УДК 355.488: 681.3

М. Ю. Богославський,
здобувач, Національна Академія управління, м. Київ, Україна

КОМПЕНСАТОРНИЙ МЕХАНІЗМ НІВЕЛІЗАЦІЇ ВТРАТ КІБЕРАТАК ДЛЯ КОМЕРЦІЙНОГО БАНКУ

N. Bogoslavskij,
Applicant National Academy of Management, Kyiv, Ukraine

COMPENSATORY MECHANISM OF LOSS LIABILITY WHILE CYBERATTACKS OF COMMERCIAL BANK

Виходячи з актуальних проблем інформаційної безпеки банку, постає необхідність у розробці ефективного компенсаторного механізму нівелізації втрат кібератак для комерційного банку, які зменшать кількісні та якісні втрати активів та пасивів, скоротивши при цьому норму недоотримання прибутку. У межах розрахункового блоку було використано відповідні обчислювальні моделі та перевірено їх на адекватність. Встановлено, що найбільш важливими підрозділами реагування інформаційної безпеки та протидії кібератакам є такі служби згідно з пріоритетністю: управління фінансової безпеки, служба фінансового моніторингу, операційне управління. У ході дослідження були проаналізовані такі процеси збереження фінансової інформації, як маршрутизація та кешування, відповідно, при їх аналізі були застосовані такі форми, як миттєва форма перерахунку коштів клієнтів в критичних ситуаціях, хеджування залишків банку, банківських резервів та інших коштів банку на трьох базових рівнях: внутрішньобанківський, зовнішньобанківський, кошти на рахунках НБУ. За результатами розглянутих прийомів було синхронізовано методичні аспекти та протидію проблематиці у відповідних компенсаторних механізмах нівелізації втрат кібератак для комерційного банку.

Proceeding from the current problems of the bank's information security, it becomes necessary to develop an effective compensatory mechanism for eliminating losses of cyberattacks for a commercial bank, which will reduce the losses of assets and liabilities and reduce the lack of profit. In the calculation of the block, appropriate computing models were used and checked for adequacy. It is established that the most important units of information security and counteraction response to cyberattacks are such services according to priority financial security, financial monitoring, operational management. In the course of the study, such processes of saving financial information as routing and caching were analyzed. In their analysis, the following forms were used as an instant form of customer cash balances, bank balances, bank reserves and other bank balances, and an instantaneous form of customer cash balances, bank balances, bank reserves and other bank balances throughout the day according to periods. According to the results of the considered methods, the methodical aspects and counteraction to problems in the corresponding compensatory mechanisms of the caveat loss elimination for a commercial bank were synchronized.

Ключові слова: компенсаторний механізм, нівелізація, кібератака, маршрутизація, кешування, актив банку, пасив банку.

Key words: compensatory mechanism, leveling, cyberattack, routing, caching, bank active, passive bank.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ

У наш час для оптимальної діяльності банківських установ та гарантування захисту фінансових даних є актуальною проблематика кібератак в Україні. Зі швидкоплинним розвитком комп'ютерних технологій для безпеки банків виникає неабияка загроза. Саме тому постає необхідність у дослідженні компенсаторного механізму нівелізації втрат кібератак для комерційного банку, які зменшать втрати активів та пасивів фінансових установ.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

До науковців, які займалися дослідженням компенсаторного механізму нівелізації втрат кібератак, зокрема, у банківському секторі, відносять: Р. Грищук, В. Охрімчук, В.Я. Пєвнєва, М.В. Цуранов, О.Г. Корченко, І.А. Терейковський, К.А. Колосова, І.М. Пістунов та ін.

МЕТА СТАТТІ

Метою статті є підбір складових частин для побудови компенсаторного механізму нівелі-

Передплатний індекс 21847

Таблиця 1. Реагування підрозділів інформаційної безпеки відповідно до напрямків діяльності банку

