ГРОШІ, ФІНАНСИ І КРЕДИТ

УДК 336.7:004.056
DOI: https://doi.org/10.32782/2224-6282/183-13

Міщенко В.І.
доктор економічних наук, професор,
Інститут економіки та прогнозування НАН України
ORCID: https://orcid.org/0000-0002-8565-2686

Науменкова С.В.
доктор економічних наук, професор,
Київський національний університет імені Тараса Шевченка
ORCID: https://orcid.org/0000-0001-8582-6044

Міщенко С.В.
доктор економічних наук, професор,
Львівський національний університет імені Івана Франка
ORCID: https://orcid.org/0000-0002-1840-8579

Mishchenko Volodymyr
Institute for Economics and Forecasting of the NAS of Ukraine
Naumenkova Svitlana
Taras Shevchenko National University of Kyiv
Mishchenko Svitlana
Ivan Franko National University of Lviv

УПРАВЛІННЯ ОПЕРАЦІЙНИМИ РИЗИКАМИ В ПЛАТІЖНИХ СИСТЕМАХ

У статті досліджено особливості управління операційними ризиками в платіжних системах в умовах поглиблення цифровізації платіжного ринку. Визначено головні джерела виникнення, наведено характеристику форм прояву окремих видів операційних ризиків, проведено їх класифікацію, визначено головні результати потенційного впливу на діяльність платіжних систем, запропоновано метод розрахунку показника притаманності ризику. Охарактеризовано структуру, головні складові системи управління ризиками та розроблено схему функціонування механізму управління ними. Запропоновано систему ключових індикаторів, що характеризують граничні межі зміни рівня операційного ризику. Визначено головні джерела покриття збитків і втрат, що виникають унаслідок реалізації подій операційного ризику. Охарактеризовано головні джерела виникнення та особливості впливу на діяльність платіжних систем кіберзагроз. Запропоновано систему заходів щодо підвищення ефективності управління операційними ризиками на основі вдосконалення техніко-технологічних та організаційно-управлінських характеристик функціонування платіжних систем.

Ключові слова: *платіжна система, платіжна організація, операційний ризик, механізм управління ризиками, кіберзагрози, інформаційний ризик, кіберризик.*

MANAGEMENT OF OPERATIONAL RISKS IN PAYMENT SYSTEMS

The article examines the peculiarities and forms of manifestation of operational risks in payment systems in the conditions of increased digitalization of the payment services market. Based on the analysis of the recommendations of international financial organizations and the National Bank of Ukraine, a classification of operational risks inherent in the activity of payment systems was carried out, and four types of them were distinguished: information risk, risk of errors in management processes, cyber risk and risk of user errors. The main sources of operational risks are identified and it is proven that the vast majority of them are related to the use of new information technologies and the strengthening of cyber threats in the market of payment services. The analysis of operational risk management practices in payment systems allows to conclude that they are heterogeneous and depend on factors that expose payment organizations and payment systems to risks. The characteristics of the forms of manifestation of certain types of operational risks in payment systems are given. The main results of the potential impact of operational risks on the activity of payment systems are characterized, and a method of calculating the indicator of inherent risk is proposed, which characterizes the level of its priority for the payment organization. It is determined that the main goal of operational risk management in payment systems is to maintain the operational stability of the payment organization and ensure the continuity of the payment system. The structure and main components of the operational risk management system are characterized. A functioning scheme of the operational risk management mechanism in the payment system has been developed, the use of which makes it possible to increase the efficiency of their management. A system of key indicators characterizing the limits of changes in the level of operational risk is proposed and can be used for the purpose of early detection and assessment of the potential impact of individual risk factors. The main sources of coverage of damages and losses arising as a result of implementation of operational risk events in the payment system are determined. The main sources of occurrence and features of the influence on the activity of payment systems of

cyber threats are characterized. A system of measures to increase the efficiency of operational risk management based on the improvement of the technical-technological and organizational-management characteristics of the functioning of payment systems is proposed.

Keywords: *payment system, payment organization, operational risk, mechanism of risk management, cyber threats, information risk, cyber risk.*

JEL classification: *D81, G35, G39*

Постановка проблеми. В умовах поглиблення процесів цифровізації фінансового сектору найбільш динамічного розвитку набув ринок платіжних послуг. Сучасні платіжні системи ґрунтуються на використанні електронних платіжних інструментів і є високотехнологічними сервісами, що забезпечують здійснення розрахунків і платежів з використання інформаційно-комунікаційних технологій. Крім банків і фінансових установ, такі послуги надають нефінансові організації та fintech-компанії, на які припадає більше чверті платіжного ринку. Станом на 01.01.2022 р. в Україні функціонувало вже понад сто платіжних систем, і кожного року їх кількість збільшується.

Актуальність розвитку платіжного ринку та безперебійного функціонування платіжних систем суттєво посилилась у зв'язку з поширенням через пандемію COVID-19 віддаленої роботи та е-комерції. Збільшення обсягів платіжного ринку стимулювало створення нових платіжних інструментів і систем, а також розширення кола їх учасників, що, в свою чергу, урізноманітнило форми зовнішнього впливу та інсайдерського втручання, підвищило рівень ризиковості їх діяльності. Особливо посилюється вплив на роботу платіжних систем операційних ризиків, джерелом виникнення яких можуть бути проблеми у функціонуванні інформаційно-комунікаційних систем, використанні програмного забезпечення, кіберзагрози тощо.

У світовій практиці вже накопичено певний досвід управління операційними ризиками, що виникають у платіжних системах. Разом з тим, існують певні проблеми щодо ідентифікації таких ризиків, використання індикаторів оцінки їх впливу на діяльність платіжних організацій та методів управління ризиками, особливо в умовах посилення кібератак і кіберзагроз, що й обумовлює актуальність теми дослідження.

