ГРОШІ, ФІНАНСИ І КРЕДИТ

УДК 336.71

Богославський М.Ю.,
аспірант,
Національна академія управління

МЕТОДИЧНІ ПІДХОДИ ДО ФІНАНСОВОГО ЗАМІЩЕННЯ ТА ЕЛАСТИЧНОСТІ В РАМКАХ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРАТАКАМ БАНКУ

Богославський М.Ю. Методичні підходи до фінансового заміщення та еластичності в рамках забезпечення протидії кібератакам банку. У статті здійснено підбір певного ряду методичних підходів до фінансового заміщення та еластичності в рамках забезпечення супротиву кібератакам на комерційні установи. Встановлено актуальні способи заміщення втрат клієнтських ресурсів у банку, еластичності грошових потоків та основні дестабілізаційні чинники, що негативно впливають на функціонування комерційних банків на ринку і послаблюють систему, породжуючи кібератаки. Розглянуто формування еластичності грошових потоків комерційного банку за стабільних видатків та нормального показника видатків по кіберзагрозам відповідно до очікуваних сценаріїв. Відтворено математичні формули, графік і таблиці, що зображують ступінь протидії банку до кіберзагроз та рівні еластичності й заміщення ресурсів. У процесі дослідження з'ясовано, що комерційні структури є досить стійкими до кібератак, фінансових махінацій та злочинів проникнення до банківської системи. Визначено, що індикатори еластичності компенсаторних видатків є показниками поточного стану фінансової системи та сприяють тому, щоб керівництво підбирало або змінювало стратегії діяльності залежно від різного стану комерційного банку.

Ключові слова: фінансове заміщення ресурсів, еластичність грошових потоків, сценарії розвитку грошових потоків, нівелювання загроз, стрес-фактор, гранична норма заміщення, грошові потоки банку.

Богославский М.Ю. Методические подходы к финансовому замещению и эластичности в рамках обеспечения противодействия кибератакам банка. В статье осуществлен подбор определенного ряда методических подходов к финансовому замещению и эластичности в рамках обеспечения сопротивления кибератакам на коммерческие учреждения. Установлены актуальные способы замещения потерь клиентских ресурсов в банке, эластичности денежных потоков и основные дестабилизирующие факторы, отрицательно влияющие на функционирование коммерческих банков на рынке и ослабевающие систему, порождая кибератаки. Рассмотрено формирование эластичности денежных потоков коммерческого банка при стабильных расходах и нормальном показателе расходов по киберугрозам в соответствии с ожидаемыми сценариями. Воспроизведены математические формулы, график и таблицы, изображающие степень противодействия банка к киберугрозам и уровни эластичности и замещения ресурсов. В процессе исследования выяснено, что коммерческие структуры являются достаточно устойчивыми к кибератакам, финансовым махинациям и преступлениям проникновения в банковскую систему. Определено, что индикаторы эластичности компенсаторных расходов являются показателями текущего состояния финансовой системы и способствуют тому, чтобы руководство подбирало или меняло стратегии деятельности в зависимости от различного состояния коммерческого банка.

Ключевые слова: финансовое замещение ресурсов, эластичность денежных потоков, сценарии развития денежных потоков, нивелирование угроз, стресс-фактор, предельная норма замещения, денежные потоки банка.

Bogoslavsky M.Yu. Methodical approaches to financial substitution and elasticity for providence cyber attacks' counteraction. The article is dedicated to the selection of methodical approaches to financial substitution and elasticity in order to provide resistance to cyber-attacks of commercial institutions. There have been established actual ways of replacing the client resources losses in the bank, the cash flows elasticity and the main destabilization factors that negatively affect the functioning of commercial banks in the market and weaken the system by generating cyber-attacks. The formation of the commercial bank cash flows elasticity in the course of stable expenditures and the normal rate of expenditure on cyber threats in accordance with the expected scenarios. The mathematical formulas, graphs and tables, depicting a phase of counteraction to the elasticity levels cyber-threat and resources replacement are generated. The study found that commercial structures are quite resistant to cyber-attacks, financial fraud and penetration into the banking system. It has been found that elasticity indicators of compensatory expenditures are the current state indicators of the financial system and help the management to select or modify strategies for activities depending on different state of a commercial bank.

Key words: financial substitution of resources, elasticity of cash flows, scenarios of cash flow development, leveling of threats, stress factor, marginal rate of replacement, cash flows of the bank.

