https://doi.org/10.31891/2307-5740-2022-310-5(1)-8
УДК 336.7:004.056

Раїса КВАСНИЦЬКА
Хмельницький національний університет
https://orcid.org/orcid.org/0000-0002-0443-9390
e-mail: rstepanivna@gmail.com
Ірина ФОРКУН
Хмельницький національний університет
https://orcid.org/0000-0002-4588-6349
e-mail: ivforkun@gmail.com
Тетяна ГОРДЄЄВА
Хмельницький національний університет
https://orcid.org/0000-0003-3546-4238
e-mail: gordeevat_2004@ukr.net

СУЧАСНІ ПІДХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ ТА ЇХ КІБЕРЗАХИСТУ

В статті здійснено аналіз вітчизняних та світових підходів науковців та фінансових інституцій щодо трактування сутності платіжних систем, проаналізовано особливості їх функціонування та можливості врахування міжнародних стандартів обміну фінансовими повідомленнями ISO 20022 у платіжній інфраструктурі України.

Визначено, що сфера функціонування платіжних систем відноситься до ризикових сфер діяльності, якій притаманні такі види ризиків: правовий, розрахунковий, операційний, системний та фінансові ризики. Обґрунтовано, що основою ефективного функціонування банківських установ в умовах невизначеності є ідентифікація та управління ризиками, притаманними банківській діяльності. При цьому, акцент зроблено на тому, що складовою операційного ризику є такий вид ризику як кіберризик, який розглядається як ризик реалізації кіберзагроз щодо інформаційних ресурсів та/або інформаційної інфраструктури, а також наслідки таких подій. Враховуючи те, що сучасні платіжні системи є посередниками у русі грошових коштів, а тому перебувають під ризиком негативних впливів, викликів, загроз та небезпек, що може привести до нанесення збитків національним інтересам держав, запропоновано розглядати кіберризик як окремий тип ризиків функціонування платіжних систем.

Ключові слова: платіжна система, міжнародна платіжна система, ризики платіжних систем, інформаційна безпека розрахунків, політика інформаційної безпеки банку.

Raisa KVASNYTSKA, Iryna FORKUN, Tetyana GORDEEVA
Khmelnytskyi National University

MODERN APPROACHES TO PROVIDING INFORMATION SECURITY OF PAYMENT SYSTEMS AND THEIR CYBER PROTECTION

The article analyzes the domestic and international approaches of scientists and financial institutions regarding the interpretation of the concept of payment systems and proposes the author's interpretation of this category as "an organizationally formed set of system participants and the relations between them regarding the transfer of funds based on recognized legal norms at the level of sovereign countries or at the international level. The peculiarities of the payment systems' functioning and the possibility of taking into account the international standards for the exchange of financial messages ISO 20022 in the payment infrastructure of Ukraine were analyzed, which will allow to harmonize the Ukrainian payment area with the world, to expand the details of payments with additional information, to increase the level of service and efficiency of payments, to enrich the functional content of payment instruments for the benefit of banks and their customers, increase the level of automation of payments.

It was determined that the area of the payment systems' functioning belongs to the risky spheres of activity. The typification of the payment systems' risks of banking and non-banking institutions, determined by the regulations of the National Bank of Ukraine, defines such types of risks as legal, payment, operational, systemic and financial risks. It is substantiated that the basis of the effective functioning of banking institutions in conditions of uncertainty is the identification and management of risks inherent in banking activity. At the same time, the emphasis is on the fact that a component of operational risk is such a type of risk as cyber risk, which is considered as the risk of realizing cyber threats to information resources and/or information infrastructure, as well as the consequences of such events. Because modern payment systems are intermediaries in the movement of funds, and therefore are at risk of negative influences, challenges, threats and dangers, which can lead to damage to the national interests of states, it is proposed to consider cyber risk as a separate type of risks of the payment systems' functioning.