Реагування підрозділів інформаційної безпеки відповідно до напрямів діяльності банку			
Назва напряму діяльності	Модель обчислення	Підтвердження адекватності	Характеристика
Фінансова безпека	$I_S = 2,35 + 1,28 + S + 3,11 \bullet x_2$	$I_S (6,71 + S) > R$	
Фінансовий моніторинг	$I_S = 3,06 + 1,41 + S + 2,91 \bullet x_2$	$I_S (7,21 + S) > R$	
Операційна робота та звітність	$I_S = 2,74 + 1,33 + S + 3,06 \bullet x_2$	$I_S (7,11 + S) > R$	
Управління міжнародними розрахунками	$I_S = 2,56 + 2,75 + S - 2,85 \bullet x_2$	$I_S (8,22 + S) > R$	
Картковий бізнес	$I_S = 2,57 + 2,17 + S - 2,61 \bullet x_2$	$I_S (7,35 + S) > R$	
Кредитні відносини	$I_S = 3,27 - 2,78 + S + 2,53 \bullet x_2$	$I_S (8,63 + S) > R$	
Депозитні відносини	$I_S = 2,37 + 2,49 + S + 3,73 \bullet x_2$	$I_S (9,24 + S) > R$	
IT служба	$I_S = 2,65 + 2,28 + S + 2,61 \bullet x_2$	$I_S (7,87 + S) > R$	
Цінні папери	$I_S = 3,15 - 2,52 + S + 2,89 \bullet x_2$	$I_S (8,41 + S) > R$	
Аудит	$I_S = 3,28 + 1,15 + S + 3,77 \bullet x_2$	$I_S (8,92 + S) > R$	
Управління валютного контролю	$I_S = 2,74 + 2,28 + S + 4,16 \bullet x_2$	$I_S (9,63 + S) > R$	

Джерело: складено автором на основі [5, с. 117].

зації фінансових витрат від кібератак та інформаційних загроз для комерційного банку.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Основою нівелізації фінансових втрат від кібератак та інформаційних загроз є оперативне реагування підрозділів інформаційної безпеки відповідно до напрямків діяльності банку. Для розгляду даного процесу вважаємо необхідним синхронізувати діяльність наступних служб банку: фінансова безпека, фінансовий моніторинг, операційна робота та звітність, управління міжнародними розрахунками, картковий бізнес, кредитні та депозитні відносини, функціонування IT служби, аудит, цінні папери та управління валютного контролю [1, с. 278—279]. Власне компенсаторний механізм має умовний характер та передбачає превітивізацію несанкціонованого втручання в цикл банківських операцій. Цільовою метою розробки компенсаторного механізму є мінімізація втрат та максимізація прибутку банку. Тому поєднання функціональних обов'язків, їх розподіл між службами банку відповідно періодизації має бути доповнений прогнозними та очікуваними регресійними трендами по кібератакам та кіберзлочинності [2, с. 96].

Проведення огляду внутрішньобанківських бізнеспроцесів та їх характеристика розвитку щодо нівелізації загроз інформаційної безпеки дозволить виділити пріоритетність структурних підрозділів банку в ході виконання завдань з компенсації потенційних втрат. Тому реагування підрозділів інформаційної безпеки відповідно до напрямків діяльності банку випливає, що найбільш вагомими службами у забезпеченні захисту фінансової установи є фінансова безпека, фінансовий моніторинг та операційна робота й звітність [5, с. 117].

Одним із засобів збереження фінансової інформації у результаті кібератаки є її маршрутизація та кешування. Під час дослідження цих процесів були використані миттєві форми перерахунку коштів клієнтів, залишків банку, банківських резервів та інших коштів банку відповідно до часових проміжків [7, с. 147].

Виходячи з проведеного дослідження етапів маршрутизації та кешування фінансової інформації комерційного банку у випадку кібератаки, можемо стверджувати, що організація роботи банку із щоденним розміщенням коштів

Передплатний індекс 21847

Таблиця 2. Маршрутизація та кешування фінансової інформації комерційного банку у випадку кібератаки

