Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України від 11.07.2019 № 975)
www. economy.nayka.com.ua | № 10, 2020 | 29.10.2020 р.

DOI: 10.32702/2307-2105-2020.10.50

УДК 336.717

О. А. Криклій,
к. е. н., доцент, доцент кафедри фінансів, банківської справи та страхування,
Навчально-науковий інститут бізнес-технологій
«УАБС» Сумського державного університету (м. Суми)
ORCID ID: 0000-0002-4825-3950

ТЕОРІЯ ТА ПРАКТИКА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ БАНКІВ

O. Kryklii
PhD in Economics, Associate Professor, Associate Professor of the Department of Finance, Banking and Insurance, Scientific-Educational Institute of Business Technologies «UABS» of Sumy State University (Sumy)

THEORY AND PRACTICE OF ENSURING CYBER-RESILIENCE OF BANKS

У статті доведено важливість формування концепції забезпечення 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. Автором на основі узагальнення досліджень з цієї тематики уточнено зміст поняття "кіберстійкість банку" та визначено його сутнісні характеристики за якісним та кількісним підходами. В статті проведено дослідження теоретичних підходів до забезпечення кіберстійкості банків та на цій основі розроблено модель механізму забезпечення кіберстійкості, адекватну сучасному стану та умовам, в яких функціонують банки України. За результатами дослідження визначено, що ефективне функціонування механізму забезпечення кіберстійкості потребує відповідного організаційного забезпечення, зокрема створення Центра кіберстійкості банку.

The article proves the importance of forming the concept of ensuring the cyber resilience of banks at the present stage of development of the country's digital economy in the transition to the sixth technological mode and the associated use of industry 4.0 technologies, such as artificial intelligence, «cloud» and «foggy» computing, IoT / IIoT, Big Data, Blockchain, VR / AR. This leads to a significant complication of the cyber threat landscape, an increase in the number of cyberattacks with a significant increase in the negative financial and non-financial consequences that cyberattacks have on the banking system and the economy as a whole. The author, based on the generalization of research on this topic, clarified the content of the concept of "cyber resilience of a bank". Its essential characteristics were determined in the context of qualitative and quantitative approaches. The article studies theoretical approaches to ensuring the cyber resilience of banks, which made it possible to develop a conceptual model of the mechanism for ensuring cyber resilience, adequate to the current state and conditions in which the banks of Ukraine operate. The developed mechanism for ensuring cyber resilience allows for: 1) the formalization of the landscape of real and potential cyber threats; 2) ensures the consistency of mechanisms and tools

for countering them, adapting and/or recovering from cyber incidents; 3) allows not only to adequately respond to existing cyber threats but also to identify negative factors that can lead to the emergence and implementation of new cyber threats and cyber-attacks. According to the results of the study, it was found that the effective functioning of the mechanism for ensuring the cyber resilience of the bank requires appropriate organizational support. For this, the author substantiated the need to create a Bank Cyber Resilience Center. It should include representatives from the departments responsible for banking business continuity, cybersecurity, cyber risk management and IT quality. This will allow obtaining a synergistic effect by creating a single interconnected process-based model, including metrics of the bank's cyber resilience level and KPIs, as well as tools for monitoring, controlling and resisting external and internal cyber threats, adaptation and/or recovery after them.

Ключові слова: *банк; кіберстійкість банку; кіберзагрози; механізм забезпечення кіберстійкості банку.*

Key words: *bank; cyber-resilience of bank; cyber threats; mechanism of ensuring cyber-resilience of banks.*

Постановка проблеми. 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 [1].

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 який постійно трансформується та оновлюється.

Так, в останньому Звіті про глобальні ризики Всесвітнього економічного форуму кібератаки включені до складу основних ризиків, з якими світ зіткнеться в наступні десять років [2]. У Звіті Accenture State of Cyber Resilience (Accenture) за 2019 рік зазначено, що протягом останніх п'яти років кількість порушень кібербезпеки зросла більш ніж на 65 % [3]. У результаті розвитку цифрової інфраструктури, за оцінками експертів, негативні фінансові наслідки від реалізації кіберзагроз зростуть з 3 трлн доларів США до більше ніж 5 трлн доларів США у 2024 році [4].

