УДК [347.73:336.717](4-6ЄС+477)
DOI https://doi.org/10.51547/ppp.dp.ua/2025.5.20

Товкун Людмила Вікторівна
кандидатка економічних наук, доцентка,
доцентка кафедри фінансового права
Національного юридичного університету імені Ярослава Мудрого
ORCID ID: 0000-0002-4769-9379

Бондаренко Кирило Андрійович
студент 3 курсу 1 групи
факультету юстиції
Національного юридичного університету імені Ярослава Мудрого
ORCID ID: 0009-0007-6817-468X

ПРАВОВЕ РЕГУЛЮВАННЯ ПЛАТІЖНИХ ІНСТРУМЕНТІВ ТА ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОНАННІ ПЛАТІЖНИХ ОПЕРАЦІЙ В УКРАЇНІ В КОНТЕКСТІ ПРАВА ЄС

LEGAL REGULATION OF PAYMENT INSTRUMENTS AND INFORMATION PROTECTION IN THE EXECUTION OF PAYMENT TRANSACTIONS IN UKRAINE IN THE CONTEXT OF EU LAW

Стаття присвячена комплексному дослідженню сучасних підходів до правового регулювання платіжних інструментів та механізмів захисту інформації під час виконання платіжних операцій. У роботі проаналізовано еволюцію платіжних інструментів – від традиційних форм до токенізованих і цифрових рішень – показано, як їх техніко-юридична природа зумовлює нові вимоги до безпеки, автентифікації та управління ризиками. За таких умов ефективність правових механізмів захисту інформації та прав користувачів стає визначальним чинником довіри до платіжної інфраструктури й надійності цифрових фінансових сервісів. Особливу увагу приділено положенням Закону України «Про платіжні послуги» № 1591-IX та нормативно-правовим актам Національного банку України, які встановлюють обов'язкові стандарти конфіденційності, цілісності й доступності платіжної інформації, а також визначають порядок реагування на інциденти інформаційної безпеки. Зазначені нормативні акти імплементують у національне законодавство ключові положення Директиви PSD2 та Регламенту ЄС 2018/389 (RTS щодо сильної автентифікації клієнтів і загальних захищених каналів зв'язку). Виходячи з цього, платіжний інструмент розглядається як елемент цифрової екосистеми, що поєднує ідентифікацію користувача, формування його волевиявлення, передачу даних і виконання операції незалежно від конкретного носія чи каналу доступу. З урахуванням підходів, відображених у звітах Європейського центрального банку та Європейського банківського органу, окреслено ключові тенденції європейського регулювання у сфері платіжних послуг. Зокрема, акцент зроблено на розвитку відкритих банківських систем (Open Banking) та посиленні вимог до токенізації платіжних даних і динамічного зв'язування. Обґрунтовано, що посилення правових вимог до обробки платіжної інформації в Україні є логічним наслідком цифровізації фінансового сектору та необхідністю забезпечення довіри користувачів до платіжної інфраструктури. Зроблено висновок, що ефективність національної моделі регулювання залежить від здатності об'єднати технологічні інновації, правові механізми захисту й належне управління інформаційною безпекою на всіх етапах платіжної операції. Подальший розвиток цього напрямку має відбуватися з урахуванням постійного моніторингу кіберзагроз та гармонізації українського законодавства з європейськими стандартами.

Ключові слова: *фінансове право, платіжні інструменти, прямий дебет, кредитовий трансфер, електронні платіжні засоби, захист інформації.*

The article is devoted to a comprehensive study of modern approaches to the legal regulation of payment instruments and mechanisms for protecting information during the execution of payment transactions. The work analyzes the evolution of payment instruments – from traditional forms to tokenized and fully digital solutions – and demonstrates how their technical-legal nature gives rise to new requirements for security, authentication, and risk management. Under these conditions, the effectiveness of legal mechanisms for protecting information and user rights becomes a decisive factor in building trust in payment infrastructure and the reliability of digital financial services. Particular attention is paid to the provisions of the Law of Ukraine "On Payment Services" No. 1591-IX and the regulatory acts of the National Bank of Ukraine, which establish mandatory standards of confidentiality, integrity, and availability of payment information, as well as define the procedure for responding to information security incidents.