Маршрутизація та кешування фінансової інформації комерційного банку у випадку кібератаки						
	Внутрішньобанківський		Зовнішньобанківський		Кошти на рахунках НБУ	
Миттєва форма перерахунку коштів клієнтів, залишків банку, банківських резервів та інших коштів банку	Модель	Нормалізація	Модель	Нормалізація	Модель	Нормалізація
	$B_c = 1,53 – 2,79 + R + -0,18409 \bullet x$	$B_c > R + x^2 + 0,18409$	$B_c (R) = 1,86 – 3,09 + 0,21712 \bullet x$	$B_c > R + x^2 + 0,21712$	$B_c = 1,74 – 2,99 + R + -0,21615^2$	$B_c > R + x^2 + 0,21615$
Миттєва форма перерахунку коштів клієнтів, залишків банку, банківських резервів та інших коштів банку впродовж дня	Модель	Нормалізація	Модель	Нормалізація	Модель	Нормалізація
	$B_c = 2,37 – 3,89 + R + -0,19167 \bullet x$	$B_c > R + x^2 + 0,1916$	$B_c (R) = 2,75 – 3,93 + 0,35183 \bullet x$	$B_c > R + x^2 + 0,35183$	$B_c = 2,61 – 4,79 + R + -0,38523^2$	$B_c > R + x^2 + 0,38523$
Миттєва форма перерахунку коштів клієнтів, залишків банку, банківських резервів та інших коштів банку на наступний день	Модель	Нормалізація	Модель	Нормалізація	Модель	Нормалізація
	$B_c = 2,38 – 3,51 + R + -0,27254 \bullet x$	$B_c > R + x^2 + 0,27254$	$B_c (R) = 2,38 + 3,29 -0,37592 \bullet x$	$B_c > R + x^2 + 0,37592$	$B_c = 2,53 – 2,37 + R + -0,32758^2$	$B_c > R + x^2 + 0,32758$

Джерело: складено автором на основі [7, с. 147] .

на рахунках НБУ є найбільш безпечною та прозорою моделлю функціонування фінансової установи.

Актуальність досліджуваного питання вимагає ефективного компенсаторного механізму нівелізації втрат кібератак для комерційного банку, які зменшать втрати активів та пасивів. Беручи до уваги дослідження Європейського банку реконструкції та розвитку щодо майбутніх кібератак на фінансові установи, було спрогнозовано значення втрат активів на наступні 6 років (2019—2024 рр. відповідно) [4, с. 99].

Керуючись результатами дослідження прогнозного значення втрат активів банків, завданих кібератаками, можемо припустити, що у 2024 році масштаби кіберзагроз стосовно банківських установ досягнуть позначки 4,36, порівняно з 2019 роком, де цей показник становить 0,84. Це говорить про те, що кібератаки на фінансові установи збільшаться на 519 % за наступні 6 років.

Прогнозне значення втрат пасивів банків, завданих кібератаками, дозволить зменшити наслідки порушень циклу банківських операцій і скоротити число прямих втрат банку від кібератак [3, с. 169].

Дослідивши прогнозне значення втрат пасивів банків, завданих кібератаками, на майбутні роки, а саме 2019—2024 рр., було виявлено та проаналізовано, що до 2024 року кіберзагрози становитимуть 1.65. Порівнюючи цей показник з 2019 роком (0,77), то різниця сягає 0,88. Це дає змогу припустити, що кібератаки на банківські установи зростуть на 214% протягом наступних років.

ВИСНОВКИ

Встановлено, що у зв'язку з масштабними проблемами безпеки інформаційних систем банківських установ виникає потреба у дослідженні компенсаторного механізму нівелізації втрат кібератак для комерційного банку, які зменшать втрати активів та пасивів. Було

Таблиця 3. Прогнозне значення втрат активів банків завданих кібератаками

Прогнозне значення втрат активів банків завданих кібератаками						
Банки	Роки					
	2019	2020	2021	2022	2023	2024
Приватбанк	0,15	0,43	0,59	0,82	0,89	0,94
Банк Аваль	0,13	0,26	0,37	0,59	0,74	0,81
Укрсиббанк	0,09	0,18	0,24	0,37	0,58	0,72
Ощадбанк	0,17	0,23	0,31	0,43	0,55	0,68
Укргазбанк	0,19	0,26	0,30	0,37	0,42	0,54
Радабанк	0,11	0,16	0,28	0,37	0,45	0,67
Всього	0,84	1,52	2,09	2,95	3,63	4,36

Джерело: складено автором на основі [4, с. 99].

Передплатний індекс 21847

Таблиця 4. Прогнозне значення втрат пасивів банків завданих кібератаками

Прогнозне значення втрат пасивів банків завданих кібератаками						
Банки	Роки					
	2019	2020	2021	2022	2023	2024
Приватбанк	0,11	0,32	0,27	0,31	0,24	0,27
Банк Аваль	0,07	0,36	0,29	0,27	0,28	0,25
Укрсиббанк	0,14	0,40	0,24	0,29	0,30	0,30
Ощадбанк	0,20	0,27	0,31	0,23	0,27	0,31
Укргазбанк	0,10	0,22	0,25	0,28	0,25	0,24
Радабанк	0,15	0,19	0,28	0,32	0,22	0,28
Всього	0,77	1,76	1,64	1,70	1,56	1,65

Джерело: складено автором на основі [3, с. 169].

