

Євген О. Сопін*

УДОСКОНАЛЕННЯ МЕТОДИЧНИХ ОСНОВ ОЦІНКИ РИЗИКІВ НАДАВАЧІВ ПЛАТІЖНИХ ПОСЛУГ У ЦИФРОВІЙ ЕКОНОМІЦІ

Становлення цифрової економіки супроводжується розвитком FinTech, що охоплює ринок платіжних послуг. Із бурхливим розвитком електронної комерції зростає попит на забезпечення платіжних операцій в мережі Інтернет. У надавачів платіжних послуг виникають нові види ризиків, які потрібно оцінювати. З огляду на це, важливою практичною проблемою стає оцінка ризиків, які виникають у надавача платіжних послуг у цифровій економіці. Це передбачило розробку відповідних методичних основ, які практика вимагає постійно удосконалювати. Тому метою цієї статті стала розробка пропозицій щодо удосконалення методичних основ оцінки ризиків надавачем платіжних послуг у цифровій економіці.

Охарактеризовано механізм надання платіжних послуг у цифровій економіці щодо забезпечення різних видів електронної комерції з визначенням специфіки платіжних операцій та їх учасників. Роз'яснено роль надавача платіжних послуг. Також уточнено розуміння платіжного процесора і основні його види. У загальному виді описано порядок, за яким відбувається платіжна операція, а також основні типи ризиків, які несе надавач платіжних послуг або платіжний процесор (операційні, людські, ризики кібербезпеки, репутаційні, компласнс, кредитні, фрод та чарджбек ризики).

Оцінка ризику визначена як процес виявлення небезпеки, аналізу та визначення ризиків. Оцінка ризику в цілому розуміється як розрахункова величина, яка відображає серйозність ризику, обумовленого деякими об'єктивними чи суб'єктивними чинниками. З точки зору удосконалення методичних основ оцінки ризиків надавачем платіжних послуг у цифровій економіці уточнено розуміння: активного ризику, потенційної загрози, ймовірності, впливу, заходів безпеки чи міри контролю, невід'ємного або потенційного та залишкового ризику. Представлена методика оцінки ризику з поясненнями кожного її етапу (визначення найбільш релевантних ризиків, вимірювання невід'ємного ризику, кваліфікація засобів контролю, розрахунок залишкового ризику). Охарактеризовано основні види ризику, які оцінює надавач платіжних послуг. Наведені приклади оцінки технічного, компласнс ризику, фінансового та фрод ризику платіжного процесора з описом заходів контролю.

Ключові слова: цифрова економіка, платіжна послуга, надавач платіжних послуг, платіжний процесор, оцінка ризиків, управління ризиками.

Рис. 1. Табл. 4. Літ. 22.

DOI: 10.32752/1993-6788-2021-1-229-93-104

Евгений О. Сопин

СОВЕРШЕНСТВОВАНИЕ МЕТОДИЧЕСКИХ ОСНОВ ОЦЕНКИ РИСКОВ ПОСТАВЩИКОВ ПЛАТЕЖНЫХ УСЛУГ В ЦИФРОВОЙ ЭКОНОМИКЕ

Становление цифровой экономики сопровождается развитием FinTech, что охватывает рынок платежных услуг. С бурным развитием электронной коммерции растет спрос на обеспечение платежных операций в сети Интернет. У представителей платежных услуг возникают новые виды рисков, которые необходимо оценивать. Учитывая это, важной практической проблемой становится оценка рисков, возникающих у поставщика платежных услуг в цифровой экономике. Это предусматривало разработку соответствующих методических основ, которые практика требует

¹ National University of Water and Environmental Engineering, Rivne, Ukraine. ORCID: 0000-0001-5012-0332

постоянно совершенствовать. Поэтому целью данной статьи стала разработка предложений по совершенствованию методических основ оценки рисков представителей платежных услуг в цифровой экономике.

Охарактеризован механизм предоставления платежных услуг в цифровой экономике по обеспечению различных видов электронной коммерции с определением специфики платежных операций и их участников. Разъяснена роль поставщика платежных услуг. Также уточнено понимание платежного процессора и основные его виды. В общем виде описан порядок, по которому происходит платежная операция, а также основные типы рисков, которые несет предоставитель платежных услуг или платежный процессор (операционные, человеческие, риски кибербезопасности, репутационные, комплаенс, кредитные, фрод и чарджбек риски).

Оценка риска определена как процесс выявления угрозы, анализа и определения рисков. Оценка риска в целом понимается как расчетная величина, которая отражает серьезность риска, обусловленного некоторыми объективными или субъективными факторами. С точки зрения совершенствования методических основ оценки рисков предоставителем платежных услуг в цифровой экономике уточнено понимание: активного риска, потенциальной угрозы, вероятности, влияния, мер безопасности или меры контроля, неотъемлемого или потенциального и остаточного риска. Представленная методика оценки риска с объяснениями каждого ее этапа (определение наиболее релевантных рисков, измерение неотъемлемого риска, квалификация средств контроля, расчет остаточного риска). Охарактеризованы основные виды риска, которые оценивает предоставитель платежных услуг. Приведены примеры оценки технического, комплаенс риска, финансового и фрод риска платежного процессора с описанием мер контроля.

Ключевые слова: цифровая экономика, платежная услуга, предоставитель платежных услуг, платежный процессор, оценка рисков, управление рисками.

