РОЗДІЛ 11. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФІНАНСОВОГО КІБЕРПРОСТОРУ[1]

WAYS TO ENSURE THE RESILIENCE OF FINANCIAL CYBERSPACE

УДК 330.46
DOI: https://doi.org/10.32843/infrastruct49-61

Гриценко К.Г.
к.т.н., доцент, доцент кафедри економічної кібернетики
Сумський державний університет

Gritsenko Konstantin
Sumy State University

Фінансовий сектор має значний потенціал щодо цифровізації, вплив якої поширюється на весь ландшафт операційних ризиків, головним серед яких є ризик кібершахрайства. У зв'язку з цим актуальною є проблема забезпечення стійкості фінансового кіберпростору до шахрайських дій і, як наслідок, виконання фінансовим сектором покладених на нього функцій у непередбачуваних несприятливих умовах. При цьому надзвичайно важливу роль відіграє організаційне забезпечення. У статті розроблено модель механізму забезпечення кіберстійкості фінансового сектору, яка передбачає моніторинг і координацію фінансових установ, засновані на принципах теорії життєздатних систем. Наведеено модель організаційної побудови системи управління кіберризиками фінансовової установи, яка передбачає захист від кіберризиків на рівні бізнес-підрозділів, рівні підрозділу з управління операційними ризиками та рівні підрозділу внутрішнього аудиту.

Ключові слова: *цифровізація, фінансовий сектор, кіберінцидент, кіберстійкість, організаційне забезпечення, життєздатна система.*

Финансовый сектор имеет значительный потенциал цифровизации, влияние которой распространяется на весь ландшафт операционных рисков, главным среди которых является риск кибермошенничества. В связи с этим актуальной является проблема обеспечения устойчивости финансового киберпространства к мошенническим действиям и, как следствие, выполнения финансовым сектором возложенных на него функций в непредсказуемых неблагоприятных условиях. При этом особенно важную роль играет организационное обеспечение. В статье разработана модель механизма обеспечения киберустойчивости финансового сектора, которая предусматривает мониторинг и координацию финансовых учреждений, основанные на принципах теории жизнеспособных систем. Представлена модель организационного построения системы управления киберрисками финансового учреждения, которая предусматривает защиту от киберрисков на уровне бизнес-подразделений, уровне подразделения по управлению операционными рисками и уровне подразделения внутреннего аудита.

Ключевые слова: *цифровизация, финансовый сектор, киберинцидент, киберустойчивость, организационное обеспечение, жизнеспособная система.*

The financial sector has significant potential for digitization which is most actively implemented by banking institutions. The impact of digitization extends to the entire landscape of operational risks, the main of which is the risk of cyber fraud. The number of cyber incidents in the financial sector is constantly increasing, their consequences lead to significant financial losses, leakage of important information, deterioration of the reputation of financial institutions, loss of people confidence. In this regard, the problem of ensuring the resilience of financial cyberspace to fraud and, consequently, performing financial sector its functions in unforeseen adverse conditions is relevant. In this relation, organizational support plays an extremely important role. There are fundamental principles inherent in organizations that function effectively: manageability, ability to learn, adapt and develop. The article develops a model of the mechanism supporting cyber resilience of the financial sector, which provides for monitoring and coordination of financial institutions based on the principles of the theory of viable systems. Each financial institution independently chooses the model of organizational construction of the cyber risk management system. This takes into account the peculiarities of the financial institution, the level of digitalization of financial services, information infrastructure, as well as the existing opportunities and needs in the field of cyber resilience and cyber risk management. The model of organizational construction of the cyber risk management system of a financial institution is presented in the article, which provides protection against cyber risks at the level of business departments, at the level of the department of operational risk management and at the level of the internal audit department. The department of operational risk management carries out compliance control of business departments. Role of internal audit department is to assess the overall effectiveness of the actions performed by the first and second level of defense. The head of the internal audit department is directly accountable to the member of the supervisory board who heads the audit committee of financial institution.