Аналіз останніх досліджень і публікацій. Дослідження питань управління операційними ризиками в платіжних системах у вітчизняній науковій літературі розглядається, переважно, в загальному контексті управління ризиками діяльності фінансових установ. Можна виокремити лише деякі наукові праці С. Буковинського [23], О. Дзюблюка [2], А. Гриценка [22], Д. Дорофєєва [16], Р. Квасницької [10], Є. Тіщенка [4], І. Форкун [10] та інших учених, що безпосередньо стосуються управління ризиками в платіжних системах. Серед зарубіжних науковців, які досліджують ці проблеми, можна назвати праці О. Аканфе [14], І. Бонета [27], С. Варгааба [32], Д. Гаудіо [34], Т. Іварінена [12], Б. Кларка [25], Х. Лейнонена [12], У. Франкіда [32] та інших.

Значну увагу питанням управління операційними ризиками в платіжних системах приділяють Базельський комітет з банківського нагляду (БКБН), Банк міжнародних розрахунків (БМР), ЄЦБ і центральні банки окремих країн. Разом з тим невирішеними частинами проблеми залишається дослідження особливостей і форм прояву операційних ризиків, обумовлених використанням нових інформаційний технологій та посиленням кіберзагроз.

Метою статті є дослідження особливостей і форм прояву операційних ризиків у платіжних системах та розроблення пропозицій щодо вдосконалення управління ними.

Виклад основних результатів дослідження. Операційні ризики притаманні всім напрямам діяльності платіжної організації та процесам функціонування платіжної системи. Вони мають різноманітні джерела походження та форми прояву, що ускладнює їх виявлення та організацію управління ними [1, с. 104; 2, с. 188; 3, с. 151; 4, с. 94; 5, с. 131; 6, с. 61].

Національний банк України визначає операційний ризик у платіжних системах, як ризик того, що недоліки у функціонуванні інформаційних систем, програмного забезпечення або у виконанні внутрішніх процесів, людські помилки, операційні збої, втрата або витік інформації, шахрайство, порушення в управлінні внаслідок впливу зовнішніх подій призведуть до скорочення, погіршення або зупинення надання послуг платіжною системою [7].

У сучасних умовах головними джерелами виникнення операційних ризиків у платіжних системах є порушення режимів функціонування інформаційно-комунікаційних систем і мереж зв'язку, операційні збої через помилки у використанні технічних засобів і програмного забезпечення, а також зовнішнє втручання у вигляді кіберзагроз, що потребує суттєвого посилення рівня захисту платіжних систем та обумовлює необхідність використання відповідних методів та інструментів управління ризиками [8, с. 39; 9, с. 48; 10, с. 49; 11, с. 62].

Аналіз практики управління операційними ризиками в платіжних системах свідчить про те, що такі ризики є неоднорідними, і залежно від чинників, які впливають на їх виникнення, можна виокремити окремі їх види. Наприклад, Т. Іварінен, Х. Лейнонен, М. Лукка та В. Саарінен головними видами операційного ризику, притаманного платіжним системам, вважають інформаційні, технологічні, адміністративні та кримінальні [12]. Існують пропозицій щодо виокремлення й інших видів ризиків, зокрема, ризику шахрайства, кіберризику, агентського, ділового, інвестиційного ризику, ризику конфіденційності [13, с. 9; 14; 15, с. 368; 16, с. 197]. Базельський комітет з банківського нагляду для банківської діяльності виокремлює 7 видів операційного ризику [17, 2011].

На основі аналізу рекомендацій БКБН, БМР, ЄЦБ та центральних банків окремих країн світу нами виокремлено 4 види операційних ризиків, притаманних сучасним платіжним системам: інформаційний ризик, ризик помилок в управлінських процесах, кіберризик і ризик помилок користувачів, взаємозв'язок між якими представлено на рис. 1.

Кожен із виокримлених видів операційних ризиків має свої специфічні чинники виникнення та особливі форми прояву, які можуть завдавати платіжним сис-

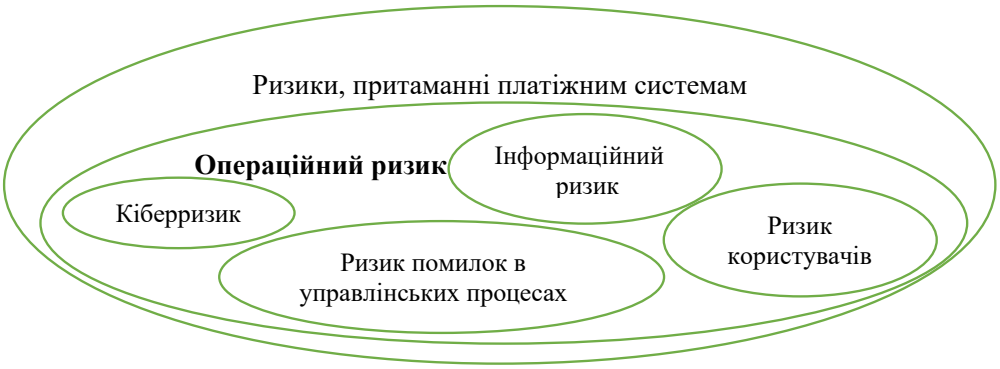

Рис. 1. Взаємозв'язок окремих видів операційних ризиків, притаманних платіжним системам

Джерело: побудовано авторами на основі [17; 18; 19, с. 23; 20]

темам і платіжним організаціям значних фінансових збитків, втрат або інших негативних наслідків. Характеристику події за окремими видами операційних ризиків, які можуть спричинити їх реалізацію, в узагальненому вигляді наведено в табл. 1.

Головною метою управління операційними ризиками, притаманними платіжним системам, повинні бути підтримка операційної стійкості платіжної організації та забезпечення безперервності діяльності платіжної системи. Для цього органи управління платіжною організацією зобов'язані в загальній структурі системи управління ризиками сформувати підсистему управління операційними ризиками, яка характеризується сукупністю методів та інструментів виявлення, аналізу, оцінки впливу та управління операційними ризиками, які об'єднані в єдиний механізм моніторингу та контролю процесу функціонування платіжної системи [23, с. 157].