These regulatory acts implement into national legislation the key provisions of Directive PSD2 and EU Regulation 2018/389 (RTS on strong customer authentication and common secure communication channels). Based on this, a payment instrument is considered as an element of the digital ecosystem that combines user identification, the formation of their intent, data transmission, and transaction execution regardless of the specific medium or access channel. Taking into account the approaches reflected in the reports of the European Central Bank and the European Banking Authority, the key trends in European regulation in the field of payment services are outlined. In particular, emphasis is placed on the development of open banking systems (Open Banking) and the strengthening of requirements for payment data tokenization and dynamic linking. It is substantiated that the strengthening of legal requirements for the processing of payment information in Ukraine is a logical consequence of the digitalization of the financial sector and the need to ensure user confidence in the national payment infrastructure. It is concluded that the effectiveness of the national regulatory model depends on the ability to harmoniously combine technological innovations, legal protection mechanisms, and proper information security management at all stages of the payment transaction. Further development of this area should take place with constant monitoring of cyber threats and harmonization of Ukrainian legislation with European standards.

Keywords: *financial law, payment instruments, direct debit, credit transfer, electronic payment instruments, information protection.*

Постановка проблеми. Стрімкий розвиток фінансових технологій та цифровізація платіжної інфраструктури зумовили активний перехід значної частини розрахунків у безготівкову форму. Якщо раніше домінували класичні форми переказу коштів, то нині ключове значення мають комплексні рішення, що поєднують платіжні картки, кредитові трансферти, прямий дебет, мобільні застосунки, «цифрові гаманці» та інші електронні сервіси. Запровадження Закону України «Про платіжні послуги» № 1591-IX закріпило нову модель правового регулювання платіжного ринку, у якій у центр уваги поставлено не окремі технічні форми розрахунків, а весь життєвий цикл платіжної операції [1]. Водночас зростання частки дистанційних і електронних операцій об'єктивно посилює ризики неправомірних платіжних дій, несанкціонованого доступу до рахунків, порушення конфіденційності та цілісності платіжної інформації. У цих умовах питання захисту інформації, що формується, передається та зберігається при використанні платіжних інструментів, набуває ключового значення як для фінансової безпеки споживачів, так і для стабільності ринку платіжних послуг загалом. Норми Закону № 1591-IX у поєднанні з нормативно-правовими актами Національного банку України та європейськими стандартами (зокрема підходами, закріпленими в Директиві (ЄС) 2015/2366 «Про платіжні послуги на внутрішньому ринку» (далі – PSD2)) формують нову систему вимог до сильної автентифікації, управління ризиками та розподілу відповідальності між надавачем платіжних послуг і користувачем [2]. За таких обставин виникає потреба у комплексному дослідженні сучасних правових вимог до застосування платіжних інструментів, режиму захисту інформації при їх використанні та тенденцій подальшого вдосконалення правового регулювання у цій сфері.

Аналіз останніх досліджень і публікацій. Питання платіжних послуг, платіжних інструментів, захисту інформації у сфері платіжних послуг є предметом активних досліджень у міжнародному та вітчизняному науковому середовищі. Так, Б. Суходолський у статті «Платіжні послуги у цивільному праві України та їх правова природа», досліджує питання правової природи платіжних послуг та місця електронних платіжних засобів у системі правовідносин [3]. Автор пропонує концептуально відмежувати електронні платіжні засоби як окремий вид платіжних інструментів, що поєднують матеріальні та нематеріальні елементи, і робить акцент на нормативному закріпленні сильної клієнтської автентифікації (далі – SCA) як ключової гарантії належної авторизації операцій. Такий підхід логічно підводить до питання перерозподілу відповідальності між надавачем послуг і користувачем за несанкціоновані транзакції, де вирішальним є саме доведення факту належного застосування процедури SCA.

А. Клочко у статті «Біометричні технології у забезпеченні безпеки банківських операцій», розглядаючи техніко-правовий вимір безпеки платіжних операцій та електронних платіжних засобів доповнює його біометричною автентифікацією як компонентом платіжної безпеки з притаманними їй ризиками приватності [4]. Автор обґрунтовує, що запровадження біометричної автентифікації неминуче супроводжується посиленням вимог до законності обробки біометричних даних (чіткого визначення мети, обсягу та строків їх зберігання), належного інформування користувача та регламентації порядку зберігання біометричних шаблонів. Водночас біометрія, за його підходом, має розглядатися як додатковий, а не єдиний спосіб доступу до платіжних послуг і захисту інформації, оскільки монополізація доступу виключно біометричними засобами може створювати непропорційні та потенційно дискримінаційні бар'єри для окремих категорій користувачів.

У зарубіжній доктрині правові засади електронних платіжних засобів і захисту інформації розглядаються науковцями насамперед у зв'язку з режимом PSD2 та SCA. Так, Danaja Fabcic у праці *«Strong Customer Authentication in Online Payments Under GDPR and PSD2: A Case of Cumulative Application»* зазначає, що норми PSD2 про сильну автентифікацію клієнта мають застосовуватися разом із вимогами GDPR (General Data Protection Regulation (Загальний регламент захисту даних (Регламент (ЄС) 2016/679)), а не підмінювати їх як спеціальні норми, що скасовують загальні [5].