In order to prevent, detect, respond, absorb cyber risk, and ensure adaptability and the ability to restore the payment system, the central bank of the state should increase the level of information security and cyber protection in the field of funds transfer. The information security policy of banks must be constantly supplemented and changed in accordance with the specified set of criteria for assuring information security.

Key words: payment system, international payment system, risks of payment systems, information security of payments, the bank's information security policy.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Важливою складовою економічної та фінансової інфраструктури країн світу є різноманітні платіжні системи. В цьому сенсі не є винятком і Україна, за останні роки в економіці і банківській системі якої

відбулися радикальні зміни, обумовлені розвитком ринкових відносин національної економіки. Сьогодні стан внутрішньодержавних і міжнародних розрахунків країни характеризується стрімким зростанням обсягів грошового обороту, зменшенням імовірності настання ризиків, підвищенням безпеки здійснення розрахунків через платіжні системи та системи переказів грошей. Це зумовлює необхідність дослідження суті, різновидів та особливостей функціонування платіжних систем в сучасних мінливих умовах розвитку економічних відносин між суб'єктами економіки національного та міжнародного рівнів.

Аналіз останніх досліджень і публікацій

Стратегічному розвитку діджиталізації розрахунково-платіжних операцій між суб'єктами економіки приділено велику увагу на урядовому рівні багатьох провідних країн світу (США, Китаю, Японії, Канади, Австралії та ін.). Питання розвитку інформаційної (цифрової) економіки є постійними в напрямах досліджень міжнародних організацій, таких як: Світовий банк, ОЕСР, Європейська Комісія тощо. Розгляду функціоналу різних платіжних та грошових систем, дослідженню їх переваг, безпечності та можливостей розвитку приділено увагу в працях багатьох економістів, а саме: П. Адамик, О. Вовчак, О. Джусов, І. Кравченко, Т. Коккола, А. Сааді, Б. Саммерс, Дж. Спиндлер, Н. Трусова, І. Чкан та інші. В них проведено ґрунтовні дослідження функціонування та розвитку платіжних систем, виділено недоліки електронних платежів, акцентовано увагу на їх низькій захищеності. Значну увагу автори приділяють питанням рівня безпеки платіжних систем та їх трансформації під впливом інноваційного розвитку і новітніх технологій.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується стаття

Існуючі та потенційні загрози безпеці платіжних систем створюють імовірність порушення штатного режиму їх функціонування (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів, що вимагає додаткових досліджень за даним напрямом.

Формулювання цілей статті

Метою дослідження є обґрунтування сутності платіжних систем, їх ролі в забезпечені прискорення грошового обороту як на рівні окремої країни, так і на міжнародному рівні, дослідження міжнародного досвіду центральних банків та підходів експертів Світового банку та Міжнародного валютного фонду щодо оверсайту платіжних систем з метою забезпечення ефективного їх функціонування.

Виклад основного матеріалу дослідження

Розрахункові операції та платежі займають вагоме місце в ринковій економіці будь якої держави, обслуговуючи переміщення грошей між суб'єктами економіки, а також в міжнародному економічному просторі. Адже, суб'єкти економіки щодня здійснюють велику кількість операцій з обміну товарів, послуг і фінансових активів, які, своєю чергою, опосередковуються грошовими розрахунками та переказами. За умов розвитку економіки нового типу важливою запорукою стабільного функціонування економіки як окремих країн, так і світової економіки є активне використання функціоналів платіжних систем, які останнім часом отримали стрімкий розвиток і в Україні. Саме розширення видів платіжних систем, спектру їх функціональних можливостей здійснює вагомий вплив на розвиток платіжної інфраструктури країни, виникнення нових видів платіжних інструментів, які, залежно від їх конкретних видів, можуть стимулювати появу нових ринків, зростання національних економік, підвищення їх конкурентоспроможності, зменшення безробіття, покращення рівня життя.