Підсистема управління операційними ризиками повинна включати відповідні положення, правила, процедури, а також організаційну структуру з чітким визначенням відповідальності окремих підрозділів і уповноважених осіб; порядок інформування керівництва про стан управління операційними ризиками; правила обміну інформацією між підрозділами та учасниками платіжної системи; наявність необхідних технологічних засобів і процедур, а також сукупність методів та інструментів для ідентифікації, оцінювання, управління та моніторингу операційних ризиків [24, с. 424; 25; 26, с. 108].

Початковим етапом процесу управління операційними ризиками є визначення джерел їх виникнення, детальний опис ризикових подій, складання карти профілю ризиків та оцінка характеру і масштабів впливу ризиків на діяльність всіх учасників платіжної системи. Складність виявлення та ідентифікації операційних ризиків полягає в тому, що вони стосуються широкого кола напрямів функціонування платіжної системи, її учасників, третіх сторін, зокрема, операторів послуг платіжної інфраструктури, діяльності яких найбільше притаманні інформаційні ризики та кіберзагрози.

Кількісне оцінювання дії операційних ризиків дозволяє визначити їх вплив на діяльність платіжної організації та функціонування платіжної системи. Результатами такого впливу можуть бути прямі чи непрямі втрати (збитки), недоотримані доходи або додаткові витрати на усунення наслідків реалізації ризикових подій, тимчасова недоступність або втрата коштів користувачів, зниження якості платіжних послуг, втрата клієнтів та інші негативні результати реалізації подій операційного ризику.

Визначення ймовірності реалізації окремих операційних ризиків і потенційного рівня збитків від них дозволяє визначити показник притаманності ризику, який характеризує рівень його пріоритетності для платіжної організації. Приклад розрахунку рівня притаманності операційних ризиків у платіжній системі наведено в табл. 2.

Кількісне оцінювання ризиків та їх пріоритезація дозволяють платіжній організації визначити загальний прийнятний їх рівень (толерантність до ризику), який повинен бути узгоджений із завданнями забезпечення фінансової стійкості платіжної організації відповідно до затвердженої стратегії, характеру, масштабів та умов її діяльності на платіжному ринку.

Проведення пріоритезації ризиків і визначення рівня притаманності для кожного із них дозволяє розробити систему ключових індикаторів (KRI), що характеризують допустимі (граничні) межі зміни рівня операційного ризику та можуть бути використані для раннього виявлення та оцінки потенційного впливу окремих факторів ризику. З метою оцінки та характеристики операційних ризиків у платіжних системах такими індикаторами можуть бути:

1) відношення кількості невиконаних платіжних операцій до загальної кількості проведених операцій упродовж певного проміжку часу;

2) тривалість припинення (обмеження) роботи платіжної системи через реалізацію ризикових подій;

3) тривалість відновлення роботи інформаційних систем після припинення діяльності платіжної системи в разі настання ризикової події;

4) проміжок часу між двома послідовними ризиковими подіями, що призвели до припинення (обмеження) функціонування платіжної системи, який характеризує неперервність її роботи.

5) кількість випадків несанкціонованого втручання (доступу) в роботу платіжної системи за певний проміжок часу [28, с. 91; 29, с. 37].

З метою забезпечення ефективного управління операційними ризиками в платіжній системі платіжна

Таблиця 1

Види та характеристика форм прояву операційних ризиків у платіжних системах

Вид ризику	Події, що наражають на ризик	Реєстрація та опис подій, які можуть спричинити реалізацію ризику
1.Інформаційний ризик	Пошкодження або унеможливлення функціонування ІК-систем, що призводить до витоку інформації, її спотворення, викрадення та неправомірного використання	– відсутність у платіжної організації процедур, політик і стандартів інформаційної безпеки; – несанкціоноване втручання в роботу ІК-систем; – знищення, викрадення, викривлення, розголошення конфіденційної інформації з метою неправомірного її використання; – неправомірні дії працівників або третіх осіб, спрямовані на порушення роботи ІК-систем, програмного забезпечення і каналів зв'язку; – неналежні процедури з управління та контролю інформаційних систем і процесів; – непередбачувані обставини.
2. Ризик помилок в управлінських процесах	Несвоєчасне або неякісне виконання управлінських функцій та надання платіжних послуг	– відсутність положень, інструкцій, регламентів виконання операцій; – неналежна ідентифікація або нерозуміння ризиків і контролів, необхідних для управління ними; – низький рівень організації взаємодії підрозділів у системі управління ризиками; – неналежне здійснення контролю інформаційних систем і процесів; – недосконалість систем моніторингу ризиків; – недосконалість процесів обліку та звітності; – низький рівень кваліфікації працівників.
3.Кібер-ризик	Пошкодження, знищення або викрадення активів або інформації	– порушення роботи обладнання та ІК-систем унаслідок кібератак і використання зловмисниками шкідливого програмного забезпечення; – недостатній рівень технічної безпеки ІК-систем; – викрадення, знищення або пошкодження інформації, порушення її конфіденційності та цілісності; – недостатній рівень цифрової грамотності персоналу.
4. Ризик помилок користувачів	Порушення правил ідентифікації та розкриття інформації, низький рівень обізнаності та недбалість користувачів, шахрайство	– порушення правил ідентифікації користувачів; – неправильне використання технічних засобів і програмних комплексів; – некоректне введення, недбале зберігання або розголошення даних та інформації; – нерозуміння ризиків; – незнання умов виконання операцій; – виконання заборонених або незаконних операцій.

