якщо напрям оптимізації показника прагне збільшення:

$$x_i = \frac{a_i}{a_i^n} \quad (1)$$

якщо напрям оптимізації показника прагне зменшення:

$$x_i = \frac{a_i^n}{a_i} \quad (2)$$

де a_i — фактичне значення показника; $a^n{}_i$ — нормативне значення цього показника.

На четвертому етапі розраховують інтегральний показник фінансової безпеки, для чого можна використати таку формулу:

$$R_{ФБ} = (x_1 + x_2 + x_3 + ... + x_n) / n \quad (3)$$

Кожен індикатор (x_1, x_2, x_3, ..., x_n) представляє певний аспект фінансової безпеки, такий як ліквідність, прибутковість, кредитний ризик, ринковий ризик тощо. Розрахунок інтегрального показника дозволяє отримати узагальнену оцінку рівня фінансової безпеки шляхом комбінування та зважування різних індикаторів.

Для оцінки фінансової безпеки інтегральний показник необхідно порівняти з нормативним, який дорівнює 1. Це пояснюється тим, що отриману суму значень показників ми ділимо на їхню кількість.

При цьому рівень фінансової безпеки, розрахований за формулою (3), посилюватиметься зі збільшенням інтегрального показника (1 — нормативне значення рівня фінансової безпеки для кредитної організації).

Розрахуємо інтегральний показник фінансової безпеки АТ «Ощадбанк» (табл. 3, 4).

У 2021–2022 роках АТ «Ощадбанк» демонстрував нижчі показники рентабельності власного капіталу (ROE) та рентабельності активів (ROA) порівняно із середніми значеннями за банківською системою. У 2023 році ситуація значно покращилася — банк досяг високих показників ROE та ROA, істотно перевищивши середні значення по системі. Зростання рентабельності у 2023 році може бути пов'язане з ефективними заходами керівництва банку щодо підвищення прибутковості діяльності, оптимізації витрат, покращення управління активами та капіталом.

Нами обрано 5 показників: рентабельність власного капіталу (ROE), рентабельність активів (ROA), норматив достатності (адекватності) регулятивного капіталу (Н2), норматив достатності основного капіталу (Н3), норматив максимального розміру кредитного ризику на одного контрагента (Н7)

$R_{ФБ\ 2021}$ = (0,718 + 0,492 + 1,548 + 1,690 + + 0,910)/5 = 5,358/5 = 1,072;

Таблиця 3

Розрахунок фінансових показників АТ «Ощадбанк» (1 група)

Показник	2021		2022		2023		x_i		
	банк	В цілому за системою	банк	В цілому за системою	банк	В цілому за системою	2021	2022	2023
Рентабельність власного капіталу (ROE)	13,8	19,22	5,1	9,68	35,08	9,68	0,718	0,527	3,624
Рентабельність активів (ROA)	1,2	2,44	0,5	1,04	4,09	1,04	0,492	0,481	3,933

Джерело: розроблено автором на основі [16; 17]

Таблиця 4

Розрахунок фінансових показників АТ «Ощадбанк» (2 група)

Показник	Норматив	Показники			x_i		
		2021	2022	2023	2021	2022	2023
Норматив достатності (адекватності) регулятивного капіталу (Н2)	10	15,48	14,48	16,57	1,548	1,448	**1,657**
Норматив достатності основного капіталу (Н3)	7	11,83	10,52	8,3	1,690	1,503	**1,186**
Норматив максимального розміру кредитного ризику на одного контрагента (Н7)	25	27,46	9,79	7,44	0,910	2,554	**3,360**
Норматив великих кредитних ризиків (Н8)	800	102,37	80,07	54,91	7,815	9,991	**14,569**
Норматив максимального розміру кредитного ризику за операціями з пов'язаними з банком особами (Н9)	5	0,36	0,26	0,08	13,889	19,231	**62,500**

Джерело: розроблено автором на основі [16; 17]

$R_{ФБ\ 2022} = (0,527 + 0,481 + 1,448 + 1,503 + 2,554)/5 = 6,513/5 = 1,303;$

$R_{ФБ\ 2023} = (3,624 + 3,933 + 1,657 + 1,186 + 3,360)/5 = 13,760/5 = 2,752.$

Отже, АТ «Ощадбанк» показав за інтегральним показником фінансової безпеки значення вище 1, що свідчить про фінансову безпеку банку. Крім того, деякі нормативні показники АТ «Ощадбанк» значно вище за показники банківської системи у цілому.