Що ж представляє собою платіжна система? Варто зазначити, що єдиного підходу до трактування поняття «платіжна система» не вироблено ні на рівні нормативного визначення в міжнародних сферах функціонування цих систем, ні на рівні позиціювання в наукових колах. Так, Комітет з платіжних систем та систем розрахунків Банку міжнародних розрахунків регламентує платіжну систему як «набір інструментів, процедур і правил переказу коштів між учасниками чи серед учасників; система включає учасників та організацію, яка є її оператором» [1] Представник Європейського центрального банку Том Коккола зазначав, що платіжна система є «офіційною угодою на основі приватного договору або законодавства з кількома членами, загальними правилами і стандартизованими механізмами для передачі, клірингу, неттингу та/або погашення грошових зобов'язань, що виникають між його членами» [2] У Законі України «Про платіжні послуги» визначено платіжну систему як «систему для виконання платіжних операцій із формальними та стандартизованими домовленостями і загальними правилами щодо процесингу, клірингу та/або виконання розрахунків між учасниками платіжної системи [3]. Узагальнюючи можемо стверджувати, що платіжна система є саме організаційно сформованою сукупністю учасників системи та відносин між ними щодо проведення переказів коштів основі визнаних норм законодавства на рівні окремих країн чи на міжнародному рівні.

Слід зазначити, що в Україні як і в усьому світі спостерігається тенденція до стрімкого зростання обсягів безготівкових розрахунків та платежів. Переказ грошей в Україні здійснюється за допомогою внутрішньодержавних та міжнародних платіжних систем. На 01.01.2022 р. в Україні функціонувало 54

платіжні системи, з яких [4]:

2 - державні платіжні системи (Система електронних платежів (СЕП) та Національна платіжна система «Український платіжний простір», що налічує 78 банків-учасників);

9 - платіжних систем, платіжною організацією якої є банку, які налічують 165 учасників. Найбільшою за кількістю учасників (51 учасник) є міжнародна платіжна система «Welsend» АТ «УКРГАЗБАНК» (Україна);

21 - платіжна система, платіжною організацією якої є небанківська установа, які налічують 157 учасників. Найбільшою за кількістю учасників (26 учасників) є міжнародна система переказу коштів «AVERS №1» АТ «ФК "АВЕРС» (Україна);

6 - міжнародних карткових платіжних систем, які налічують 119 учасників. Найбільшою за кількістю учасників (55 учасників) є міжнародна карткова платіжна система «MasterCard» (США);

10 - міжнародних систем переказу коштів, які налічують 71 учасника. Найбільшою за кількістю учасників (18 учасників) є міжнародні системи переказу коштів «RIA» та «MoneyGram» (США);

6 – внутрішньобанківських платіжних систем.

Відмітимо, що сьогодні Національний банк України у партнерстві із компанією SWIFT реалізовує проект з впровадження міжнародного стандарту обміну повідомленнями ISO 20022 в платіжній інфраструктурі України. Перехід на використання міжнародних стандарті обміну фінансовими повідомленнями у платіжній інфраструктурі України, дасть можливість: гармонізувати український платіжний простір зі світовим; розширити реквізити платежів додатковою інформацією; підвищити рівень обслуговування та ефективності платежів; збагатити функціональне наповнення платіжних інструментів на користь банків та їх клієнтів; підвищити рівень автоматизації платежів [5].

