МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 303.06[004]:336.719
DOI: https://doi.org/10.37320/2415-3583/12.36

Яровенко Г.М.
кандидат економічних наук, доцент,
Навчально-науковий інститут бізнес-технологій «УАБС»
Сумського державного університету
ORCID: https://orcid.org/0000-0002-8760-6835

Ковач В.О.
аспірант кафедри економічної кібернетики,
Навчально-науковий інститут бізнес-технологій «УАБС»
Сумського державного університету
ORCID: https://orcid.org/0000-0002-1083-0003

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СИСТЕМАХ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БАНКІВ[1]

Виявлення та попередження кіберзагроз системами захисту є актуальним питанням для банків. Забезпечення цього процесу потребує застосування надійних, ефективних та сучасних технологій. Автори присвятили статтю дослідженню перспектив застосування технології блокчейн у системах кібербезпеки банків. У роботі визначено особливості проблематики забезпечення кібербезпеки банків та її актуальність. Охарактеризовано основні технології та інструменти, які нині активно застосовуються задля протидії кібератакам на банківські установи та їхніх клієнтів. Проаналізовано можливості використання основних переваг технології блокчейн у боротьбі з основними кіберзагрозами. Виявлено, що ця технологія потенційно може суттєво знизити або взагалі усунути деякі види вразливостей наявних банківських систем. Проведено аналіз рівня інтересу до технології блокчейн за напрямами комп'ютерної безпеки та банківської діяльності у світі за останні 5 років з використанням бази даних Google Trends. Здійснено порівняння інтересу до технології блокчейн та технології штучного інтелекту в світі та в окремих країнах. У результаті виявлено, що обидві технології є досить популярними та їх використання може взаємодоповнювати одне одного для реалізації у системах забезпечення кібербезпеки банків.

Ключові слова: *банк, блокчейн-технологія, вразливість системи, кібербезпека, кіберзагроза, штучний інтелект.*

Постановка проблеми. В умовах активного становлення четвертої промислової революції, прогресивного розвитку нових цифрових технологій та комунікацій, їхньої комплексної інтеграції в глобальний бізнес питання кібербезпеки стає все більш актуальним та певною мірою критичним для деяких сфер діяльності. З упровадженням нових інформаційних технологій сфера кіберзагроз суттєво розширюється, не тільки за рахунок вже існуючих видів, але й за рахунок нових, досі не ідентифікованих та не вивчених кіберзагроз. За даними досліджень мультинаціональної консалтингової компанії Accenture Security [1], з 2017 по 2018 роки кількість потенційних «гілок» кіберзагроз зросла з 130 до 145, що дорівнює 11% приросту за рік. Відповідно, середньорічні втрати від кіберзлочинності за той самий період зросли на 12% і становили в межах 13 мільйонів доларів США в розрахунку на одне підприємство, що на 72% більше, ніж 5 років тому. Вищенаведені показники свідчать про необхідність посилення заходів кібербезпеки, створення та дослідження нових технологій, які б дозволяли забезпечувати високий рівень кіберзахисту в умовах постійного росту кіберзлочинності в світі.

Впродовж десятиліть індустрія фінансових послуг залишається найбільш привабливою мішенню для кіберзлочинців, особливо діяльність банків. IBM X-Force Threat Intelligence Report [2] за 2017 рік показав, що серед клієнтів, які обслуговуються IBM Security Services, компанії, які надають фінансові послуги, зазнавали на 65% більше кібератак, ніж представники усіх інших галузей. Діяльність банків пов'язана із генерацією підвищеного кіберризику, що передбачає високу імовірність серйозних фінансових втрат від кіберзлочинів як для банків, так й для клієнтів, які у них обслуговуються. Тенденція зростання кіберзлочинності у банківському секторі спостерігається серед країн усього світу. З 2014 року кіберугрупування все більше зазіхають на бізнесові банківські рахунки, використовуючи при цьому таке зловмисне програмне забезпечення, як Dyre, Dridex, GozNym and TrickBot. Навіть міжнародна міжбанківська система передачі інформації та здійснення платежів SWIFT, якою користуються тисячі банків та окремих компаній по всьому світі, щороку потерпає від зростаючої кількості атак як окремих зловмисників, так і професійних організова-

[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».

них злочинних кіберугрупувань. Так, у 2016 році спостерігався значний спалах організованих масових атак, у результаті яких мільйони доларів США були виведені з різних міжнародних банків шахрайським шляхом за допомогою клієнтського зловмисного програмного забезпечення, яке одночасно видаляло будь-які сліди таких транзакцій. Як повідомляє незалежна організація IT-моніторингу ISACA в Україні, в 2016 році хакери через міжнародну банківську систему SWIFT вкрали 10 мільйонів доларів з рахунків одного із українських банків [3]. Таким же чином хакери свого часу вкрали з Центрального банку Бангладешу 81 мільйон доларів. Це лише кілька прикладів, які вказують на існування проблем, пов'язаних із кіберзахистом, особливо фінансових установ.

Ефективне управління ризиками, пов'язаними з кіберзлочинністю, є одним із першочергових завдань банківського управління, а побудова надійної системи кібербезпеки є критично важливим завданням. Банки повинні забезпечувати кіберзахист усіх здійснюваних операцій насамперед задля захисту активів власних клієнтів. Зростає кількість безготівкових операцій, користувачів онлайн-банкінгу, що суттєво підвищує ризик перехоплення транзакцій та персональних даних клієнтів зловмисниками, що несе за собою величезні фінансові втрати як для клієнтів банків, так і для самих банків. У результаті шахрайських дій банки втрачають довіру своїх клієнтів та інших фінансових установ.