проведено огляд складових частин даного механізму та змодельовано на базі розрахунків ситуації при кібератаках на банк, з перевіркою їх на ефективність. Виявлено, що провідними підрозділами реагування інформаційної безпеки та протидії кібератакам є такі служби: управління фінансової безпеки, служба фінансового моніторингу, операційне управління.

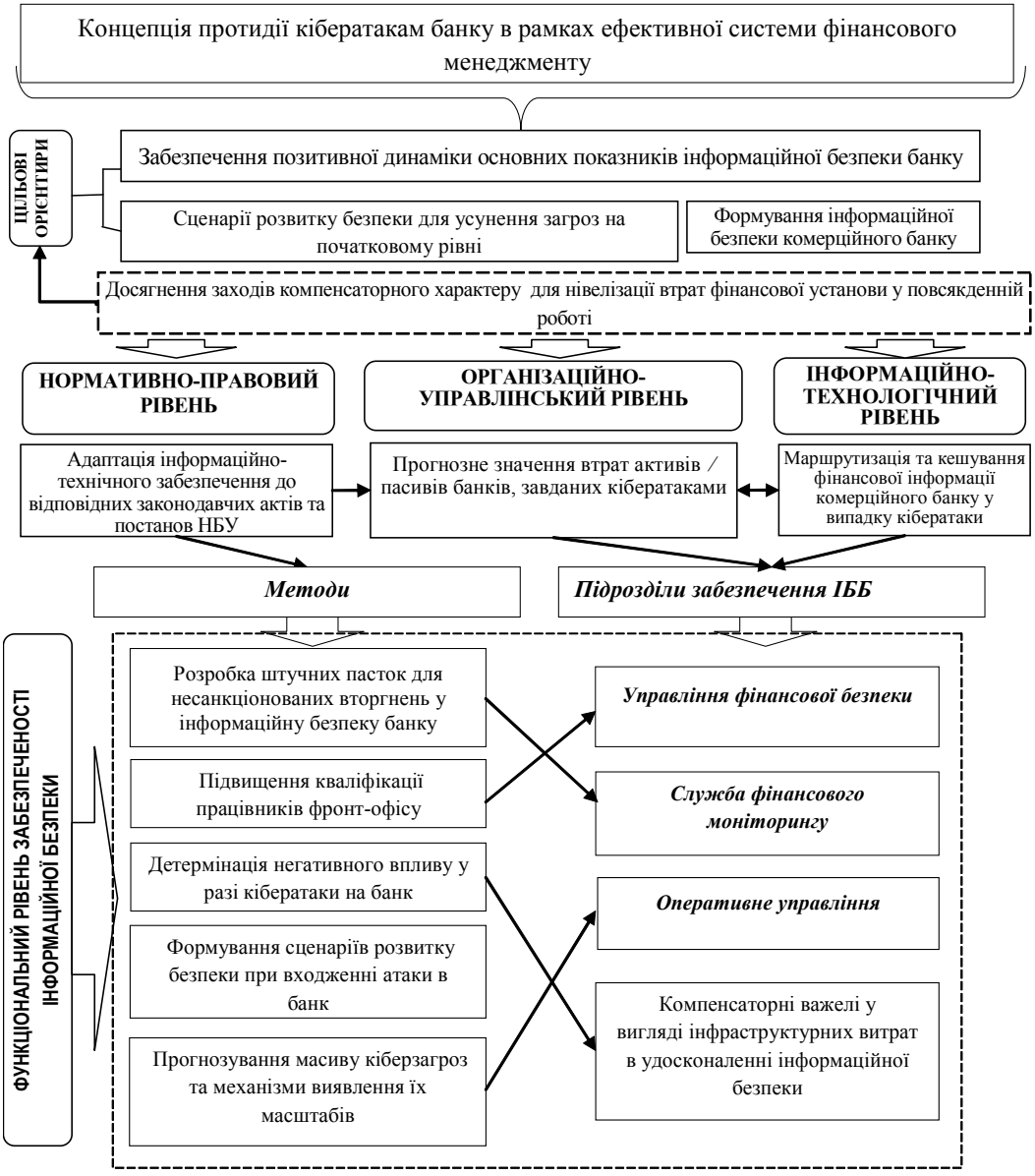

Рис. 1. Концепція протидії кібератакам банку в рамках ефективної системи фінансового менеджменту