Yevhen O. Sopin

IMPROVEMENT OF METHODOICAL BASIS OF RISK ASSESSMENT OF PAYMENT SERVICE PROVIDERS IN THE DIGITAL ECONOMY

The formation of the digital economy is accompanied by the development of FinTech, which covers the market of payment services. With the rapid development of e-commerce, the demand for payment transaction processing over the Internet is growing. The new types of risks faced by payment service providers need to be properly assessed. Given this, an important practical issue is to assess the risks that arise for the payment service provider in the digital economy. This leads to the development of appropriate methodological frameworks, which should be constantly improved due to practical reasons. Therefore, the purpose of this article was to develop proposals for improving the methodological framework of risk assessment by payment service providers in the digital economy.

The mechanism of providing payment services for various types of e-commerce with the definition of the specifics of payment transactions and their participants is described. The role of the payment service provider is explained. The understanding of the payment processor and its main types are also clarified. Overall, the order of the payment transaction is described, as well as the main types of risks borne by the payment service provider or payment processor (operational, human, cybersecurity risks, reputational, compliance, credit, fraud and chargeback risks).

Risk assessment is defined as the process of identifying, analyzing and evaluating risks. Risk assessment is generally understood as a calculated value that reflects the severity of the risk due to certain objective or subjective factors. In terms of improving the methodological framework for risk assessment by payment service providers in the digital economy, the understanding of active risk, potential threat, probability, impact, security measures or control measures, inherent or potential and residual risk has been clarified. The method of risk assessment is presented with explanations of each stage (determination of the most relevant risks, measurement of inherent risk, qualification of

control measures, calculation of residual risk). The main types of risk assessed by the payment service provider are described. Examples of assessment of technical, compliance risk, financial and fraud risk of the payment service provider with a description of control measures are outlined.

Keywords: digital economy, payment service, payment service provider, payment processor, risk assessment, risk management.

Peer-reviewed, approved and placed: 12.07.2020.

Постановка проблеми. Перехід до цифрової економіки супроводжується трансформацією фінансового сектору та розвитком так званого FinTech, що значно вплинуло, поміж іншого, на забезпечення ринку платіжних послуг. У результаті виникнення нової технологічної бази та організаційних форм функціонування цього ринку, з'явилися і нові ризики, що зажадало нових підходів до їх оцінки та мінімізації. Надавачі цифрових платіжних послуг мають здійснювати оцінку ризиків використовуючи стандартні методи задля низки цілей, зокрема, виконання своїх ліцензійних зобов'язань перед національними та міжнародними (наднаціональними) фінансовими регуляторами, періодичних звітів рад директорів, фокусування топ-менеджменту та управлінців різних рівнів, на найбільш пріоритетних ризиках. Реалістична та адекватна оцінка ризиків є передумовою функціонування будь-якої фінансової інституції (зокрема тієї, що діє у цифровому середовищі) та здійснення ринкових трансакцій, оскільки передбачає визначення засобів для контролю і, відповідно, зменшення небажаних наслідків, а також усвідомлення неприйнятних ризиків, яких необхідно уникати. При цьому потрібно враховувати, що оцінка ризику у нових умовах цифрової економіки частіше виконується не на належному рівні або у недостатньому обсязі, навіть у тих випадках, коли управління ризиками впроваджено на підприємстві. Особливо це спостерігається в Україні, що породжує відповідні негативні наслідки для надавачів платіжних послуг, фінансових установ, покупців і продавців товарів чи послуг. З огляду на це, важливим науково-практичним завданням є удосконалення методичних основ оцінки ризиків надавачем платіжних послуг у цифровій економіці.

Аналіз останніх досліджень і публікацій. Теоретичним основам ідентифікації і оцінки ризиків, зокрема у фінансовій сфері, присвячені праці: Дж. Талбота і М. Джейкмана [1], Г. Гігеренцер [2], М. Фіелдса [3], Л. Коха [4]. Місце FinTech у структурі фінансової системи визначені у дослідженні Г. Поченчук [5]. Особливості становлення і розвитку FinTech в Україні досліджуються у роботі С. В'язового та І. Пасічника [6].

Тенденції розвитку фінансових технологій як фактору модернізації фінансової системи визначаються у статті Л. Дудинець [7]. Особливості появи фінансових інновацій в умовах цифровізації економіки розглянуті у роботі Н. Пантелеєва [8]. Загрози та перспективи FinTech для банків України досліджуються у роботі В. Коваленко [9]. Види ризиків у платіжних системах та питання їх оцінки досліджені таким вченими, як: С. Глібо [10], І. Ситник, А. Новак [11], А. Савченко [12]. Незважаючи на великий інтерес до становлення FinTech, нових платіжних систем та ризиків у них, методичні основи оцінки ризиків надавачем платіжних послуг у цифровій економіці розглянуті фрагментарно. Особливо малодослідженими залишаються класифікація ризиків та їх вплив на надавача цифрових платіжних послуг; визначення рівня

ризик, враховуючи його масштаб; оцінка елементів управління ризиками у платіжних системах, а також оцінка ризиків платіжного процесора.

Мета дослідження: розробити пропозиції щодо удосконалення методичних основ оцінки ризиків надавачем платіжних послуг у цифровій економіці.