Аналіз останніх досліджень і публікацій. З моменту публікації у 2008 році праці Сатоші Накамото «Bitcoin: A Peer-to-Peer Electronic Cash System», в якій вперше було досить детально описано основи технології блокчейн, інтерес до цієї технології та можливостей її застосування почав стрімко зростати серед науковців по всьому світі. Так, за даними бази Scopus, у 2019 році було опубліковано 5738 наукових праць, присвячених блокчейн-технології, проти 1 статті, опублікованої у 2012 році, що свідчить про зростання зацікавленості науковців до цієї теми [4]. Якщо проаналізувати ті сфери, в яких здійснювалися дослідження науковців та в яких вирішувалися питання, пов'язані із застосуванням та розвитком блокчейн-технології, то найбільший відсоток належить науковим працям у сфері комп'ютерних наук (36%), інженерії (18,4%), математичних методів (9,3%), прийняття рішень (8,4%), бізнесу, менеджменту та бухгалтерського обліку (6,3%), соціальних наук (5,4%), медицини (2,7%), енергетики (2,6%), фізики та астрономії (2,2%), матеріалознавства (2,0%), економіки, економетрики та фінансів (2,0%), та інших (5%) [5]. Тобто нині більшість дослідників пов'язують технологію блокчейн саме із комп'ютерними науками, хоча ця технологія набуває свого розвитку й у інших сферах діяльності людини.

Аналізуючи публікації вчених за географічним охопленням, можна дійти висновку, що найбільша кількість публікацій належить ученим Китаю (2604 публікації) та США (1958 публікацій) [6]. Це пов'язано з тим, що сьогодні Китай є прогресивною країною із потужним економічним, технічним та людським потенціалом, яка намагається зайняти провідні позиції у світі. Вчені цієї країни є вкрай зацікавленими у вивченні останніх новітніх технологій у світі. Китайським науковцям не уступають також і американські дослідники, які за кількістю публікацій займають друге місце. Так, найбільший внесок у дослідження блокчейн-технології було зроблено такими закордонними фахівцями, як: K.K.R. Choo, F.Y. Wang, M. Guizani, Y. Yuan, N. Javaid, K. Salah, D. Niyato, B. Stiller, N. Kumar, Z. Zheng, X. Xu, I. Weber, X. Du, J.H. Park, L. Zhu, S. Shetty, P. Wang, L. Njilla, A. Kiayaias, A. Norta, R. State, R.M. Parizi, Y. Zhang, L. Xu. Кожним із них було опубліковано більше 20 наукових праць у Scopus міжнародних виданнях, що свідчить про їхній безперечний науковий внесок у дослідження блокчейн-технологій.

Українські вчені тільки набирають обертів. За останні 10 років ними було опубліковано лише 72 статті у міжнародних виданнях, що індексуються у базі Scopus [6]. Це свідчить про недостатній інтерес до цієї сфери з боку українського наукового осередку. Певний науковий доробок із питання розвитку та використання блокчейн-технології належить таким українським ученим, як: О. Летичевський, Р. Олійников, В. Пещаненко, М. Родінко, Д. Кайдалов, Л. Ковальчук, А. Кузнєцов, А. Настенко, Н. Полуяненко, В. Радченко, О. Шевцов, П. Кравченко, О. Курбатов, О. Шаповал, які опубліковували більш ніж 3 статті у виданнях, що індексуються у базі Scopus.

Можна також зазначити, що дослідженнями у галузі блокчейн-технологій займаються і провідні міжнародні компанії та організації. Так, технологічні консалтингові компанії світу, такі як IBM, Microsoft, Accenture та Deloitte, проводять численні статистичні дослідження, спрямовані на вивчення перспектив залучення технології до різних сфер бізнесу, зокрема і в галузі кібербезпеки фінансових організацій. Такі міжнародні організації, як OECD, The World Economic Forum та The World Trade Organization, публікують низку досліджень стосовно напрямів застосування технології блокчейн на рівні міжнародної співпраці задля вирішення глобальних економічних питань.

Мета статті полягає в аналізі перспектив застосування технології блокчейн у системах кібербезпеки банків через призму здійснення аналізу рівня зацікавленості цією технологією порівняно із технологією штучного інтелекту та з використанням бази даних Google Trends.

Виклад основного матеріалу дослідження. Зважаючи на всю серйозність кіберзагроз для сектору фінансових послуг, банки та інші організації фінансового сектору порівняно з представниками інших галузей інвестують набагато більше коштів у створення та розвиток власної системи кібербезпеки [7]. Сучасні системи кібербезпеки банків є досить складними та багаторівневими, враховуючи природу та механізми формування ризиків у кіберпросторі. Вони повинні враховувати постійно зростаючу тенденцію розширення поля кіберзагроз, наявність багатьох відомих і невідомих потенційних каналів здійснення атак. Слід зазначити, що джерела кіберзагроз можуть бути не тільки зовнішніми, але і внутрішніми, що також передбачає інтеграцію окремих різноспрямованих механізмів захисту.

Основним завданням наявних систем кібербезпеки є максимальна протидія усім можливим кібератакам, за допомогою яких могли би бути здійснені кіберзло-

чини. В ідеалі системи кіберзахисту повинні не тільки виступати бар'єром для всіх відомих видів кіберзагроз, але і вміти ідентифікувати досі невідомі види кібератак до того, як вони могли б завдати шкоди банку та його клієнтам. Зазвичай система кібербезпеки банку являє собою комплексне програмне рішення, яке базується на низці технологій, здатних захистити інформаційний простір банку від окремих видів та типів загроз залежно від їх характеру дії та сфери виникнення. Використання цілого портфелю технологій дає змогу максимально мінімізувати наявний загальний рівень кіберризику, оскільки немає єдиної технології, яка б ефективно спрацьовувала проти усіх можливих типів загроз.