Key words: *digitalization, financial sector, cyber incident, cyber resilience, organizational support, viable system.*

Постановка проблеми. Цифрова економіка становить значну частину світової економіки і, за оцінками Конференції ООН із торгівлі та розвитку (UNCTAD), досягне на початку третього десятиріччя XXI століття 15,5% світового ВВП. Фінансовий сектор, більша частина якого припадає на банківський сегмент, має значний потенціал щодо цифровізації, яку найбільш активно впроваджують банківські установи [1]. Насамперед це стосується мобільного банкінгу. Проведене Juniper Research дослідження Digital Banking: Banking-as-a-Service, Open Banking & Digital Transformation 2020–2024 показує, що до 2024 року кількість користувачів цифрового банкінгу досягне 3,6 млрд, що на 54% більше, ніж у 2020 році.

Водночас банки є об'єктами критичної інфраструктури України [2]. Кількість кіберінцидентів у фінансовому секторі постійно збільшується, а їх наслідки призводять до значних фінансових втрат, витоку важливої інформації, погіршення репутації

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи №0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України»

фінансових установ, втрати довіри населення [3]. Вплив цифровізації поширюється на весь ландшафт операційних ризиків, головним серед яких, на думку топ-менеджерів, є ризик кібершахрайства [4]. Майже 80 відсотків фінансових установ впроваджують цифрові технології швидше, ніж забезпечують їх кіберзахист [5]. Як зазначено в роботі [6], до ключових загроз цифрової економіки відносяться несправності IT-систем, що спричинені кібератаками, а також недооцінка ризиків, пов'язаних із цифровими технологіями, і, як наслідок, ризик стати жертвою кібершахрайства. Згідно зі звітом про глобальні ризики Всесвітнього економічного форуму кібератаки та кібершахрайства входять до топової п'ятірки глобальних ризиків за частотою появи [7]. Тільки в Україні за 9 місяців 2020 року було зафіксовано 1,2 млн кіберінцидентів, серед яких – поширення шкідливого програмного забезпечення, фішинг, DDOS-атаки [8].

Цифровізація фінансового сектору збільшує кількість кіберінцидентів, яким не можна повністю запобігти [9]. У зв'язку з цим актуальною є проблема забезпечення кіберстійкості фінансового сектору до шахрайських дій і, як наслідок, виконання фінансовим сектором покладених на нього функцій у непередбачуваних несприятливих умовах.

Аналіз останніх досліджень і публікацій. Окреслена проблема розглядається в наукових працях таких вітчизняних та іноземних учених, як Б. Дюпон (Dupont B.) [9], Ф. Бьорк (Bjorck F.), Дж. Штірна (Stirna J.), М. Хенкель (Henkel M.), Дж. Здравкович (Zdravkovic J.) [10], С. Петренко [11], Т. Шугунов, А. Жуков, Ф. Хочуєва [12], О. Криклій [13], К. Хаускен (Hausken K.) [14] та інші. Проте питанням забезпечення стійкості фінансового кіберпростору присвячено недостатньо уваги. Це відносно новий науковий напрям, який потребує подальшого розвитку.

Постановка завдання. Метою статті є вивчення теоретичних засад і пошук шляхів забезпечення стійкості фінансового кіберпростору.

Виклад основного матеріалу дослідження. Як зазначено в роботі [9], цілями кіберстійкості є попередження кіберзагроз, протистояння кібератакам, відновлення (подолання шкоди, заподіяної кіберінцидентами) та адаптація до кіберризиків. Слід відзначити, що сьогодні у сфері кібербезпеки домінують два міжнародних стандарти, які хоч і не декларують кіберстійкість своєю метою, але включають заходи, що можуть бути використані для досягнення цілей кіберстійкості: серія міжнародних стандартів ISO 27000 і Cybersecurity Framework від NIST (Національний інститут стандартів і технологій США). Серія міжнародних стандартів ISO 27000 містить такі заходи, що сприяють кіберстійкості, як [15]: поінформованість про інформаційну безпеку, освіта та навчання; резервне копіювання інформації; навчання на інцидентах інформаційної безпеки тощо. NIST Cybersecurity Framework описує такі функції кіберзахисту, як ідентифікація, захист, виявлення та відновлення [16]. Постанова Національного банку України «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» № 95 від 28.09.2017 року передбачає впровадження банківськими установами системи управління інформаційною безпекою згідно з Національними стандартами, розробленими на основі міжнародних стандартів серії ISO 27000. Зауважимо, що з 01.07.2020 року в Україні регулятором як ринку банківських фінансових послуг, так і ринків небанківських фінансових послуг є Національний банк України.

