РОЗДІЛ 10. ЕКОНОМІЧНА БЕЗПЕКА

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БАНКУ[1]

WAYS TO RAISE THE EFFICIENCY OF PROVIDING BANK'S CYBERSECURITY

УДК 330.46
https://doi.org/10.32843/infrastruct45-44

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

Gritsenko Konstantin
Sumy State University

Кібербезпека є головним пріоритетом для ризик-менеджменту банку. Незадовільний стан забезпечення кібербезпеки призводить до значних фінансових втрат, витоку важливої інформації, погіршення репутації банку та зниження його конкурентоспроможності. У зв'язку з цим актуальною є проблема підвищення ефективності забезпечення кібербезпеки банку. Метою статті є пошук шляхів підвищення ефективності забезпечення кібербезпеки банку. Виділено організаційний та технологічний аспекти вирішення цієї проблеми. Визначено слабкі сторони у забезпеченні кібербезпеки банку. Розглянуто взаємодію суб'єктів забезпечення кібербезпеки в банківській сфері, особливості впровадження внутрішнього аудиту кібербезпеки банку, незалежного зовнішнього оцінювання його роботи, питання вдосконалення політики інформаційної безпеки банку, міжнародні стандарти управління інформаційною безпекою, інноваційні технології у сфері кіберзахисту.

Ключові слова: *кібербезпека банку, підвищення ефективності, внутрішній аудит, політика безпеки, інцидент, управління ризиками.*

Кибербезопасность является главным приоритетом для риск-менеджмента банка. Неудовлетворительное состояние кибербезопасности приводит к значительным финансовым потерям, утечке важной информации, ухудшению репутации банка и снижению его конкурентоспособности. В связи с этим актуальной является проблема повышения эффективности обеспечения кибербезопасности банка. Целью статьи является поиск путей повышения эффективности обеспечения кибербезопасности банка. Выделены организационный и технологический аспекты решения этой проблемы. Определены слабые стороны в обеспечении кибербезопасности банка. Рассмотрено взаимодействие субъектов обеспечения кибербезопасности в банковской сфере, особенности внедрения внутреннего аудита кибербезопасности банка, независимого внешнего оценивания его работы, вопросы совершенствования политики информационной безопасности банка, международные стандарты управления информационной безопасностью, инновационные технологии в сфере кибербезопасности.

Ключевые слова: *кибербезопасность банка, повышение эффективности, внутренний аудит, политика безопасности, инцидент, управление рисками.*

Cyberattacks are on the top of the bank risks list, so cybersecurity is a top priority for the bank's risk management. The unsatisfactory state of cybersecurity leads to significant financial losses, leakage of valuable information, deterioration of the bank's reputation, and reduction of its competitiveness. In this regard, the problem of improving the efficiency of the bank's cybersecurity is relevant. The purpose of the article is to find ways to improve the efficiency of cybersecurity of the bank. The organizational and technological aspects of solving this problem are highlighted. New challenges in the field of cybersecurity are the increasing variety of cyber threats, the need for rapid processing of cyber attack data, the large number of messages generated by the cybersecurity system and requiring a prompt response, management of large data sets, analysis and modernization of cybersecurity system based on new information. Common weaknesses in ensuring the bank's cybersecurity have been identified. The architecture of the Security Operations Center is presented to improve the interaction of cybersecurity entities in the banking sector. This approach makes it possible to apply artificial intelligence, machine learning, and big data analytics to the analysis of data on implemented and potential cyber threats, and to detect and prevent cyber fraud. A list of tasks that cybersecurity entities should perform within their remit is presented. It is emphasized that the internal audit of cybersecurity is an important component of the cybersecurity of the bank. The features of the internal bank cybersecurity audit, relationship of the internal audit department with the bank's cybersecurity entities are considered. For improving the bank's cybersecurity efficiency, it is necessary to bring the bank's cybersecurity system in line with international standards. Implementing international information security standards ensures compliance with the requirements of the Basel Committee Basel II to reduce operational risks of banks. Improvement of the bank's information security policy and using innovative technologies in the field of cybersecurity are considered.
Key words: *bank cybersecurity, efficiency gains, internal audit, security policy, incident, risk management.*

