DOI: https://doi.org/10.32782/2524-0072/2025-71-165

УДК 336.7

ПЛАТІЖНА СИСТЕМА УКРАЇНИ: АНАЛІЗ ТА ДИНАМІКА ШАХРАЙСЬКИХ ОПЕРАЦІЙ

UKRAINIAN PAYMENT SYSTEM: ANALYSIS AND DYNAMICS OF FRAUDULENT TRANSACTIONS

Любкіна Олена Вікторівна
доктор економічних наук, професор,
Київський національний університет імені Тараса Шевченка
ORCID: https://orcid.org/0000-0002-8245-8300

Тараба Віктор Сергійович
аспірант,
Київський національний університет імені Тараса Шевченка
ORCID: https://orcid.org/0000-0002-5265-8571

Liubkina Olena, Taraba Viktor
Taras Shevchenko National University of Kyiv

Стаття ґрунтується на проведенні дослідження сучасного стану та динаміки шахрайських операцій у вітчизняній платіжній системі та методів боротьби з такими операціями. Розглянуто сучасні тенденції розвитку кіберзлочинності у сфері платіжних систем. Висвітлено та комплексно проаналізовано проблему «грошових мулів» у банківській системі України, масштаби якої значно зросли протягом кількох останніх років. Охарактеризовано основні методи міжбанківської взаємодії з метою попередження та блокування шахрайських операцій на прикладі існуючих сервісів Української міжбанківської Асоціації членів платіжних систем. Проаналізовано структуру шахрайських операцій в розрізі їх типів. Надано рекомендації для боротьби з протиправним використанням платіжної інфраструктури з використанням математичних методів, зокрема машинного навчання та мережевого аналізу.

Ключові слова: шахрайство, платіжна система, грошові мули, банк, міжбанківська взаємодія, кібершахрайство, соціальна інженерія, платіжна інфраструктура, інформаційні технології.

Financial fraudsters continuously upgrade their methods of illegally obtaining funds by leveraging cutting-edge technologies, social engineering, and vulnerabilities in financial monitoring systems. However, due to the use of modern technologies, fraudsters often manage to stay ahead. In recent years, the number of «money mules» in the Ukrainian banking sector has significantly increased. As a result, it is necessary to upgrade the tools to counter such fraudulent activities. The aim of this article is to analyze empirical data at a generalized level to identify and examine the latest trends, as well as to develop recommendations for the possible prevention of fraudulent transactions and more effective counteraction against the illegal use of payment infrastructure. The following methods were used in the research: theoretical analysis and systematization (to study and summarize information on recent changes in fraudsters' activities and banks' approaches to combating them), graphical methods (to compare and visually represent the effectiveness of fraud prevention services), and logical generalization of results (to formulate conclusions and identify future research directions). The article is based on a study of the current state and dynamics of fraudulent transactions in the national payment system, as well as methods of combating such activities. Modern trends in the development of cybercrime in the field of payment systems are examined. The issue of «money mules» in Ukraine's banking system, which has significantly expanded in recent years, is highlighted and comprehensively analyzed. The main methods of interbank interaction aimed at preventing and blocking fraudulent transactions are characterized using the example of existing services of the Ukrainian Interbank Payment Systems Member Association «EMA». The structure of fraudulent transactions is analyzed in terms of their types. The practical significance of this article lies in providing recommendations for automating the financial monitoring process and utilizing machine learning and network analysis methods to prevent and detect modern fraud techniques, particularly large-scale fraudulent networks, as well as analyzing international experience in combating «money mules».

Keywords: fraud, payment system, money mules, bank, interbank relations, cyber fraud, social engineering, payment infrastructure, information technology.

Постановка проблеми у загальному вигляді. Розвиток цифрових фінансових технологій та зростання обсягів безготівкових платежів в Україні мають і зворотній ефект у вигляді протиправного використання платіжної інфраструктури та збільшення рівня фінансового шахрайства. Зловмисники постійно вдосконалюють методи шахрайства, використовуючи новітні технології, соціальну інженерію та вразливості у системах фінансового моніторингу. Це створює значні ризики як кінцевих користувачів платіжних послуг та банківських установ, так і для фінансової системи України в цілому.

Одним із найсерйозніших викликів останніх років, задля вирішення якого НБУ змушений запроваджувати додаткові обмеження, є діяльність «грошових мулів» – осіб, які, свідомо або несвідомо, сприяють відмиванню коштів та реалізації шахрайських схем. Масштаби цього явища в Україні продовжують зростати, що вимагає ефективних механізмів виявлення та протидії.