Найбільша кількість кібератак, згідно з аналітичними даними, відбувається і буде відбуватись у фінансовому секторі з постійним збільшенням кількості клієнтів, що зазнаватимуть втрат від реалізації кіберзагроз. У [5] шляхом проведення актуарних розрахунків визначено, що сукупні збитки від кібератак на 7947 банків у світі складають 97 млрд доларів на рік (9 % чистого прибутку), а вартість ризику (VaR) коливається від 147 до 201 млрд доларів (14 % - 19 % від чистого прибутку). Крім прямих фінансових втрат, наслідки кібератак мають різноманітні негативні прояви: репутаційні (наприклад, втрата ключових клієнтів та персоналу, знецінення банківського бренду); соціальні (наприклад, порушення повсякденного життя споживачів банківських послуг через наслідки кібератак, наприклад втрату коштів з банківського рахунка, негативне сприйняття споживачами банківських послуг цифрових технологій); фізичні (наприклад, пошкодження банківської інфраструктури).

Зважаючи на це, банки мають формувати комплекс заходів, інструментів та механізмів для забезпечення кіберстійкості як здатності протистояти зовнішнім та внутрішнім загрозам, спричинених кіберризиками, адаптуватися до них та / або відновлюватися після них.

Аналіз останніх досліджень і публікацій. Дослідження кіберстійкості банків є відносно новим напрямом у науковій літературі, як вітчизняній, так і закордонній, а системні дослідження в цій сфері практично відсутні.

Ґрунтовне дослідження концепції кіберстійкості фінансових посередників зроблено Б. Дюпоном [6]. Ним обґрунтовується необхідність забезпечення кіберстійкості в фінансовому секторі, систематизуються типи загроз та різноманітні прояви їх негативного впливу на діяльність фінансових посередників. На підставі цього автор зробив висновок про те, що базова парадигма «запобігати та захищати» є неадекватною, і що для забезпечення ефективного функціонування фінансових посередників слід орієнтуватись на активне забезпечення кіберстійкості. Також автором досліджується еволюція концепції «стійкість», що дало йому змогу визначити поняття «кіберстійкість» та виокремити п'ять основних її параметрів: динамічний, мережевий, практичний, адаптивний та заперечуваний. Вченим систематизовано інституційні підходи, що використовуються для підвищення кіберстійкості в фінансовому секторі: фінансові посередники здійснюють просування кіберстійкості як майбутнього кібербезпеки; органи стандартизації включають кіберстійкість до

стандартів кібербезпеки; регуляторні органи розробляють широкий спектр інструментів відповідності, спрямованих на підвищення кіберстійкості.

Висновки Б. Дюпона щодо неефективності базової парадигми кіберстійкості «запобігати та захищати» підтверджено висновками, наведеними у звіті Accenture за 2019 рік. За результатами опитування виявлено дві окремі групи фінансових посередників, що мають значні відмінності у показниках кіберстійкості: група лідерів з високим рівнем кіберстійкості (15 % фінансових посередників) та група наслідувачів (75 % фінансових посередників) з середнім рівнем кіберстійкості. Індикатором для виділення групи лідерів у сфері забезпечення кіберстійкості є швидкість, з якою останні виявляють та усувають кіберзагрози, перш ніж буде завдано значних фінансових та нефінансових втрат. Ці фінансові посередники виявляють аномалії, ініціюють розслідування та оперативно усувають загрозу. Решта 75% фінансових посередників, навпаки, надлишково витрачають кошти на оборону від кіберзагроз та занижують витрати та час на створення можливостей виявлення та реагування на них [3].

Важливі висновки щодо необхідності забезпечення кіберстійкості індустрії 4.0 зроблені С. Петренком у [8]. Він визначив, що якщо «…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 %).

При цьому доведено наявність значних фінансових переваг саме в разі реалізації активної стратегії забезпечення кіберстійкості. Згідно з результатами дослідження Accenture за 2019 рік [3], середні втрати від реалізації одного кіберінцидента становлять 380 тис. доларів США, при цьому фінансові посередники-лідери можуть знизити ці втрати, в середньому, до 72 % (273 тис. доларів економії на одне порушення). З огляду на те, що в середньому щорічно відбувається 22 інциденти, це становить 6 млн доларів потенційної економії.

Т. Шугунов, А. Жуков, Ф. Хочуєва у [7] визначили основні проблеми забезпечення кібербезпеки банківського сектора Російської Федерації у правовому та методологічному аспектах. Також ними проведеного поглиблений аналіз стану системи забезпечення кіберстійкості кредитно-фінансової системи в умовах становлення та розвитку цифрової економіки.