Звичайно, сфера функціонування платіжних систем відноситься до ризикових сфер діяльності, що пояснюється наявністю значної кількості зв'язків між учасниками, обсягом та розміром виконуваних у цих системах операцій, високою мобільністю та оперативністю розрахунків, швидким розвитком новітніх технологій, розвитком систем дистанційного банківського обслуговування, що своєю чергою створює потенційні можливості для порушення нормального проходження платежів, що може негайно викликати величезні негативні наслідки для усієї платіжної системи. Управління рівнем ризику передбачає проведення аналізу ризиків у процесі стратегічного, тактичного та оперативного планування і дає змогу отримати якісну та кількісну оцінку можливих ризиків [6, p.47]. Так, Національним банком України розроблено Положення про порядок здійснення оверсайту платіжної інфраструктури в Україні [7], Методичні рекомендації з управління ризиками в платіжних системах [8] та Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури [9], які враховують кращий міжнародний досвід центральних банків та підходи експертів місій Світового банку та Міжнародного валютного фонду з питань оверсайту платіжних систем. Серед основних ризиків у банківській і небанківській сферах є операційний ризик, тобто ризик втрати прибутку через помилки здійснення щоденних традиційних фінансових операцій [10, p. 261]. При цьому, нормативними документами Національного банку України визначено, що кіберризик є складовою операційного ризику. Однак, враховуючи те, що сучасні платіжні системи є посередниками у русі грошових коштів, а тому перебувають під ризиком негативних впливів, викликів, загроз та небезпек, що може привести до нанесення збитків національним інтересам держави, кіберризик варто розглядати як окремий тип ризиків платіжної системи (табл. 1).

Для попередження та уникнення кіберризику центральний банк держави має підвищувати рівень інформаційної безпеки та кіберзахист у сфері переказу коштів. З метою посилення надійності та ефективності роботи платіжних систем регулятор має встановлювати чіткі вимоги до учасників платіжного ринку щодо:

- побудови системи захисту інформації та забезпечення кібербезпеки;
- готовності до можливих кібератак, захищеності, здатності виявляти кібератаки, реагувати та поглинати їх, забезпечення адаптивності та можливості їх відновлення [11] та порядку дій під час виявлення кібератак, що знижують надійність функціонування платіжних систем.

Одними з основних суб'єктів створення платіжних систем, їх платіжними організаціями та учасниками є банківські установи. Саме банки, в процесі здійснення платежів, переказів та розрахунків через функціонал певної платіжної системи, стикаються з необхідністю захисту власної та клієнтської інформації та забезпечення кібербезпеки. Тому, питання щодо політики інформаційної безпеки банківських установ не є новим, воно періодично висвітлюється у наукових працях вчених протягом останніх десятиліть, оскільки саме протягом них йшла активна інформатизація банківської діяльності, але на особливої актуальності набирає це питання в наш час, на який припав бум діджиталізації послуг. Політика інформаційної безпеки — набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації [12]. Так, з метою проведення аналізу сучасних банківських практик щодо забезпечення ними інформаційної безпеки в Україні, було зроблено таку вибірку банків: з числа лідерів за обсягами активів в межах кожної групи, виділеної відповідно до рішення Комітету з питань нагляду та регулювання діяльності

банків, нагляду (оверсайту) платіжних систем НБУ від 5 лютого 2021 року № 40, було обрано по два банки. Такими банками є: банки з державною часткою: АТ КБ «ПРИВАТБАНК» та АТ «Державний ощадний банк України); банки іноземних банківських груп: АТ «РАЙФФАЙЗЕН БАНК» та АТ «УКРСИББАНК»; банки з приватним капіталом: АТ «УНІВЕРСАЛ БАНК» та АТ «ТАСКОМБАНК».