У роботі [13] зазначено, що важливим для забезпечення кіберстійкості банківської установи є належне організаційне забезпечення. Воно має поєднати всіх суб'єктів банківського менеджменту, долучених до процесів забезпечення кібербезпеки, управління кіберризиками та безперервності банківського бізнесу. Існують фундаментальні принципи, властиві організаціям, що ефективно функціонують. У середовищі фахівців з організаційного управління добре відома кібернетична модель життєздатної системи VSM (Viable Systems Model), розроблена С. Біром [17]. Принципами VSM є керованість, здатність до навчання, адаптації та розвитку, що відповідають наведеним вище цілям кіберстійкості.

VSM має п'ять базових управлінських функцій (підсистем): операційної діяльності, координації, контролю, розвитку, формування політики. Постулюється принцип: кожна життєздатна система містить у собі життєздатну систему і сама є елементом життєздатної системи. Така самоподібність вважається запорукою життєздатності. Кожній з п'яти підсистем, які включає в себе життєздатна система, повинно бути надано стільки автономії, наскільки це можливо без порушення цілісності системи.

В основу моделі життєздатної системи С. Біра покладено «закон необхідної різноманітності», сформульований Р. Ешбі, який вимагає, щоб набір управлінських впливів був не менш різноманітним, ніж набір можливих станів системи. Згідно з цим законом, управління полягає в такому перетворенні множини станів керованої системи, в результаті якого ймовірності небажаних станів зменшуються, а ймовірності бажаних станів збільшуються. Управління складністю системи здійснюється за допомогою самоорганізації (рис. 1).

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних)

Рис. 1. Система відносин у процесі управління складністю системи відповідно до концепції VSM

Джерело: побудовано автором на основі [17]

комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. У фінансовому секторі кіберризики відносяться до операційних ризиків. Різноманітність середовища більша за різноманітність технологічних операцій бізнес-підрозділів, яка, у свою чергу, перевищує різноманітність керування. У структурі правильно організованої системи відбувається спрямоване звуження різноманітності середовища (аттенюація) з одночасним збільшенням різноманітності управління (підсилення).

Розглянемо побудовану нами з використанням принципів теорії життєздатних систем С. Біра узагальнену модель механізму забезпечення кіберстійкості фінансового сектору, наведену в наочному вигляді на рис. 2.

Підсистема 1 представлена у вигляді фінансової установи, яка здійснює свою діяльність у відповідності з отриманими ліцензіями. Кожна Підсистема 1 виконує свої функції в межах горизонтальної площини, взаємодіючи в кіберпросторі та підкоряючись власній системі управління кіберризиками. Кожна фінансова установа самостійно вибирає модель організаційної побудови системи управління кіберризиками. При цьому враховуються особливості діяльності фінансової установи, рівень цифровізації фінансових послуг, інформаційна інфраструктура, а також наявні можливості та потреби у сфері забезпечення кіберстійкості та управління кіберризиками. Один із можливих варіантів такої моделі наведено на рис. 3.

Першу лінію захисту від кіберризиків утворюють бізнес-підрозділи та підрозділ інформацій-