Значний внесок у визначення практичних аспектів забезпечення кіберстійкості банків зроблено міжнародними фінансовими організаціями, органами банківського регулювання та нагляду. У [9] визначено, що більшість наглядових органів використовують раніше розроблені національні або міжнародні стандарти, а саме: рамки кібербезпеки Національного інституту стандартів і технологій США (NIST), серію стандартів ISO 27000 та керівництво CPMI-IOSCO 2016 (Committee on Payments and Market Infrastructures- International Organisation of Securities Commissions) для забезпечення кіберстійкості інфраструктури фінансового ринку.

Групою Світового банку у відповідь на кіберзагрози, рівень яких постійно зростає, підготовлено збірник нормативних документів, в якому узагальнюються наявні нормативні та наглядові практики, включаючи закони, постанови, керівні принципи та інші важливі документи з кібербезпеки для фінансового сектора [10] та документ про регулювання й нагляд кібербезпеки фінансового сектора [11].

Європейський центральний банк (ЄЦБ) у 2018 році опублікував рекомендаційний документ «Очікування щодо нагляду за кіберстійкістю» (CROE) [12], що наразі застосовується практично всіма операторами фінансової інфраструктури в Європі. Світовий банк офіційно прийняв CROE, щоб забезпечити кіберстійкість інфраструктур фінансових ринків та сприяти глобальної гармонізації в рамках Глобальної ініціативи фінансової доступності (FIGI) [13].

Як доповнення до CROE, ЄЦБ розробив стандарт для перевірки стійкості фінансового сектора до кібератак шляхом симуляції їх наслідків на критичні системи в банківській системі Європейського союзу (Threat Intelligence-based Ethical Red Teaming, TIBER-EU). Він передбачає, що за допомогою «етичного злому» так звана «червона команда» допомагає оцінити здатність фінансової установи протистояти кібератаці [14].

Зважаючи на початковий етап наукових розробок, присвячених забезпеченню кіберстійкості банків на сучасному етапі розвитку цифрової економіки, подальшого розвитку потребує комплекс питань щодо теоретико-методологічного підґрунтя та практичного впровадження механізму забезпечення кіберстійкості, що дозволяє здійснити формалізацію ландшафту реальних та потенційних кіберзагроз; забезпечує узгодженість механізмів та інструментів для протистояння зовнішнім та внутрішнім загрозам, спричинених кібератаками, адаптації та / або відновлення після них; дозволяє не лише адекватно реагувати на наявні кіберзагрози, а й ідентифікувати негативні фактори, що можуть призвести до виникнення та реалізації нових кіберзагроз та кібератак.

Метою статті є визначення концептуальних засад формування механізму забезпечення кіберстійкості, впровадження якого забезпечуватиме ефективне функціонування банків в умовах зростання та ускладнення ландшафту кіберзагроз та підвищення на цій основі кіберстійкості банківської системи в цілому.

Виклад основного матеріалу. Особливість кіберстійкості банку в механізмі її забезпечення полягає в тому, що, з одного боку, вона є об’єктом застосування регуляторних та управлінських впливів (керівна підсистема), з іншого – є системним параметром функціонування, без якої банк не матиме змогу продовжувати виконувати свою місію та здійснювати безперервну діяльність. Відповідно до цього, показники кіберстійкості мають включатись до загальної стратегії банку та узгоджуватись з цільовими кількісними та якісними параметрами стратегічних планів.

При розгляді питання щодо сутності поняття «кіберстійкість банку» як керівної підсистеми застосовуються якісний та кількісний підходи.

За результатами проведеного дослідження з'ясовано, що у визначенні поняття «кіберстійкість» за якісним підходом спостерігається неоднозначність трактувань, що демонструє таблиця 1.