Авторка аналізує статус постачальника платіжних послуг як контролера персональних даних, розглядає можливі правові підстави обробки даних платіжних операцій і персональних даних користувача та підкреслює, що винятки з SCA створюють додаткові кіберризики й впливають на розподіл відповідальності за шахрайські операції.

Hassan, M. A. у статті *«A Review on Electronic Payments* Sec*urity»* здійснює комплексний огляд сучасних електронних платіжних систем і пов'язаних з ними загроз безпеці [6]. Дослідження охоплює технічні та організаційні аспекти захисту електронних платежів, включно з криптографічними методами, протоколами автентифікації, засобами запобігання шахрайству та підходами до оцінки ризиків. Особлива увага приділена вразливостям мобільних та онлайн-платіжних рішень, зокрема ризикам, пов'язаним із відкритими мережами, слабкими схемами ідентифікації та недостатніми механізмами шифрування. Автор підкреслює, що ефективний захист електронних платежів потребує поєднання технологічних інструментів і політики управління безпекою, а також узгодженості між фінансовими установами й регуляторами.

Узагальнені вище наукові напрацювання дозволяють окреслити основні проблеми правового регулювання надання платіжних послуг, застосування платіжних інструментів та організацію захисту інформації під час здійснення платіжних операцій. Попри значний розвиток національної доктрини, більшість досліджуваних питань залишаються безпосередньо пов'язаними з європейським нормативним середовищем, у межах якого формуються сучасні стандарти платіжної безпеки, вимоги до SCA, а також правила захисту інформації у сфері платіжних послуг.

З огляду на це для комплексного аналізу проблеми доцільним є звернення до зарубіжних доктринальних підходів і практики наднаціональних регуляторів, насамперед Європейського центрального банку (ЄЦБ) та Європейського банківського органу (ЕВА). Їхні керівні принципи, технічні стандарти та аналітичні звіти визначають підходи до безпеки платіжних операцій, сильної клієнтської автентифікації, управління операційними й кіберризиками, а також вимоги до прозорості та захисту платіжної інформації і формують єдину модель безпеки цифрових платежів у державах ЄС. Так, річні статистичні дані, наведені у спільному звіті Європейського центрального банку та Європейського банківського органу «Report on Payment Fraud 2024», показують, що там, де запроваджено сильну автентифікацію клієнта і протокол тривимірної захищеної автентифікації платника (Three-Domain Secure (далі- 3-D Secure 2)), частка спірних та проблемних платіжних операцій суттєво зменшується [7]. Це підтверджує, що поєднання чітких регуляторних вимог і технічних стандартів обов'язково підвищує безпеку платежів.

На галузевому рівні Європейська платіжна рада у звіті «Payments Threats and Fraud Trends Report» (2024) окреслює коло ключових загроз для безпечного функціонування платіжних інструментів. Серед них – фішингові кампанії, операції, ініційовані самим користувачем під впливом введення в оману з боку третіх осіб (моделі типу Authorised Push Payment), підміна SIM-карт, зловживання платіжними запитами, маніпуляції з QR-кодами та інші форми соціальної інженерії, що створюють ризик несанкціонованого списання коштів і порушення конфіденційності платіжної інформації.

У цьому ж звіті наголошується на ключовій ролі застосування міжнародних стандартів, зокрема міжнародного стандарту ISO 20022 (Universal financial industry message scheme – Універсальна схема повідомлень для фінансової індустрії) для електронного обміну фінансовими повідомленнями та Стандарту безпеки даних індустрії платіжних карток (Payment Card Industry Data Security Standard) [8].

Мета статті полягає в тому, щоб комплексно проаналізувати правове регулювання платіжних інструментів в Україні, з'ясувати зміст та механізми захисту інформації під час виконання платіжних операцій, оцінити дієвість вимог до автентифікації користувача і розподілу відповідальності між надавачем платіжних послуг та користувачем, а також окреслити основні напрями подальшої гармонізації національного законодавства з правом Європейського Союзу.

Виклад основного матеріалу. Правове регулювання платіжних послуг в Україні зазнало суттєвого оновлення після набуття чинності Закону України «Про платіжні послуги» №1591-IX. Новий закон замінив модель платіжного ринку,

закріплену Законом «Про платіжні системи та переказ коштів в Україні» від 05. 04. 2001 року № 2346-111, та сформував сучасну нормативно – правову основу регулювання платіжних послуг в Україні орієнтовану на європейські стандарти. Зміни торкнулися як самої концепції платіжних послуг, так і кола їх надавачів, платіжних інструментів, вимог до безпеки, механізмів автентифікації, процедур вирішення спорів та технічних стандартів, які забезпечують функціонування платіжної інфраструктури.