Основні результати дослідження. У цифровій економіці формується попит на платіжні послуги у Інтернеті, що насамперед пов'язано з розвитком електронної комерції (Інтернет-торгівлі), що стосується купівлі-продажу товарів або послуг за допомогою Інтернету, а також переказів грошей та даних для здійснення цих операцій (транзакцій). Електронна комерція часто використовується для позначення продажу фізичних товарів в Інтернеті, але вона також може описувати будь-яку комерційну операцію, яка здійснюється через Інтернет. Електронна комерція може приймати різні форми, що включають різні транзакційні відносини між бізнесом та споживачами, а також різні об'єкти, якими обмінюються як частина цих операцій, наприклад: роздрібна торгівля (продаж продукту бізнесом безпосередньо клієнту без посередника); краудфандинг (збір грошей від споживачів заздалегідь, коли товар доступний, щоб зібрати стартовий капітал, необхідний для виведення його на ринок); передплата (автоматичне регулярне придбання товару або послуги на регулярній основі, доки абонент не вирішить скасувати); фізичні вироби (будь-який матеріальний товар, який вимагає поповнення запасів та фізичної доставки замовлення клієнтам у міру здійснення продаж); цифрові продукти (цифрові товари, що завантажуються, шаблони та курси або засоби масової інформації, які потрібно придбати для споживання або отримати ліцензію на використання); послуги (набір навичок, що надаються в обмін на компенсацію, час постачальника послуг можна придбати за окрему плату). Це охоплює сегменти: B2C, B2B, C2C, C2B.

Платіжні операції у цих випадках забезпечують на основі комплексу спеціальних технологій – Fintech, що означає інтеграцію технологій у пропозиції компаній фінансових послуг з метою покращення їх використання та доставки споживачам. Fintech описує різноманітні фінансові заходи, такі як грошові перекази в обхід відділення банку, щоб подати заявку на отримання кредиту, залучення грошей для запуску бізнесу або управління інвестиціями, як правило, без допомоги людини [13; 14; 15]. У кожній операції з кредитною картою беруть участь чотири або п'ять сторін: - мерчант (підприємство/онлайн-підприємство); - покупець (користувач); - банк-емітент, який видав кредитну картку клієнта; - еквайринг-банк, який збирає кошти у банку-емітента; - надавач платіжних послуг.

Надавач платіжних послуг є ліцензованою фінансовою установою і зазвичай з використанням Fintech. Надавач (постачальник) платіжних послуг – це стороння компанія, яка допомагає підприємствам приймати широкий спектр методів оплати в Інтернеті, таких як онлайн-банкінг, кредитні картки, дебетові картки, електронні гаманці, готівкові картки тощо. Надавач гарантує безпечне та надійне здійснення транзакцій клієнта та стежить за тим, щоб транзакції були завершені – від початку, коли клієнт вводить свої реквізити та ініціює платіж, до кінця, коли його отримує підприємство, що надає послуги, або товари. Надавачі платіжних послуг стають все більш важливими гравцями у глобальній платіжній екосистемі.

Надавач платіжних послуг може ідентифікуватись як платіжний процесор, адже забезпечує відповідний процес. Під процесингом платежів

розуміють всю сукупність операцій над грошима, які виробляються в той проміжок, коли покупець ці гроші вже віддав, заплативши через програму або сайт за товар і послугу, а продавець ці гроші ще не отримав. Маршрут від продавця до покупця електронні гроші роблять через кілька інстанцій [13; 14; 15].

Платіжний процесор зазвичай розглядається як інституція, яка виконує обробку транзакцій, які здійснюються через Інтернет, включаючи операції з використанням карт, дебетових і кредитових, взаємодіючи з компаніями онлайн-бізнесу і виконуючи всі необхідні дії по обробці з платежів і переказу коштів (частина процесорів розглядаються як прямі еквайєри). В результаті платіжні процесори отримують повноваження виконувати процесинг платежів з використанням карт від імені емітував їх банку.

Однак у цій статті потрібно уточнити розуміння платіжного процесора, який необхідно визначати як певного оператора фінансових розрахунків, що призначений продавцем і технічно забезпечує обробку транзакцій з різних каналів, таких як кредитні картки та дебетові картки для банків-еквайєрів. Надавач платіжних послуг частіше за все є третьою стороною і може застосовувати певну інформаційно-технічну систему — платіжний процесор. Фронт-енд (front-end) процесори мають зв'язки з різними асоціаціями карт і надають послуги авторизації та розрахунків продавцям комерційних банків. Внутрішні (back-end) процесори приймають розрахунки з Інтернет-процесорів і переміщують гроші від банку-емітента до банку-продавця. Під час операції, яка зазвичай триває кілька секунд, платіжний процесор перевірятиме отримані реквізити, надсилаючи їх до банку-емітента картки або асоціації карт для перевірки, а також здійснюватиме ряд заходів проти шахрайства щодо транзакції. Додаткові параметри, включаючи країну випуску картки та її попередню історію платежів, також використовуються для оцінки ймовірності затвердження транзакції. Після того, як процесор оплати отримає підтвердження, що дані кредитної картки перевірені, інформація передається через платіжний шлюз продавцю, який потім завершить платіжну операцію. Якщо карткова асоціація відхиляє перевірку, обробник платежів передасть інформацію продавцю, який потім відхилить транзакцію.