Постановка проблеми. Нині оперативні заходи комерційного банку щодо захисту власних інформаційно-технічних мереж є технологічними властивостями операційної системи та захисту серверу. Крім того, важливу роль відіграє індикатор фінансового заміщення та нівелювання отриманої шкоди від зовнішнього середовища.

Аналіз останніх досліджень і публікацій. Серед авторів, які займалися проблематикою фінансової та інформаційної безпеки банків, можна виділити таких, як А. Губаренко, Т. Болгар, О. Жабинець, С. Іванишин, О. Чуб, А. Єпіфанов, Т. Васильєва, В. Лєонов, І. Мігус, М. Мельник, В. Домарев. Попри значний пласт досліджень за цією тематикою, на нашу думку, недостатньо уваги приділено розробці методичних підходів до заміщення втрат від інформаційної безпеки комерційних банків.

Цей інструментарій дасть змогу підвищити авторитетність банківських установ в полі ризикового середовища кібератак і нівелюватиме їх прямий вплив контрольованим чином з резервів банківської установи.

Хоча дослідження технологічних властивостей програмного захисту від кібератак банків не є фінансовою складовою, проте його слабкість безпосередньо впливає на платоспроможність та стабільність роботи банківської установи.

Формулювання цілей статті. Метою статті є пропонування актуальних підходів до фінансового заміщення втрат та еластичності грошових потоків у рамках забезпечення супротиву кібератакам, які дестабілізують фінансовий стан комерційних банків.

Виклад основного матеріалу. Під час аналізування поточного стану розвитку фінансової захищеності комерційних банків вихідними завданнями є компенсація втрат видатків та не отриманих вигід за критичних ситуацій, прямих кіберзагроз, альтернативних утручань у платіжну систему банку тощо.

На нашу думку, забезпечення еластичності грошових потоків у разі отримання збитків по кібератакам банку може ефективно компенсувати втрати в рамках критичного стану. Гранична норма заміщення втрат комерційних банків характеризує компенсаторні властивості фінансово-аналітичної складової банку як елементу стратегічного менеджменту. Ці аспекти також включають репутаційні ризики та втрати від недоотримання клієнтів та їхньої лояльності, вираженої в оборотних коштах.

Введемо поняття граничного заміщення ресурсів комерційного банку в разі кібератак та завданої ними шкоди. Цей підхід вказуватиме на еластичність грошових потоків у рамках забезпечення супротиву кібератакам, які дестабілізують фінансовий стан комерційних банків, та об'єднує перехідні втрати та компенсаторні заходи. Зобразимо ці точки взаємодії на рис. 1, виділивши зони допустимого компоненту та нереалістичного сценарію.

Відповідно до графіку можемо охарактеризувати ступінь залежності від обсягу портфелів банку, його прибутковості та очікуваних максимальних втрат від кібератак у контексті виконання своїх зобов'язань.

Тим самим можемо виділити поняття еластичності заміщення втрачених коштів від кібератак як здатність банку нівелювати загрози на компенсаційній основі за дотримання адекватного рівня платіжного балансу фінансової установи та виконання своїх поточних зобов'язань.

Рух грошових потоків банку можемо охарактеризувати як три вектори розподілу за трьома прогнозами, такими як позитивний, негативний та позитивно-негативний. Розглянемо ці сценарії розвитку у табл. 1.

Розглянемо формування еластичності грошових потоків банку за стабільних загальних видатків та нормального значення видатків по кіберзагрозам згідно з очікуваними сценаріями. Цей показник обчислюється як зважена функція граничних потенціалів незалежних змінних та індукує обсяг компенсаторних втрат на кіберзлочинність комерційним банком.

Якщо обсяг втрат активів банку збільшився більше ніж на 5% відношення до загального рівня, то компенсаторні заходи мають бути збільшені на 1,3246 порівняно з видатками для ефективного розподілу грошових потоків банку та хеджування подібних ризиків у майбутньому [1].

$$E_i = \frac{x_i}{Y} \cdot \frac{\partial Y}{\partial x_i} = \frac{\partial Y}{\partial x_i} : \frac{Y}{x_i}, \qquad (1)$$

де часткова похідна $\frac{\partial Y}{\partial x_i}$ становить граничну ефективність протидії кібератакам на фінансову систему комерційних банків;