Щодо надавачів платіжних послуг, то раніше такі повноваження фактично були зосереджені у банках. Нині участь у платіжному ринку можуть брати платіжні установи, установи електронних грошей, фінансові установи, що мають право на надання платіжних послуг, оператори поштового зв'язку, філії іноземних платіжних установ та інше.

Важливою зміною є і нова класифікація платіжних послуг та відповідних платіжних інструментів, яка стала ближчою до стандартів Європейського Союзу. Поряд із такими інструментами, як прямий дебет, кредитовий переказ і електронні платіжні засоби, законодавство передбачило сервіси ініціювання платежу та надання інформації про рахунок. Це створило умови для розвитку відкритого банкінгу, у межах якого операції здійснюються через прикладні програмні інтерфейси без передачі реквізитів платіжної картки торговцю.

Передусім нове законодавство переосмислило поняття платіжного інструмента. Якщо раніше акцент робився переважно на платіжній картці та класичних формах переказу коштів, то нині платіжний інструмент охоплює значно більший спектр технологічних рішень. Закон України «Про платіжні послуги» № 1591-IX визначає платіжний інструмент «як персоналізований засіб, пристрій та/або набір процедур, що відповідають вимогам законодавства та погоджені користувачем і надавачем платіжних послуг для надання платіжної інструкції» [1]. Також в Законі № 1591 прямо визначено коло платіжних інструментів, дозволених до використання учасниками платіжного ринку, а саме: прямий дебет, кредитовий трансфер (банківський переказ коштів від платника до одержувача) та електронні платіжні засоби. Кожен з цих інструментів виконує специфічну роль у платіжній інфраструктурі та орієнтований на різні моделі розрахунків.

Так, в умовах дії попередньої моделі платіжного ринку прямий дебет в Україні практично не використовувався, оскільки законодавство не передбачало його як самостійний платіжний інструмент. Після введення в дію Закону України «Про платіжні послуги» № 1591-IX прямий дебет уперше отримав нормативно-правове закріплення та був віднесений до платіжних інструментів: відповідно до п. 76 ч. 1 ст. 1 цього Закону прямий дебет визначається «як платіжний інструмент, що використовується для ініціювання платіжної операції дебетового переказу».

Його юридична природа ґрунтується на наданні платником попередньої згоди – дозволу на списання коштів зі свого рахунку за визначених умов. Саме тому прямий дебет відрізняється від інших платіжних інструментів тому, що ініціатива проведення операції належить не платнику, а отримувачу, тоді як банк забезпечує перевірку поданого розпорядження та технічної відповідності параметрів списання коштів умовам договору і платіжного інструменту.

У контексті розвитку платіжного ринку прямий дебет виконує низку системно важливих функцій. По-перше, він забезпечує стабільність і передбачуваність регулярних платежів, що є особливо значущим для комунальних послуг, телекомунікацій, страхових продуктів, абонентських сервісів і довгострокових зобов'язань, зокрема погашення кредитів. По-друге, цей інструмент зменшує операційне навантаження на споживача, усуваючи необхідність самостійно ініціювати кожний платіж, що мінімізує ризик прострочення з технічних чи поведінкових причин. По-третє, він сприяє зниженню вартості оброблення платежів у масштабах ринку, оскільки автоматизація процесу робить регулярні списання швидшими та економічно ефективнішими для фінансових установ.

З погляду безпеки оброблення інформації прямий дебет має специфічні вимоги. Оскільки механізм списання ґрунтується на попередньо наданій згоді платника, законодавство приділяє особливу увагу: захисту даних, що підтверджують таку згоду; перевірці цілісності інформації під час опрацювання запиту на списання; збереженню та відстежуванню записів операцій у спосіб, що дозволяє встановити факт належної авторизації у разі виникнення спору. Перевагою прямого дебету є також його відповідність тенденціям цифровізації. Цей інструмент може бути повністю інтегрований у електронні платіжні сервіси, мобільні застосунки та системи відкритого банкінгу, що дає змогу автоматично оновлювати реквізити, керувати згодами дистанційно та забезпечувати вищу прозорість для користувачів.

Поряд із прямим дебетом, який орієнтований насамперед на автоматизацію регулярних списань, важливе місце в структурі безготівкових

розрахунків посідає й інший ключовий інструмент – кредитовий трансфер**,** що забезпечує переважну частину ініційованих платником переказів коштів у сучасній платіжній інфраструктурі. Закон України «Про платіжні послуги» № 1591-IX у п. 30 ч. 1 ст. 1 визначає його як «платіжний інструмент у вигляді сукупності процедур, передбачених нормативно-правовими актами Національного банку України, що використовується для ініціювання кредитового переказу або миттєвого кредитового переказу» [1]. На відміну від прямого дебету, де ініціатором списання є отримувач коштів на підставі попередньо наданої платником згоди на списання коштів з його рахунку, кредитовий трансфер передбачає активну поведінку платника, який самостійно формує та подає доручення на переказ.