Нині до ключових технологій, які використовуються для забезпечення кібербезпеки в банківському секторі, належать: збір і аналіз даних щодо безпеки та обміну загрозами; автоматизація, штучний інтелект та машинне навчання; розширене прогресивне управління ідентифікацією та доступом; аналітика кіберповедінки користувачів; криптографічні технології; управління виконанням процесів та ризиком на підприємствах; автоматизоване стратегічне управління; попередження втрат даних та розширений контроль периметру. Всі вищенаведені технології можуть бути дуже ефективними в протидії окремим видам кіберзагроз на різних рівнях функціонування банківських інформаційних систем. Вони активно застосовуються різними банками по всьому світі, постійно доопрацьовуються та вдосконалюються у відповідь на постійне посилення рівня кіберзлочинності та безперервне розширення поля кіберзагроз.

Нині найбільш прогресивними технологіями, які застосовуються для забезпечення кібербезпеки банків, є технології штучного інтелекту та машинного навчання. Основною їхньою перевагою є можливість об'єднання різних каналів, таких як цифровий банкінг, аутентифікація, картковий банкінг та відкритий банкінг. За допомогою технології штучного інтелекту можна в одному місці опрацьовувати величезні обсяги інформації з різних каналів, що дає змогу набагато ефективніше моніторити та виявляти кібератаки, аналізуючи при цьому комплексну картину усіх наявних транзакцій у різних каналах. Аналіз активності в окремих каналах часто не здатен ідентифікувати окрему підозрілу злочинну транзакцію. Зазвичай кібератаки реалізуються шляхом здійснення низки дій із застосуванням різних каналів. Кожна така окрема дія може не викликати жодних підозр, але відстежування цілої послідовності дій може ідентифікувати злочинний сценарій кібератаки. Багато спеціалістів в сфері банкінгу та кібербезпеки вважають, що саме застосування технології штучного інтелекту стане передовою тенденцією для постачальників фінансових послуг.

Поряд із технологіями, які вже активно використовуються у системах кібербезпеки, можна виділити технологію блокчейн, яка є відносно новою та перспективною. Допоки вона не знайшла широкого розповсюдження, але її використання, на нашу думку, в системах забезпечення кіберзахисту банку змогла б суттєво підвищити рівень їхньої ефективності. Блокчейн став широко відомим завдяки активному розвитку криптовалют, більшість з яких базується саме на цій технології. Нині по всьому світі вже є низка стартапів, які намагаються реалізовувати та тестувати концепції різноспрямованих проектів на базі технології блокчейн. Зокрема, її починають використовувати під час побудови прогресивних систем електронного голосування, ведення різних глобальних реєстрів (наприклад, реєстрів нерухомості, земельних ділянок), у маркетингових системах, у системах управління ланцюгами поставок тощо [8].

Технологія блокчейн, яку ще називають технологією розподілених реєстрів, є досить універсальним інструментом, який може бути використаним для вирішення широкого спектру завдань. До основних її переваг відносять децентралізованість, повну прозорість, конфіденційність, захищеність від несанкціонованого доступу та реалізацію компромісу. Всі вищенаведені переваги можуть бути спрямованими на вирішення наявних проблем забезпечення кібербезпеки банків. Тому їх було перекладено на площину проблематики кібербезпеки банків (таблиця 1).

Аналізуючи переваги, можна стверджувати, що застосування технології блокчейн в інформаційних системах банків може суттєво підвищити рівень їхньої захищеності від кібератак різного роду. Також використання технології блокчейн здатне усунути основні вразливості сучасних банківських систем, які роблять можливим здійснення таких основних типів кібератак, як Malware, веб-атаки, DOS, атаки зловмисних інсайдерів, зловмисний код та ін. [9].

Основними недоліками банківських інформаційних систем є їх централізованість та непрозорість. У таких системах, як і в більшості корпоративних, всі основні дані перебувають в одному місці. Для того, щоб повністю захопити систему або критично її уразити, досить успішно атакувати її центральний сервер даних. Отримавши доступ до центрального реєстру даних, зловмисник отримує можливість без перешкод здійснювати всі можливі маніпуляції із системою. Ця проблема вирішується технологією блокчейн шляхом створення численних копій розподілених реєстрів даних, які розміщуються в різних вузлах системи. За таких умов ураження одного реєстру не може призвести до краху всієї системи. Припустимо, якщо інформаційна система банку матиме численну кількість копій реєстрів даних у різних відділеннях, вузлах системи, то захоплення кіберзлочинцем реєстру в одному з відділень ніяк не вплине на всю інформаційну систему банку, і будь-які підміни існуючих записів даних будуть заблоковані у зв'язку з невідповідністю численним копіям даних в інших реєстрах інших відділень.

Непрозорість банківських інформаційних систем створює суттєві перешкоди під час ідентифікації злочинних сценаріїв кібератак. За таких умов навіть системи штучного інтелекту та машинного навчання не можуть працювати максимально ефективно. Також непрозорість банківських систем створює сприятливі умови для шахрайств з боку співробітників банків. Відомо, що близько 48% кібератак на банківські установи здійснюється саме зловмисними інсайдерами [12]. Саме атаки з їхнього боку вважаються найбільш небезпечними та призводять до найбільших грошових втрат. Але в умовах інформаційної системи, що функ-

Таблиця 1 – Переваги застосування технології блокчейн у системах кібербезпеки банків