Джерело: розроблено авторами на основі [7; 23, с. 68; 22, с. 149]

Таблиця 2

Розрахунок рівня притаманності операційного ризику в діяльності платіжної системи

Вид ризику	Ймовірність реалізації	Потенційний рівень збитків	Притаманність ризику
1. Інформаційний ризик	3	3	9
2. Ризик помилок в управлінських процесах	3	3	9
3. Кіберризик	1	5	5
4. Ризик помилок користувачів	1	1	1

Примітка. Шкала оцінок. Ймовірність реалізації ризику: низька – 1; середня – 3; висока – 5. Потенційний ризик збитків: низький – 1; середній – 3, високий – 5.

Джерело: розроблено авторами на основі [7; 27]

організація повинна розробити адекватний економічним умовам механізм управління ними. Ґрунтуючись на аналізі досвіду управління платіжними системами, нами розроблено принципову схему функціонування такого механізму, яка представлена на рис. 2.

Механізм управління операційними ризиками в платіжних системах, крім зазначених вище загальних вимог, повинен також включати чіткий перелік методів та інструментів ідентифікації, вимірювання, моніторингу та управління операційними ризиками, забезпечення фізичної та інформаційної безпеки платіжної системи, обов'язкове періодичне тестування систем, операційних політик і процедур, оцінку якості функціонування операційних і технологічних засобів, проведення періодичного аудиту системи управління та регулярне інформування керівництва про стан управління ризиками.

При цьому основою організації процесу управління операційними ризиками повинен бути обґрунтований вибір та поєднання методів управління, до яких належать: обмеження (зниження) впливу ризиків на діяльність платіжної системи; прийняття ризиків; передавання (розподіл ризиків з іншою стороною, наприклад, страхування) та ухилення (уникнення) від ризиків, наприклад, шляхом відмови від виконання певних операцій або процесів.

Важливим аспектом функціонування механізму управління операційними ризиками в платіжних системах є визначення джерел покриття збитків і втрат, що виникають унаслідок реалізації ризикових подій.

Рис. 2. Схема функціонування механізму управління операційними ризиками в платіжній системі

Джерело: розроблено авторами на основі [7; 30; 31, с. 189]

Зазвичай, головними джерелами покриття збитків від реалізації подій операційного ризику в платіжних системах є капітал платіжної організації, а також кошти спеціально створених резервних фондів. Страхування наслідків реалізації операційних ризиків, зокрема інформаційних і кіберризиків, як свідчить аналіз світового досвіду, ще перебуває на етапі свого становлення [32; 33, с. 156].

Завершальним етапом процесу управління операційними ризиками в платіжній системі є оцінка його ефективності, яку здійснює служба внутрішнього аудиту платіжної організації. При цьому головними показниками для оцінки ефективності управління повинні бути мінімізація впливу операційних ризиків на процес здійснення розрахунків і платежів, а також забезпечення безперервної діяльності платіжної системи.

Останнім часом значний негативний і часто непередбачуваний вплив на діяльність платіжних систем спричиняють кіберзагрози та кібератаки, результатом яких стають тривалі та суттєві збої в роботі інформаційних систем і мереж зв'язку, а платіжні організації наражаються на значні фінансові збитки та репутаційні втрати. При цьому кіберзагрози розглядають як несприятливі події, що порушують конфіденційність, доступність, цілісність інформації, цифрових активів або захищеність інформаційно-комунікаційних систем, які використовуються у процесі надання платіжних послуг [30; 34; 35, с. 186].

Особливість кіберзагроз (кібератак)полягає в тому, що їх виникнення дуже складно прогнозувати, а наслідками можуть бути тривалі збої або затримки в наданні платіжних послуг, фінансові збитки учасників платіжної системи, зниження рейтингу, втрата клієнтів тощо. В окремих випадках кіберзагрози можуть призвести до системних збоїв у діяльності платіжних систем та функціонуванні платіжного ринку загалом, тобто до виникнення системного ризику [31, с. 189; 32].

На практиці під кіберризиком розуміють ризик втрат або виникнення додаткових витрат унаслідок навмисних протиправних дій щодо комп'ютерних та інформаційних систем, інформаційних ресурсів або інформаційної інфраструктури з використанням сучасних інформаційно-комунікаційних технологій [30]. Метою кібератак на платіжні системи можуть бути протиправне заволодіння, спотворення, розкриття або знищення інформації та цифрових активів, припинення діяльності системи або відмова в обслуговуванні клієнтів.

Головними причинами виникнення кіберризиків у платіжних системах можуть бути недостатній рівень захисту інформаційно-комунікаційних систем і каналів зв'язку, несвоєчасне оновлення програмного забезпечення і технічних засобів, порушення мережевих протоколів, зараження програмного забезпечення, несанкціоновані дії співробітників або третіх сторін. Тому заходи щодо підвищення ефективності управління кіберризиками повинні бути спрямовані на поліпшення техніко-технологічних характеристик функціонування платіжних систем і вдосконалення організації та управління діяльністю платіжної організації [10, с. 50; 36, с. 148].

До техніко-технологічних заходів можна віднести: підвищення рівня захисту інформації та забезпечення її конфіденційності; періодичну діагностику засобів управління доступом до інформаційних систем; захист програм, мереж і обладнання; використання безпечних методів кодування та спеціальних систем контролю аномальної поведінки клієнтів і співробітників; копіювання, архівування даних та інформаційних ресурсів;

створення резервних потужностей програмно-технічних засобів; використання ліцензованого та сертифікованого програмного забезпечення тощо.

Головними організаційно-управлінськими заходами протидії кіберзагрозам повинні бути: створення надійної системи ідентифікації та контролю кіберризиків з метою своєчасного їх виявлення; розроблення планів реагування на кіберзагрози; постійний перегляд і оновлення стандартів діяльності платіжних систем; вдосконалення технологічних вимог до здійснення переказу коштів і розрахунків; розроблення плану безперервної роботи та відновлення діяльності платіжної системи після збоїв; підвищення кваліфікації персоналу та інші [37, с. 124].