З правової точки зору кредитовий трансфер є класичною формою розпорядження коштами, у якій поєднуються дві ключові ознаки: одностороння воля платника на здійснення переказу та обов'язок установи, що надає платіжні послуги, виконати цю операцію в межах установлених строків та стандартів інформаційної безпеки. У сучасній моделі платіжного ринку кредитовий трансфер має багаторівневе функціональне значення. По-перше, він забезпечує переважну більшість безготівкових платежів між фізичними та юридичними особами, включно із оплатою товарів і послуг, переказами між власними рахунками та здійсненням бюджетних платежів. По-друге, кредитовий трансфер є основою корпоративних та банківських розрахунків. По-третє, цей інструмент відіграє ключову роль у міжнародних переказах, адже саме через нього відбувається виконання транскордонних платежів у міжбанківській інфраструктурі. Щодо поширення кредитового трансферу в Україні, то за статистикою Національного банку України він домінує серед безготівкових інструментів. Так, за даними «Платіжної інфраструктури України» за 2024 рік, понад 96 % усіх безготівкових операцій за сумою виконуються саме шляхом кредитових трансфертів. Цей інструмент охоплює найбільшу частку міжбанківських переказів, бюджетних платежів та операцій суб'єктів господарювання. Водночас кількісні показники зростають і серед фізичних осіб: відповідно до Звіту НБУ про платіжний ринок (2024), кількість кредитових переказів, ініційованих через мобільні застосунки банків, зросла на понад 35 % порівняно з попереднім роком [9].

У межах такої трансформації особливе місце посідають електронні платіжні засоби, оскільки вони поєднують у собі технічну, інформаційну та правову складові. На відміну від прямого дебету й кредитового трансферу, які описують спосіб ініціювання переказу коштів, електронний платіжний засіб є передусім засобом доступу до рахунку користувача і виконання платіжних операцій. Відповідно до п. 13 ч. 1 ст. 1 Закону №1591, електронні платіжні засоби визначаються як «інструмент реалізований на будь-якому носії, що містить в електронній формі дані, необхідні для ініціювання платіжної операції та/або здійснення інших операцій, визначених договором з емітентом» [1]. До цієї категорії належать платіжні картки, мобільні платіжні застосунки, «цифрові гаманці», токенізовані версії карток у смартфоні чи годиннику, інтернет-банкінг, а також інші пристрої й програмні комплекси, які забезпечують електронну ідентифікацію користувача та формування платіжного доручення. Сукупність таких рішень фактично виходить за межі традиційного розуміння платіжного інструменту як окремого матеріального носія і перетворює його на комплекс взаємопов'язаних цифрових сервісів. У перспективі їх розвитку можна говорити про формування «єдиного цифрового платіжного профілю» користувача, коли фізична картка перетворюється на похідний елемент, а доступ до рахунку забезпечується через набір токенізованих ідентифікаторів, біометричну автентифікацію та відкриті банківські інтерфейси.

Характерною рисою електронних платіжних засобів є поєднання їх технічної та юридичної природи: з одного боку, вони є програмно-технічними продуктами, які забезпечують передачу, обробку та підтвердження даних під час проведення операції, а з іншого – вони виступають юридично значущими інструментами, що формують волевиявлення платника і породжують правові наслідки. Їхній статус визначається не лише технічною здатністю ініціювати платіж, а й дотриманням вимог автентифікації, захисту інформації, документування та інформування користувача, встановлених законодавством і нормативно-правовими актами Національного банку України. Також, електронні платіжні засоби концентрують у собі основні правові ризики сучасних розрахунків: несанкціонований доступ до інформації, порушення конфіденційності даних, спірні транзакції. Крім того, саме для цієї групи інструментів законодавство встановлює найдетальніші вимоги до автентифікації, інформування споживача та розподілу відповідальності. НБУ, користуючись своїми регуляторними повноваженнями, деталізує ці вимоги у підзаконних нормативно-правових актах.

Таке переосмислення платіжних інструментів дає підстави говорити про новелу українського платіжного права: перехід від регулювання окремих технічних форм (картка, переказ, дебет) до регулювання цілісного життєвого циклу платіжної транзакції й цифрової ідентичності користувача, створення комплексної цифрової екосистеми, у межах якої взаємодія надавача платіжних послуг з користувачем здійснюється через послідовність електронних ідентифікаційних процесів. У цьому контексті важливим завданням законодавця стає не лише фіксація переліку інструментів, а й встановлення єдиних стандартів безпеки, прозорості умов та розподілу відповідальності для всіх моделей розрахунків, які еволюціонують на базі зазначених трьох основних платіжних інструментів.