Таблиця 1

Типізація ризиків платіжних систем банківських і небанківських установ

Типізація ризиків	Характерні ознаки
Правовий ризик	ризик відсутності правового регулювання, зміни або непередбачуваного застосування положень законодавства України, що можуть призвести до виникнення збитків об'єкта оверсайту
Фінансові ризики	кредитний ризик – ризик того, що об'єкт оверсайту не зможе виконати свої фінансові зобов'язання в повному обсязі в установлений момент часу або в будь-який момент у подальшому
	ризик ліквідності – ризик того, що об'єкт оверсайту не матиме достатньо коштів для виконання своїх фінансових зобов'язань належним чином у повному обсязі в установлений момент часу, але він зможе їх виконати в інший момент часу в подальшому
	загальний комерційний ризик – ризик погіршення фінансового стану об'єкта оверсайту в результаті зниження його доходів або збільшення видатків, унаслідок якого витрати перевищують доходи та призводять до втрат, покриття яких здійснюється за рахунок капіталу
	депозитарний ризик - ризик втрати фінансових активів об'єкта оверсайту
	інвестиційний ризик - ризик втрати або недоступності фінансових активів об'єкта оверсайту, що виникає внаслідок їх інвестування
Розрахунковий ризик	ризик того, що розрахунки в платіжній системі не здійснюватимуться належним чином
Операційний ризик	ризик того, що недоліки інформаційних систем або внутрішніх процесів, людські помилки, операційні збої, втрата або витік інформації, шахрайство або порушення в управлінні внаслідок зовнішніх подій призведуть до скорочення, погіршення або зупинення надання послуг об'єктом оверсайту
Кіберризик	ризик реалізації кіберзагроз щодо інформаційних ресурсів та/або інформаційної інфраструктури, а також наслідки таких подій
Системний ризик	ризик того, що неспроможність одного з учасників платіжної системи та/або оператора послуг платіжної інфраструктури виконати свої зобов'язання або порушення безперервності діяльності самої платіжної системи призведе до порушення діяльності учасників платіжної системи, інших установ або функціонування фінансової системи в цілому

Складено авторами за джерелами [7-9]

Ці банки пропонують клієнтам широкий спектр платіжних та розрахункових послуг, оскільки вони є учасниками багатьох міжнародних платіжних систем та систем термінових грошових переказів. Різноманіття використання банками України систем термінових грошових переказів та платіжних послуг призводить до зростання ймовірності реалізації ризику порушення інформаційної безпеки під час проведення розрахунків за їх допомогою. При цьому, проблеми із порушенням інформаційної безпеки слід розглядати з двох сторін:

1) зі сторони клієнта, що може виконувати частину банківських операцій самостійно завдяки технологіям дистанційного обслуговування та e-banking;

2) зі сторони банківського працівника, що зумисно або з необережності може порушувати запроваджену у банку політику інформаційної безпеки.

Перший напрям забезпечення інформаційної безпеки передбачає підвищення фінансової грамотності клієнтів. За другим напрямом убезпечення та попередження інцидентів інформаційної безпеки, банками розробляється такий внутрішній нормативний документ, як «Політика інформаційної безпеки», який в обов'язковому порядку оприлюднюється на офіційному сайті кожного банку. Таким чином, «Політика інформаційної безпеки» є документом, який формулює та висловлює позицію керівництва банку щодо інформаційної безпеки, а також визначає основні принципи та завдання забезпечення інформаційної безпеки в банку [13]. Основними цілями забезпечення інформаційної безпеки є забезпечення таких якісних характеристик інформації, як: конфіденційність, цілісність, доступність, спостережність. Зауважимо, що в банках, які попали до нашої вибірки, є спільним те, що суттєвий вплив на політику інформаційної безпеки чинить саме тип власності, до якої належить банк.

Пропонуємо проводити аналіз інформаційної політики за такими критеріями: нормативно-правовий; організаційний (рівні ієрархії в СУІБ); технічний (принцип надання мінімального рівня повноважень під час доступу до ІС банку); психологічний (фактор «людини-виконавця»).

Так, по першому з запропонованих нами критеріїв, а саме нормативно-правовому, АТ «КБ «ПриватБанк» і АТ «Державний ощадний банк України», що є банками з державною часткою, надають детальний перелік законів України, нормативно-правових актів НБУ з інформаційної безпеки та стандартів безпеки даних індустрії платіжних карток PCI DSS [13, 14]. АТ «РАЙФФАЙЗЕН БАНК» та АТ «УКРСИББАНК», що входять до іноземних банківських груп, характеризують свою політику, яка регламентує систему управління інформаційною безпекою як таку, що відповідає вимогам законодавства України з інформаційної безпеки. Водночас, додатково посилаються на нормативні документи міжнародних банківських груп. Так, політика АТ «РАЙФФАЙЗЕН БАНК» ґрунтується на нормативному документі

Групи РБІ REG-2016-0065 Group IT Security [15]; в АТ «УКРСИББАНК» – на Політиці інформаційної безпеки BNP Paribas Group та програмі CyberSecurity Program 2020 [16]. Банки з приватним капіталом – АТ "УНІВЕРСАЛ БАНК" та АТ "ТАСКОМБАНК" – лише в загальному зазначають, що політика банку відповідає законодавству України та нормативно-правовим актам НБУ, які стосуються інформаційної безпеки [17].