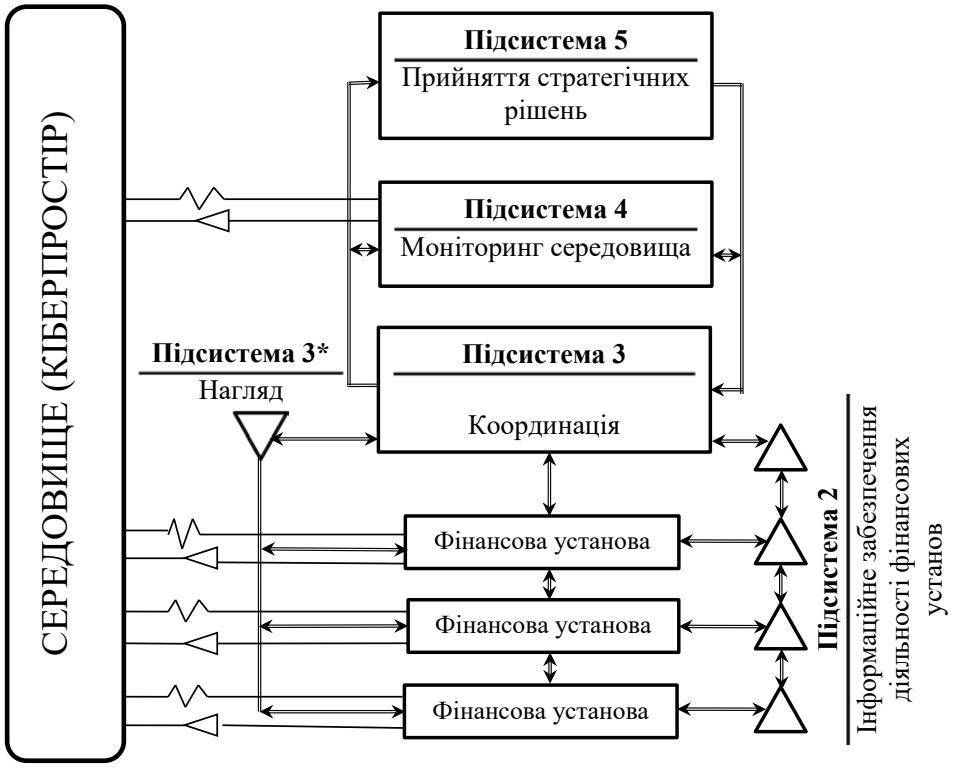

Рис. 2. Модель механізму забезпечення кіберстійкості фінансового сектору

Джерело: побудовано автором на основі [17]

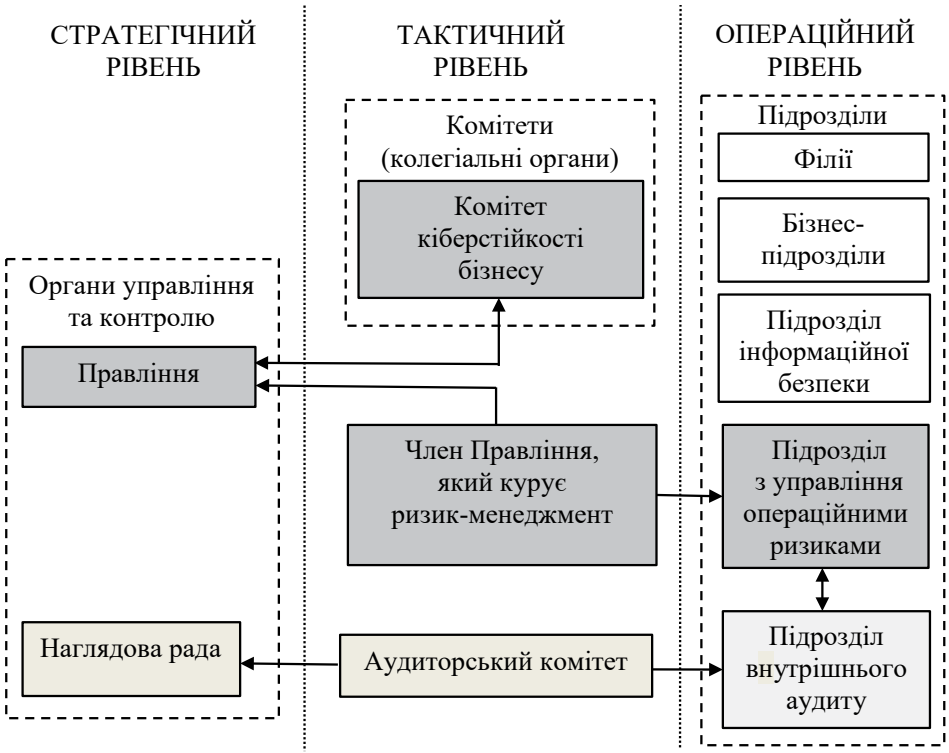

Рис. 3. Модель організаційної побудови системи управління кіберризиками фінансової установи

Джерело: побудовано автором на основі [18; 19]

ної безпеки. Другу лінію захисту утворює підрозділ з управління операційними ризиками, який здійснює комплаєнс-контроль бізнес-підрозділів. Третю лінію захисту утворює підрозділ внутрішнього аудиту, який не бере безпосередньої участі в управлінні кіберризиками. Його роль полягає в оцінці загальної ефективності дій, що виконуються першою та другою лініями захисту. Керівник підрозділу внутрішнього аудиту підзвітний безпосередньо члену наглядової ради, що очолює аудиторський комітет. Комітет кіберстійкості бізнесу є колегіальним органом з ключовими повноваженнями в цій сфері. До його складу доцільно включити членів Правління, які відповідають за безперервність банківського бізнесу, управління кіберризиками та якість інформаційної інфраструктури.