Унаслідок такої трансформації платіжних інструментів у центр регулювання неминуче виходить питання захисту інформації, яка формується, передається та зберігається під час виконання платіжних операцій. Вимоги до конфіденційності, цілісності та доступності даних, закріплені Законом України «Про платіжні послуги» № 1591-IX та нормативно-правовими актами Національного банку України, поширюються на всі види платіжних інструментів і визначають єдині мінімальні стандарти безпеки для учасників ринку. У Положенні Національного банку України № 43 від 2021 року вони конкретизуються через поняття інформаційної безпеки як «збереження конфіденційності, цілісності та доступності інформації», а також через категорій інциденту інформаційної безпеки як «події чи серії подій порушення інформаційної безпеки, що можуть призвести до збитків або втрат для суб'єкта інформаційного захисту або користувачів платіжних послуг» [10]. Під суб'єктом інформаційного захисту розуміють надавача платіжних послуг (крім установ електронних грошей, Національного банку, органів державної влади та органів місцевого самоврядування), оператора платіжної системи-резидент та технологічного оператора платіжних послуг у разі надання інших видів послуг, крім оброблення платіжних операцій в міжнародних карткових платіжних системах» [10]. Ці підходи дозволяють розглядати захист інформації у сфері платіжних послуг як самостійний елемент правового режиму платіжних інструментів. Фактично законодавець виокремлює дві групи учасників, щодо яких можуть виникати наслідки інциденту інформаційної безпеки: з одного боку, суб’єкт інформаційного захисту, а з іншого – користувачі платіжних послуг. Це означає, що порушення конфіденційності, цілісності чи доступності даних під час виконання платіжної операції автоматично виходить за межі суто технічної проблеми та набуває правового значення: воно впливає на розподіл відповідальності, порядок відшкодування збитків, обов’язок повідомлення про інцидент і застосування превентивних заходів. У такій ситуації ключовим елементом забезпечення належного рівня інформаційної безпеки стають механізми перевірки особи та підтвердження волевиявлення платника, адже саме вони визначають правомірність транзакції та її захищеність.

Саме тому при здійсненні платіжних операцій набули нового змісту вимоги до безпеки оброблення платіжних даних та автентифікації користувача. Сильна автентифікація клієнта закріплена як обов’язковий елемент правового режиму будь-якого платіжного інструмента. Вона передбачає підтвердження операції щонайменше двома взаємно незалежними елементами з різних категорій: знання (пароль, код, персональний ідентифікатор), володіння (платіжна картка, телефон, токен, інший пристрій) та притаманна клієнтові характеристика (біометричні дані, зокрема відбиток пальця або розпізнавання обличчя) [10].

Використання таких елементів має забезпечувати, з одного боку, однозначну ідентифікацію особи платника, а з іншого – мінімізувати ризик несанкціонованого використання платіжного інструмента третіми особами.

Нормативно-правові акти Національного банку України деталізують ці вимоги через встановлення критеріїв захищеності каналів передавання даних, порядку формування одноразових ідентифікаторів, використання протоколів багатофакторного підтвердження операцій, а також запровадження ризик-орієнтованих підходів до автентифікації. Для дистанційних та електронних операцій це означає обов’язковість поєднання традиційних реквізитів (логін, пароль, реквізити картки) з додатковими чинниками – одноразовими паролями, push-підтвердженнями в мобільному застосунку, біометричною перевіркою тощо. Саме ці процедури стають центральною ланкою в оцінці того, чи була операція належним чином авторизована користувачем, і, відповідно, чи покладається на надавача платіжних послуг обов’язок відшкодувати збитки у випадку спірних або неправомірних платіжних дій. Практичну ефективність таких рішень підтверджують статистичні дані. За даними Європейського банківського органу, після запровадження сильної автентифікації користувача (SCA) рівень шахрайства за онлайн-платежами у 2022–2023 роках зменшився більш ніж на 40 %, а частка успішних шахрайських транзакцій

у країнах ЄС стала однією з найнижчих за останнє десятиліття [7]. У свою чергу, статистика НБУ демонструє, що в Україні понад 64 % операцій за сумою та понад 94 % за кількістю здійснюються у безготівковій формі, причому основну частку складають операції, що виконуються через захищені цифрові канали [11].