Таблиця 1.
Підходи до трактування поняття «кіберстійкість»

№	Джерело	Визначення
1	Європейський центральний банк [12]	здатність продовжувати виконувати свою місію, прогнозуючи кіберзагрози та інші відповідні зміни в операційному середовищі та адаптуючись до них, а також витримуючи, стримуючи кіберінциденти та швидко відновлюючись після них.
2	Комітет з питань платежів та ринкової інфраструктури [15]	здатність прогнозувати, протистояти, стримувати та швидко відновлюватися після кібератак
3	Д. Бодо, Р. Граубарт [16]	здатність підтримувати свої основні функції і цілісність при впливі потенційних атак з загрозою її інформаційної безпеки. Кіберстійка організація – … здатна запобігати, виявляти, стримувати кібератаки та відновлюватися після них, мінімізуючи вразливість до атаки та її вплив на бізнес
4	Комісія з цінних паперів та інвестицій Австралії [17]	здатність підготуватися до кібератак, відреагувати на них і відновитися після них. .. це більше, ніж просто запобігання кібератаки або реагування на неї – вона також бере до уваги здатність функціонувати під час такої події, а також адаптуватися та відновлюватися після неї
5	Кіберлексикон, Рада з фінансової стабільності [18]	здатність продовжувати виконувати свою місію, передбачаючи та пристосовуючись до кіберзагроз та інших відповідних змін в операційному середовищі, витримуючи, стримуючи та швидко відновлюючись від кіберінцидентів.

Джерело: систематизовано автором

Результати дослідження щодо визначення сутності поняття «кіберстійкість банку», враховуючи необхідність її розгляду в якісному та оцінювальному розрізах, систематизовано та схематично зображено на рисунку 1.

На основі узагальнення напрацювань щодо визначення сутності поняття «кіберстійкість» пропонуємо визначати кіберстійкість банку за якісним підходом як здатність безперебійно виконувати покладені на нього функції, протистояти та / або адаптуватись до дії внутрішніх та зовнішніх кіберзагроз за умови максимальної ефективності та мінімальних кіберризиків шляхом прогнозування, ідентифікації, попередження кібератак та відновлення після них.

Рис. 1. Підходи до визначення сутності поняття «кіберстійкість банку»
Джерело: розроблено автором

Відповідно до оцінювального підходу пропонуємо розглядати кіберстійкість у розрізі якісного та кількісного оцінювання.

Якісне оцінювання передбачає визначення відповідності та якості або ступеня застосування принципів, механізмів та інструментів забезпечення кіберстійкості в банку.

Кількісне оцінювання кіберстійкості банку здійснюється за допомогою аналізу різних наборів показників, що дають змогу оцінити параметри кіберстійкості: фізичні, інформаційні / технічні, управлінські, організаційні, галузеві, регіональні, національні або транснаціональні. При цьому в контексті кількісного оцінювання кіберстійкості банку важливим є визначення її видів за рівнями, а саме:

- нормальний рівень кіберстійкості банку, що характеризується цільовим рівнем всіх параметрів кіберстійкості, контрольованим рівнем кіберризиків, безперервністю та стійкістю банківського бізнесу;
- низький рівень кіберстійкості банку, що характеризується стійким погіршенням всіх параметрів кіберстійкості, зростанням рівня кіберризиків, зростанням термінів, необхідних для відновлення безперервності банківського бізнесу;
- критичний рівень кіберстійкості банку, що характеризується зниженням параметрів кіберстійкості до критично низького рівня, невиконанням державних регуляторних вимог, значними порушеннями в безперебійності банківського бізнесу.

За результатами вивчення теоретичних підходів до забезпечення кіберстійкості банків ми розробили модель механізму забезпечення кіберстійкості, адекватну сучасному стану та умовам, в яких працюють банки України, у наочному вигляді представлену на рисунку 2.