Постановка проблеми. У спільному дослідженні тенденцій розвитку світового банківського сектору, проведеному в 2019 році Інститутом міжнародних фінансів і міжнародною аудиторською компанією Ernst & Young, особи, що відповідають за ризик-менеджмент банків, вважають кібербезпеку головним пріоритетом [12]. У глобальному дослідженні банківських шахрайств, проведеному у 2019 році форензік-компанією KPMG, саме кібератаки очолюють список банківських ризиків [15]. У 2019 році в результаті злому системи кіберзахисту американського банку Capital One кібершахраї отримали доступ до даних 100 млн клієнтів і 80 тис. банківських рахунків. Збитки через витік цих даних оцінюються в суму 150 млн доларів США [10].

Вітчизняні банки відчули потужну руйнівну дію кібератак у 2017 році в результаті атаки вірусу-шифрувальника NotPetya. І хоча після цієї кібератаки банки почали посилювати кіберзахист,

[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»

менеджмент багатьох із них все ще не сприймає кібератаки як ризик, здатний завдати непоправної шкоди репутації та призвести до банкрутства банку [10]. А тим часом кількість кіберзлочинів в Україні за останні п'ять років зросла вдвічі [4].

Незадовільний стан забезпечення кібербезпеки банку веде до значних фінансових втрат, витоку важливої інформації, погіршення репутації банку та втрати довіри населення до банківської системи. Тому вкрай актуальною та практично значущою є проблема підвищення ефективності забезпечення кібербезпеки банку, від вирішення якої залежить конкурентоспроможність банку та його репутація.

Аналіз останніх досліджень і публікацій. Окреслена проблема розглядається в наукових працях таких вітчизняних та іноземних учених, як Д. Безштанько [1], В. Бурячок, В. Толубко, В. Хорошко, С. Толюпа [2], В. Домарєв, Д. Домарєв [3], Л. Кібальник, І. Напора [5], О. Криклій, Л. Павленко [6], О. Курченко, А. Головатенко, Л. Карасевич [7], С. Майданюк [8], В. Страхарчук, А. Страхарчук [9], Л. Брок, Ю. Леві (*Brock L., Levy Y.*) [11], Р. Кірілов [14], С. Палфі, М. Мурешан [16], А. Усман, М. Шах [18] та інші.

Проте увага науковців зосереджується в основному на окремих складниках системи забезпечення кібербезпеки банку. Пошуку шляхів підвищення ефективності забезпечення кібербезпеки банку присвячено не досить уваги.

Постановка завдання. Метою статті є вивчення теоретичних і практичних засад забезпечення кібербезпеки банку і пошук шляхів підвищення його ефективності.

Виклад основного матеріалу дослідження. Дослідження [12] показало, що менеджмент банку насамперед піклується про цілісність даних, втрату або розкриття даних (особливо персональних даних клієнтів банку), вразливість (кібератаки на аутсорсингові компанії, внутрішні загрози, а також кібернетичні ризики, пов'язані з використанням банком хмарних технологій), операційну стійкість банку (його спроможність відновити операційну діяльність після кібератаки та надати клієнтам доступ до банківських сервісів). Інструменти для здійснення кібератак невпинно розвиваються та стають доступнішими. У багатьох випадках кіберзлочини здійснюються за участі персоналу банку, а також із використанням методів соціальної інженерії. Спостерігається сплеск нових загроз у сфері соціальних мереж, мобільних пристроїв, а також хмарних технологій. Дослідження компанії EPG виявило такі слабкі сторони в забезпеченні кібербезпеки банків, як відсутність форензік-аналізу для визначення першопричин інцидентів інформаційної безпеки, відсутність необхідних даних для точного усвідомлення ситуації, відсутність ретроспективного аналізу та оперативної адаптації системи кіберзахисту для запобігання подібним атакам у майбутньому [13]. Тому надзвичайної гостроти та актуальності набуває проблема підвищення ефективності забезпечення кібербезпеки банку.