Окремі вимоги у Законі № 1591 сформульовано щодо біометричної автентифікації: законодавство зобов'язує постачальника платіжних послуг забезпечити наявність належної правової підстави для обробки біометричних даних, надати користувачеві повну й зрозумілу інформацію про мету та обсяг такої обробки, а також гарантувати можливість доступу до платіжних послуг альтернативним способом, без використання біометричних ідентифікаторів. Такий підхід покликаний поєднати підвищені вимоги до надійності автентифікації з дотриманням прав користувачів на приватність та автономність вибору способу ідентифікації. Таку практику можна прямо пов'язати з підходами Європейського Союзу. Зокрема, регулятивні технічні стандарти до Директиви (ЄС) 2015/2366 щодо сильної клієнтської автентифікації передбачають можливість використання кількох факторів автентифікації та не вимагають обов'язкового застосування біометрії, а наглядові органи ЄС з захисту даних (зокрема Європейська рада із захисту даних) у своїх рекомендаціях наголошують на неприпустимості «примусової» біометричної ідентифікації та необхідності надання користувачам альтернативних, не біометричних способів доступу до платіжних послуг. Це дозволяє обґрунтувати, що вимога про альтернативний канал доступу без біометрії відповідає не лише українському законодавству, а й загальноєвропейській регуляторній та наглядовій практиці.

Окремий акцент у законодавстві зроблено на захисті користувача у випадках платіжних операцій, не ініційованих ним. Закон № 1591 передбачає інший розподіл тягаря доказування: саме надавач платіжних послуг повинен довести належність автентифікації та відсутність технічної несправності під час ініціювання, передавання й оброблення щодо неавторизованих та неналежно виконаних платіжних операцій у своїх інформаційних системах. Такий підхід зафіксовано у статті 86 Закону України «Про платіжні послуги», яка прямо покладає на постачальника послуг обов'язок довести, що операція була коректно автентифікована, належно зафіксована та не містила ознак технічної помилки. Дана норма суттєво підсилює позицію користувача, адже у разі виникнення спору презумпція діє на користь клієнта: постачальник платіжних послуг зобов'язаний довести належність автентифікації та захищеність каналу передавання даних. До моменту надання таких доказів операція вважається такою, що була виконана без належної згоди користувача. У свою чергу, це зобов'язує надавачів платіжних послуг забезпечувати детальну фіксацію кожного етапу здійснення платіжної операції, включно з журналами доступу, результатами перевірки факторів автентифікації, записами технічних подій інформаційної системи та іншими даними, необхідними для подальшого відтворення перебігу транзакції. Крім того, законодавство зобов'язує провайдерів забезпечити наявність прозорої, зрозумілої та доступної процедури розгляду звернень щодо неавторизованих та неналежно виконаних платіжних операцій, встановити чіткі строки для їх опрацювання та гарантувати інформування користувача про результати розгляду. У комплексі це формує нову модель відповідальності, орієнтовану на превентивний захист користувача та підвищення стандартів інформаційної безпеки у сфері застосування платіжних інструментів.

Важливо й те, що платіжні інструменти тепер тісно пов'язані з процедурами фінансового моніторингу й ідентифікації клієнтів. Застосування заходів протидії легалізації (відмиванню) доходів, встановлення особи та її верифікація розглядаються не як додаткові опції, а як обов'язкова передумова надання й подальшого використання платіжного інструмента. Таке поєднання платіжної інфраструктури з механізмами фінансового моніторингу має і змістовні правові наслідки. Для надавача платіжних послуг воно створює розширений обов'язок щодо перевірки інформації, оцінки ризиковості операції, збереження відповідних даних і своєчасного подання повідомлень про підозрілі дії. Для користувача це гарантує більший рівень захищеності його фінансових операцій, оскільки будь-які нетипові сценарії доступу або ініціювання платежу підлягають автоматичному контролю та можуть бути заблоковані або переведені в режим додаткової автентифікації. У результаті фінансовий моніторинг перетворюється не лише на інструмент протидії злочинним діям, а й на важливий механізм забезпечення інформаційної безпеки платіжних операцій, який мінімізує ризики несанкціонованого доступу, шахрайства та маніпуляцій із цифровими платіжними інструментами.

Висновки. Трансформація платіжних інструментів, закріплена Законом України «Про платіжні послуги» № 1591-IX, демонструє системний перехід українського платіжного ринку від технологій

попереднього покоління до комплексної цифрової моделі, у якій електронні ідентифікаційні процеси та високий рівень захисту даних стають ключовими компонентами правового регулювання. У сучасних умовах платіжний інструмент більше не обмежується матеріальним носієм чи певною технічною формою; він функціонує як елемент цифрової екосистеми, що об'єднує ідентифікацію користувача, формування волевиявлення, передачу інформації та виконання операції.