Забезпечення стійкості платіжної організації до кіберризиків обов'язково повинно передбачати підтримку цілісності, доступності та конфіденційності даних, а також можливість швидкого відновлення діяльності платіжної системи. Відповідно до вимог БМР, платіжна система після суттєвих збоїв повинна відновити діяльність і продовжити виконання своїх головних функцій не пізніше, ніж через дві години після настання критичної події [18].

З метою підвищення ефективності управління операційними ризиками в платіжних системах запропоновано сукупність заходів, які наведено в табл. 2.

Крім того, в зв'язку з необхідністю посилення протидії кіберзагрозам платіжні організації повинні розробляти політики кібербезпеки та використовувати такі перспективні інструменти захисту як штучний інтелект, аналітика великих даних, машинне навчання, біометрія, мобільний електронний підпис, шифрування та інші.

Висновки. Проведене дослідження особливостей і форм прояву операційних ризиків у платіжних системах свідчить про те, що значна їх частина обумовлена широким використанням нових інформаційно-комунікаційних технологій та посиленням кіберзагроз на платіжному ринку. Головними завданнями управління операційним ризиками у платіжних системах повинні бути забезпечення операційної стійкості платіжної організації та безперервності діяльності платіжної системи. Тому система управління операційними ризиками повинна передбачати наявність необхідних положень, правил і процедур, відповідну організаційну структуру управління, порядок інформування керівництва про стан управління ризиками; правила обміну інформацією, наявність необхідних технологічних засобів, а також сукупність методів та інструментів для ідентифікації, оцінювання, управління, контролю та моніторингу операційних ризиків.

Розроблені в ході дослідження схема функціонування механізму управління операційними ризиками, система ключових індикаторів їх граничного рівня та сукупність заходів щодо попередження та обмеження дії факторів операційного ризику на основі дотримання вимог до інформаційної безпеки, забезпечення безперервності бізнес-процесів, посилення моніторингу та вдосконалення організації і контролю сприятимуть підвищенню ефективності управління операційними ризиками в платіжних системах.

У зв'язку з посиленням кіберзагроз та інформаційних ризиків подальші дослідження питань управління операційними ризиками в платіжних системах повинні ґрунтуватися на вдосконалення методів та інструментів їх виявлення, попередження, обмеження дії, посилення моніторингу та контролю, а також мінімізації наслідків прояву з метою забезпечення безперервності бізнес-процесів і підтримання операційної стійкості платіжної організації.

Таблиця 2

Заходи попередження та обмеження дії факторів операційного ризику в платіжних системах

Заходи	Характеристика заходів
Дотримання вимог до інформаційної безпеки та операційної надійності	– регулярний перегляд та оновлення політик, процедур і стандартів підтримки інформаційної безпеки; – періодична оцінка безпеки програмного забезпечення та даних; – періодичне тестування внутрішніх регламентів, положень та інструкцій щодо інформаційної безпеки; – автоматизація процесів реагування на кіберзагрози; – розмежування доступу до систем і даних та недопущення несанкціонованого доступу; – копіювання й архівування даних та інформаційних ресурсів.
Забезпечення безперервності бізнес-процесів	– розроблення та постійне оновлення плану безперервності діяльності платіжної системи; – періодичне оновлення програмного забезпечення; – створення резервних потужностей; – регулярне тестування ІК-систем і програмно-апаратних комплексів.
Посилення моніторингу та контролю за операційними ризиками	– вдосконалення методів виявлення та управління операційними ризиками; – посилення контролю за дотриманням установлених правил і процедур; – моніторинг і своєчасне реагування на кіберзагрози; – регулярне стрес-тестування подій операційного ризику; – посилення механізмів регулювання та нагляду за діяльністю платіжних систем з боку НБУ.
Організаційно-управлінські заходи мінімізації наслідків реалізації факторів операційних ризиків	– організація системи моніторингу та контролю потенційних вразливостей і кіберзагроз; – вдосконалення правил і процедур здійснення операцій; – використання технологій мобільного електронного підпису; – надання учасникам платіжної системи достовірної інформації; – навчання та підвищення кваліфікації обслуговуючого персоналу.

Джерело: розроблено авторами на основі [7; 22, с. 153; 30; 38; 39, с. 476]

Список використаних джерел:

1. Міщенко В. І., Науменкова С. В. Вдосконалення механізмів управління операційними ризиками банку. *Наукові записки Національного університету «Острозька академія». Серія «Економіка».* 2022. № 25 (53). С. 102–109.

2. Дзюблюк О. В. Теорія і практика грошового обігу та банківської справи в умовах глобальної фінансової нестабільності: монографія. Тернопіль : ФОП Осадца Ю. В., 2017. 298 с.

3. Науменкова С. В., Міщенко С. В. Оверсайт платіжних систем на засадах ризик-орієнтованого нагляду. *Науковий погляд: економіка та управління*. 2018. №2 (60). С. 149–157. DOI: https://doi.org/10.32836/2521-666X/2018-2-60-20.

4. Тіщенко Є. Управління операційними ризиками. *Фінансовий простір.* 2017. № 4 (28). С. 91–96.

5. Ivanov V. V., Lvova N. A., Pokrovskaia N. V., Naumenkova S. V. Determinants of tax incentives for investment activity of enterprises. *Journal of Tax Reform*. 2018. T. 4. № 2. P. 125–141.

6. Міщенко С. Сутність економічного капіталу та його роль у забезпеченні фінансової стійкості банку. *Вісник НБУ*. 2008. № 1. С. 58–64.

7. Методичні рекомендації з управління ризиками в платіжних системах. НБУ. 2018. URL: https://bank.gov.ua/admin_uploads/article/Guidelines_risk_management_ps.pdf?v=4.

8. Науменкова С. В. Ринок фінансових послуг: основні тенденції розвитку. *Вісник НБУ.* 2000. № 1. С. 36–43.

9. Міщенко С. В. Проблеми вдосконалення системи саморегулювання на фінансовому ринку. *Фінанси України.* 2009. № 9. С. 43–52.