Перевага	Сутність переваги	Значення переваги для систем кібербезпеки банків
Децентралізація	Відсутність єдиного головного серверу зберігання даних; всі записи зберігаються у кожного учасника системи, на кожному її вузлі.	Сучасні системи кібербезпеки банків є централізованими, мають головні сервери даних, що породжує їх основну вразливість. Блокчейн-технологія дозволить під час атаки одного вузла зберегти дані на інших вузлах.
Повна прозорість системи	Всі транзакції, які відбуваються в системі, можуть відстежуватися на всіх вузлах системи.	Технологія блокчейн у банківській системі надасть можливість аналізувати всі транзакції на кожному окремому вузлі. При цьому, кожна наступна транзакція перед її виконанням перевіряється всіма вузлами системи, і не може бути здійснена при виявленні найменшої невідповідності до усіх попередньо здійснених транзакцій.
Конфіденційність	Всі дані зберігаються в зашифрованому вигляді. Користувач, відслідковуючи всі транзакції, не може розпізнати окремі дані про них, а для здійснення операцій потрібний унікальний ключ доступу.	Застосування в банківських системах блокчейнів дозволить захистити від зовнішніх кіберзлочинців та інсайдерів-співробітників особисті дані клієнтів, про їх банківські рахунки, оскільки, маючи всю історію транзакцій, злочинці не зможуть нею скористатись та ідентифікувати дані.
Захищеність від несанкціонованого доступу	Будь-яка спроба внесення несанкціонованих змін автоматично відхиляється системою через невідповідність численним копіям даних, розміщених на різних вузлах системи. Для легального внесення змін в систему та здійснення транзакцій необхідно мати спеціальний унікальний код, який видається та підтверджується системою.	Зловмисники часто здійснюють маніпуляції та фальсифікації даних в системі банку, доступ до якої отримують обхідним шляхом, використовуючи вразливості системи. Якщо зловмисник заволодіє спеціальним унікальним кодом системи, що малоймовірно, в системі завжди зберігатиметься інформація про кожну транзакцію. Будь-яке зловживання правами в системі буде відоме всім іншим її членам, і зловмисник не матиме можливості приховати сліди власного злочину.
Компроміс	Компроміс реалізується шляхом попередньої перевірки кожним членом системи даних, які додаються до неї. Прийняття рішення щодо додавання нового блоку відбувається за умови згоди всіх учасників. Досягнення консенсусу здійснюється у відповідності до одного протоколу консенсусу з урахуванням особливостей та специфіки системи.	З погляду кібербезпеки банківських операцій, проведення процедури перевірки кожної транзакції іншими вузлами системи створює додатковий бар'єр для реалізації атак. Будь-яка спроба підміни даних в одному з вузлів системи буде заблокована іншими вузлами системи, які мають свої копії усіх даних в системі. Цей механізм може захистити банківську систему від таких типів афер, як підміна кредитної історії, реквізитів рахунків, махінації із банківською звітністю тощо.

Джерело: складено авторами на основі [10; 11]

ціонує на базі блокчейн, жоден співробітник не зміг би внести зміни до системи, будучи непоміченим, а всі його маніпуляції з системою постійно фіксувалися б та зберігалися в кожній копії реєстру даних на кожному вузлі. За таких умов будь-яка спроба перевищення службових повноважень досить швидко стає відомою на всіх вузлах системи.

Враховуючи всі вищенаведені переваги та перспективи технології блокчейн, можна стверджувати, що майбутні напрями її застосування у банківських системах є цілком прогнозованими. Якщо порівнювати можливості технології штучного інтелекту, що зараз масово впроваджується, та блокчейнів, то можна з впевненістю сказати, що обидві не можуть замінити один одного, оскільки вони спрямовані вирішувати різні завдання. Але їх комбінація є можливою та взаємодоповнюючою, тому логічним є підвищення рівня зацікавленості до цих технологій з боку різних суб'єктів господарювання, в тому числі й банківських установ. Так, було проведено аналіз рівня інтересу до технології блокчейн та технологій штучного інтелекту, щодо їх застосування у сфері комп'ютерної безпеки та у банківській діяльності за останні 5 років з використанням бази даних Google Trends [13].

На рис. 1 наведено зміну за часом рівня зацікавленості до тематики «Блокчейн» та «Штучний інтелект» у категорії запитів «Комп'ютерна безпека». Графік динаміки вказує на те, що відбувається підвищення інтересу до блокчейн-технології порівняно з 2015 роком. На кінець 2017 року припадає значний стрибок, що зумовлено збільшенням кількості кібератак, хоча нині спостерігається певний спад.

Якщо порівнювати інтерес до обох технологій, то тема штучного інтелекту досі значно переважає тему блокчейн у категорії запитів, які стосуються комп'ютерної безпеки. Це можна пояснити тим, що технологія штучного інтелекту вже стала активно застосовуватися у сфері комп'ютерної безпеки, є досить вивченою та вже показала фактичну результативність та досить високу ефективність вкладених інвестицій. А технологія блокчейн досі є не досить вивченою на практиці, не має такої великої кількості вже реалізованих проектів, також імплементація та ефективність інвестування в технологію блокчейн досі є невизначеною.

Якщо порівнювати інтерес до цих двох технологій у різних країнах, то можна помітити, що в таких країнах світу, як Нідерланди, Франція, Швейцарія, Китай, Австралія Сінгапур, Німеччина, Україна та інші, інтерес до технології блокчейн у категорії комп'ютерної безпеки переважає (рисунок 2). Але такі країни, як Росія, Велика Британія, Сполучені Штати,

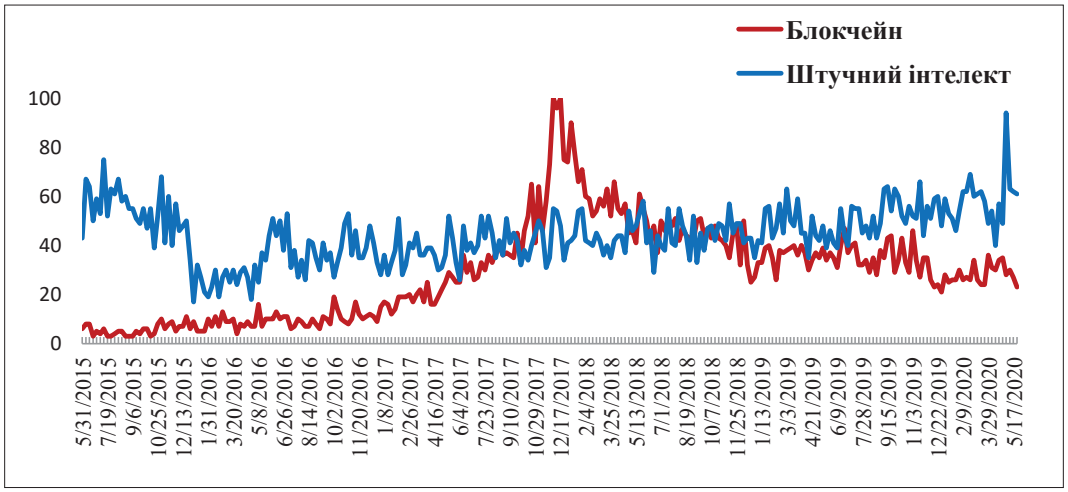

Рисунок 1 – Зміни рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» у категорії запитів «Комп'ютерна безпека» за часом