Розглянемо управління ліквідністю АТ «Ощадбанк». Для більш ефективного контролю над ризиком ліквідності в умовах кризи у Банку розроблено «Положення про роботу АТ «Ощадбанк» при виникненні кризи ліквідності банку в разі непередбачених обставин». Цей документ встановлює процедури прийняття рішень та дій Банку в разі непередбачених обставин, включаючи План дій у разі кризи ліквідності.

У ефективній системі кризового управління ліквідністю банку ключову роль відіграє планування заходів з попередження та подолання кризи ліквідності. Результатом такого планування є створення Плану заходів з антикризового управління ліквідністю (ПАУЛ). Цей план відрізняється від Плану дій у разі кризи ліквідності тим, що ПАУЛ спрямований на попередження кризи ліквідності до її початку. План є внутрішнім документом, який регулює діяльність банку при перших ознаках кризи ліквідності або її швидкому розгортанні. Він забезпечує алгоритмізацію заходів з попередження, подолання кризи та зменшення її наслідків.

Метою розробки ПАУЛ є визначення стратегії, процедур і заходів з управління ліквідністю, виконання яких забезпечує оперативну адаптацію банку до різких змін умов діяльності і пом'якшення або попередження негативних наслідків кризи. Антикризова стратегія формується на основі результатів ранньої діагностики кризи та стрес-тестування і визначає загальний напрямок діяльності банку на період управління ліквідністю в кризових умовах.

Основним документом, що регулює процес управління ліквідністю в Банку, є Положення про управління ризиком ліквідності АТ «Ощадбанк».

Положення визначає наступні принципи управління ліквідністю в банку (Рис. 5).

Моніторинг і контроль за виконанням нормативних вимог до рівня ліквідності здійснює Управління ринкових ризиків (УРР). Управлінські рішення щодо коригування структури активів та пасивів з метою запобігання порушення нормативів ліквідності НБУ приймаються Комітетом управління активами та пасивами (КУАП) на основі звітів про виконання нормативів НБУ та рекомендацій, наданих Департаментом економіки та планування (ДЕП), Казначейством та Управлінням ринкових ризиків (УРР).

Крім того, в банку встановлюються внутрішні вимоги до рівня ліквідності, спрямовані на мінімізацію ймовірності дефіциту ліквідності або порушення нормативних вимог до управління ліквідністю. КУАП встановлює внутрішні ліміти ризику ліквідності та переглядає їх не рідше одного разу на рік на основі рекомендацій УРР. Моніторинг і контроль виконання внутрішніх вимог банку до рівня ризику ліквідності здійснює Управління ринкових ризиків.

Процес управління ліквідністю банку складається з двох етапів: управління короткостроковою ліквідністю та управління середньо- та довгостроковою ліквідністю.

Управління короткостроковою ліквідністю в Банку здійснюють Комітет управління активами та пасивами (КУАП) та Казначейство, яке має виключні повноваження щодо проведення операцій на міжбанківському ринку. Казначейство керує ресурсною позицією на підставі даних, що протягом дня подаються структурними підрозділами. Ефективність управління ризиком ліквідності в цілому оцінюється за допомогою звітності, яка представляється на вимогу КУАП та Управління ринкових ризиків (УРР) [16].

