

SECTION 5. FINANCE, BANKING, INSURANCE

10.46299/ISG.2022.MONO.ECON.4.5.1

5.1 Реалії функціонування платіжних систем в Україні та їх вплив на забезпечення інформаційної безпеки

Сьогодні надважливу роль у функціонуванні та розвитку економіки будь-якої держави відіграють платіжно-розрахункові системи, які забезпечують здійснення переказів коштів та розрахунків між контрагентами за зобов'язаннями, що виникають в процесі їх економічної діяльності. Саме раціональна організація функціоналу платіжних систем сприяє вдосконаленню грошово-кредитних відносин, підвищує ефективність функціонування фінансової системи країни, забезпечує можливості здійснення міжнародних валютних розрахунків. Так, динамічний розвиток платіжних систем відіграє важливу роль у формуванні нових механізмів функціонування платіжної інфраструктури країни, виникнення нових видів платіжних інструментів, а також форм здійснення розрахунків, істотно впливає на всі сфери життя суспільства, одночасно сприяючи стабільному економічному зростанню різних галузей і економіки у цілому або гальмуючи його [388, с. 5]. З огляду на це, актуалізується розгляд питання сучасного розвитку платіжно-розрахункових систем в Україні та їх надійності щодо здатна забезпечення фінансової безпеки їх учасників та користувачів.

Основи змістової суті платіжних систем регламентуються багатьма міжнародними організаціями та визначаються багатьма зарубіжними вченими. Так, за визначенням Комітету з платіжних систем та систем розрахунків Банку міжнародних розрахунків платіжна система - це «набір інструментів, процедур і правил переказу коштів між учасниками чи серед учасників; система включає учасників та організацію, яка є її оператором. Основою платіжної системи, як правило, є угода між учасниками й оператором, а переказ коштів відбувається відповідно до узгодженої ними операційної інфраструктури» [389]. За трактуванням Том Коккола (представника Європейського центрального банку)

платіжна система - це «система переказу коштів, тобто офіційна угода 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» [390]. Відомий американський вчений на Ф. Мишкін розглядає платіжну систему, як систему, що «визначає порядок проведення угод купівлі-продажу в економіці, не залежно від конкретної форми грошей, якої вони набувають на певний час» [391, с. 66].

Розуміючи важливість платіжних систем як елементів інфраструктури електронної комерції, яка теж стрімко розвивається останнім часом на теренах світового економічного простору, так й в межах України, зокрема, вважаємо, що платіжну систему варто розглядати саме як 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 [392, с. 48].

Загальні засади функціонування платіжних систем в Україні визначено Законом України «Про платіжні послуги», в якому зазначено, що платіжна система є «системою для виконання платіжних операцій із формальними та стандартизованими домовленостями і загальними правилами щодо процесингу, клірингу та/або виконання розрахунків між учасниками платіжної системи» [393].

Отже, платіжні системи вирішують такі важливі завдання, як: гарантування безперебійного функціонування всіх елементів самої системи; забезпечення безпеки здійснення розрахунків та платежів; страхування від будь-яких збоїв у фінансових операціях.

Сучасна видова класифікація платіжно-розрахункових систем, що функціонують на території України представлена такими їх видами, які внесені до Реєстру платіжної інфраструктури [394]:

1) внутрішньодержавні платіжні системи, в яких платіжна організація є резидентом та, які здійснюють свою діяльність і забезпечують проведення переказу коштів виключно в межах України:

- 2 – державні платіжні системи (Система електронних платежів (СЕП) - системно важлива платіжна система та Національна платіжна система «Український платіжний простір», учасниками якої є 54 банки та 17 небанківських установ);

- 6 – внутрішньобанківських платіжних систем;

- 1 – платіжна система (система переказу грошей), платіжною організацією якої є банку («FLASHPAY» система переказу грошей АТ «БАНК ФАМІЛЬНИЙ», яка налічує 41 учасника);