Коли клієнти оформляють покупки в інтернет-магазині, вони вводять свою платіжну інформацію на сторінці оформлення замовлення. Тут потрібно мати платіжний шлюз. Шлюз є віртуальними «воротами», через які проходить онлайн-транзакція під час процесу оплати; він шифрує дані та надсилає їх платіжному процесору банку-еквайєру. Платіжний шлюз — це сервіс переказів, який дозволяє здійснювати платежі за кредитними і дебетовими картками, а також іншими методами. Він необхідний будь-якому Інтернет-магазину або компанії, яка продає свої товари і послуги в інтернеті за допомогою сайту або програми. Банк-еквайєр надсилає платіжну вимогу до банку-емітента через платіжний процесор, а банк-емітент повертає схвалення чи відмову. Якщо транзакція схвалена, платіжний шлюз передає схвалення клієнту та закриває продаж. Платіжний процесор для онлайн-транзакцій працює з платіжним шлюзом замість фізичного платіжного терміналу. Процесор оплати здійснює транзакцію, як тільки дані проходять через шлюз. Коли клієнт використовує свою картку особисто в платіжному терміналі, термінал автентифікує картку, а потім надсилає інформацію в банк-емітент, банк-емітент схвалює або відхиляє операцію. Процесор обробки

платежів передає терміналу схвалення чи відмову. Якщо транзакція затверджена, платіжний процесор надсилає платіжну інформацію банку-еквайєру.

Серед типів ризиків, які несе надавач платіжних послуг (платіжний процесор) є наступні [13; 14; 15]: 1) операційні ризики, які можуть призвести до потенційних втрат, як то ІТ та системні ризики, що можуть виникнути внаслідок відмов системи, або помилок програмування; 2) людські ризики, які можуть бути наслідком людської помилки та пресингові ризики, як наслідок неправильної обробки інформації, неточної обробки даних, витоку або зламу інформації; 3) ризики кібербезки, які виникають внаслідок відсутності розподілу прав користувачів, недосконалі політики зі збереження паролів, відсутності бізнес контролю за транзакціями та недоліків у перевірці персоналу; 4) репутаційні ризики, які можуть виникнути, як через нездатність платіжного процесора дотримуватись регулятивних зобов'язань та національного законодавства, так і через маніпулювання клієнтською базою; 5) комплаєнс ризики (compliance risk), який визначається як ризик юридичних або нормативних санкцій, суттєвих фінансових збитків або втрати репутації платіжного процесора, що може бути спричинено внаслідок невиконання законів, регламентів, правил, зовнішніх та внутрішніх стандартів; 6) кредитні ризики (credit risk), які для платіжного процесора полягають у потенційній неспроможності торгівцем покрити будь-які фінансові втрати внаслідок власного фінансового становища; 7) фрод ризики (Fraud risk), які полягають у неспроможності організувати задовільний рівень менеджменту з боротьби з шахрайством та досягненні встановлених платіжними системами порогових значень. У разі перевищення вказаних лімітів, платіжні системи мають програми, які спонукають платіжних процесорів до зменшення фрод показників шляхом створення спеціального плану для виправлення ситуації, а також стимулюють прискорення цього процесу вводячи фінансові штрафи;

Перед надавачами платіжних послуг постає ціла низка завдань пов'язаних зі зниженням фроду. Ефективний фрод менеджмент вимагає балансу між трьома незалежними вимірами, а саме:

а) збільшенням прибутків через максимізацією та пришвидшенням прийому платежів, тобто передачею позитивного досвіду для справжніх користувачів;

б) мінімізацією втрат від фроду через максимізацію відхилень та мінімізацію чарджбеків, тобто через акуратність розпізнання фроду та його профілактику;

в) мінімізацією операційних витрат через ефективний, інтегрований та автоматизований процес фрод менеджменту.

8) чарджбек ризики (Chargeback risk), які можуть виникнути через неспроможність надавача платіжних послуг контролювати показники зворотних платежів, що здійснюють банки-емітенти, які вбачають порушення прав платника під час здійснення транзакції. У разі недотримання встановлених платіжними системами порогових значень, аналогічно з фрод-програмами, існують чарджбек-програми, які спрямовані на зменшення чарджбек показників платіжними процесорами, які у свою чергу мають розробляти та дотримуватися планів для виправлення ситуації.

Методика оцінки ризиків, що використовують надавачі цифрових платіжних послуг, зазвичай, базується на передових галузевих практиках. За її

допомогою визначаються основні ризики, ймовірність та вплив кожного з них, а також здійснюється оцінка заходів безпеки та контролю для розрахунку кінцевого залишкового ризику.

Оцінка ризику — процес виявлення небезпеки, аналізу та визначення ризиків; це термін, який використовується для опису загального процесу або методу, для: - визначення небезпеки та факторів ризику, які потенційно можуть завдати шкоди (виявлення небезпеки); - аналізу та визначення ризиків, пов'язаних з цією небезпекою (аналіз ризику та визначення ризику); - визначення відповідних шляхів усунення небезпеки або контролю ризиків, коли небезпеку неможливо усунути (контроль ризику).

Оцінка ризику в цілому розуміється як розрахункова величина (кількісна), яка відображає серйозність ризику, обумовленого деякими об'єктивними чи суб'єктивними чинниками. Зазвичай оцінки ризику певних проектів або процесів розраховуються шляхом множення ймовірності і впливу, хоча інші фактори, такі як визначення значущості, також можуть бути частиною розрахунків. Для якісної оцінки ризику бали ризику зазвичай розраховуються з використанням факторів, заснованих на діапазонах ймовірності і впливу. При кількісній оцінці ризику вихідні дані ймовірності ризику та впливу можуть бути дискретними значеннями або статистичними розподілами.