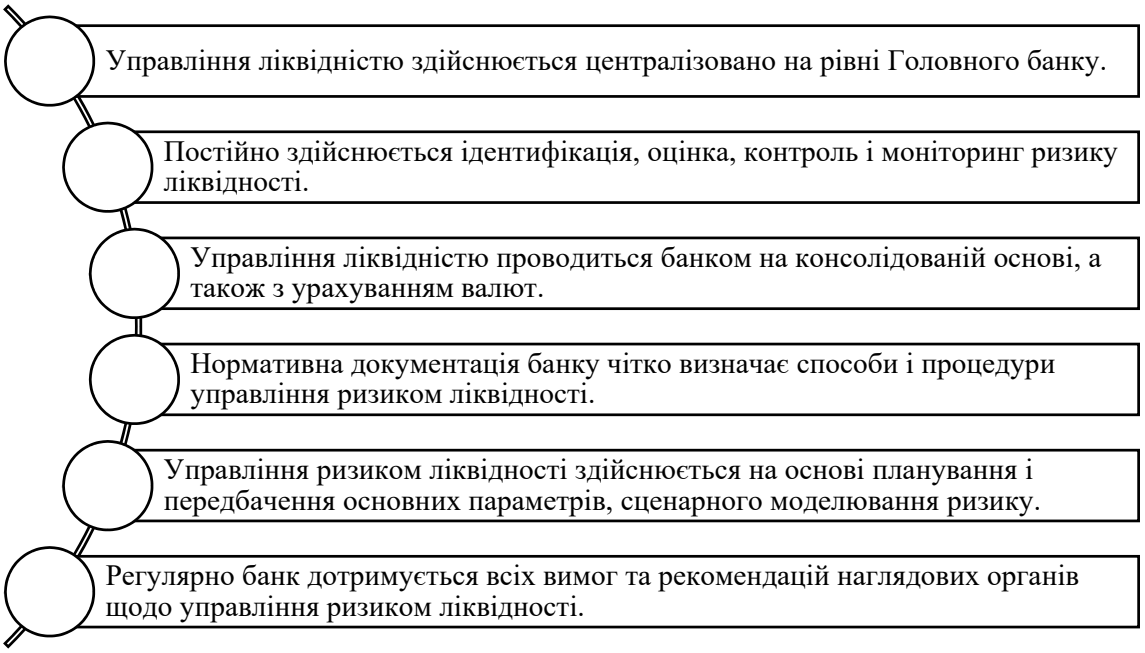

Рис. 5. Принципи управління ліквідністю в банку
Джерело: розроблено автором

Управління середньо- та довгостроковою ліквідністю виконують КУАП, Департамент економіки та планування (ДЕП) та Управління ринкових ризиків. УРР щоденно аналізує ризик ліквідності за допомогою GAP-аналізу. Щоденно ДЕП складає звіти щодо структури балансу, основних показників аналітичного балансу Банку та надає їх УРР та Правлінню Банку за потреби. УРР щоденно аналізує звіт форми № 631 «Про структуру активів та пасивів за строками до погашення» на предмет дотримання балансу активів та пасивів за строками погашення в гривні, іноземній валюті та загальному гривневому еквіваленті.

Щомісяця Управління ринкових ризиків подає на засідання КУАП звіт щодо виконання нормативів та лімітів ризику ліквідності, а також інформацію про фактичні значення, динаміку та прогноз розривів ліквідності та рекомендації щодо усунення дисбалансу ресурсів.

Кожен місяць УРР проводить аналіз умовно постійних залишків на поточних та строкових рахунках клієнтів (період оцінки — 1 рік), виявляє сезонність та циклічність фінансових потоків на основі структурного аналізу клієнтських груп.

Довгострокове планування ліквідності здійснює ДЕП. Управління довгостроковою ліквідністю структурних підрозділів здійснюється на основі рішень КУАП через встановлення лімітів на структуру вкладень та керуванням ціною залучення ресурсів певного строку та валюти.

У разі виникнення кризи ліквідності розробляється План дій та плануються конкретні антикризові заходи. Такі заходи можуть включати: введення режиму антикризового управління; інвентаризацію активів, пасивів, позабалансових зобов'язань та витрат Банку; прийняття рішення щодо залучення міжбанківських ресурсів за ставками вище ринкових; підвищення ставок з клієнтських депозитів; реалізація ліквідних активів; переговори з Національним банком України щодо можливості рефінансування Банку для підтримки поточної ліквідності та платоспроможності у період кризи ліквідності; звернення до Національного банку України для отримання стабілізаційного кредиту; визначення джерела підтримки Банку готівкою для безперервної роботи операційної каси; забезпечення жорсткого контролю за виконанням договірних умов за активними операціями; роботу по досягненню угод з клієнтами стосовно призупинення раніше відкритих кредитних ліній; досягнення угод зі стратегічними клієнтами Банку щодо продовження строку дії діючих депозитних угод з метою їх переоформлення з короткострокових на довгострокові; проведення заходів відносно реструктуризації вимог з метою скорочення суми платежів.

Розглянемо управління безпекою АТ «Ощадбанк» в умовах зовнішнього середовища. На кінець 2022 року найбільшим ризиком для стабільної роботи банківської системи вважалися масштабні ракетні удари по енергетичній інфраструктурі України, які завдали російські війська, та загроза відключення електроенергії, оскільки це могло шкодити банківській системі з кількох причин.