- 15 – платіжних систем, платіжною організацією якої є небанківська установа. Найбільшою за кількістю учасників (25 учасників) є соціально важлива платіжна система (система переказу коштів) «Фінансовий світ» ТОВ «Українська платіжна система»;

2) міжнародні платіжні системи, в яких платіжна організація може бути як резидентом, так і нерезидентом і які здійснюють свою діяльність на території двох і більше країн та забезпечують проведення переказу коштів у межах цієї платіжної системи, у тому числі з однієї країни в іншу:

- 8 – платіжних систем (систем переказу грошей), платіжною організацією якої є банку. Найбільшою за кількістю учасників (50 учасників) є міжнародна платіжна система «Welsend» АТ «УКРГАЗБАНК» (Україна);

- 6 – платіжних систем, платіжною організацією якої є небанківська установа. Найбільшою за кількістю учасників (26 учасників) є міжнародна система переказу коштів «AVERS №1» АТ «ФК "АВЕРС"» (Україна);

- 6 – міжнародних карткових платіжних систем. Найбільшою за кількістю учасників (53 учасників) є соціально важлива платіжна система - міжнародна карткова платіжна система «MasterCard» (США);

- 10 – міжнародних систем переказу грошей. Найбільшою за кількістю учасників (18 учасників) є важлива платіжна система - міжнародна система переказу коштів «RIA» (США).

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 [395, р.47]. Так, Національним банком України розроблено Положення про порядок здійснення оверсайту платіжної інфраструктури в Україні [396], Методичні рекомендації з управління ризиками в платіжних системах [397] та Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури [398], 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 [12, р. 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. Під кіберризиком варто розглядати ризик реалізації кіберзагроз щодо інформаційних ресурсів та/або інформаційної інфраструктури, а також наслідки таких подій. 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 [400] та порядку дій під час виявлення кібератак, що знижують надійність функціонування платіжних систем. Ватро зауважити, що тема кібербезпеки та платіжного шахрайства сьогодні, як ніколи, актуалізується в усьому світі і Україна також не є винятком. Так, Національним банком України констатується зростання активності шахраїв протягом 2021 року. «Найпопулярнішим» методом шахрайства з платіжними картками в Україні, як і у світі, традиційно залишається соціальна інженерія, завдяки застосуванню якої люди самі переказують гроші аферистам або розкривають їм дані своїх карток. Тому, з метою активізації на макрорівні боротьби із подібними інцидентами у 2022 р. центробанк України, разом із Департаментом кіберполіції Національної поліції України, а також за підтримки: Міжнародної фінансової корпорації (IFC) у партнерстві з Державним секретаріатом Швейцарії з економічних питань (SECO) та Фондом ефективного врядування Великобританії; Міністерства цифрової трансформації України, розпочав загальнодержавну інформаційну кампанію з платіжної безпеки під назвою «Шахрай Гудбай». Інформаційними партнерами цієї кампанії стали українські банки, представники найбільших інтернет-платформ для ведення бізнесу, мобільні та поштові оператори, а також центральні органи управління і обласні державні адміністрації. Метою кампанії є поліпшення обізнаності громадян про кібергігієну, сприяння формуванню культури безпечної поведінки у віртуальному просторі, а також засвоєння основних правил безпеки безготівкових розрахунків в різних платіжних системах [401].

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. Сучасна практика пошуку та запровадження нових підходів до забезпечення інформаційної безпеки банків відзначається певною різноманітністю. 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 НБУ, було обрано по два банки. Такими банками є:

- банки з державною часткою: АТ КБ «ПРИВАТБАНК» (JSC CB PRIVATBANK) та АТ «Державний ощадний банк України»;
- банки іноземних банківських груп: АТ «РАЙФФАЙЗЕН БАНК» (RAIFFEISEN BANK JSC) та АТ «УКРСИББАНК» (JSC UKRSIBBANK);
- банки з приватним капіталом: АТ "УНІВЕРСАЛ БАНК" (JSC UNIVERSAL BANK) та АТ "ТАСКОМБАНК" (TASCOMBANK JSC).