Підсистема 1 сама є життєздатною системою відповідно до рекурсивного характеру моделі життєздатної системи. Вона автономно утримує свої параметри кіберстійкості на цільовому рівні шляхом активного реагування на кіберзагрози. У роботі [13] запропоновано оцінювати кіберстійкість за такими рівнями:

– нормальний рівень кіберстійкості, що характеризується цільовим рівнем всіх параметрів кіберстійкості, контрольованим рівнем кіберризиків, безперервністю та стійкістю бізнесу;

– низький рівень кіберстійкості, що характеризується стійким погіршенням всіх параметрів кіберстійкості, зростанням рівня кіберризиків, зростанням термінів, необхідних для відновлення безперервності бізнесу;

– критичний рівень кіберстійкості, що характеризується зниженням параметрів кіберстійкості до критичного рівня, невиконанням державних регуляторних вимог, значними порушеннями в безперебійності бізнесу.

Мета Підсистеми 2 – запобігання некерованим коливанням, що виникають між різними підсистемами життєздатної системи. Вона забезпечує обмін інформацією між Підсистемами 1 та Підсистемою 3 для контролю і координації діяльності Підсистем 1. У концепції механізму забезпечення кіберстійкості фінансового сектору Підсистема 2 представлена законами, підзаконними актами, постановами Національного банку України та іншими нормативними документами у сфері кібербезпеки, які регулюють діяльність фінансових установ. Функції Підсистеми 2 відносяться до функцій Департаменту безпеки Національного банку України та Управління фінансових та операційних ризиків. Однією з основних функцій Департаменту безпеки є розроблення та реалізація стратегії і політики інформаційної безпеки Національного банку України, впровадження новітніх технологій у частині забезпечення ефективного і цілеспрямованого захисту інформації в інформаційній інфраструктурі Національного банку України та банківської системи України.

Підсистема 3 є системою координації. Вона виконує роль арбітра у разі виникнення нетипових проблем і забезпечує взаємодію з Підсистемами 4 і 5. Підистема 3* здійснює аудит і виявляє неусвідомлені системами 1 проблеми.

Підсистема 4 – система моніторингу внутрішнього та зовнішнього середовища. Функції моніторингу відносяться до функцій Центру кіберзахисту, що входить до складу Департаменту безпеки Національного банку України. Система моніторингу повинна здійснювати оцінку діяльності фінансових установ з погляду кіберстійкості, проведення регулярних сканувань для визначення уразливостей у технологіях і бізнес-процесах фінансових установ, тестування на проникнення. Результати такого моніторингу використовуються під час планування розвитку кіберстійкості фінансового сектору. На нашу думку, доцільним є впровадження на цьому рівні центру моніторингу та реагування на інциденти інформаційної безпеки (Security Operations Center, SOC), що дає змогу централізовано обробляти події інформаційної безпеки з підключених джерел і припиняти можливі кіберінциденти ще до їх виникнення.

Підсистема 5 – система прийняття рішень. Під час ухвалення рішень на цьому рівні використовується інформація про стан автономного управління, що йде нагору від Підсистеми 3, та результати моніторингу, надані Підсистемою 4. Основні функції із прийняття рішень лежать на регуляторі. Згідно із Законами України «Про Національний банк України» та «Про основні засади забезпечення кібербезпеки України», а також Стратегією кібербезпеки України, на Національний банк України покладено завдання із встановлення правил захисту інформації, визначення порядку, вимог і заходів із забезпечення кіберзахисту та інформаційної безпеки в банківській системі України та здійснення контролю за їх виконанням.

Стійкість фінансового кіберпростору забезпечуватиметься шляхом виконання двох основних умов: кіберстійкості Підсистем 1 та існування й ефективній взаємодії Підсистем 2-5.