По другому, організаційному критерію, спільною є наявність «Системи управління інформаційною безпекою» (СУІБ), через яку організовується управління інформаційною безпекою банку завдяки консолідації людських, методологічних, інтелектуальних та програмно-технічних ресурсів [18]. Однак, у рівнях СУІБ та їх ієрархії проглядаються певні особливості. Так, у банків з державною часткою є спільна риса – розгалужена багаторівнева СУІБ, хоча в АТ «КБ «ПриватБанк» СУІБ більш компактна. Управління інформаційною безпекою у банках іноземних банківських груп та у банках з приватним капіталом здійснюється через СУІБ банку, що спрямована на захист інформаційних ресурсів та активів банків від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями його працівників чи третіх осіб.

Технічний критерій забезпечення інформаційної безпеки можна охарактеризувати через: забезпечення конфіденційності інформації; захист від шкідливого програмного забезпечення; резервне копіювання і відновлення інформації; ліцензійну чистоту; забезпечення фізичної безпеки; управління доступами; управління правами та повноваженнями; управління способами авторизації. Більшість з перерахованого не деталізується банками в «Політиці інформаційної безпеки», оскільки має характер банківської та комерційної таємниці. Усі банки із вибірки дотримуються принципу надання мінімального рівня повноважень під час надання доступу.

В розвиток дотримання цього принципу доцільно проводити і за четвертим критерієм, оскільки дотримання усіх правил, виконання обов'язків та повноважень залежить у першу чергу від конкретної «людини-виконавця». Так, банки покладають на працівників відповідальність за невиконання вимог інформаційної безпеки, встановлених внутрішніми документами банку та нормами чинного законодавства. АТ «УКРСИББАНК» окремо виділяє пункт «Реагування на інциденти інформаційної безпеки»[16]. Цікавою особливістю забезпечення інформаційної безпеки в АТ "УНІВЕРСАЛ БАНК" є Політика «Чистого робочого столу» (відносно робочих місць, паперових носіїв, змінних електронних носіїв інформації) та «Чистого екрану» (відносно автоматизованих робочих місць з метою зменшення ризику неавторизованого доступу) спрямована на забезпечення додаткового захисту інформації в приміщеннях банку [17]. Зауважимо, що у АТ "ТАСКОМБАНК" в політиці інформаційної безпеки є пункт «Модель загроз та модель порушника» [18]. Цей пункт дає опис актуальних загроз інформаційній безпеці та опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей.

Таким чином, банками використовуються стандартизовані положення у забезпеченні інформаційної безпеки, які ґрунтуються на світових стандартах та правилах і вітчизняному законодавстві та нормативному регулюванні НБУ. Окремі особливості можуть бути продиктовані приналежністю банків до різних груп за правом власності, корпоративною культурою тощо. Вважаємо за доцільне також акцентувати увагу на наведених вище особливостях політик інформаційної безпеки АТ "ТАСКОМБАНК", а саме опис «Моделі загроз та моделі порушника» із ранжуванням типів загроз та притаманних їм рівнів ризику, та АТ "УНІВЕРСАЛ БАНК", а саме впровадження правил «Чистого робочого столу» та «Чистого екрану», оскільки їх більш широка імплементація у практику забезпечення інформаційної безпеки більшості вітчизняних банків підвищить ефективність управління ризиками та рівень захисту від кібер-загроз.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