Джерело: складено авторами на основі бази даних Google Trends [13]

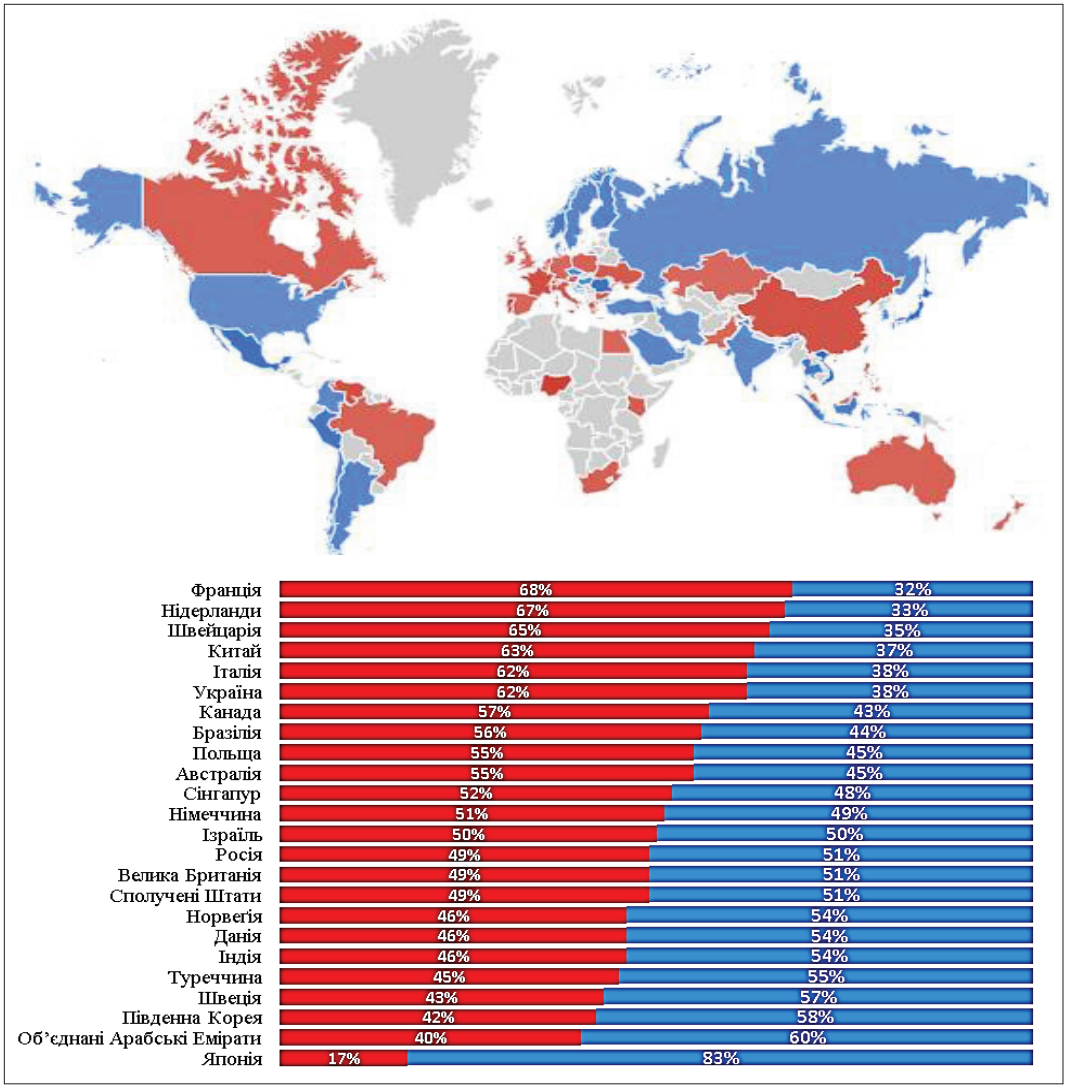

Рисунок 2 – Інфографіка рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» у категорії запитів «Комп'ютерна безпека» за географією

Джерело: складено авторами на основі бази даних Google Trends [13]

Норвегія, Данія, Індія, Туреччина, Швеція, Південна Корея, Об'єднані Арабські Емірати, Японія, зосередили свою увагу саме на технологіях штучного інтелекту у сфері комп'ютерної безпеки (рис. 2). Такий розкид зумовлений тим, що різні країни намагаються сформувати власні ніші на ринку систем комп'ютерної безпеки та намагаються використовувати останні розробки сучасних технологій.

У категорії запитів «Банківська діяльність» інтерес до обох технологій знаходиться приблизно на одному рівні вже більше одного року (рисунок 3). Це говорить про те, що банки вбачають перспективи в застосуванні технології блокчейн поряд із штучним інтелектом. Обумовлені стрибки протягом 2017–2018 років, які показали значне зростання зацікавленістю технологією блокчейн, пояснюються зростанням в цей період популярності криптовалют на фінансових ринках.