Для оцінки ризиків при використанні платіжного процесора необхідно визначити:

1) ризики, пов'язані з об'єктом надання платіжних послуг, що аналізуються, а потім надається оцінка ймовірності їх виникнення;

2) контроль чи заходи безпеки, які вже існують у платіжного процесора, що зменшують вплив чи ймовірність виникнення ризику.

До основних понять оцінки ризику відносяться: - активний ризик; - потенційна загроза; - ймовірність; - вплив; - заходи безпеки чи міра контролю; - невід'ємний або потенційний ризик та залишковий ризик.

Для удосконалення методичних основ оцінки утонемо їх розуміння.

Активний ризик — це сукупність ресурсів, які втручаються у бізнес-процеси надавача платіжних послуг із використанням платіжного процесора, що мають матеріальну або нематеріальну цінність, яку необхідно захищати, включаючи людей, інформацію, інфраструктуру, фінансові аспекти чи репутацію. Ці активи класифікуються та оцінюються для отримання залежностей між ними та розуміння наслідків, які б спричинила їх прогрес чи деградація для ефективності бізнес-процесів та бізнесу в цілому.

До потенційних загроз відносяться загрози, що можуть призвести до небажаного інциденту, який може викликати чи зумовити пошкодження всієї платіжної системи, організацію роботи, дії організаційно-економічних механізмів. Ці загрози, маючи людське походження чи ні, здатні змінювати стан безпеки активу. У першому випадку вона може бути навмисною або випадковою, тоді як у другому випадку — системною або природною.

Ймовірність є кількісною оцінкою частоти (ступеню впевненості) виникнення потенційної загрози, настання небажаних наслідків цієї загрози. Може враховуватись різні рівні або інтервали оцінки шкідливого впливу загрози (втрат), певні сценарії розвитку негативних подій, оцінка збитків за цими втратами. Розуміння ймовірності може бути частотним (чи індуктивний), а може бути дедуктивним, виходячи із властивостей об'єкту.

Під впливом розуміють вимірювання стану безпеки активу чи сфери ризику. Його значення визначається оцінкою зазначеного активу та деградацією, що викликає загрозу цього активу.

Під заходами безпеки чи мірами контролю мається на увазі дія, процедура, технологічний механізм або пристрій, фізичний або логічний, що допомагає запобігти, стримувати чи реагувати проти загроз активам.

В широкому сенсі, ризик — це можливість конкретного негативного впливу на актив. Його значення обчислюється виходячи з впливу та ймовірності виникнення певної загрози, яка актуалізується.

Існує декілька типів ризику: 1. Невід’ємний або потенційний ризик, тобто ризик, що притаманний кожній діяльності, без урахування здійснюваного контролю. Цей ризик виникає внаслідок впливу конкретної діяльності, ймовірності виникнення та негативного впливу, який він може нести для організації. Невід’ємний ризик властивий процесу і не може бути усунений; тобто в кожному процесі будуть існувати ризики для людей або для виконання самого бізнес-процесу [16]. 2. Залишковий ризик. Враховуючи набір розгорнутих засобів контролю, заходів безпеки та рівень процесу управління, система перебуває під впливом саме цього типу ризику [17].

Оцінка ризиків є прикладним завданням, що має базуватися на перевірній методиці, що кількісно визначає події та їх можливі наслідки на основі ймовірності виникнення та впливу на фінансову інституцію.

Методика оцінки ризику визначає ризик кількісно, тобто використовуючи шкалу, що кваліфікує атрибути відповідно до класифікації на основі ймовірності виникнення та впливу, який конкретний ризик мав би на надавача цифрових платіжних послуг [18]. Використовувана методологія складається з:

1. Визначення найбільш релевантних ризиків. Мета ідентифікації ризику — визначення подій, які можуть статися з платіжним процесором та можливі наслідки на нього. 2. Вимірювання невід’ємного ризику (чи ризику, що впливає із характеру, продукту, каналу та юрисдикції). Завдяки аналізу ризику визначається ймовірність присутності невід’ємного ризику кожної з ризикових подій, пов’язаних із цифровими платіжними послугами, що надає платіжний процесор, а також величина їх впливу, у разі, якщо процес відбувається через споріднені ризики. Класифікація ризиків (ймовірність виникнення наслідків та їх вплив на надавача цифрових платіжних послуг) наведені у табл. 1.

Таблиця 1. Класифікація ризиків та їх вплив на надавача цифрових платіжних послуг, складено автором на основі [1; 20]

Ймовірність виникнення наслідків				Вплив	
Масштаб	Рівень	Ймовірність	Частота	Значення впливу	Тип
Дуже високий	5	Відбувається увесь час	Щодня	5	Дуже Серйозний
Високий	4	Це трапляється більшість часу	Щомісяця	4	Серйозний
Помірний	3	Це може статися кілька разів	Щопівроку	3	Помірний
Низький	2	Є можливість того, що подія відбудеться	Щороку	2	Низький
Дуже низький	1	Незначна можливість того, що подія трапиться	Кожні 5 років	1	Дуже низький

Скоринг від 1 до 5 використовується при оцінці ризиків для зручності і є поширеним (наприклад, [19]).