На основі отриманих результатів дослідження можна зробити висновок, що важливою запорукою стабільного функціонування економіки як окремих країн, так і світової економіки є активне використання функціоналів платіжних систем, що є організаційно сформованою сукупністю учасників системи та відносин між ними щодо проведення переказів коштів основі визнаних норм законодавства на рівні окремих країн чи на міжнародному рівні. Наявність значної кількості зв'язків між учасниками платіжних систем, обсягом та розміром виконуваних у цих системах операцій, високою мобільністю та оперативністю розрахунків, швидким розвитком новітніх технологій, розвитком систем дистанційного банківського обслуговування є визначальними чинниками ризиковості сфери функціонування платіжних систем. Одним із ризиків, що може виникнути внаслідок реалізації кіберзагроз щодо інформаційних ресурсів та/або інформаційної інфраструктури, а також може бути наслідком таких подій, є ризик кіберризик. Для попередження виявлення, реагування, поглинання кіберризику, забезпечення адаптивності та можливості відновлення платіжної системи центральний банк держави має підвищувати рівень інформаційної безпеки та кіберзахист у сфері переказу коштів. Політика інформаційної безпеки банків має постійно доповнюватися і змінюватися згідно із зазначеною критеріальною сукупністю її забезпечення, що підлягає захисту. Ефективне управління кіберризиком є важливою складовою у забезпеченні загальної безпеки функціонування платіжної системи. З метою ефективного управління кіберризиками доцільно

удосконалювати підходи до розробки політики інформаційної безпеки платіжних організацій платіжних систем. Тому предметом подальших досліджень слід обрати розробку ефективних способів ідентифікації кіберризику, оцінки його впливу на ефективність функціонування платіжних систем.

Література

1. Principles for financial market infrastructures. CPSS-IOSCO. URL: https://cutt.ly/EBeDZtU (28.09.2022)
2. Kokkola T. The payment system payments, securities and derivatives, and the role of the Eurosystem. ECB, 2010, 369 p.
3. Про платіжні послуги : Закон України № 2180-IX від 01.04.2022. URL: https://cutt.ly/oBeDNov (28.09.2022)
4. Інформація з Реєстру платіжних систем, систем розрахунків, учасників цих систем та операторів послуг платіжної інфраструктури НБУ. URL: https://bit.ly/3fmoBzm (28.09.2022)
5. ISO 20022 implementation in the payment infrastructure of Ukraine. URL: https://bank.gov.ua (23.09.2022)
6. Kvasnytska R., Dotsenko I., Matviychuk L., Oliinyk L. Organization of Management of Moral Risks of Banking Activity in a Modern Business Environment. Lecture Notes in Networks and Systemsthis link is disabled, 487, 243–249 (2022).
7. Про порядок здійснення оверсайту платіжної інфраструктури в Україні : Постанова НБУ № 187 від 24.08.2022. URL: https://cutt.ly/gBeF76G (29.09.2022)
8. Національний банк України, Методичні рекомендації з управління ризиками в платіжних системах. URL: https://cutt.ly/sBeGc5q (29.09.2022)
9. Національний банк України, методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури. URL: https://bit.ly/3rhGHW6 (29.09.2022)
10. Трусова Н., Чкан І. Платіжні системи в Україні та ризики їх функціонування. *Бізнес Інформ.* 2021, № 1. С. 257–263.
11. Lysenko S., Bobrovnikova K., Gaj P., Sochor T., Forkun I. Resilient computer systems development for cyberattacks resistance. *CEUR Workshop Proceedings 2853.* 2021, P. 353–361. URL: http://ceur-ws.org/Vol-2853/short41.pdf
12. Політика інформаційної безпеки. URL: https://bit.ly/3Cnkf47 (29.09.2022)
13. Політика інформаційної безпеки в АТ «ОЩАДБАНК». URL: https://cutt.ly/kVVLPnG (29.09.2022)
14. Політика інформаційної безпеки АТ КБ «ПРИВАТБАНК». URL: https://cutt.ly/TVVXhc8, (29.09.2022)
15. Політика інформаційної безпеки АТ «Райффайзен Банк Аваль». URL: https://cutt.ly/3VVL4pC, (29.09.2022)
16. Політика інформаційної безпеки АТ «УКРСИББАНК». URL: https://cutt.ly/OVVZTWO, (29.09.2022)
17. Політика інформаційної безпеки АТ «УНІВЕРСАЛ БАНК». URL: https://ppt-online.org/931513, (29.09.2022)
18. Політика інформаційної безпеки АТ «ТАСКОМБАНК». URL: https://cutt.ly/eVVZ7bm (29.09.2022)