Карта порівняння інтересу до технологій в різних країнах вказує та те, що все ж таки в більшості країн світу інтерес до технології блокчейн в категорії запитів «банківська діяльність» переважає інтерес до технології штучного інтелекту (рисунок 4). Це є цілком зрозумілим, адже технологія блокчейн має досить високий потенціал застосування в сфері банкінгу, а не тільки як засіб забезпечення кібербезпеки. Слід такої зазначити, що інтерес до технології блокчейн загалом досить високий серед найбільш економічно та технологічно розвинених країнах, які можуть стати досить потужною базою для практичної реалізації потенціалу технології блокчейн.

Якщо порівнювати технологію блокчейн з іншими технологіями, які застосовуються в системах кібербезпеки, то можна стверджувати, що вона може бути не менш ефективною, а деякі технології здатна успішно замінити. Технологія блокчейн спроможна вирішувати ті ж задачі, що зараз вирішуються за допомогою таких технологій, як розширене управління ідентифікацією та доступом, криптографічні технології, попередження втрат даних, автоматизоване управління політиками та ін. Ланцюг блоків транзакцій, кожен з яких має хеш з даними про попередні транзакції, здатен фіксувати кожну найменшу зміну в системі та зберігати історичні дані про будь-які зміни в системі на кожному її вузлі. І якщо на сьогодні розслідування кіберзлочинів в банківському секторі займає від кількох місяців до року, то використання технології блокчейн може в рази або навіть в десятки разів пришвидшити процедуру розслідування злочинів.

Висновки. Технологія блокчейн має значний потенціал застосування в інформаційних системах кібербезпеки банків. Аналіз основних її переваг, таких як децентралізованість, прозорість, конфіденційність, захищеність від несанкціонованого доступу та реалізація компромісу, показав, що вони можуть бути спрямовані на вирішення широкого спектру проблем кібербезпеки банків. Впровадження технології блокчейн у банківських системах може усунути низку їхніх головних вразливостей з погляду кібербезпеки. Результати аналізу даних Google Trends показали, що інтерес до питання її застосування в сферах кібербезпеки та банківської діяльності є досить значним порівняно з інтересом до технології штучного інтелекту, яка вже досить активно застосовується за цими напрямками, хоча їй надають перевагу саме в реалізації заходів комп'ютерної безпеки, що пов'язано з результативністю штучного інтелекту та ефективністю вкладених в нього інвестицій. Більшість економічно та технологічно розвинених країн світу проявляють суттєвий інтерес до застосування технології блокчейн саме у сфері банкінгу, що зумовлює формування та розвиток значних перспектив практичної реалізації її потенціалу. Можна припустити, що блокчейн-технологія може бути не менш ефективною в боротьбі з кіберзлочинністю, аніж інші, які нині активно застосовуються в банківських інформаційних системах, причому вона може доповнювати наявні системи для вирішення завдань із протидії кіберзагрозам.

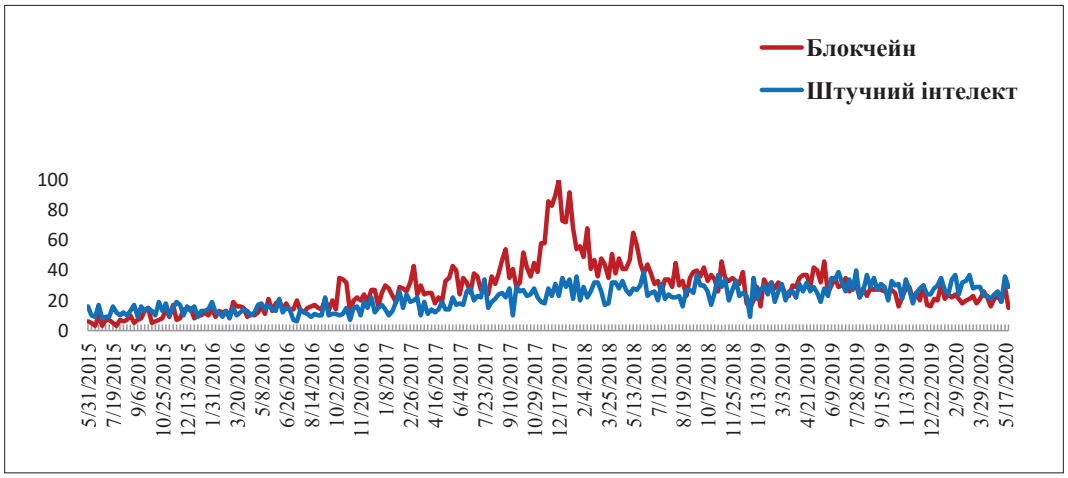

Рисунок 3 – Зміни рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Банківська діяльність» за часом

Джерело: складено авторами на основі бази даних Google Trends [13]