По-перше, це призвело б до паралічу роботи відділень, знизило б потік коштів за розрахунками картками та безготівковими переказами, і спонукало б до додаткових витрат на генератори для доступу до Інтернету.

По-друге, через можливі перебої з електропостачанням можливий ризик збільшення неплатоспроможності позичальників та невиплат за кредитами.

Оскільки Україні вдалося уникнути тривалого відключення електроенергії, песимістичні передбачення щодо банківської системи не підтвердилися. Кошти юридичних осіб у банках зросли завдяки адаптації бізнесу до умов війни. За підсумками 2022 року загальний заробіток всіх банків склав 24,7 млрд. грн, що приблизно в три рази менше, ніж у 2021 році. Кількість оперативно неприбуткових установ скоротилась майже до рівня 2021 року після значного зростання на початку агресії. Два ключових джерела доходів банків — чисті відсоткові доходи та чисті комісійні доходи — зростають.

На тлі військової агресії в Україні та падіння доходів населення актуальною проблемою є фізична безпека АТ «Ощадбанк».

Ризик фізичної небезпеки може змінюватися відповідно до ширшого соціального контексту. Сьогодні наростає напруга. Спостерігається ескалація проблем глобальної економіки, зростання інфляції, збільшення витрат домогосподарств і політичні та соціальні розбіжності. Деякі люди стурбовані за майбутнє своєї роботи. Це збільшує спокуси людей; у деяких може з'явитися бажання вчинити незаконні дії через складні життєві обставини, в яких вони опинилися. Фахівці з банківської безпеки повинні бути готові до різних інцидентів, спрямованих на їхні установи, від пограбувань у відділенні банку до дій політичних активістів, спрямованих на фінансові установи, в які вони інвестують свої кошти.

Посилення банківської безпеки в умовах загроз потребує комплексного використання всіх засобів та методів для її захисту.

Технології грають ключову роль, від відеокамер з безперешкодним оглядом до сучасних систем керування інцидентами та аналітичних інструментів. Також враховується необхідність вдосконалення процесів навчання, щоб кожен співробітник знав, як діяти в разі інциденту. Згідно з даними Асоціації американських банкірів (ABA), страх перед провалом, арештом або цими чинниками одночасно, перш за все зупиняє людей від грабежу фінансових установ. Ці стримуючі фактори можуть ефективно застосовуватись проти більшості потенційних злочинців [18].

ABA рекомендує комплексний підхід до фізичної безпеки банків, який охоплює будівлю, персонал, вивіски та правила.

Куленепробивне скло, що розділяє касирів і клієнтів банку, відоме як бандитський бар'єр, є важливим елементом безпеки банків. Деякі дослідження показують, що близько 85–90% банківських пограбувань відбуваються у банках без таких бар'єрів. Згідно зі звітами, банки з куленепробивним склом помітно менше стають жертвами пограбувань.

Більшість банків обирають або віконну систему з перегородками, або систему аркових вікон. Обидва стилі використовують шматки куленепробивного скла, розташовані у шаховому порядку, що забезпечує абсолютно безперешкодний огляд для касирів, персоналу служби безпеки та камер. Вони також забезпечують безперешкодний зв'язок між клієнтами та персоналом, одночасно підвищуючи чіткість голосу — все це полегшує спілкування через бар'єр і покращує взаємодію з клієнтами.

Щодо внутрішнього скління, більшість банків використовують акрил (для рівнів 1 і 2) або ламінований полікарбонат/полікарбонат зі склом (доступний з будь-яким рівнем безпеки). АТ «Ощадбанк» використовує балістичне захисне скління на своїх зовнішніх вікнах.

Фінансовим установам потрібна інтегрована система безпеки, яка включає керований контроль доступності для обмеження доступу до чутливих зон або місць, внутрішнє/зовнішнє відеоспостереження для запобігання крадіжкам, вандалізму, а також пристрої виявлення пожежі/диму.

Наведемо деякі рішення, які електронна система безпеки може надати для банківських і фінансових установ:

- системи замкнутого телебачення (CCTV) з візуалізацією та дистанційним керуванням;
- безперервне відеоспостереження і виявлення вторгнень;
- рішення безпеки для банкоматів;
- аналіз відео для безпеки та бізнес-аналітики;
- доступ до рішень для управління картками, електронний контроль доступу та біометрія;
- системи безшумної сигналізації, пристрої паніки та стримування.