References

1. Principles for financial market infrastructures. CPSS-IOSCO. URL: https://cutt.ly/EBeDZtU (28.09.2022)
2. Kokkola T. The payment system payments, securities and derivatives, and the role of the Eurosystem. ECB, 2010, 369 r.
3. Pro platizhni posluhy : Zakon Ukrainy № 2180-IX vid 01.04.2022. URL: https://cutt.ly/oBeDNov (28.09.2022)
4. Informatsiia z Reiestru platizhnykh system, system rozrakhunkiv, uchasnykiv tsykh system ta operatoriv posluh platizhnoi infrastruktury NBU, URL: https://bit.ly/3fmoBzm (28.09.2022)
5. ISO 20022 implementation in the payment infrastructure of Ukraine. URL: https://bank.gov.ua (23.09.2022)
6. Kvasnytska R., Dotsenko I., Matviychuk L., Oliinyk L. Organization of Management of Moral Risks of Banking Activity in a Modern Business Environment. Lecture Notes in Networks and Systemsthis link is disabled, 487, 243–249 (2022).
7. Pro poriadok zdiisnennia oversaitu platizhnoi infrastruktury v Ukraini : Postanova NBU № 187 vid 24.08.2022. URL: https://cutt.ly/gBeF76G (29.09.2022)
8. Natsionalnyi bank Ukrainy, Metodychni rekomendatsii z upravlinnia ryzykamy v platizhnykh systemakh. URL: https://cutt.ly/sBeGc5q (29.09.2022)
9. Natsionalnyi bank Ukrainy, metodychni rekomendatsii shchodo upravlinnia operatsiinym ryzykom (u tomu chysli kiberryzykom ta bezperervnistiu diialnosti) ta zabezpechennia zberihannia informatsii pro kliientiv obiektamy platizhnoi infrastruktury. URL: https://bit.ly/3rhGHW6 (29.09.2022)
10. Trusova N., Chkan I. Platizhni systemy v Ukraini ta ryzyky yikh funktsionuvannia. Biznes Inform. 2021, № 1, S. 257–263.
11. Lysenko S., Bobrovnikova K., Gaj P., Sochor T., Forkun I. Resilient computer systems development for cyberattacks resistance. CEUR Workshop Proceedings 2853. 2021, R. 353–361. URL: http://ceur-ws.org/Vol-2853/short41.pdf
12. Polityka informatsiinoi bezpeky. URL: https://bit.ly/3Cnkf47 (29.09.2022)
13. Polityka informatsiinoi bezpeky v AT «OShchADBANK». URL: https://cutt.ly/kVVLPnG (29.09.2022)
14. Polityka informatsiinoi bezpeky AT KB «PRYVATBANK». URL: https://cutt.ly/TVVXhc8, (29.09.2022)
15. Polityka informatsiinoi bezpeky AT «Raiffaizen Bank Aval». URL: https://cutt.ly/3VVL4pC, (29.09.2022)
16. Polityka informatsiinoi bezpeky AT «UKRSYBBANK». URL: https://cutt.ly/OVVZTWO, (29.09.2022)
17. Polityka informatsiinoi bezpeky AT «UNIVERSAL BANK». URL: https://ppt-online.org/931513, (29.09.2022)
18. Polityka informatsiinoi bezpeky AT «TASKOMBANK». URL: https://cutt.ly/eVVZ7bm (29.09.2022)