Передплатний індекс 21847

Під час аналізу процесів збереження фінансової інформації, а саме маршрутизації та кешування, були застосовані миттєві форми перерахунку коштів клієнтів, залишків банку, банківських резервів та інших коштів банку відповідно до періодів. Можемо стверджувати, що організація роботи банку із щоденним розміщенням коштів на рахунках НБУ є найбільш оптимальною моделлю функціонування фінансової установи. Дослідивши прогнозне значення втрат активів та пасивів банків, завданих кібератаками, можемо припустити, що кібератаки на фінансові установи збільшаться на 519 % та 214 % відповідно протягом наступних 6 років. За результатами дослідження було синхронізовано методичні аспекти та протидію проблематиці у відповідних компенсаторних механізмах нівелізації втрат кібератак для комерційного банку.

Література:

1. Грищук Р. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак [Електронний ресурс]/ Р. Грищук, В. Охрімчук // Безпека інформації. — 2015. — Т. 21, № 3. — С. 276 — 282. — Режим доступу: http://nbuv.gov.ua/

2. Колосова К.А. Компенсаторні механізми та алгоритм управління стійкістю підприємств [Електронний ресурс] / К.А. Колосова // Управління проектами та розвиток виробництва. — 2012. — № 4. — С. 94—100. —Режим доступу: http://nbuv.gov.ua/

3. Корченко О.Г. Верифікація нейромережевих методів розпізнавання кібератак [Електронний ресурс] / О.Г. Корченко, І.А. Терейковський // Управління розвитком складних систем. — 2014. — Вип. 17. — С. 168 — 172. — Режим доступу: http://nbuv.gov.ua/

4. Пєвнєв В.Я. Збільшення швидкості передачі як засіб протидії кібератакам / В.Я. Пєвнєв, М.В. Цуранов //Системи управління, навігації та зв'язку. — 2017. — Вип. 2. — С. 98—101. — Режим доступу: http://nbuv.gov.ua/

5. Пістунов І.М. Визначення рівня безпеки електронної комерції І.М. Пістунов // Науковий вісник Національного гірничого університету. — 2015. — № 1. — С. 114—120. — Режим доступу: http://nbuv.gov.ua/

6. Райзберг Б.А. Современный экономический словарь / Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б.; 5-е изд., перераб. и доп. — М.: ИНФРА-М, 2006. — 495 с.

7. Смирнов А.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы [Електронний ресурс]/ А.А. Смирнов, А.К. Дидык, С.А. Смирнов // Системи озброєння і військова техніка. — 2016. — № 2. — С. 146 — 149. — Режим доступу: http://nbuv.gov.ua/

References:

1. Hryschuk, R. and Okhrimchuk, V. (2015), "Setting up a scientific task for developing templates for potentially dangerous cyber attacks", Bezpeka informatsii, vol. 21, no. 3, pp. 276—282.

2. Kolosova, K.A. (2012), "Compensatory mechanisms and algorithm for enterprise sustainability management", Upravlinnia proektamy ta rozvytok vyrobnytstva, vol. 4, pp. 94—100.

3. Korchenko, O.H. and Terejkovs'kyj, I.A. (2014), "Verification of neural network recognition methods for cyber attacks", Upravlinnia rozvytkom skladnykh system, vol. 17, pp. 168—172.

4. Pievniev, V.Ya. and Tsuranov, M.V. (2017), "Increase the speed of transmission as a means of counteracting cyber attacks", Systemy upravlinnia, navihatsii ta zv'iazku, vol. 2, pp. 98—101.

5. Pistunov, I.M. (2015), "Determine the level of e-commerce security", Naukovyj visnyk Natsional'noho hirnychoho universytetu, vol. 1, pp. 114—120.

6. Rajzberh, B.A. Lozovskyj, L.Sh. and Starodubtseva, E.B. (2006), Sovremennyj ekonomycheskyj slovar' [The modern economic dictionary], YNFRA-M, Moscow, Russia.

7. Smyrnov, A.A. Dydyk, A.K. and Smyrnov, S.A. (2016), "Method of secure routing of metadata to cloud antivirus systems", Systemy ozbroiennia i vijs'kova tekhnika, vol. 2, pp. 146—149.

Стаття надійшла до редакції 05.09.2018 р.