Безпека в банкоматах може складатися з пристроїв, які сповіщають про порушення роботи банкомату, і прихованих камер для запису користувачів банкомату.

Служба безпеки має більше уваги приділяти дотриманню посадових та робочих інструкцій тощо. Усі масштабні соціальні тенденції впливають на те, як керівники служби безпеки працюють над захистом фінансових установ. А на сьогоднішній день наслідки пандемії та війни ще більше ускладнюють захист банківської системи.

Дистанційна робота в наш час стала все більш необхідною, що робить завдання фізичної безпеки також значно складнішими.

Керівники служби безпеки можуть підвищити рівень захисту шляхом оновлення процесів повідомлення про інциденти в масштабах всього банку. Ефективний процес управління інцидентами оптимізує повідомлення про них, забезпечує сортування та аналіз, управління справами/інцидентами та звітування.

Керівникам служби безпеки слід впроваджувати системи повідомлень, які інформують про поточний стан та контрольні показники.

Система повинна зберігати інформацію про справу та будь-які електронні докази, пов'язані з безпекою. Крім того, керівники служби безпеки мають шукати можливості для звітування, щоб сприяти аналізу тенденцій, плануванню майбутніх проектів, визначенню потреб у навчанні та ефективному управлінню ресурсами.

У сучасну епоху керівники служби безпеки повинні розглядати комплексну стратегію управління інцидентами. Це включає надання співробітникам швидких можливостей повідомляти про різні інциденти за допомогою телефонів чи спеціальних додатків, що дозволяє їм приймати оперативні та обґрунтовані рішення та своєчасно реагувати на події.

Атаки на безпеку залишаються постійними. Опитування, проведене Vanson Bourne серед 100 осіб, які приймають стратегічні рішення в галузі фінансових послуг у Великобританії, показало, що 70% зазнали інцидентів безпеки протягом останніх дванадцяти місяців. Тим часом, Boston Consulting Group відзначила, що фінансові установи стають мішенями кібератак у 300 разів частіше, ніж інші компанії. Боротьба з такими атаками та їхніми наслідками призводить до вищих витрат для банків та менеджерів капіталу, ніж для будь-якого іншого сектору [19].

Хакери не завжди спрямовують свої зусилля на викрадення даних; іноді їх мета — зміна цих даних. Ці зміни часто важко помітити, оскільки дані залишаються незмінними. Однак точні дані — ключ до успіху банку, а зміни можуть завдати репутаційної та фінансової шкоди.

Кіберзлочинці періодично намагаються знищувати інформацію. За даними VMware у звіті Modern Bank Heists, 63% фінансових установ за 2022 рік стали свідками збільшення деструктивних атак, що на 17% перевищує попередні показники [20].

Програми-вимагачі продовжують активно діяти, оскільки близько 75% респондентів вже стали жертвами принаймні однієї атаки такого типу, і 63% із них заплатили викуп. Незважаючи на те, що старі загрози ніколи не втрачають актуальності, постійно з'являються нові. Щодо банків, то групи кіберзлочинців все частіше спрямовують свої зусилля на отримання непублічної ринкової інформації. Ці дані служать злодійською альтернативою інсайдерській торгівлі. Отже, вкрадені номери кредитних карток не є єдиним шляхом для шахрайства, оскільки непублічні оцінки прибутків, транзакції та інформація про публічні пропозиції надають можливість злочинним групам інвестувати свої кошти, отримані шахрайським шляхом, в акції, вартість яких зміниться за інсайдерською інформацією, коли ці дані стануть відомими.

Фактично, щорічний звіт Modern Bank Heists показує, що 66% фінансових установ стали мішенями таких атак [20]. Середній час виявлення, ідентифікації та локалізації витоку даних складає 287 днів, а чим більше цей процес триває, тим більше витрат. Звіт IBM Cost of a Data Breach Report вказує, що порушення даних, виявлення яких зайняло понад 200 днів, в середньому коштують 4,87 мільйонів доларів США, порівняно з 3,61 мільйонами доларів США за порушення, виявлені менш ніж за 200 днів [21].