Відповідно до такого підходу оцінки ризику, можна також визначити його рівень за формулою: величина ймовірності * значення впливу (формула 1). Визначення рівня ризику із врахуванням його масштабу наведені у табл. 2.

Таблиця 2. Визначення рівня ризику, враховуючи його масштаб,
складено автором на основі [1; 20]

Масштаб	Рівень	Визначення
Дуже високий	1	≥ 20
Високий	2	≥ 15 та/або < 20
Помірний	3	≥ 10 та < 15
Низький	4	≥ 5 та < 10
Дуже низький	5	< 5

3. Кваліфікація засобів контролю, що дозволяють зменшити несприятливі ризики для надання платіжних послуг. Ця кваліфікація здійснюється за допомогою аналізу контролю, встановленого надавачем платіжних послуг, визначена його політикою, діяльністю та процедурами, у порівнянні зі статусом їх впровадження. Основні види контролю за даною класифікацією [13; 14; 15; 18; 20; 21; 22]:

- профілактичний контроль: застосовується до причини ризику та його генератора, щоб зменшити можливість його виникнення;
- пошуковий контроль: захід, який виконується в умовах ненормальної ситуації;
- корекційний контроль: контроль, спрямований на пом'якшення впливу при реалізації ризику;
- впроваджений контроль: необхідний контроль існує і працює належним чином;
- контроль у стадії розробки: контроль існує, але він все ще не призвів до необхідного ефекту;
- інертний контроль: контроль не було розроблено, впроваджено чи здійснено; суб'єкт знає про можливі загрози, але не здійснює будь-яких дій щодо оцінки, запобігання чи мінімізації ризиків.

Особливості управління визначаються відповідно до наведеної табл. 3, де їх типологія та статус впровадження поєднуються для отримання уніфікованої шкали.

Таблиця 3. Особливості управління ризиками при різних видах контролю,
складено автором на основі [1; 20]

Вид контролю	Особливості управління
Сильний	визначений, задокументований, впроваджений, керований та оцінений задовільно;
Помірний	визначений, задокументований, впроваджений та керований;
Прийнятний	визначений, задокументований, впроваджений;
Слабкий	визначений та задокументований;
Інертний	визначений.

4. Розрахунку залишкового ризику. Після того, як визначений невід’ємний ризик та кваліфікація засобів контролю, обчислюється залишковий ризик з метою оцінки впливу, на платіжний процесор після здійснення заходів із контролю за невід’ємним ризиком.

Категоризація відображає класифікацію ризиків за пріоритетами: «високий» – «середній» – «низький». У деяких випадках може бути достатньо лише ранжувати ризики один проти одного, щоб визначити їх відносну пріоритетність. Матриця ризику із залишковою величиною наведена на рис. 1. У матриці може використовуватись різні кольорові забарвлення для позначення різної пріоритетності ризиків. Усі «червоні» ризики потрібно розглядати як першочергові.

Ймовірність	Дуже висока	5	10	15	20	25
	Висока	4	8	12	16	20
	Помірна	3	6	9	12	15
	Низька	2	4	6	8	10
	Дуже низька	1	2	3	4	5
		Дуже низький	Низький	Помірний	Серйозний	Дуже серйозний
		Вплив				

Рис. 1. Матриця ризику, складено автором на основі [1; 20]

Надавач цифрових платіжних послуг повинен підходити до оцінки своїх ризиків ґрунтовно, враховувати основні їх типи з метою визначення адекватного рівня контролю та оцінки рівня залишкового ризику. У цифровому середовищі важливо оцінити: ризики, пов'язані з катастрофічними подіями, що впливають на людські, матеріальні ресурси та фізичне обладнання для виконання послуг; ризики переривання діяльності через серйозні інциденти чи надзвичайні ситуації; викрадення, або порушення підтримки конфіденційності даних про оплату, включаючи персональні дані; технічні ризики, що пов'язані з можливим порушенням у наданні послуг, спричиненим банками-еквайєрами; залежність від ключових постачальників; вихід з ладу комп'ютерних систем компанії або платформи надання платіжних послуг; хакерська атака, що призводить до відмови в обслуговуванні; фінансові ризики як наслідок того, що онлайн-підприємство не в змозі покрити будь-які фінансові втрати через власний можливий нестабільний фінансовий стан; ризики аутсорсингу операційних функцій платіжного сервісу; операційні ризики, спричинені несанкціонованим доступом до ІТ-систем

Оцінка ризиків не має бути формальним документом, що надається фінансовою інституцією до національного або наднаціонального регулятора в рамках виконання ліцензійних зобов'язань, втім має бути ретельно підготовленим, на системній основі (один раз на півроку, або щорічно), аналізом, що здійснюється із залученням досвідчених експертів ключових підрозділів надавача платіжних послуг, та ескалується на найвищий рівень менеджменту інституції та заслуховується на заїданні ради директорів.