10. Квасницька Р., Форкун І., Гордєєва Т. Сучасні підходи забезпечення інформаційної безпеки платіжних систем та їх кіберзахисту. *Вісник Хмельницького національного університету.* 2022. № 5. Т. 1. С. 47–52.

11. Міщенко В. І., Міщенко С. В. Основні напрями забезпечення стабільності фінансового сектору України в контексті глобалізаційних процесів. *Фінанси України.* 2008. № 5. С. 56–69.

12. Iivarinen T., Leinonen H., Lukka M., Saarinen V. Regulation and control of payment system risks – a Finnish perspective. Bank of Finland. 2003. URL: https://helda.helsinki.fi/bof/bitstream/handle/123456789/9452/110738.pdf?sequence=1&is.

13. Науменкова С. В., Міщенко В. І. Сучасні проблеми капіталізації банківської системи України. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2013. № 2 (15). С. 3–11.

14. Akanfe O., Valecha R., Rao H. R. Assessing country-level privacy risk for digital payment systems. *Computers & Security.* 2020. Vol. 99. 102065. ISSN 0167-4048. https://doi.org/10.1016/j.cose.2020.102065.

15. Naumenkova S. V. Financial Inclusivity: Economic Contents and the Approaches to its Assessment. *Actual Problems of Economics*. 2015. № 4. P. 363–371.

16. Mishchenko S., Naumenkova S., Mishchenko V., Dorofeiev D. Innovation risk management in financial institutions. *Investment Management and Financial Innovations*. 2021. Vol. 18. Is. 1. P. 190–202.

17. Principles for the Sound Management of Operational Risk. BCBS. BIS. June, 2011. URL: https://www.bis.org/publ/bcbs195.pdf.

18. Principles for operational resilience. BIS. Consultative Document. August 2020. URL: https://www.bis.org/bcbs/publ/d509.htm.

19. Міщенко В. І., Науменкова С. В. Банківська система України: проблеми становлення та розвитку. *Фінанси України*. 2016. № 5. С. 7–33.

20. Eurosystem oversight framework for electronic payment instruments, schemes and arrangements. November 2021. URL: https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.

21. Науменкова С. В., Мищенко С. В. Регулирование денежного обращения на основе использования методов и инструментов денежно-кредитной политики. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2013. № 6 (147). С. 66–72.

22. Mishchenko V., Naumenkova S., Grytsenko A., Mishchenko S. Operational Risk Management of Using Electronic and Mobile Money. *Banks and Bank Systems.* 2022. Vol. 17. Is. 3. P. 142–157. DOI: http://dx.doi.org/10.21511/bbs.17(3).2022.12.

23. Буковинський С. А. та ін. Банківська система України на шляху євроінтеграції / за ред. С. А. Буковинського. Київ : ЦНД НБУ, 2015. 496 с.

24. Міщенко В. І., Міщенко С. В. Удосконалення дії каналів трансмісійного механізму грошово-кредитної політики в Україні в умовах таргетування інфляції. *Актуальні проблеми економіки*. 2015. № 1 (163). С. 421–428.

25. Clark B., Ebrahim A. Risk shifting and regulatory arbitrage: Evidence from operational risk. *Journal of Financial Stability*. 2022. Vol. 58. 100965, ISSN 1572-3089. DOI: https://doi.org/10.1016/j.jfs.2021.100965

26. Міщенко В. І. Перспективи розвитку IT-сектору та цифрової інфраструктури України. *Науковий вісник Ужгородського національного університету. Міжнародні економічні відносини та світове господарство.* 2022. № 43. С. 105–111. DOI: https://doi.org/10.32782/2413-9971/2022-43-18.

27. Bonet I. et al. Applying fuzzy scenarios for the measurement of operational risk. *Applied Soft Computing*. 2021. Vol. 112. 107785. ISSN 1568-4946. DOI: https://doi.org/10.1016/j.asoc.2021.1077857.

28. Міщенко С. Удосконалення управління економічним капіталом банку з урахуванням ризику ліквідності. *Вісник Університету банківської справи Національного банку України*. 2008. № 3. С. 90–93.

29. Науменкова С. В., Міщенко В. І. Валюта і валютна політика. Київ : Знання, 2010. 84 с.

30. Методичні рекомендації щодо управління операційним ризиком та зберігання інформації про клієнтів об'єктами платіжної інфраструктури. НБУ. 2020. URL: https://new.bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi

31. Міщенко В. І., Науменкова С. В. Поняття системного ризику та підходи до визначення системно значущих банків. *Соціально-економічні проблеми сучасного періоду України.* 2014. Т.1. № 105. С.186–196.

32. Vargaab S., Brynielssonac J., Frankead U. Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security.* 2021. Vol. 105. 102239. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2021.102239.

33. Міщенко В. І. Світовий досвід державної підтримки використання цифрових технологій та можливості його адаптації в умовах України. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»*. 2022. Т. 57. № 1. С. 148–160. DOI: https://doi.org/10.25313/2520-2294-2022-1-7858.

34. Del Gaudio B. L., Porzio C., Sampagnaro G., Verdoliva V. How do mobile, internet and ICT diffusion affect the banking industry? An empirical analysis. *European Management Journal*. 2021. Vol. 39. Is. 3. P. 327–332.

35. Міщенко В. І. Цифровізація регулювання та нагляду за діяльністю фінансових установ. *Економічний простір*. 2022. № 180. С. 182–189. DOI: https://doi.org/10.32782/2224-6282/180-30.

36. Міщенко В., Науменкова С. Напрями протидії кіберзагрозам та зниження рівня кіберризиків. *Modern transformations in economics and management*. Riga, Latvia: "Baltija Publishing", 2022. P. 144–149. DOI: https://doi.org/10.30525/978-9934-26-222-7-30.

37. Міщенко В. І. Вдосконалення управління кіберризиком у платіжних системах. *Наукові проблеми господарювання на макро-, мезо- та мікроекономічному рівнях*. Одеса : ОНЕУ, 2022. С. 123–125.