Висновки з проведеного дослідження. За результатами дослідження виявлено, що цифрова економіка становить значну частину світової економіки, а її стрімкий розвиток безпосередньо впливає на цифровізацію фінансового сектору та, як наслідок, на стійкість фінансового кіберпростору. В цих умовах фінансові установи мають ефективно протидіяти зовнішнім і внутрішнім кіберзагрозам, швидко відновлюватися після кібератак та адаптуватися до кіберризиків. При цьому важливу роль відіграє організаційне забезпечення, що повинно поєднувати суб'єктів менеджменту фінансового сектору, долучених до забезпечення кіберстійкості та безперервності бізнесу. Розглянута автором модель організаційної побудови системи управління кіберризиками фінансової установи передбачає три лінії захисту від кіберризиків (на рівні бізнес-підрозділів, підрозділу з управління операційними ризиками та підрозділу внутрішнього аудиту). Запропонована автором модель механізму забезпечення кіберстійкості фінансового сектору передбачає моніторинг і координацію фінансових установ, засновані на принципах теорії життєздатних систем. Перспективою подальших досліджень є детальне розроблення окремих підсистем цієї моделі, що в сукупності забезпечують кіберстійкість фінансового сектору.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Корнівська *В.О. Цифровий банкінг: ризики фінансової дигіталізації. Проблеми економіки*. 2017. № 3. С. 254–261.
2. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України № 942 від 09.10.2020. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (дата звернення: 27.11.2020).
3. Accenture. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. URL: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (дата звернення: 27.11.2020).
4. E-governance academy. National Cyber Security in Practice. URL: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf (дата звернення 27.11.2020).
5. Bitglass. The Financial Matrix: Bitglass' 2019 Financial Breach Report. URL: https://www.bitglass.com/blog/the-financial-matrix-bitglass-2019-financial-breach-report (дата звернення: 27.11.2020).
6. ORX. Operational Risk Horizon. URL: https://managingrisktogether.orx.org/sites/default/files/public/downloads/2020/09/orxoperationalriskhorizon-summaryreport2020.pdf (дата звернення: 27.11.2020).
7. World Economic Forum. The Global Risks Report 2020. URL: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата звернення: 27.11.2020).
8. Держспецзв'язку створює експертну раду з кібербезпеки. URL: https://nv.ua/ukr/biz/tech/v-ukrajini-z-yavivsya-ekspertna-rada-z-kiberbezpeki-novini-ukrajini-50116214.html (дата звернення: 27.11.2020).
9. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. Volume 5. Issue 1. DOI: 10.1093/cybsec/tyz013
10. Bjorck F., Stirna J., Henkel M., Zdravkovic J. Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing / New Contributions in Information Systems*. Springer. 2015. Pp. 311–316. DOI: 10.1007/978-3-319-16486-1_31
11. Петренко С.А. Киберустойчивость систем индустрии 4.0. *Защита информации*. *Инсайд*. 2019. № 3. С. 6–15.
12. Шугунов Т., Жуков А., Хочуева Ф. Проблемы обеспечения киберустойчивости банковской системы Российской Федерации: правовой и методологичес-

кий аспекты. *Пробелы в российском законодательстве*. 2019. № 6. С. 250–253.

13. Криклій О.А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: 10.32702/2307-2105-2020.10.50

14. Hausken K. Cyber resilience in firms, organizations and societies. *Internet of things*. 2020. Volume 11. DOI: 10.1016/j.iot.2020.100204

15. Домарєв В.В., Домарєв Д.В. Управліннння інформаційною безпекою в банківських установах (теорія і практика впровадження стандартів серії ISO 27k). Донецьк : Велстар, 2012. 146 с.

16. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата звернення: 27.11.2020)

17. Бир С. Мозг фирмы. Москва : Радио и связь, 1993. 416 с.

18. Криклій О.А., Павленко Л.Д. Внутрішній аудит як превентивна складова в системі кібербезпеки банку. *Облік і фінанси*. 2019. № 2(84). С. 124–133.

19. Гриценко К.Г. Шляхи підвищення ефективності забезпечення кібербезпеки банку. *Інфраструктура ринку*. 2020. Випуск 45. С. 274–279. URL: http://www.market-infr.od.ua/uk/45-2020 (дата звернення: 27.11.2020).