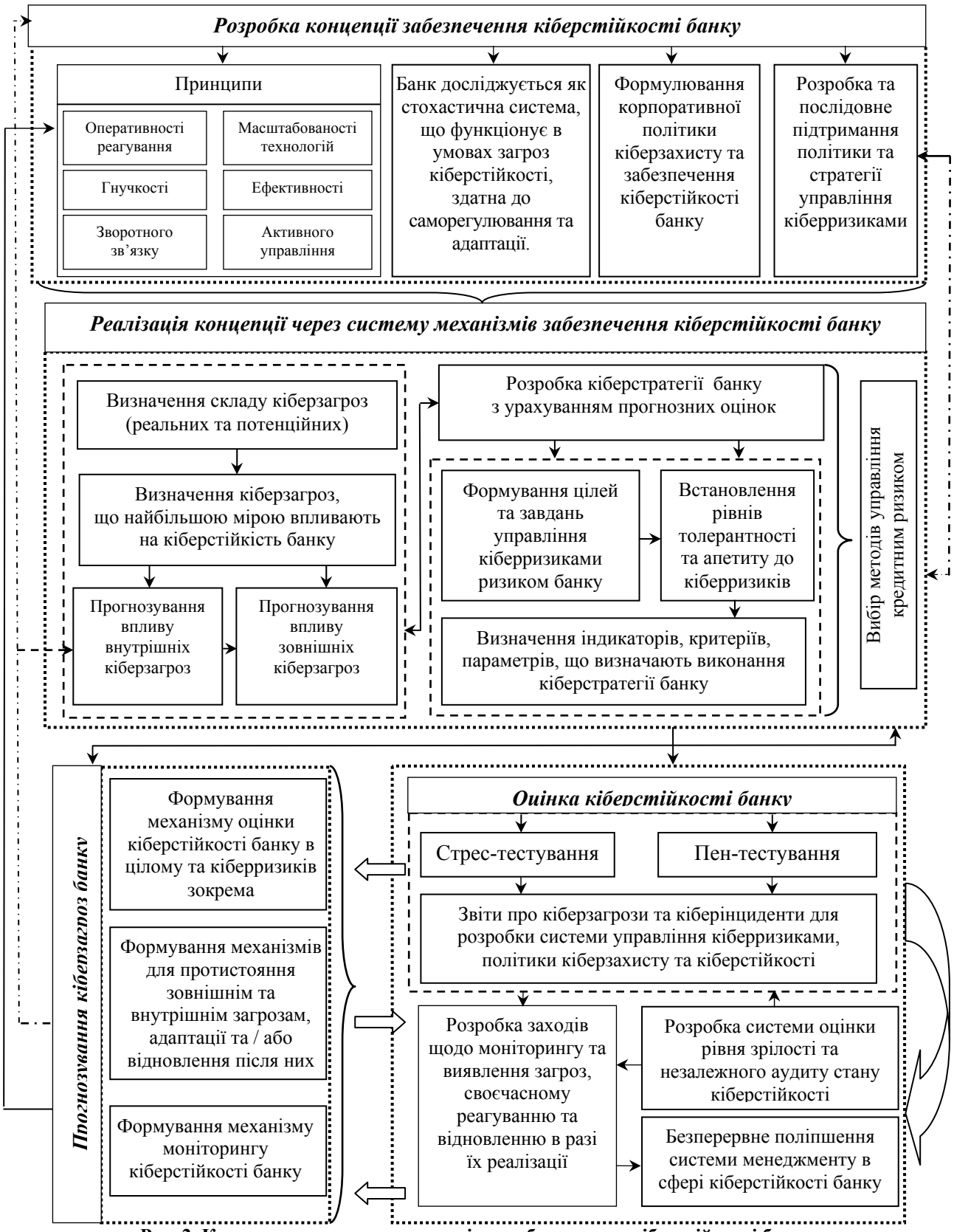

Рис. 2. Концептуальна модель механізму забезпечення кіберстійкості банку

Джерело: розроблено автором

Розроблений механізм забезпечення кіберстійкості банку дозволяє: ідентифікувати ландшафт реальних кіберзагроз та прогнозувати потенційні кіберзагрози; забезпечує узгодженість механізмів та інструментів їх попередження, адаптації та / або відновлення від кібератак; дозволяє не тільки адекватно реагувати на наявні кіберзагрози, а й виявляти негативні фактори, що можуть призвести до появи та реалізації нових кіберзагроз та кібератак.

Ми визначили, що важливим для забезпечення кіберстійкості банку є належне організаційне забезпечення. Воно має поєднати всіх суб'єктів банківського менеджменту, долучених до процесів забезпечення кібербезпеки, управління кіберризиками та безперервності банківського бізнесу. При цьому слід наголосити на тому, що кожен банк обирає таку модель організаційної будови, що найкращим чином відповідає особливостям його діяльності, характеру та обсягу банківських послуг, їх цифровізації, рівню розвитку та структурі інформаційних систем, а також наявним можливостям та потребам у сфері забезпечення кіберстійкості банку та ризик-менеджменту.