38. Principles for financial market infrastructures. Committee on Payment and Settlement Systems. Technical Committee of the International Organization of Securities Commissions. April 2012. URL: https://www.bis.org/cpmi/publ/d101a.pdf.

39. Економічні суперечності глобалізації та локалізації в умовах гібридної війни та післявоєнної реконструкції: монографія / за ред. академіка Гриценка А. А.; НАН України, ДУ "Інститут економіки та прогнозування НАН України". Київ, 2022. 636 с. URL: http://ief.org.ua/wp-content/uploads/2022/12/Ec-superech-globaliz-ta-localiz-v-umomah-gibryd-viyny.pdf.

References:

1. Mishchenko V. I., Naumenkova S. V. (2022). Vdoskonalennja mekhanizmiv upravlinnja operatsiynymy ryzykamy banku [Improving the bank's operational risk management mechanisms]. *Naukovi zapysky Natsionalnoho universytetu «Ostrozka akademija». Serija: «Ekonomika»*, vol. 53, no. 25, pp. 102–109.

2. Dzyublyuk O. V. et al. (2017.) *Teoriia i praktyka hroshovoho obihu ta bankivskoi spravy v umovakh globalnoi nestabilnosti* [Theory and practice of monetary circulation and banking in the conditions of global financial instability]. Ternopil: Osadtsa Yu. V. (in Ukrainian)

3. Naumenkova S. V., Mishchenko S. V. (2018). Oversayt platizhnykh system na zasadakh ryzyk-orientovanoho nahljadu [Oversite of payment systems on the basis of risk-oriented supervision]. *Naukovyi pohljad: ekonomika ta upravlinnja*, vol. 60, no. 2, pp. 149–157. DOI: https://doi.org/10.32836/2521-666X/2018-2-60-20.

4. Tishchenko E. (2017). Upravlinnja operatsiynymy ryzykamy [Operational risk management]. *Finansovyi prostir*, vol. 28, no. 4, pp. 91–96.

5. Ivanov V. V., Lvova, N. A., Pokrovskaia, N. V., Naumenkova S. V. (2018). Determinants of tax incentives for investment activity of enterprises. *Journal of Tax Reform*, vol. 4, no. 2, pp. 125–141.

6. Mishchenko S. (2008). Sutnist ekonomichnoho kapitalu ta yoho rol u zabezpechenni finansovoi stiykosti banku [The essence of economic capital and its role in ensuring the financial stability of the bank]. *Visnyk NBU*, no. 1, pp. 58–64.

7. NBU (2018). Metodychni rekomendacii z upravlinna ryzykamy v platizhnyh systemah [Guidelines for risk management in payment systems]. *Available at:* https://bank.gov.ua/admin_uploads/article/Guidelines_risk_management_ps.pdf?v=4.

8. Naumenkova S. V. (2000). Rynok finansovykh posluh: osnovni tendentsii rozvytku [Financial services market: main development trends]. *Visnyk NBU*, no. 1, pp. 36–43.

9. Mishchenko S. V. (2009). Problemy vdoskonalennja systemy samorehulyvannja na finansovomu rynku [Problems of improving the system of self-regulation in the financial market]. *Finansy Ukrainy*, no. 9, pp. 43–52.

10. Kvasnytska R., Forkun I., Hordeeva T. (2022). Suchasni pidkhody zabezpechenna informatsiynoi bezpeky platizhnyh system ta kiberzahystu [Modern approaches to ensuring information security of payment systems and their cyber defense]. *Visnyk Khmelnyckoho nacionalnoho universytetu*, vol. 5, no. 1, pp. 47–52.

11. Mishchenko V. I., Mishchenko S. V. (2008). Osnovni naprjamy zabezpechennja stabilnosti finansovoho sektoru v konteksti hlobalizatsiynykh protsesiv [The main directions of ensuring the stability of the financial sector of Ukraine in the context of globalization processes]. *Finansy Ukrainy*, no. 5, pp. 56–69.

12. Iivarinen T., Leinonen H., Lukka M., Saarinen V. (2003). Regulation and control of payment system risks – a Finnish perspective. *Available at:* https://helda.helsinki.fi/bof/bitstream/handle/123456789/9452/110738.pdf?sequence=1&is.

13. Naumenkova S. V., Mishchenko V. I. (2013). Suchasni problemy kapitalizatsii bankivskoi systemy Ukrainy [Modern problems of capitalization of the banking system of Ukraine]. *Finansovo-kredytna dijalnist: problemy teorii ta praktyky*, no. 2, pp. 3–11.

14. Akanfe O., Valecha R., Rao H. R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, vol. 99. 102065. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2020.102065

15. Naumenkova S. (2015). Financial Inclusivity: Economic Contents and the Approaches to its Assessment. *Actual Problems of Economics*, no. 4, pp. 363–371.

16. Mishchenko S., Naumenkova S., Mishchenko V., Dorofeiev D. (2021). Innovation risk management in financial institutions. *Investment Management and Financial Innovations*, vol. 18, no. 1, pp. 190–202.

17. BCBS. (2011). Principles for the Sound Management of Operational Risk. BCBS. Available at: https://www.bis.org/publ/bcbs195.pdf.

18. BIS (2020). Principles for operational resilience. Consultative Document. Available at: https://www.bis.org/bcbs/publ/d509.htm.

19. Mishchenko V. I., Naumenkova S. V. (2016). Bankivska systema Ukrainy: problemy stanovlennja ta rozvytku [Banking system of Ukraine: problems of formation and development]. *Finansy Ukrainy*, no. 5, pp. 7–33.

20. ECB. (2021). Eurosystem oversight framework for electronic payment instruments, schemes and arrangements. Available at: https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.