Слідкування за пропускною здатністю мережі та пристроїв може допомогти виявити потенційні порушення, часто на етапі їх спроби. IT-спеціалісти можуть проводити експертизу з безпеки за допомогою мережевих журналів, аналізу записів та звітності. Таким чином, IT-персонал дізнається, що трапилося і чому. Озброївшись цією інформацією, IT-фахівці можуть мінімізувати поточні збитки та, знаючи джерело, запобігти їх повторенню.

Незважаючи на те, що системи призначені для полегшення роботи, такі інструменти як оповіщення у сфері інформаційних технологій можуть навпаки збільшити навантаження на IT-фахівців. Більшість організацій інвестують в багатофункціональні платформи, які пропонують різноманітні можливості: відстеження пропускної здатності, управління журналами подій, аналіз мережевого трафіку, моніторинг віртуальних середовищ та інше. Дослідження банків, проведене Stowarzyszenie Ovum, показало, що в середньому 40% щодня отримують 160 000 помилкових, надлишкових або непотрібних повідомлень. Причиною цього є перенасичення сповіщень від безлічі інструментів безпеки. Stowarzyszenie Ovum встановила, що 73% установ мають принаймні 25 окремих інструментів безпеки [22].

Стосовно конвергенції, фахівці з безпеки мають бути налаштовані на інтеграцію цифрової та фізичної безпеки. Зокрема, існує кіберризик, пов'язаний із застарілими пристроями фізичного захисту. Камери відеоспостереження, системи сигналізації, контрольно-пропускні пристрої, системи контролю доступу — все це може стати ціллю для винахідливих кіберзлочинців. Керівники служби безпеки можуть об'єднати свої команди для консолідації та підтримки своїх зусиль щодо підвищення безпеки. Тісніша інтеграція кібербезпекових підрозділів і груп фізичної безпеки допоможе краще зрозуміти ці ризики та мінімізувати їх.

Висновки і перспективи подальших досліджень. Дослідження безпеки показало, що оскільки АТ «Ощадбанк» є найбільшим державним банком України зі значною клієнтською базою та обслуговує широкий спектр фінансових операцій, йому важливо мати ефективну систему управління безпекою, яка забезпечувала б захист його активів від загроз.

У цілому, система управління безпекою акціонерного товариства «Державний ощадний банк України» є комплексною, системною та орієнтованою на постійне вдосконалення, що дозволяє забезпечувати високий рівень захищеності та стабільності фінансових операцій та активів банку.

Оскільки кіберзагрози стають все більш серйозним викликом для банків, наступні дослідження будуть спрямовуватися на аналіз сучасних тенденцій кібербезпеки та розробку стратегій захисту від кібератак, що будуть вивчати роль новітніх технологій, таких як штучний інтелект, блокчейн тощо, у забезпеченні безпеки банківських операцій та захисті інформації. Також в подальших дослідженнях будуть розглядатися ефективні методи підвищення свідомості персоналу банку щодо безпеки та навчання їх діяти в умовах загроз.

Література

1. Jore S. H. The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*. 2019. 4 (1). P. 157–174.doi: https://doi.org/10.1007/s41125-017-0021-9.

2. Hirschfield A. Inter-Relationships between Perceptions of Safety, Anti-Social Behaviour and Security Measures in Disadvantaged Areas. *Security Journal*. 2004. 17 (1). P. 9–20.

3. George R., Mawby R. I. Security at the 2012 London Olympics: Spectators' Perceptions of London as a Safe City. *Security Journal*. 2013. 28 (1). P. 93–104. doi: https://doi.org/10.1057/sj.2013.37.

4. Borodzicz, Edward P., and Steven D. Gibson. Corporate Security Education: Towards Meeting the Challenge. *Security Journal*. 2007. 20 (2). P. 142. https://doi.org/10.1057/palgrave.sj.8350032.

5. Goosman A. Evolving Corporate Crisis Response Coordination for Maximum Resilience. *Journal of Business Continuity & Emergency Planning*. 2022. 15 (3). P. 237–244.

6. Dau L. A, Moore E. M., Abrahms M. Global Security Risks, Emerging Markets and Firm Responses: Assessing the Impact of Terrorism. *In Contemporary Issues in International Business: Institutions, Strategy and Performance*, edited by Davide Castellani, Rajneesh Narula, Quyen T. K. Nguyen, Irina Surdu and James T. Walker, 2018. P. 79–97. Cham: Springer International Publishing.