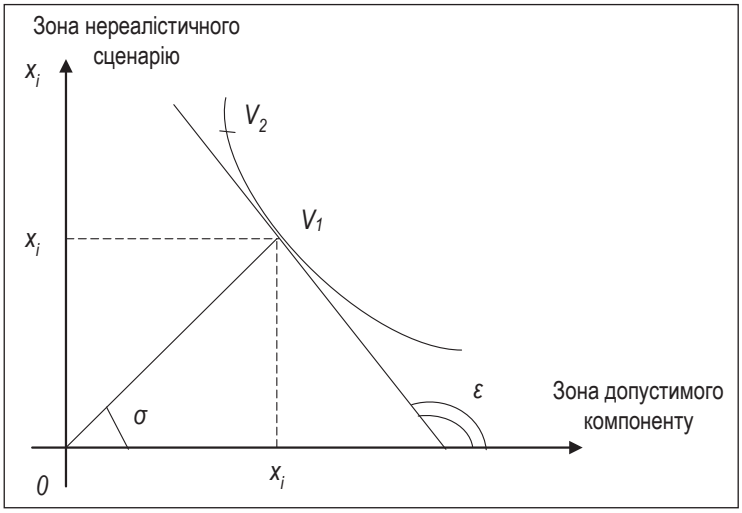

Рис. 1. Еластичність грошових потоків у рамках забезпечення супротиву кібератакам [2; 8]

$\frac{Y}{x_i}$ – це середнє значення ефективності протидії кіберзлочинам;

E_i – індикатор впливу на граничну ефективність захисту інформації під час кібератак.

Показники фінансового заміщення від кібератак на банківську систему характеризуються змінними складними до прогнозування та моделювання. Розглянемо вихідні значення у табл. 2 в рамках еластичності фінансового заміщення від рівня кібератак.

Завдяки індикаторам еластичності компенсаторних видатків, що вказані у табл. 3, можемо зробити висновки щодо стану фінансової системи комерційного банку під час регулювання втрат від кібератак. Розподілимо ці показники під час дослідження еластичності компенсаторних видатків банку для врегулювання втрат по кібератакам на різні рівні у табл. 3.

Таблиця 1

Сценарії розвитку руху грошових потоків

Позитивний	Негативний	Позитивно-негативний
Прискорений обіг коштів суб'єктів господарювання – клієнтів банку в умовах забезпеченої діяльності на відкритому ринку. У разі настання критичних ситуацій приймаються рішення компенсаторного характеру, на які спираються очікування із зовнішнього середовища.	Втрата дієздатності банку у вигляді блокування функціоналу операційного дня чи платіжної системи у контексті неможливості заміщення втрат від операційної діяльності та відновлення клієнтських збитків.	Двояка ситуація розвитку подій банку, коли фактичні втрати банку наносяться опосередковано відповідно до інституційних обмежень та охоплення баз даних. Приймаються до розгляду антикризові програми, що не мають змогу вчасно ідентифікувати ризик та переспрямувати потоки.

Джерело: складено автором на основі [8]

Таблиця 2

Фінансове заміщення втрат від рівня кібератак

Рівень	Період		
	Короткостроковий	Середньостроковий	Довгостроковий
Низький	0,1063	0,1086	0,1042
Нижче середнього	0,1814	0,2031	0,2016
Середній	0,3951	0,4719	0,4592
Вище середнього	0,6397	0,7205	0,7506
Високий	1,3214	1,1825	1,1384

Джерело: складено автором на основі [4]

Таблиця 3

Дослідження еластичності компенсаторних видатків банку для врегулювання втрат по кібератакам

Рівень еластичності	Період		
	Короткострокові	Середньострокові	Довгострокові
Низький	6,49	5,94	5,82
Нижче середнього	11,57	10,13	10,07
Середній	12,33	12,18	11,94
Вище середнього	15,42	15,06	14,83
Високий	17,91	17,54	16,99
Дуже високий	20,07	19,86	19,58

Джерело: складено автором на основі [3]

Таблиця 4

Детермінація граничної норми заміщення ресурсів у рамках кібератак

Рівень	Період		
	Короткостроковий	Середньостроковий	Довгостроковий
Низький	3,561	3.592	3,769
Середній	6,543	5,894	5,481
Високий	8,464	9,216	8,692
Загальний	18,5	18,7	17,9

Джерело: складено автором на основі [7]

За допомогою показників, наведених у табл. 3, комерційні установи можуть легко орієнтуватися щодо еластичності видатків для регулювання наслідків скоєних злочинів на фінансову систему. Усі показники поділені за рівнями та періодами часу, що, беззаперечно, дасть можливість вдало підбирати та вдосконалювати стратегії протидії атакам.