Аналіз наукових публікацій у сфері кібербезпеки дає змогу виділити організаційний та технологічний аспекти забезпечення кібербезпеки банку. Згідно із Законами України «Про Національний банк України» та «Про основні засади забезпечення кібербезпеки України», а також Стратегією кібербезпеки України, на НБУ 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.

У складі НБУ функціонує Департамент безпеки, однією з основних функцій якого є розроблення та реалізація стратегії і політики інформаційної безпеки НБУ, упровадження новітніх технологій у частині забезпечення ефективного і цілеспрямованого захисту інформації в інформаційній інфраструктурі НБУ та банківської системи України. В НБУ створено Центр кіберзахисту з командою реагування на кіберінциденти в банківській системі (CSIRT-NBU), який співпрацює з Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, підрозділом якого є урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA). НБУ співпрацює також із Національним координаційним центром кібербезпеки, який є робочим органом РНБО, та Департаментом кіберполіції Національної поліції України.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», суб'єкти забезпечення кібербезпеки в межах своєї компетенції:

– здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки;

– забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління.

Водночас на рівні бізнесу за кібербезпеку комерційного банку відповідає його власник. Зокрема, Постанова НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» № 95 від 28.09.2017 року передбачає впровадження банками процесу управління ризиками інформаційної безпеки в межах системи управління ризиками банку, систем виявлення

атак і моніторингу подій управління інцидентами. У зв'язку з цим основними шляхами підвищення ефективності забезпечення кібербезпеки банку в організаційному аспекті, на нашу думку, є:

1) покращення взаємодії суб'єктів забезпечення кібербезпеки в банківській сфері;

2) впровадження внутрішнього аудиту кібербезпеки банку;

3) забезпечення відповідності системи управління інформаційною безпекою банку міжнародним стандартам;

4) вдосконалення політики інформаційної безпеки банку.

У провідній компанії в галузі бізнес-аналітики SAS Institute вважають, що новими викликами у сфері кібербезпеки є зростаюче розмаїття кіберзагроз, необхідність швидкої обробки даних про кібератаки, велика кількість повідомлень, що генеруються системою кіберзахисту та вимагають оперативного реагування, управління великими масивами даних, аналіз і модернізація системи кіберзахисту на підставі нових відомостей [17]. Тому для підвищення ефективності протидії кібератакам важливо забезпечити обмін інформацією про інциденти інформаційної безпеки. Покращення взаємодії суб'єктів забезпечення кібербезпеки в банківській сфері ми вбачаємо у впровадженні Security Operations Center (центру моніторингу та реагування на інциденти інформаційної безпеки), архітектура якого складається з двох основних компонентів:

1) розподіленої системи збору подій інформаційної безпеки, розгорнутої в межах інформаційної інфраструктури банку, яка відповідає за збір і первинну обробку подій інформаційної безпеки з підключених джерел (серверів, що забезпечують обробку пластикових карт, міжмережевих екранів, мережевого обладнання, системи автентифікації, контролю цілісності, антивірусів тощо);

2) центрального ядра, що відповідає за автоматичне виявлення інцидентів інформаційної безпеки на підставі даних, отриманих від розподіленої системи збору подій інформаційної безпеки, а також зберігання подій інформаційної безпеки для їх ретроспективного аналізу.

Такий підхід дає можливість застосовувати для аналізу даних щодо реалізованих та потенційних кіберзагроз технології штучного інтелекту, машинного навчання та аналітики великих даних, виявляти та попереджувати кібершахрайства.