За результатами дослідження вважаємо за необхідне створювати в банках спеціалізований Центр кіберстійкості як колегіальний орган з ключовими повноваженнями у цій сфері, до складу якого доцільно включити представників підрозділів, які відповідають за безперервність банківського бізнесу, кібербезпеку, управління кіберризиками та якість ІТ систем. Це дозволить домогтися синергетичного ефекту та об'єднати зусилля всіх суб'єктів банківського менеджменту різних бізнес-напрямків, центрів інфраструктури та забезпечення бізнес-процесів шляхом створення єдиної взаємозалежної процесно-орієнтованої моделі, включаючи метрики кіберстійкості та KPI, а також інструменти для моніторингу, контролю та протидії зовнішнім та внутрішнім кіберзагрозам, адаптації та / або відновлення після кібератак.

До функцій цього спеціалізованого колегіального підрозділу доцільно віднести:

- інтеграцію процесів безперервності банківського бізнесу, якості ІТ, управління кіберризиками та кібербезпеки в єдиний механізм забезпечення кіберстійкості;
- нормативне, методологічне та інформаційне забезпечення механізму кіберстійкості банку;
- розробка звітних форм та створення бази даних щодо кіберінцидентів, їх фінансових та нефінансових наслідків;
- розробка багатоетапних та багатофакторних сценаріїв реагування на кіберінциденти;
- координація підрозділів банку в сфері реагування на кіберінциденти, прийняття рішення про ескалацію реагування на кіберінциденти на рівень топ-менеджменту банку;
- формування інструментів прогнозування, ідентифікації, попередження кібератак та відновлення після них;
- розробка планів розвитку механізму забезпечення кіберстійкості, моніторинг та аудит їх виконання.

Отже, банкам України необхідно сформувати комплекс заходів щодо формування механізму забезпечення кіберстійкості та його належного організаційного забезпечення.

Висновки. Кіберстійкість банку доцільно розглядати за якісним та оцінювальним підходами. За якісним підходом кіберстійкість банку – це здатність безперебійно виконувати покладені на нього функції, протистояти та / або адаптуватись до дії внутрішніх та зовнішніх кіберзагроз за умови максимальної ефективності та мінімальних кіберризиків шляхом прогнозування, ідентифікації, попередження кібератак та відновлення після них.

Відповідно до оцінювального підходу кіберстійкість запропоновано розглядати в розрізі якісного (визначення відповідності та якості або ступеня застосування принципів, механізмів та інструментів забезпечення кіберстійкості в банку) та кількісного (формування наборів показників, що дають змогу оцінити параметри кіберстійкості: фізичні, інформаційні / технічні, управлінські, організаційні, галузеві, регіональні, національні або транснаціональні) оцінювань.

Запропонована автором модель механізму забезпечення кіберстійкості банку передбачає розробку концепції забезпечення кіберстійкості банку та її реалізацію через систему механізмів оцінки, моніторингу, контроля та аудита кіберстійкості, адаптації та / або відновлення після реалізації кіберзагроз.

Встановлено, що важливим для забезпечення кіберстійкості банку є належне організаційне забезпечення, зокрема створення спеціалізованого Центру кіберстійкості як ключового колегіального органу в цій сфері.

Список літератури.

1. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: затверджений постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 URL: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text (дата звернення: 23.09.2020).
2. The Global Risks Report 2020. *World Economic Forum.* 2020. URL:http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата звернення: 23.09.2020).
3. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. *Accenture*. 2019. URL: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (дата звернення: 23.09.2020).
4. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate / I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, D. Upton. *Journal of Cybersecurity.* 2018. Volume 4, Issue 1. URL: https://doi.org/10.1093/cybsec/tyy006 (дата звернення: 23.09.2020).
5. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*. 2018. WP/18/143. P. 28. URL: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 (дата звернення: 23.09.2020).
6. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. Volume 5, Issue 1. URL: https://doi.org/10.1093/cybsec/tyz013 (дата звернення: 23.09.2020).

7. Шугунов Т., Жуков А., Хочуева Ф. Проблемы обеспечения киберустойчивости банковской системы Российской Федерации: правовой и методологический аспекты. *Пробелы в российском законодательстве*. 2019.№ 6: С. 250-253.

8. 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.

9. Cyber-resilience: Range of practices. *Basel Committee on Banking Supervision*. 2018. URL: https://www.bis.org/bcbs/publ/d454.pdf (дата звернення: 23.09.2020).

10. Financial Sector's Cybersecurity: A Regulatory Digest. *The World Bank Group.* 2017. URL: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf (дата звернення: 23.09.2020).

11. Almansi A. A. Financial sector's cybersecurity : regulations and supervision. FCI Insight Washington, D.C. World Bank Group. 2018. 38 P.