Висновки та перспективи подальших досліджень. Перехід до цифрової економіки супроводжується глибокою трансформацією фінансового сектору та

розвитком FinTech, що охопило ринок платіжних послуг. У цифровій економіці формується попит на платіжні послуги у Інтернеті, що насамперед пов'язано з розвитком електронної комерції (роздрібна торгівля, краудфандинг, передплата, цифрові продукти, послуги). Платіжні операції у цих випадках забезпечують на основі Fintech. У кожній операції приймають участь різні сторони: мерчант, покупець, банк-емітент, еквайринг-банк, надавач платіжних послуг. У надавача платіжних послуг, який може ідентифікуватись як платіжний процесор, виникають різні типи ризиків (операційні, людські, ризики кібербезпеки, репутаційні, комплаєнс, кредитні, фрод та чарджбек ризики).

З точки зору удосконалення методики оцінки ризиків уточняється розуміння оцінки ризику та інших основних понять, визначення типів ризику. Методика оцінки ризику включає: визначення найбільш релевантних ризиків; вимірювання невід'ємного ризику (з їх класифікацією та оцінкою рівня); кваліфікацію засобів контролю (визначення основних видів контролю та особливостей управління при них); розрахунку залишкового ризику із використанням спеціальної матриці. Досвід оцінки дозволяє визначити основні заходи контролю за різними видами ризиків. Недостатня робота з оцінкою ризиків сама по собі є загрозою для надавача платіжних послуг. Тому у майбутніх дослідження передбачається розробити концептуальні засади системи управління ризиками надавача цифрових платіжних послуг.

1. Talbot J., Jakeman M. Security Risk Management Body of Knowledge. NY: Wiley Interscience, 2009. 472 p.
2. Gigerenzer G. Calculated Risks: How to Know When Numbers Deceive You. NY: Simon & Schuster, 2002.
3. Fields M. Visa Acquirer Risk Management Guide. Tools and Best Practices for Acquirer Loss Prevention. Visa, 2003. 218 p. URL: <https://silo.tips/download/visa-acquirer-risk-management-guide>
4. Cox L.A. What's Wrong with Risk Matrices? Risk Analysis. 2008. Vol. 28, № 2. URL: <https://doi.org/10.1111/j.1539-6924.2008.01030.x>
5. Поченчук Г. FinTech у структурі фінансової системи. Глобальні та національні проблеми економіки. 2018. № 21. С. 49-55.
6. В'язовий С.М., Пасичник І.В. Розвиток FinTech-індустрії в Україні та її ризики для банківської діяльності. Східна Європа: економіка, бізнес та управління. 2019. Вип. 4(21). С. 480-484.
7. Дудинєць Л. Розвиток фінансових технологій як фактор модернізації фінансової системи. Глобальні та національні проблеми економіки. 2018. Вип. 22. С. 794-798.
8. Пантелєєва Н. Фінансові інновації в умовах цифровізації економіки: тенденції, виклики та загрози. Приазовський економічний вісник. 2017. Вип. 3 (03). С. 68-73.
9. Коваленко В.В. Розвиток FinTech: загрози та перспективи для банків України. Приазовський економічний вісник. 2018. Вип. 4(09). С. 127-133.
10. Глібо С. В. Ризики розрахунків в платіжних системах: господарсько-правові питання. Економіко-правові проблеми розвитку та сприяння господарській діяльності в сучасних умовах: зб. наук. пр. за матеріалами II Круглого столу, м. Харків, 17 травня 2019 р. Харків: НДІ ПЗІР НАПрН України, 2019. С. 238-246.
11. Ситник І.П., Новак А.М. Вплив цифрової економіки на розвиток платіжних систем в Україні. Агросвіт. 2019. №8. С. 41-48. URL: <https://doi.org/10.32702/2306-6792.2019.8.41>.
12. Савченко А.С. Управління ризиками в платіжних системах: автореф. дис. ... канд. екон. наук: 08.04.01. Суми, 2000. 23 с.
13. Braun M., McAndrews J., Roberds W., Sullivan R. Understanding Risk Management in Emerging Retail Payments. Economic Policy Review. 2008. Vol. 14, №12. P. 137-159. URL: <http://dx.doi.org/10.2139/ssrn.1072914>.
14. Trautman L. E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from Paypal. SSRN Electronic Journal. 2013. Vol. 16. P. 261-307. URL: <https://doi.org/10.2139/ssrn.2314119>.
15. Summers B.J. 7 Payment System Risk and Risk Management. In: The Payment System: Design, Management, and Supervision. IMF, 1994. URL: <https://www.elibrary.imf.org/view/books/071/07212-9781557753861-en/ch07.xml>.
16. Herrera M. Understanding Inherent Vs. Residual Risk In Business Continuity. BCMMETRICS, 2017. URL: <https://bcmmetrics.com/inherent-vs-residual-risk>.
17. Thakur M. Residual Risk. WallStreetMojo, 2019. URL: <https://www.wallstreetmojo.com/residual-risk>.