Кібербезпека потребує оцінки її ефективності, яка може бути отримана підрозділом внутрішнього аудиту банку. Внутрішній аудит кібербезпеки є важливим складником забезпечення кібербезпеки. Він дає змогу об'єктивно оцінити рівень кібербезпеки банку в умовах постійного впливу зовнішніх і внутрішніх загроз, а також дотримання вимог національного законодавства, нормативних вимог регулятора та міжнародних стандартів інформаційної безпеки. Ми погоджуємося з авторами роботи [6] у тому, що в банку повинна бути передбачена можливість аудиту кібербезпеки аутсорсингових організацій, яким передана частина операційних процесів банку, бо таким чином банк потрапляє у залежність від стану кібербезпеки цих організацій.

Взаємозв'язок підрозділу внутрішнього аудиту банку із суб'єктами кібербезпеки банку наведено на рис. 1.

Для актуалізації плану роботи підрозділу внутрішнього аудиту його керівник повинен бути підзвітним безпосередньо члену наглядової ради, що очолює аудиторський комітет, щоб знати, управління якими ризиками є нині пріоритетним. Важливо також періодично проводити незалежне зовнішнє оцінювання якості методичного забезпечення та інструментарію внутрішнього аудиту кібербезпеки, кваліфікації персоналу підрозділу внутрішнього аудиту, результатів роботи та якості звітності внутрішнього аудиту. Одним із результатів незалежного зовнішнього оцінювання є дорожна карта з поліпшення якості роботи підрозділу внутрішнього аудиту в напрямі забезпечення кібербезпеки банку. Згідно з Постановою НБУ «Про затвердження Положення про організацію внутрішнього аудиту в банках України» № 311 від 10.05.2016 у 2020 році завершується п'ятирічний етап, протягом якого вітчизняні банки зобов'язані пройти зовнішнє оцінювання функції внутрішнього аудиту.

Для покращення стану кібербезпеки банку необхідно привести у відповідність до міжнародних стандартів систему управління інформаційною безпекою банку [3]. Запровадження у банку міжнародних стандартів інформаційної безпеки дає змогу оптимізувати витрати на забезпечення кібербезпеки, знизити ймовірність реалізації кіберризиків, здійснювати їх моніторинг та оцінку, розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання. Постанова НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» № 95 від 28.09.2017 року передбачає впровадження банками системи управління інформаційною безпекою згідно з Національними стандартами ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги» та ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід практик щодо заходів інформаційної безпеки», розробленими на основі міжнародних стандартів серії ISO 27k, які забезпечують відповідність вимогам Базельського комітету Basel II щодо зменшення операційних ризиків банків.