REFERENCES:

1. Kornivska V.O. (2017) Tsyfrovyi bankinh: ryzyky finansovoi dyhitalizatsii [Digital banking: risks of financial digitalization]. *Problemy ekonomiky* [Problems of the economics], no. 3, pp. 254–261.

2. Cabinet of Ministers of Ukraine (2020) Deiaki pytannia obiektiv krytychnoi informatsiinoi infrastruktury [Some issues of critical information infrastructure]. Available at: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (accessed 27 November 2020).

3. Accenture. 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 27 November 2020).

4. E-governance academy. National Cyber Security in Practice. Available at: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf (accessed 27 November 2020).

5. Bitglass. The Financial Matrix: Bitglass' 2019 Financial Breach Report. Available at: https://www.bitglass.com/blog/the-financial-matrix-bitglass-2019-financial-breach-report (accessed 27 November 2020).

6. ORX. Operational Risk Horizon. Available at: https://managingrisktogether.orx.org/sites/default/files/public/downloads/2020/09/orxoperationalriskhorizon-summaryreport2020.pdf (accessed 27 November 2020).

7. World Economic Forum. The Global Risks Report 2020. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (accessed 27 November 2020).

8. Derzhspetszviazku stvoriuie ekspertnu radu z kiberbezpeky [State Service of Special Communication and Information Protection of Ukraine creates an expert council on cybersecurity]. Available at: https://nv.ua/ukr/biz/tech/v-ukrajini-z-yavivsya-ekspertna-rada-z-kiberbezpeki-novini-ukrajini-50116214.html (accessed 27 November 2020).

9. Dupont B. (2019) The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, vol. 5, issue 1. DOI: 10.1093/cybsec/tyz013

10. Bjorck F., Stirna J., Henkel M., Zdravkovic J. (2015) Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing I New Contributions in Information Systems*. Springer, pp. 311–316. DOI: 10.1007/978-3-319-16486-1_31

11. Petrenko S.A. (2019) Kiberustoychivost' cistem industrii 4.0 [Cyber Resilience of Industry 4.0 Systems]. *Zashchita informatsii. Insayd* [Protection of information. Inside], no. 3, pp. 6–15.

12. Shugunov T., Zhukov A., Khochueva F. (2019) Problemy obespecheniya kiberustoychivosti bankovskoy sistemy Rossiyskoy Federatsii: pravovoy i metodologicheskiy aspekty [Problems of ensuring cyber resilience of the banking system of the Russian Federation: legal and methodological aspects]. *Probely v rossijskom zakonodatel'stve* [Gaps in Russian legislation], vol. 6, pp. 250–253.

13. Kryklii O.A. (2020) Teoriia ta praktyka zabezpechennia kiberstiikosti bankiv [Theory and practice of ensuring cyber-resilience of banks]. *Efektyvna ekonomika* [Efficient economics], no. 10. DOI: 10.32702/2307-2105-2020.10.50

14. Hausken K. (2020) Cyber resilience in firms, organizations and societies. *Internet of things*, vol. 11. DOI: 10.1016/j.iot.2020.100204

15. Domariev V.V., Domariev D.V. (2012) *Upravlinnia informatsiinoiu bezpekoiu v bankivskykh ustanovakh (teoriia i praktyka vprovadzhennia standartiv serii ISO 27k)* [Information security management in banking institutions (theory and practice of implementating ISO 27k series standards)]. Donetsk: Velstar. (in Ukrainian)

16. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed 27 November 2020).

17. Beer S. (1993) *Mozg firmy* [Brain of firm]. Moskva: Radio i svyaz'. (in Russian)

18. Kryklii O.A., Pavlenko L.D. (2019) Vnutrishnii audyt yak preventyvna skladova v systemi kiberbezpeky banku [Internal audit as a preventive component in the bank's cybersecurity system]. *Accounting and finance*, no. 2(84), pp. 124–133.

19. Gritsenko K.G. (2020) Shliakhy pidvyshchennia efektyvnosti zabezpechennia kiberbezpeky banku [Ways to raise the efficiency of providing bank's cybersecurity]. *Infrastruktura rynku* [Market infrastructure], is. 45, pp. 274–279. Available at: http://www.market-infr.od.ua/uk/45-2020 (accessed 27 November 2020).