21. Naumenkova S. V., Mishchenko S. V. (2013). Regulirovanie denezhnogo obrashchenija na osnove ispolzovanija metodov i instrumentov denezhno-kreditnoy politiki [Regulation of money circulation based on the use of methods and instruments of monetary policy]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Ekonomika*, vol. 6, no. 147, pp. 66–72.

22. Mishchenko, V., Naumenkova S., Grytsenko A., Mishchenko S. (2022). Operational Risk Management of Using Electronic and Mobile Money. *Banks and Bank Systems,* vol. 17, no. 3, pp. 142–157.

23. Bukovinsky S.A. et al. (2015). *Bankivska systema Ukrainy na shljakhu evrointehratsii* [The banking system of Ukraine on the path of European integration]. Kyiv: CND NBU. [in Ukrainian]

24. Mishchenko V. I., Mishchenko S. V. (2015). Udoskonalennja dii kanaliv transmisiynoho mekhanizmu hroshovo-kredytnoi polityky v Ukraini v umovakh tarhetuvannja infljatsii [Improving the operation of transmission mechanism channels in Ukraine in the context of inflation targeting]. *Aktualni problemy ekonomiky*, vol. 1, no. 163, pp. 421–428.

25. Clark B., Ebrahim A. (2022). Risk shifting and regulatory arbitrage: Evidence from operational risk. *Journal of Financial Stability*, vol. 58. 100965, ISSN 1572-3089. DOI: https://doi.org/10.1016/j.jfs.2021.100965

26. Mishchenko V. I. (2022). Perspektyvy rozvytky IT-sektoru ta tsyfrovoi infrastruktury Ukrainy [Prospects for the development of the IT sector and digital infrastructure of Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo*, no. 43, pp. 105–111. DOI: https://doi.org/10.32782/2413-9971/2022-43-18.

27. Bonet I. et al. (2021). Applying fuzzy scenarios for the measurement of operational risk. *Applied Soft Computing*, vol. 112. 107785. ISSN 1568-4946. DOI: https://doi.org/10.1016/j.asoc.2021.1077857.

28. Mishchenko S. (2008). Udoskonalennja upravlinnja ekonomachnym kapitalom banku z urakhuvannjam ryzyku likvidnosti [Improving the bank's economic capital management taking into account liquidity risk]. *Visnyk Universytetu bankivskoi spravy Natsinalnoho banku Ukrainy*, no. 3, pp. 90–93.

29. Naumenkova S. V., Mishchenko V. I. (2010). *Valyuta i valyutna polityka* [Currency and monetary policy]. Kyiv: Znannja (in Ukrainian)

30. NBU (2020). Metodychni rekomendatsii shchodo upravlinnja operatsiynym ryzykom ta zabezpechennja zberihannja informatsii pro klientiv obektamy platizhnoi infrastruktury [Methodical recommendations for managing operational risk and ensuring the storage of information about customers by payment infrastructure]. Available at: https://new.bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi.

31. Mishchenko V. I., Naumenkova S. V. (2014). Ponjattja systemnoho ryzyku ta pidkhody do vyznachennja systemno znachushchykh bankiv [The concept of systemic risk and approaches to the definition of systemically significant banks]. *Sotsialno-ekonomichni problemy suchasnoho periodu,* vol. 1, no. 105, pp. 186–196.

32. Vargaab S., Brynielssonac J., Frankead U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security,* vol. 105. 102239. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2021.102239.

33. Mishchenko V. I. (2022). Svitovyi dosvid derzhavnoi pidtrymky vykorystannja tsyfrovykh tekhnolohiy ta mozhlyvosti yoho adaptatsii v umovakh Ukrainy [World experience of state support for the use of digital technologies and the possibility of its adaptation in Ukraine]. *Mimizharodnyi naukovyi zhurnal «Internauka». Serija: «Ekonomichni nauky»*, vol. 57. no. 1, pp. 148–160. DOI: https://doi.org/10.25313/2520-2294-2022-1-7858.

34. Del Gaudio B. L., Porzio C., Sampagnaro G., Verdoliva V. (2021). How do mobile, internet and ICT diffusion affect the banking industry? An empirical analysis. *European Management Journal*, vol. 39, no. 3, pp. 327–332.

35. Mishchenko V. I. (2022). Tsyfrovizatsija rehuluyvannja ta nahljadu za dijalnistyu finansovykh ustanov [Digitalization of regulation and supervision of financial institutions]. *Ekonomichnyi prostir*, no. 180, pp. 182–189. DOI: https://doi.org/10.32782/2224-6282/180-30.

36. Mishchenko V., Naumenkova S. (2022). Naprjamy protydii kiberzahrozam ta znyzhennja ravnja kiberryzykiv [Directions of countering cyber threats and reducing the level of cyber risks]. *Modern transformations in economics and management*. Riga, Latvia: "Baltija Publishing", pp. 144–149.

37. Mishchenko V. I. (2022). Vdoskonalennja upravlinnja kiberryzykom u platizhnykh systemakh [Improving cyber risk management in payment systems]. *Naukovi problem hospodaryuvannja na makro-, mezo- ta mikroekonomichnomu rivnjakh*. Odesa: ONEU, pp. 123–125.

38. BIS. (2012). Principles for financial market infrastructures. Committee on Payment and Settlement Systems. Technical Committee of the International Organization of Securities Commissions. *Available at:* https://www.bis.org/cpmi/publ/d101a.pdf.

39. Grytsenko A. A. et al. (2022). *Ekonomichni superechnosti hlobalizatsii ta lokalizatsii v umovakh hibrydnoi viyny ta povoennoi rekonstruktsii* [Economic contradictions of globalization and localization in the context of hybrid war and post-war reconstruction]. Kyiv: NAN Ukrainy, DU "Instytut ekonomiky ta prohnozuvannja NAN Ukrainy". Available at: http://ief.org.ua/wp-content/uploads/2022/12/Ec-superech-globaliz-ta-localiz-v-umomah-gibryd-viyny.pdf. (in Ukrainian)