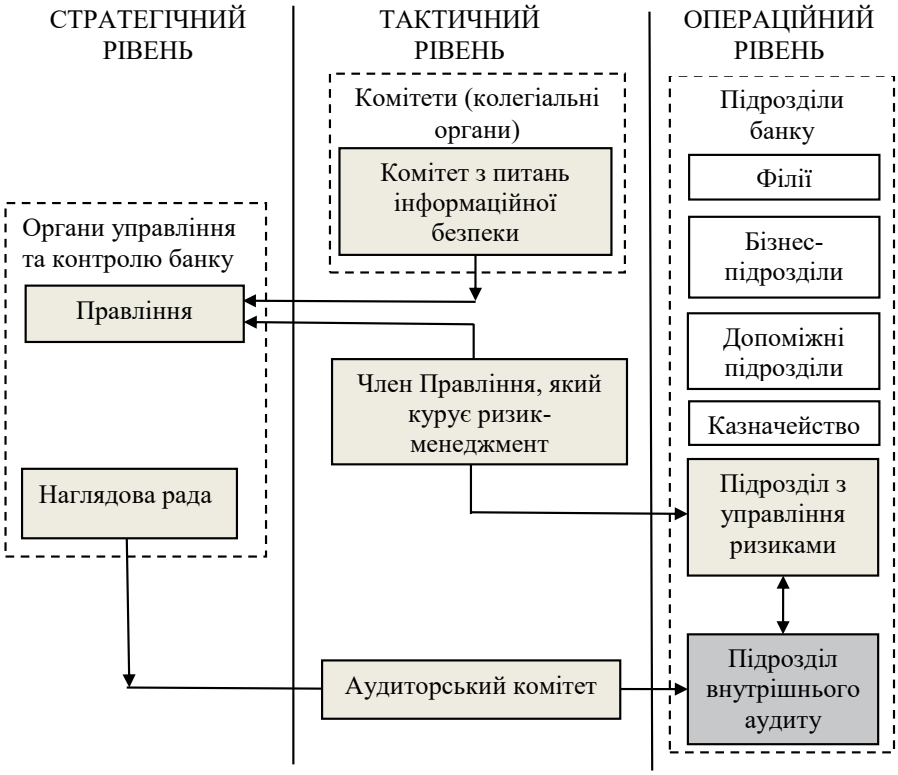

Рис. 1. Взаємозв'язок підрозділу внутрішнього аудиту банку із суб'єктами кібербезпеки банку

Джерело: побудовано автором на основі [6]

Згідно зі стандартом ДСТУ ISO/IEC 27001:2015 реалізація заходів інформаційної безпеки повинна відбуватися за допомогою політики інформаційної безпеки, яка визначає організаційні засади, напрями і цілі цих заходів, а також принципи діяльності у галузі інформаційної безпеки та кіберзахисту. Незважаючи на загальні принципи забезпечення інформаційної безпеки та кіберзахисту у банківській сфері, кожен із банків розробляє власну політику інформаційної безпеки, яка базується на результатах аудиту інформаційної інфраструктури та засобів кіберзахисту банку. Метою впровадження політики інформаційної безпеки банку є забезпечення надійного функціонування інформаційних систем банку та зниження збитків, що можуть наступити внаслідок реалізації інцидентів інформаційної безпеки. Політику інформаційної безпеки необхідно періодично переглядати з метою приведення у відповідність потребам бізнесу та стратегії розвитку банку.

У технологічному аспекті основним шляхом підвищення ефективності забезпечення кібербезпеки банку ми вбачаємо впровадження інноваційних технологій у сфері кіберзахисту. Для протидії кіберзагрозам в усьому світі традиційно використовують системи виявлення вторгнень IDS (Intrusion Detection System), що інформують про можливі порушення, та системи запобігання вторгненням IPS (Intrusion Prevention System), що відстежують трафік і здатні виявляти та блокувати потенційні небезпеки. Обмеженням у використанні цих систем є той факт, що вони засновані на виконанні певних правил реагування, які технічно неможливо неперервно поновлювати, і тому не здатні реагувати на нові кіберзагрози. Інноваційними у сфері кіберзахисту є системи управління інформацією про безпеку та поточні події SIEM (Security Information and Event Management), здатні обробляти дані в реальному часі та вчасно виявляти спроби вторгнення, хоча й вони мають певні недоліки, наведені, наприклад, у [13]. Популярною в банківській сфері стає біометрична ідентифікація, зокрема ідентифікація клієнта за відбитком пальця та розпізнавання його за голосом під час звертання до call-центру. Банки все частіше використовують аналітичні технології великих даних (BigData Analytics) для захисту від шахрайств із грошовими транзакціями та пластиковими картками. Інноваційною є технологія блокчейн, яка дає змогу зберігати інформацію у відкритому доступі для зацікавлених осіб, які не можуть змінювати раніше внесені дані. Її використовують такі провідні банки, як CreditSuisse, GoldmanSachs, JP Morgan, Barclays.