Такі зміни зумовили підвищення вимог до інформаційної безпеки, конфіденційності та цілісності даних, а також уточнення правового режиму інцидентів інформаційної безпеки. Встановлені Національним банком України стандарти визначають єдиний мінімальний рівень захисту для всіх учасників ринку, незалежно від виду платіжного інструмента чи платформи його реалізації. Центральне місце у цьому регулюванні займають механізми сильної автентифікації, ризик-орієнтованого моніторингу операцій та вимоги до технічної захищеності каналів передавання даних.

Не менш значущим є інтегрування процедур фінансового моніторингу та ідентифікації клієнтів у структуру платіжних інструментів. Це забезпечує своєчасне виявлення нетипових або ризикових операцій, запобігає шахрайству й водночас формує нову модель відповідальності між користувачем і надавачем платіжних послуг.

У підсумку можна констатувати, що сучасний підхід до регулювання платіжних інструментів ґрунтується на поєднанні технологічних та правових механізмів. Саме ця інтегрована модель створює передумови для підвищення безпеки платіжних операцій, забезпечення прозорості ринку та зміцнення довіри користувачів до цифрових фінансових сервісів. Вона також наближає національне законодавство до європейських стандартів і формує основу для подальшого розвитку інновацій у сфері платіжних послуг.

REFERENCES:

1. Verkhovna Rada of Ukraine. (2021, June 30). Zakon Ukrainy "Pro platizhni posluhy" [Law of Ukraine on payment services] (No. 1591-IX). https://zakon.rada.gov.ua/laws/show/1591-20

2. European Parliament, & Council of the European Union. (2015, November 25). Directive (EU) 2015/2366 on payment services in the internal market. Official Journal of the European Union, L 337. https://eur-lex.europa.eu/eli/dir/2015/2366/oj

3. Sukhodols′kyi, B. B. (2025). Platizhni posluhy v tsyvil′nomu pravi Ukrainy ta yikh pravova pryroda [Payment services in the civil law of Ukraine and their legal nature]. *Naukovyi visnyk Uzhhorods'koho universytetu. Seriia "Pravo"*, *90*(2), 204–209. [Ukrainian] https://doi.org/10.24144/2307-3322.2025.90.2.29

3. Klochko, A. M., & Volchenko, N. V. (2021). Biometrychni tekhnolohii dlia bezpeky provedennia bankivskykh operatsii v Ukraini ta zarubizhnykh derzhav [Biometric technologies for the security of banking operations in Ukraine and foreign states]. Chasopys Kyivs′koho universytetu prava, (1), 299–304. [Ukrainian] https://repo.snau.edu.ua/xmlui/handle/123456789/9218

4. Fabcic Povse, D. (2021). Strong customer authentication in online payments under GDPR and PSD2: A case of cumulative application. In M. Friedewald, S. Schiffner, & S. Krenn (Eds.), Privacy and identity management (IFIP Advances in Information and Communication Technology, Vol. 619, pp. 78–95). Springer. https://doi.org/10.1007/978-3-030-72465-8_5

5. Hassan, M. A. (2020). A review on electronic payments security. Symmetry, 12(8), 1344. https://doi.org/10.3390/sym12081344

6. European Banking Authority, & European Central Bank. (2024). Report on payment fraud 2024. https://www.eba.europa.eu/sites/default/files/2024-08/465e3044-4773-4e9d-8ca8-b1cd031295fc/EBA_ECB%202024%20Report%20on%20Payment%20Fraud.pdf

7. European Payments Council. (2024). Payments threats and fraud trends report 2024. https://www.europeanpaymentscouncil.eu/document-library/reports/payments-threats-and-fraud-trends-report-2024

8. National Bank of Ukraine. (2024). Platizhna infrastruktura Ukrainy (stanom na 2024 rik) [Payment infrastructure of Ukraine (as of 2024)]. https://bank.gov.ua/ua/statistic/payment/statistic#7

9. National Bank of Ukraine. (2021, May 19). Postanova No. 43: Pro zatverdzhennia Polozhennia pro zakhyst informatsii ta kiberzakhyst uchasnykamy platizhnoho rynku [Resolution No. 43: On approval of the Regulation on information protection and cybersecurity by payment market participants]. https://zakon.rada.gov.ua/laws/show/v0043500-21#Text

10. National Bank of Ukraine. (2024). Bezghotivkovi rozrakhunky u 2024 rotsi [Cashless card payments in 2024]. https://bank.gov.ua/ua/news/all/bezgotivkovi-rozrahunki-u-2024-

Дата першого надходження рукопису до видання: 22.10.2025
Дата прийнятого до друку рукопису після рецензування: 14.11.2025
Дата публікації: 10.12.2025