7. White A. The Impact of the Private Security Industry Act 2001. *Security Journal*. 2013. 28 (4). P. 425–442. doi: https://doi.org/10.1057/sj.2012.53.

8. Burns M. G. Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience. Boca Raton: CRC Press, 2016.

9. Crump J. Corporate Security Intelligence and Strategic Decision Making Taylor and Francis. 2015. doi: https://doi.org/10.1201/b18399.

10. Kryshtal H. Financial security of the banking system of Ukraine under the conditions of martial state: classification of possible threats. *Management and Entrepreneurship: Trends of Development*. 2023. 4(26). P. 39–47. doi: https://doi.org/10.26661/2522-1566/2023-4/26-03.

11. Москвін Б. Ю. Економічна безпека фінансових інституцій в умовах воєнного стану в Україні. *Економіка і організація управління*. 2022. № 2 (46). С. 110–119. doi: 10.31558/2307-2318.2022.2.11.

12. Коробцова Д. В. Правове забезпечення фінансової безпеки держави в умовах воєнного стану. Аналітично-порівняльне правознавство. 2022. № 2. С. 141–146. doi: https://doi.org/10.24144/2788-6018.2022.02.27

13. Мушеник І. М., Грушецький С. М. Забезпечення фінансової безпеки України в період воєнного часу та в умовах фінансової інклюзії. *Modern Economics*. 2022. № 32. С. 70–74. doi: https://doi.org/10.31521/modecon.V32(2022)-09.

14. Бондаренко А. І. Механізми забезпечення фінансової безпеки України при розширенні системи E-banking. *Bulletin of NUCPU. State Management series*. 2018. С. 81–88. doi: 10.5281/zenodo.1240779; URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/6926/1/13.pdf (дата звернення: 28.01.2024).

15. Varnalii Z, Mekhed A. Business entities' financial security under digital economy. *Financial and credit activity: problems of theory and practice*. 2022. Vol. 4 (45). P. 267–275. doi: 10.55643/fcaptp.4.45.2022.3813

16. *АТ «Ощадбанк»: офіційний сайт*. URL: www.oschadbank.ua/ (дата звернення: 28.01.2024).

17. Статистика фінансового сектору. *Національний банк України: офіційний сайт*. URL: http://www.bank.gov.ua/control/uk/publish/category?cat_id=44575 (дата звернення: 28.01.2024).

18. *The American Bankers Association: офіційний сайт*. URL: https://www.aba.com (дата звернення: 28.01.2024).

19. MSPs and cybersecurity: The time for turning a blind eye is over. Help *Net Security*. URL: https://www.helpnetsecurity.com/2022/09/12/msps-email-security/. (дата звернення: 28.01.2024).

20. Kellermann T. Modern Bank Heists 5.0: The Escalation from Dwell to Destruction. *VMware by Broadcom*. 2022. URL: https://news-vmware-com.translate.goog/security/modern-bank-heists-5-0-the-escalation-from-dwell-to-destruction?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc&_x_tr_hist=true (дата звернення: 28.01.2024).

21. Cost of a Data Breach Report. *IBM*. 2023. URL: https://www-ibm-com.translate.goog/reports/data-breach?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата звернення: 28.01.2024).

22. *Stowarzyszenie OVUM: офіційний сайт*. URL: https://ovum.org.pl/ (дата звернення: 28.01.2024).

References

1. Jore, S.H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*. 4 (1), 157–174. doi: https://doi.org/10.1007/s41125-017-0021-9.

2. Hirschfield, A. (2004). Inter-Relationships between Perceptions of Safety, Anti-Social Behaviour and Security Measures in Disadvantaged Areas. *Security Journal,* 17 (1), 9–20.

3. George, R., & Mawby, R.I. (2013). Security at the 2012 London Olympics: Spectators' Perceptions of London as a Safe City. *Security Journal*. 28 (1), 93–104. doi: https://doi.org/10.1057/sj.2013.37.

4. Borodzicz, E.P., & Gibson, S.D. (2007). Corporate Security Education: Towards Meeting the Challenge. *Security Journal,* 20 (2), 142. doi: https://doi.org/10.1057/palgrave.sj.8350032.

5. Goosman, A. (2022). Evolving Corporate Crisis Response Coordination for Maximum Resilience. *Journal of Business Continuity & Emergency Planning*, 15 (3), 237–244.