Висновки з проведеного дослідження. За результатами дослідження виявлено, що

кібербезпека є головним пріоритетом у банківській сфері в усьому світі. В останні роки в Україні стрімко зросла кількість кіберзлочинів, постійно з'являються нові кіберзагрози, підвищується рівень кібернетичних ризиків. У цих умовах банки мають ефективно протидіяти зовнішнім і внутрішнім кіберзагрозам. У роботі виділено організаційний та технологічний аспекти забезпечення кібербезпеки банку. Виявлено недоліки у сучасному стані кібербезпеки банків і запропоновано заходи, реалізація яких дасть змогу підвищити ефективність забезпечення кібербезпеки банку й ефективність банківського бізнесу. В організаційному аспекті необхідно покращувати взаємодію суб'єктів забезпечення кібербезпеки в банківській сфері, внутрішній аудит кібербезпеки, політику інформаційної безпеки та відповідність системи забезпечення кібербезпеки банку міжнародним стандартам. У технологічному аспекті основним шляхом підвищення ефективності забезпечення кібербезпеки банку визначено впровадження інноваційних технологій у сфері кіберзахисту. Подальші дослідження можуть розвиватися в напрямі реалізації зазначених заходів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Безштанько Д.В. Інформаційна безпека банку в системі управління операційним ризиком. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2012. № 12, том 1. URL: http://fkd.org.ua/article/view/28875 (дата звернення 29.06.2020).

2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: Державний університет телекомунікацій, 2015. 288 с.

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

4. За останні п'ять років кількість кіберзлочинів в Україні зросла вдвічі. URL: https://opendatabot.ua/blog/374-hackers (дата звернення 29.06.2020).

5. Кібальник Л.О., Напора І.Ю. Впровадження політики інформаційної безпеки банківських установ. *Причорноморські економічні студії*. 2016. Вип. 12 (2). С. 119–122. URL: http://bses.in.ua/uk/12-2016%5303 (дата звернення 29.06.2020).

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

7. Курченко О.А., Головатенко А.В., Карасевич Л.Ю. Підвищення ефективності системи управління захистом персональних даних клієнтів банку. *Сучасний захист інформації*. 2014. № 1. С. 32–37.

8. Майданюк Н.В. Перспективні технології підтримки інформаційної безпеки в банківській сфері. *Вісник Черкаського університету*. 2017. № 1. С. 88–96.

9. Страхарчук В., Страхарчук А. Шляхи підвищення ефективності електронного банківського бізнесу. *Молодь і ринок*. 2011. № 11(82). С. 117– 123.

10. Як банкам встояти в результаті кібератаки? URL: https://finclub.net/ua/priama-mova/yak-bankam-vstoiaty-u-vypadku-kiberataky.html (дата звернення 29.06.2020).

11. Brock L., Levy Y. The market value of information system (IS) security for e-banking. *Online Journal of Applied Knowledge Management*. 2013, vol. 1, pp. 1–17.

12. An endurance course: surviving and thriving through 10 major risks over the next decade: Tenth annual EY/IIF global bank risk management survey. URL: https://www.iif.com/Portals/0/Files/content/Regulatory/11062019_iif_ey_global_risk_survey_2019.pdf (дата звернення 29.06.2020).

13. EPG. Analytics-based approach to cyber security. URL: http://docplayer.net/2410200-An-analytics-based-approach-to-cybersecurity.html (дата звернення 29.06.2020).

14. Kirilov R. Effectiveness of the Information Security in the Banks. *Cybernetics and Information Technologies*. 2006, vol. 6, no. 2, pp. 70–85.

15. KPMG. Global banking fraud survey. URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf (дата звернення 29.06.2020).

16. Palfi C., Muresan M. Survey on Weaknesses of Banks Internal Control Systems. *Journal of International Finance and Economics*. 2009, no. 9 (1), pp. 106– 116.

17. SAS. Trends in combating cyber crime. Tips and technology for defending your network. URL: https://www.risktech-forum.com/research/sas-trends-in-combating-cybercrime-tips-and-techniques-for-defending-your-n (дата звернення 29.06.2020).

18. Usman A.K., Shah M.H. Critical success factors for preventing e-banking fraud. *The Journal of Internet Banking and Commerce*. 2013, no. 18 (2). URL: http://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196 (дата звернення 29.06.2020).