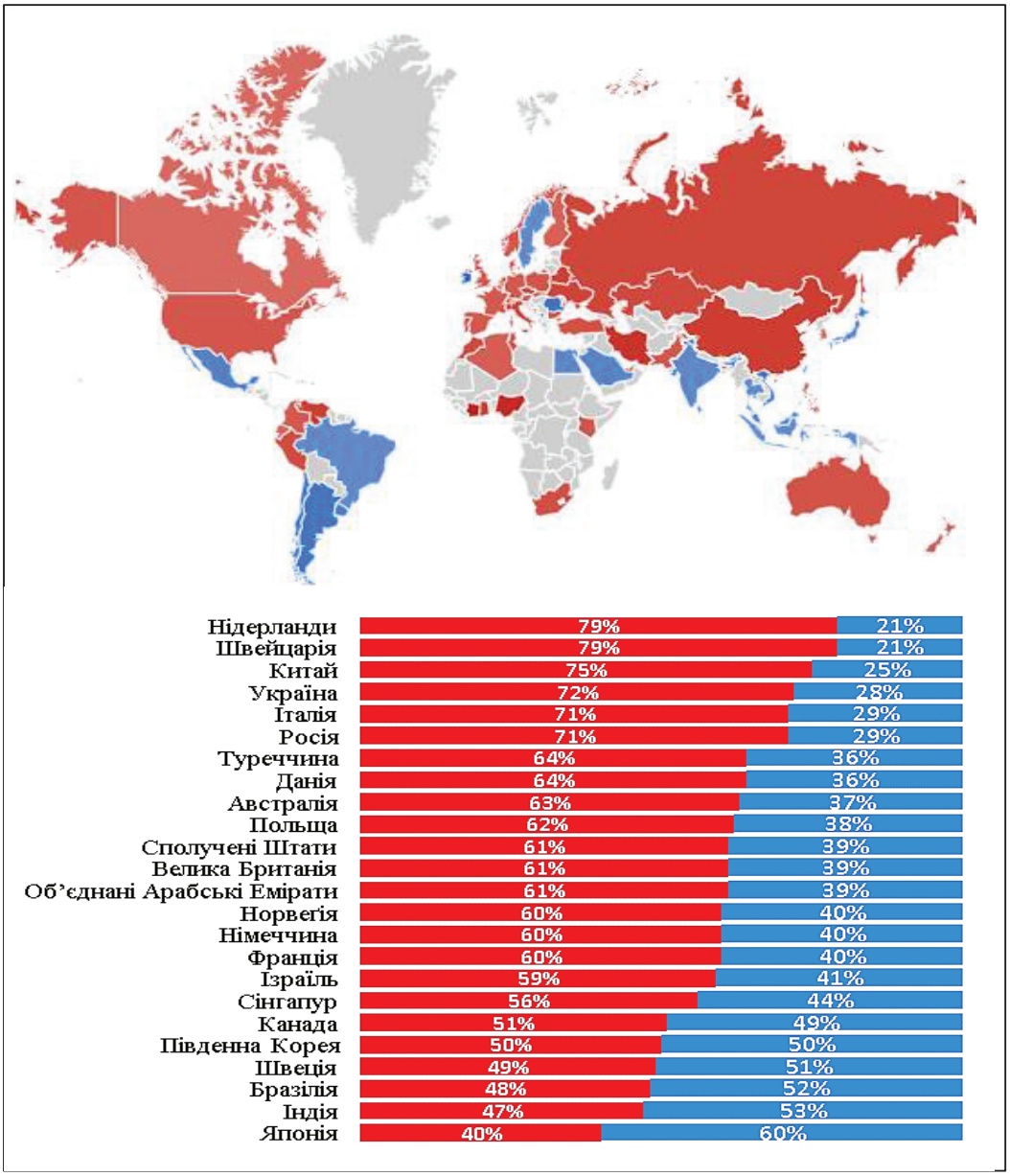

Рисунок 4 – Інфографіка рівня інтересу до тематики «Блокчейн» та «Штучний інтелект» в категорії запитів «Банківська діяльність» за географією

Джерело: складено авторами на основі бази даних Google Trends [13]

Список використаних джерел:

1. Bissel K., Lassale R.M., Dal Cin P. Ninth Annual Cost of Cybercrime Study. *Accenture* : веб-сайт. URL: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (дата звернення: 15.06.2020).

2. IBM X-Force Threat Intelligence Index. *IBM Security* : веб-сайт. URL: https://www.ibm.com/security/data-breach/threat-intelligence (дата звернення: 15.06.2020).

3. Spaic I. Ukraine: US$ 10 Million Stolen From Unnamed Bank via Swift. *Organized Crime and Corruption Reporting Project* : веб-сайт. URL: https://www.occrp.org/en/daily/5419-ukraine-us-10-million-stolen-from-unnamed-bank-via-swift (дата звернення: 15.06.2020).

4. Documents by year. *Scopus :* веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=d5f95877e42d30a74b35492c754c69f8&origin=resultslist&src=s&s=TITLE-ABS-KEY%28blockchain%29&sort=plf-f&sdt=b&sot=b&sl=25&count=12196&analyzeResults=Analyze+results&txGid=2f46048e78e0cab96ad1ca4fb03030ca (дата звернення: 15.06.2020).

5. Documents by subject area. *Scopus :* веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=d5f95877e42d30a74b35492c754c69f8&origin=resultslist&src=s&s=TITLE-ABS-KEY%28blockchain%29&sort=plf-f&sdt=b&sot=b&sl=25&count=12196&analyzeResults=Analyze+results&txGid=03c75a5c75eddec05d6295c1914e90d7 (дата звернення: 15.06.2020).

6. Documents by country or territory. *Scopus :* веб-сайт. URL: https://www.scopus.com/term/analyzer.uri?sid=d5f95877e42d30a74b35492c754c69f8&origin=resultslist&src=s&s=TITLE-ABS-KEY%28blockchain%29&sort=plf-f&sdt=b&sot=b&sl=25&count=12196&analyzeResults=Analyze+results&txGid=2f46048e78e0cab96ad1ca4fb03030ca (дата звернення: 15.06.2020).

7. Culp S., Kim F., Gomes R. Banking Risk: Evolving ecosystem, evolving threats. *Accenture* : веб-сайт. URL: https://www.accenture.com/us-en/insights/financial-services/banking-global-risk-study (дата звернення: 15.06.2020).

8. Casino F., Dasaklis T.K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*. 2019. Vol. 36. P. 55–81. DOI: https://doi.org/10.1016/j.tele.2018.11.006.

9. Bahou A.J. Blockchain and Applications in Information Security. *Information Systems Security Association* : веб-сайт. URL: https://issa-midtn.org/resources/Documents/AJ%20Bahou%20-%20Blockchain%20Applications%20in%20Information%20Security.pdf (дата звернення: 15.06.2020).

10. Sari A. Use of Blockchain in Strengthening Cybersecurity And Protecting Privacy. *International Journal of Engineering and Information Systems (IJEAIS).* 2018. Vol. 2. Issue 12. P. 59–66.