6. Dau, L.A., Moore E.M., & Abrahms M. (2018). Global Security Risks, Emerging Markets and Firm Responses: Assessing the Impact of Terrorism. *In Contemporary Issues in International Business: Institutions, Strategy and Performance*, edited by Davide Castellani, Rajneesh Narula, Quyen T.K. Nguyen, Irina Surdu and James T.Walker, 79–97. Cham: Springer International Publishing.

7. White, A. (2013). The Impact of the Private Security Industry Act 2001. *Security Journal.* 28 (4), 425–442. doi: https://doi.org/10.1057/sj.2012.53.

8. Burns, M.G. (2016). Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience. Boca Raton: CRC Press.

9. Crump, J. (2015). Corporate Security Intelligence and Strategic Decision Making Taylor and Francis. doi: https://doi.org/10.1201/b18399.

10. Kryshtal, H. (2023). Financial security of the banking system of Ukraine under the conditions of martial state: classification of possible threats. *Management and Entrepreneurship: Trends of Development*, 4(26), 39–47. doi: https://doi.org/10.26661/2522-1566/2023-4/26-03.

11. Moskvin, B.Yu. (2022). Ekonomichna bezpeka finansovykh instytutsiy v umovakh voyennoho stanu v Ukrayini [Economic security of financial institutions in the conditions of martial law in Ukraine]. *Ekonomika i orhanizatsiya upravlinnya — Economics and management organization*, 2 (46), 110–119. doi: 10.31558/2307-2318.2022.2.11 [in Ukrainian].

12. Korobtsova, D.V. (2022). Pravove zabezpechennya finansovoyi bezpeky derzhavy v umovakh voyennoho stanu. Analitychno-porivnyal'ne pravoznavstvo [Legal provision of the financial security of the state in conditions of martial law]. *Analitychno-porivnyal'ne pravoznavstvo-Analytical and comparative jurisprudence*, 2, 141–146. doi: https://doi.org/10.24144/2788-6018.2022.02.27 [in Ukrainian].

13. Mushenyk, I.M., & Hrushetskyi, S.M. (2022). Zabezpechennya finansovoyi bezpeky Ukrayiny v period voyennoho chasu ta v umovakh finansovoyi inklyuziyi [Ensuring the financial security of Ukraine during wartime and in terms of financial inclusion]. *Modern Economics*, 32, 70–74. doi: https://doi.org/10.31521/modecon.V32(2022)-09 [in Ukrainian].

14. Bondarenko, A.I. (2018). Mekhanizmy zabezpechennya finansovoyi bezpeky Ukrayiny pry rozshyrenni systemy E-banking [Mechanisms for ensuring the financial security of Ukraine during the expansion of the E-banking system]. *Bulletin of NUCPU. State Management series,* 81–88. doi: 10.5281/zenodo.1240779; Retrieved from http://repositsc.nuczu.edu.ua/bitstream/123456789/6926/1/13.pdf [in Ukrainian].

15. Varnalii, Z., & Mekhed, A. (2022). Business entities' financial security under digital economy. *Financial and credit activity: problems of theory and practice*, 4 (45), 267–275. doi: 10.55643/fcaptp.4.45.2022.3813.

16. *JSC "Oschadbank": official website*. Retrieved from www.oschadbank.ua/.

17. Statistics of the financial sector. *National Bank of Ukraine: official website*. Retrieved from http://www.bank.gov.ua/control/uk/publish/category?cat_id=44575.

18. *The American Bankers Association: official website.* Available at: https://www.aba.com.

19. MSPs and cybersecurity: The time for turning a blind eye is over. *Help Net Security*. URL: https://www.helpnetsecurity.com/2022/09/12/msps-email-security/.

20. Kellermann, T. (2022). Modern Bank Heists 5.0: The Escalation from Dwell to Destruction. *VMware by Broadcom*. Retrieved from https://news-vmware-com.translate.goog/security/modern-bank-heists-5–0-the-escalation-from-dwell-to-destruction?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc&_x_tr_hist=true.

21. Cost of a Data Breach Report. *IBM*. Retrieved from https://www-ibm-com.translate.goog/reports/data-breach?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc.

22. *Stowarzyszenie OVUM: official website.* URL: https://ovum.org.pl/.