Ці банки пропонують клієнтам широкий спектр платіжних та розрахункових послуг, оскільки вони є учасниками багатьох міжнародних платіжних систем та систем термінових грошових переказів (табл. 1; табл. 2).

Таблиця 1.

Банки-учасники платіжних систем

Платіжні системи	ПриватБанк	Ощадбанк	Райффайзен Банк	Укрсиббанк	Універсалбанк	Таскомбанк
MasterCard	+	+	+	+	+	+
Visa	+	+	+	+	+	+
China UnionPay	+	-	-	-	-	-
НПС “ПРОСТІР”	+	+	+	-	-	+

Складено авторами за даними [394]

Таблиця 2.

Системи термінових грошових переказів банківських установ

Системи термінових грошових переказів	ПриватБанк	Ощадбанк	Райффайзен Банк	Укрсиббанк	Універсалбанк	Таскомбанк
Western Union	+	+	+	+	+	-
PRIVATMONEY	+	-	-	-	-	-
MoneyGram	+	+	-	-	+	-
RIA	+	+	-	-	+	-
IntelExpress	+	+	-	-	-	-
Welsend	+	-	-	-	-	+
MEEST	+	-	+	-	-	-
Signe Money Transfer	+	-	-	-	-	-
MONEGO	-	+	-	-	-	-
My Transfer	-	+	-	-	-	-
Аваль-Експрес	-	-	+	-	-	-
Contact	-	-	-	+	-	-
Unistream	-	-	-	+	-	-
ІнтерПейСервіс	-	-	-	-	-	+
«За мить»	-	-	-	+	-	-

Складено авторами за даними [394]

Таке різноманіття 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. Основними цілями забезпечення інформаційної безпеки є забезпечення таких якісних характеристик інформації, як: конфіденційність, цілісність, доступність, спостережність. Критеріальна сукупність забезпечення інформаційної безпеки банками, при здійсненні ними розрахунків, платежів та переказів через різні платіжні системи представлена на рис. 1.

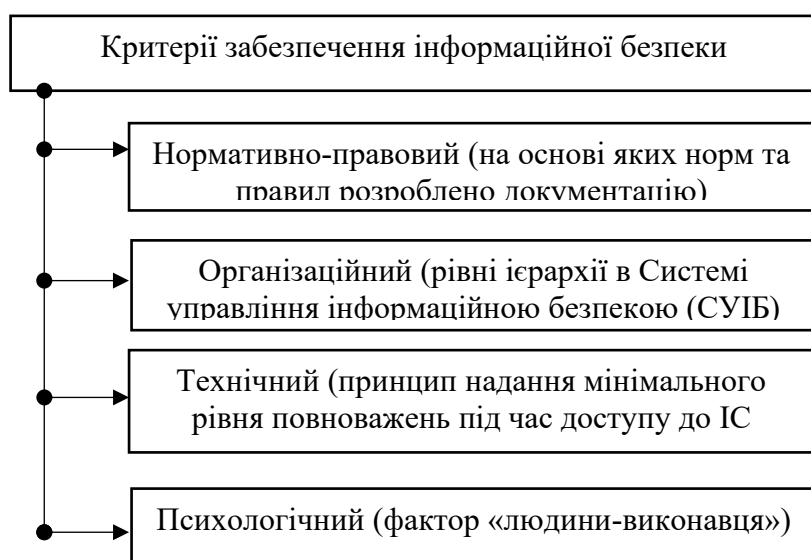


Рисунок 1. Критерії політики інформаційної безпеки банку

Сформовано авторами

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 кіберризиків, 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. При цьому, основними цілями забезпечення інформаційної безпеки є забезпечення таких якісних характеристик інформації (критеріїв забезпечення інформаційної безпеки), як: конфіденційність, цілісність, доступність), спостережність. Своєчасна ідентифікація кіберризиків 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.