REFERENCES:

1. Bezshtanko D.V.(2012) Informatsiina bezpeka banku v systemi upravlinnia operatsiinym ryzykom [Information security of the bank in the operational risk management system]. *Finansovo-kredytna diialnist: problemy teorii ta praktyky* [Financial and credit activities: problems of theory and practice] (electronic journal), vol. 1, no. 12, pp. 1–6. Available at: http://fkd.org.ua/article/view/28875 (accessed 29 June 2020).

2. Buriachok V.L., Tolubko V.B., Khoroshko V.O., Toliupa S.V. (2015) *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk* [Information and cybersecurity: socio-technical aspect: textbook]. Kyiv: Derzhavnyi universytet telekomunikatsii. (in Ukrainian)

3. 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)

4. Za ostanni piat rokiv kilkist kiberzlochyniv v Ukraini zrosla vdvichi [The number of cybercrimes in Ukraine has doubled in the last five years]. Available at: https://opendatabot.ua/blog/374-hackers (accessed 29 June 2020).

5. Kibalnyk L.O., Napora I.Yu. (2016) Vprovadzhennia polityky informatsiinoi bezpeky bankivskykh ustanov [Implementation of information security policy of banking institutions]. *Prychornomorski ekonomichni studii* [Black Sea Economic Studies] (electronic journal), vol. 12 (2), pp. 119–122. Available at: http://bses.in.ua/uk/12-2016%5303 (accessed 29 June 2020).

6. 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.

7. Kurchenko O.A., Holovatenko A.V., Karasevych L.Yu. (2014) Pidvyshchennia efektyvnosti systemy upravlinnia zakhystom personalnykh danykh kliientiv banku [Improving the efficiency of protection management system of the bank's clients personal data]. *Modern information protection*, no. 1, pp. 32–37.

8. Maidaniuk N.V. (2017) Perspektyvni tekhnolohii pidtrymky informatsiinoi bezpeky v bankivskii sferi [Promising technologies to support information security in the banking sector]. *Bulletin of Cherkasy University*, no. 1, pp. 88–96.

9. Strakharchuk V., Strakharchuk A. (2011) Shliakhy pidvyshchennia efektyvnosti elektronnoho bankivskoho biznesu [Ways to increase the efficiency of e-banking]. *Youth and the market*, no.11(82), pp.117–123.

10. Yak bankam vstoiaty v rezultati kiberataky? [How can banks withstand a cyber attack?]. Available at: https://finclub.net/ua/priama-mova/yak-bankam-vstoiaty-u-vypadku-kiberataky.html (accessed 29 June 2020).

11. Brock L., Levy Y. (2013) The market value of information system (IS) security for e-banking. *Online Journal of Applied Knowledge Management*, vol. 1. pp. 1–17.

12. An endurance course: surviving and thriving through 10 major risks over the next decade: Tenth annual EY/IIF global bank risk management survey. Available at: https://www.iif.com/Portals/0/Files/content/Regulatory/11062019_iif_ey_global_risk_survey_2019.pdf (accessed 29 June 2020).

13. EPG. Analytics-based approach to cyber security. Available at: http://docplayer.net/2410200-An-analytics-based-approach-to-cybersecurity.html (accessed 29 June 2020).

14. Kirilov R. (2006) Effectiveness of the Information Security in the Banks. *Cybernetics and Information Technologies*, vol. 6, no. 2, pp. 70–85.

15. KPMG. Global banking fraud survey. Available at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf (accessed 29 June 2020).

16. Palfi C., Muresan M. (2009) Survey on Weaknesses of Banks Internal Control Systems. *Journal of International Finance and Economics*, no. 9 (1), pp. 106–116.

17. SAS. Trends in combating cyber crime. Tips and technology for defending your network. Available at: https://www.risktech-forum.com/research/sas-trends-in-combating-cybercrime-tips-and-techniques-for-defending-your-n (accessed 29 June 2020).

18. Usman A.K., Shah M.H. (2013) Critical success factors for preventing e-banking fraud. *The Journal of Internet Banking and Commerce*, no. 18(2). Available at: http://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196 (accessed 29 June 2020).