12. Cyber resilience oversight expectations for financial market infrastructures. *European Central Bank*. 2018. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (дата звернення:23.09.2020).

13. World Bank adopts ECB's cyber resilience oversight expectations. *European Central Bank*. 2020. URL: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200106.en.html (дата звернення: 23.09.2020).

14. TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. *European Central Bank*. 2018. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (дата звернення: 23.09.2020).

15. Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO. *Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions*. 2016. URL:https://www.bis.org/cpmi/publ/d146.pdf. (дата звернення: 23.09.2020).

16. Bodeau D., Graubart R. Cyber Resiliency Design Principles. Mitre technical report. 2017. 98 P. URL: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf (дата звернення: 23.09.2020).

17. Cyber resilience: Health check. *Australian Securities and Investments Commission*. 2015. URL: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf (дата звернення: 28.09.2020).

18. Cyber Lexicon. *Financial Stability Board*. 2018. URL: https://www.fsb.org/wp-content/uploads/P121118-1.pdf (дата звернення: 23.09.2020).

References.

1. Cabinet of Ministers of Ukraine (2016), " The order of formation of the list of information and telecommunication systems of objects of a critical infrastructure of the state", available at: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text (Accessed 23 September 2020).

2. World Economic Forum (2020), "The Global Risks Report 2020", available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (Accessed: 23 September 2020).

3. Accenture (2019), "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (Accessed: 23 September 2020).

4. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., Upton, D. (2018), "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", Journal of Cybersecurity [Online], Volume 4, Issue 1. available at: https://doi.org/10.1093/cybsec/tyy006 (Accessed: 23 September 2020).

5. Bouveret, A. (2018), "Cyber risk for the financial sector: A framework for quantitative assessment", *IMF Working Paper*, WP/18/143, available at: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 (Accessed 23 September 2020).

6. Dupont, B. (2019), "The cyber-resilience of financial institutions: significance and applicability", *Journal of Cybersecurity*, Volume 5, Issue 1, available at: https://doi.org/10.1093/cybsec/tyz013 (Accessed 23 September 2020).

7. Shugunov T., Zhukov A., and Khochueva F. (2019) "Problems of ensuring cyber resilience of the banking system of the Russian Federation: legal and methodological aspects". *Probely v rossijskom zakonodatel'stve*, vol.6, pp. 250-253.

8. Petrenko, S. (2018), "Cyber Resilience Industry 4.0", *Zbirka dopovidej na Mizhnarodnij ekonomichnij konferentsii* [Conference Proceedings of the International Economic Conference], Mizhnarodna Ekonomichna konferentsiya [International economic conference], Innopolis, Russia, pp. 370-381.

9. Basel Committee on Banking Supervision (2018), "Cyber-resilience: Range of practices", available at: https://www.bis.org/bcbs/publ/d454.pdf (Accessed: 23 September 2020).

10. The World Bank Group (2017), "Financial Sector's Cybersecurity: A Regulatory Digest", available at: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf (Accessed: 23 September 2020).

11. Almansi, A. A. (2018), "Financial sector's cybersecurity : regulations and supervision". *FCI Insight Washington, D.C. World Bank Group*, 2018, 38 P.

12. European Central Bank (2018), “Cyber resilience oversight expectations for financial market infrastructures”, available at: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (Accessed: 23 September 2020).
13. European Central Bank (2020), “World Bank adopts ECB’s cyber resilience oversight expectations”, available at: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200106.en.html (Accessed: 23 September 2020).
14. European Central Bank (2018), “TIBER-EU FRAMEWORK. How to implement the European framework for Threat Intelligence-based Ethical Red Teaming”, available at: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (Accessed: 23 September 2020).
15. Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions (2016), “Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO”, available at: https://www.bis.org/cpmi/publ/d146.pdf (Accessed: 23 September 2020).
16. Bodeau, D., Graubart, R. (2017), “Cyber Resiliency Design Principles. Mitre technical report”, available at: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf (Accessed: 23 September 2020).
17. Australian Securities and Investments Commission (2015), “Cyber resilience: Health check”, available at: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf (Accessed: 23 September 2020).
18. Financial Stability Board (2018), “Cyber Lexicon”, available at: https://www.fsb.org/wp-content/uploads/P121118-1.pdf (Accessed: 23 September 2020).

Стаття надійшла до редакції 30.09.2020 р.