18. Sun J. Risk assessment methodologies and techniques by category and industry. SafetyCloud NOSA, 2017. URL: <http://blog.nosa.co.za/blog/risk-assessment-methodologies-and-techniques-by-category-and-industry>
 19. Elens G. How to Determine Risk Scores: Internal vs. External Risks. LogicGate, Inc, 2018. URL: <https://www.logicgate.com/blog/how-to-determine-risk-scores-internal-vs-external-risks/>
 20. Talbot J. What's right with risk matrices? URL: <https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices>.
 21. Bradford Ch. Examples of Internal Controls. Hearst Communications, Inc., 2018. URL: <https://smallbusiness.chron.com/examples-internal-controls-57039.html>.
 22. Weld L., Bergevin P.M., Magrath L. Anatomy of a financial fraud: A forensic examination of HealthSouth. The CPA Journal. 2004. Vol. 74. P. 44-49.
-
1. Talbot J., Jakeman M. (2009) Security Risk Management Body of Knowledge. NY: Wiley Interscience. 472 p.
 2. Gigerenzer G. (2002) Calculated Risks: How to Know When Numbers Deceive You. NY: Simon & Schuster.
 3. Fields M. (2003) Visa Acquirer Risk Management Guide. Tools and Best Practices for Acquirer Loss Prevention. Visa. 218 p. URL: <https://silo.tips/download/visa-acquirer-risk-management-guide>
 4. Cox L.A. (2008) What's Wrong with Risk Matrices? Risk Analysis. Vol. 28, № 2. URL: <https://doi.org/10.1111/j.1539-6924.2008.01030.x>
 5. Pochenchuk G. (2018) FinTech u strukturi finansovoyi sistemi (FinTech in the structure of the financial system). Globalni ta natsionalni problemi ekonomiki. № 21. P. 49-55.
 6. Vyazovyy S.M., Pasichnik I.V. (2019) Rozvitok FinTech-industriyi v Ukraini ta yiyi riziki dla bankivskoyi diialnosti (Development of FinTech-industry in Ukraine and its risks for banking). Skhidna Yevropa: ekonomika, biznes ta upravlinnia. Vol. 4(21). P. 480-484.
 7. Dudynech L. (2018) Rozvytok finansovykh tehnologiy yak faktor modernizatsii finansovoi systemy (Development of financial technologies as a factor in modernizing the financial system). Globalni ta natsionalni problemi ekonomiki. 2018. Vol. 22. P. 794-798.
 8. Panteleyeva N. (2017) Finansovi innovatsiyi v umovakh tsifrovizatsiyi ekonomiki: tendentsiyi, vikliki ta zagrozi (Financial innovations in the digitalization of the economy: trends, challenges and threats). Priazovskii ekonomichnii visnik. Vol. 3(03). P. 68-73.
 9. Kovalenko V.V. (2018) Rozvitok FinTech: zagrozi ta perspektivi dla bankiv Ukraini (FinTech development: threats and prospects for Ukrainian banks). Priazovskii ekonomichnii visnik. Vol. 4(09). P. 127-133.
 10. Glibko S. V. (2019) Riziki rozrakhunkiv v platizhnikh sistemakh: gospodarsko-pravovi pitannia (Risks of settlements in payment systems: economic and legal issues). Ekonomiko-pravovi problemi rozvitku ta spriannia gospodarskii diialnosti v suchasnikh umovakh: collection of scientific works on the materials of II Round Table, Kharkiv, May 17, 2019. Kharkiv: Scientific Research Institute of Legal Support of Innovative Development of National Academy of Legal Sciences of Ukraine. P. 238-246.
 11. Sitnik I.P., Novak A.M. (2019) Vpliv tsifrovoyi ekonomiki na rozvitok platizhnikh sistem v Ukraini (The impact of the digital economy on the development of payment systems in Ukraine). Agrosvit. №8. P. 41-48. URL: <https://doi.org/10.32702/2306-6792.2019.8.41>.
 12. Savchenko A.S. (2000) Upravlinnia rizikami v platizhnikh sistemakh (Risk management in payment systems): author's abstract ... Ph.D. in Economics: 08.04.01. Sumy. 23 p.
 13. Braun M., McAndrews J., Roberds W., Sullivan R. (2008) Understanding Risk Management in Emerging Retail Payments. Economic Policy Review. Vol. 14, №12. P. 137-159. URL: <http://dx.doi.org/10.2139/ssrn.1072914>.
 14. Trautman L. (2013) E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from Paypal. SSRN Electronic Journal. Vol. 16. P. 261-307. URL: <https://doi.org/10.2139/ssrn.2314119>.
 15. Summers B.J. (1994) 7 Payment System Risk and Risk Management. In: The Payment System: Design, Management, and Supervision. IMF. URL: <https://www.elibrary.imf.org/view/books/071/07212-9781557753861-en/ch07.xml>.
 16. Herrera M. (2017). Understanding Inherent Vs. Residual Risk In Business Continuity. BCM-METRICS. URL: <https://bcmmetrics.com/inherent-vs-residual-risk>.
 17. Thakur M. (2019) Residual Risk. WallStreetMojo. URL: <https://www.wallstreetmojo.com/residual-risk>.
 18. Sun J. (2017) Risk assessment methodologies and techniques by category and industry. SafetyCloud NOSA. URL: <http://blog.nosa.co.za/blog/risk-assessment-methodologies-and-techniques-by-category-and-industry>
 19. Elens G. (2018) How to Determine Risk Scores: Internal vs. External Risks. LogicGate, Inc. URL: <https://www.logicgate.com/blog/how-to-determine-risk-scores-internal-vs-external-risks/>
 20. Talbot J. What's right with risk matrices? URL: <https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices>.
 21. Bradford Ch. (2018) Examples of Internal Controls. Hearst Communications, Inc. URL: <https://smallbusiness.chron.com/examples-internal-controls-57039.html>.
 22. Weld L., Bergevin P.M., Magrath L. (2004) Anatomy of a financial fraud: A forensic examination of HealthSouth. The CPA Journal. Vol. 74. P. 44-49.