У ході дослідження фінансового заміщення ресурсів від кіберзлочинів на фінансову систему комерційних установ встановлено граничну норму, за якої банківська система показала добрий результат заміщення своїх втрат від кібератак. Звернемо увагу на табл. 4, де встановлено граничну норму заміщення ресурсів у рамках кібератак на банківську систему.

Обчислення граничної норми заміщення ресурсів в компенсаторних рамках під час кібератак будемо обчислювати за диференційованим підходом, який задовольнятиме умови обслуговування для ошуканих клієнтів та таких, які понесли несанкціоновані втрати з власних рахунків.

Введення показників адекватності щодо потенційної еластичності відшкодування банком клієнтських втрат перевіряється диференційованим підходом та гетероскедастичними спостереженнями, оцінюванням відмінностей стандартних помилок та припущень у ході побудови системи захисту інформаційно-технічного забезпечення банку.

Перевірка значущості понять еластичності грошових потоків комерційних банків під час кібератак відбувається за рахунок точок довірчих інтервалів

та автокореляції за факторами, які можливі в період неочікуваних сценаріїв розвитку подій.

Висування припущень щодо інформаційно-технічного забезпечення банків є необ'єктивним загалом через високу неочікуваність процесу інтеграції зовнішнього середовища та стрес-факторів. Таким чином, заміщення залишається найбільш ефективним фінансовим інструментом в кризових ситуаціях в інформаційному полі банківських установ, а розподіл потоків банку за нормалізованим алгоритмом покращить платіжний баланс банку, забезпечивши високий рівень ресурсів та резервного фонду в разі кіберзагроз [2; 5].

Позитивним аспектом залишається те, що методичні підходи до фінансового заміщення та еластичності протидії кібератакам виконують функцію відносного компенсатора та стабілізатора для фінансової установи в умовах кіберзагроз.

Висновки. У статті проведено розгляд та аналіз методичних підходів до фінансового заміщення, еластичності та захищеності банків в рамках забезпечення протидії кібератакам на комерційні структури. Встановлено, що рівень фінансового заміщення за високого рівня кібератак складає максимальне значення 1,3211 та рекомендований до покриття у додаткових 32% бюджетів на покращення інформаційно-технічних заходів. Проаналізовано найбільш ефективні моделі заміщення втрат ресурсів, еластичності грошових потоків.

Досліджено, що заміщення є одним з найефективніших стабілізаторів роботи комерційних банків під час кризових положень та значно зменшує ризики фінансової діяльності.

Зображено індикатори граничної норми заміщення ресурсів за різні періоди часу, які за короткостроковий період становлять 18,5, середньостроковий період – 18,7, довгостроковий період – 17,9. Також розглянуто формування еластичності грошових потоків як ефективний спосіб ефективного супротиву кібератакам комерційного банку, де з'ясовано рівень залежності від обсягу портфелів комерційного банку, його прибутковості та максимальних втрат. Представлено набір математичних інструментів, які включають головні показники скорочення ризиків та фінансових втрат клієнтів.

Список використаних джерел:

1. Болгар Т. Проблеми процесу прозорості саморозкриття банківської інформації. Проблеми і перспективи розвитку банківської системи України. 2011. Вип. 33. С. 15–21.
2. Губаренко А., Куценко О., Пастухова О., Швирков О. Дослідження інформаційної прозорості банків України в 2009 році: зростання прозорості на фоні падіння довіри інвесторів. Спільне дослідження Standard&Poor's та Агентства фінансових ініціатив. URL: http://www.finrep.kiev.ua/download/td_ukr_banks_2009_ua.pdf.
3. Домарев В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ООО «Тид дс», 2002. 688 с.
4. Мігус І., Дудченко Н. Транспарентність банку як складова механізму забезпечення його економічної безпеки. Бізнес-Інформ. 2013. № 10. С. 322–327.
5. Мельник К. Транспарентність як необхідна умова забезпечення ефективності системи комунікацій центрального банку. Проблеми і перспективи розвитку банківської системи України. 2010. Вип. 29. С. 23–29.
6. Чуб О. Транспарентність у діяльності ділових та центральних банків у глобальному просторі. Економіка і регіон. 2012. № 1(32). С. 81–85.
7. Іванишин С. Менеджмент безпеки ІТ комплексної автоматизації у територіально рознесених відділеннях банку. Інформаційна безпека. 2013. № 2. С. 42–47.
8. Жабинець О. Захист інформації та інформаційна безпека страхових компаній. Економічний часопис – XXI. 2014. № 7–8(2). С. 32–35.