11. English E., Kim A.D., Nonaka M. Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry. *Microsoft Corporation* : електронний документ. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1TH5G (дата звернення: 15.06.2020).

12. Building confidence: solving banking`s cybersecurity conundrum. *Accenture* : веб-сайт. URL: https://www.accenture.com/_acnmedia/pdf-44/accenture-building-confidence-solving-banking-cybersecurity-conundrum.pdf (дата звернення: 15.06.2020).

13. Google Trends. *Google Trends* : веб-сайт. URL: https://trends.google.com/trends (дата звернення: 15.06.2020).

References:

1. Bissel K., Lassale R.M., Dal Cin P. Ninth Annual Cost of Cybercrime Study. *Accenture*. Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed 15 June 2020).

2. IBM X-Force Threat Intelligence Index. *IBM Security.* Available at: https://www.ibm.com/security/data-breach/threat-intelligence (accessed 15 June 2020).

3. Spaic I. Ukraine: US$ 10 Million Stolen From Unnamed Bank via Swift. *Organized Crime and Corruption Reporting Project.* Available at: https://www.occrp.org/en/daily/5419-ukraine-us-10-million-stolen-from-unnamed-bank-via-swift (accessed 15 June 2020).

4. Documents by year. *Scopus.* Available at: https://www.scopus.com/term/analyzer.uri?sid=d5f95877e42d30a74b35492c754c69f8&origin=resultslist&src=s&s=TITLE-ABS-KEY%28blockchain%29&sort=plf-f&sdt=b&sot=b&sl=25&count=12196&analyzeResults=Analyze+results&txGid=2f46048e78e0cab96ad1ca4fb03030ca (accessed 15 June 2020).

5. Documents by subject area. *Scopus.* Available at: https://www.scopus.com/term/analyzer.uri?sid=d5f95877e42d30a74b35492c754c69f8&origin=resultslist&src=s&s=TITLE-ABS-KEY%28blockchain%29&sort=plf-f&sdt=b&sot=b&sl=25&count=12196&analyzeResults=Analyze+results&txGid=03c75a5c75eddec05d6295c1914e90d7 (accessed 15 June 2020).

6. Documents by country or territory. *Scopus.* Available at: https://www.scopus.com/term/analyzer.uri?sid=d5f95877e42d30a74b35492c754c69f8&origin=resultslist&src=s&s=TITLE-ABS-KEY%28blockchain%29&sort=plf-f&sdt=b&sot=b&sl=25&count=12196&analyzeResults=Analyze+results&txGid=2f46048e78e0cab96ad1ca4fb03030ca (accessed 15 June 2020).

7. Culp S., Kim F., Gomes R. Banking Risk: Evolving ecosystem, evolving threats. *Accenture.* Available at: https://www.accenture.com/us-en/insights/financial-services/banking-global-risk-study (accessed 15 June 2020).

8. Casino F., Dasaklis T.K., Patsakis C. (2019) A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, vol. 36., pp. 55-81. DOI: https://doi.org/10.1016/j.tele.2018.11.006.

9. Bahou A.J. Blockchain and Applications in Information Security. Information Systems Security Association. Available at: https://issa-midtn.org/resources/Documents/AJ%20Bahou%20-%20Blockchain%20Applications%20in%20Information%20Security.pdf (accessed 15 June 2020).

10. Sari A. (2018) Use of Blockchain in Strengthening Cybersecurity And Protecting Privacy. International Journal of Engineering and Information Systems (IJEAIS), vol. 2., issue 12, pp. 59–66.

11. English E., Kim A.D., Nonaka M. Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry. *Microsoft Corporation.* Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1TH5G (accessed 15 June 2020).

12. Building confidence: solving banking`s cybersecurity conundrum. *Accenture.* Available at: https://www.accenture.com/_acnmedia/pdf-44/accenture-building-confidence-solving-banking-cybersecurity-conundrum.pdf (accessed 15 June 2020).

13. Google Trends. *Google Trends.* Available at: https://trends.google.com/trends (accessed 15 June 2020).

Yarovenko Hanna, Kovach Viktoriia
Educational and Scientific Institute of Business Technologies "UAB" of Sumy State University

PROSPECTS OF USING BLOCKCHAIN TECHNOLOGY IN BANKING CYBERSECURITY SYSTEMS

Identification and prevention of cyber threats by security systems is an urgent issue for banks. Ensuring this process requires the implementation of reliable, efficient, and modern technologies. The authors have devoted the article to the study of the prospects for the use of blockchain technology in bank cybersecurity systems. The paper has identified the features of the problems of ensuring banks' cybersecurity and its relevance. There has been described the leading technologies and tools that are now actively used to counter cyber attacks on banking institutions and their customers. The authors have emphasized artificial intelligence and machine learning, which are widely implemented in banking information systems, and are also used to solve individual tasks for bank cybersecurity. They have analyzed the possibilities of using the main advantages of blockchain technology in the fight against major cyber threats. The authors highlighted such benefits as decentralization, complete transparency, confidentiality, protection against unauthorized access, and compromise. It has been revealed that blockchain technology could potentially significantly reduce or even eliminate some types of vulnerabilities in existing banking systems. The authors have carried out an analysis of the level of interest in this technology in the areas of computer security and bank activities in the world over the past five years using the Google Trends database. The level of interest in artificial intelligence exceeds the level of interest in the blockchain in the category of requests related to computer security. The main reason is the widespread use of this technology and its effectiveness in investments. The situation is opposite in the category of requests related to banking. The authors have connected it with the creation of blockchain technology that was associated with the field of financial instruments and banking. They have also compared the level of interest in blockchain and artificial intelligence in the world and individual countries. As a result, it was found that both technologies are quite famous and their use can complement each other for implementation in banks' cybersecurity systems.

Key words: *bank, blockchain technology, system vulnerability, cybersecurity, cyber threat, artificial intelligence.*

JEL classification: G20, L86, O14