Аналіз останніх досліджень і публікацій. Питання протиправного використання вітчизняної платіжної інфраструктури активно досліджується науковцями, зокрема Рисін В. В. та А. Р. Карпець [1] здійснили систематизацію новітніх схем відмивання грошей, враховуючи схеми з використанням криптовалют, визначили можливі порушення при здійсненні фінансового моніторингу та потенційні негативні наслідки для фінансової установи, запропонували правила належної обачності для фінансових установ при роботі з високоризиковими клієнтами та продемонстрували необхідність застосування ризик-орієнтованого підходу. Також Рисін В. В. та Корначук О. Ю. [2] звертають особливу увагу на ризики залучення банківських установ до незаконних схем відмивання коштів, та демонструють негативний вплив у випадку реалізації таких ризиків як на саму банківську установу, так і на фінансову систему та державу в цілому. Автори виділяють також екзогенні чинники (зокрема подолання сформованих тіньових процесів в економіці та забезпечення належної кримінальної відповідальності для організаторів шахрайських схем), які знаходяться поза контролем фінансових установ, але мають значний вплив на зменшення ризику відмивання коштів. Вишивана Б. М. та Козак Д. А. [3] досліджували шахрайські операції з платіжними картками в умовах діджиталізації та класифікували поширені схеми шахрайства і методи захисту, проаналізували динаміку та особливості шахрайських операцій в Україні. Праця Чуницької І. І. [4] присвячена висвітленню ролі міжнародних організацій, створених для боротьби з легалізацією коштів, які отримано незаконним шляхом, акцентується увага також на факторах ризику шахрайства, зокрема висвітлюється трикутник шахрайства, необхідні умови для його виникнення, та рівні ризику за секторами економіки; окрім того, авторка аналізує світовий законодавчий досвід у сфері протидії шахрайства, та порівнюючи його з вітчизняним досвідом, надає рекомендації щодо удосконалення заходів попередження шахрайства. Маршук Л. М. та Складанюк М. С. [5] досліджували найбільш поширені методи платіжного шахрайства та боротьби з ними, та сформулювали перелік рекомендацій для фізичних осіб з метою мінімізації ризики втрату коштів внаслідок платіжного шахрайства; значної уваги заслуговує також емпірична частина дослідження та виокремлення на їх основі основних тенденцій. Васильченко З. М. та Пилипенко А. М. [6] при дослідженні ринку платіжних карток та платіжної інфраструктури відносять ризик шахрайства та ризик нового клієнта до одних з основних ризиків безготівкових платежів, також автори акцентують увагу на загрозі кібератак. Сизоненко В. Ю. та Кисельов А. О. [7] досліджували особливості протидії шахрайству та відзначали швидку адаптацію фінансових шахраїв до нових умов та появи нових технологій, і як наслідок висновують необхідність системного підходу задля забезпечення ефективної боротьби з незаконними операціями з платіжними картками. Також автори підкреслюють важливість діяльності Української міжбанківської асоціації «ЄМА» та просвітницької діяльності НБУ, зокрема всеукраїнської програми з підвищення фінансової грамотності #ШахрайГудбай. Значну практичну цінність мають також огляди та аналітичні записки міжнародних платіжних систем та європейських чи міжнародних організацій, зокрема EBA (European Banking Authority) [8], EPC (European Payments Council) [9], Світового банку [10].

Виділення невирішених раніше частин загальної проблеми. Проте незважаючи на значну увагу науковців до проблеми протиправного використання платіжної інфраструктури та кібершахрайства, ця увага в більшості випадків має теоретичне спрямування та незначним чином спирається на емпіричні дані.

Окрім того, специфіка шахрайських методів, а особливо кібершахрайських, полягає в тому, що фінансові установи (в першу чергу банки) та державні органи при боротьбі є «наздоганяючими» відносно шахраїв, тобто реагують на появу нових різновидів шахрайства, методів організації шахрайських схем тощо із значним часовим лагом, коли відповідні зміни набувають достатнього масштабу. Також майже відсутній аналіз проблеми боротьби з мережами «дропів», які стали помітної проблемою протягом останніх кількох років.

Формулювання цілей статті. Метою даної статті є аналіз емпіричних даних на узагальненому рівні задля виокремлення та розгляду останніх трендів, та формування рекомендацій для можливого попередження шахрайських операцій та більш ефективної боротьби з протиправним використанням платіжної інфраструктури.

Виклад основного матеріалу дослідження. Перехід до безготівкової економіки є загальносвітовим трендом, і Україна тут не є винятком. У таблиці 1 наведено кількість ЕПЗ (електронних платіжних засобів) за даними НБУ, як бачимо за останні роки кількість платіжних засобів, зокрема і активних (за якими була здійснена хоча б одна видаткова транзакція), збільшується. Втім, зростання популярності і поширеності безготівкових розрахунків, а також спрощення та пришвидшення процесу відкриття банківських рахунків (зокрема можливість стати клієнтом багатьох українських банків через дистанційні канали), водночас полегшують і протиправне використання платіжної інфраструктури, а тому мають і зворотній ефект: виникнення методів шахрайства / відмивання коштів або більше поширення вже існуючих методів.

Як зазначає НБУ, під час війни збільшилася кількість випадків кібершахрайства та кіберзлочинності [12]. Також слід відзначити активне використання шахраями сучасних технологій, приміром, як зазначають представники банку ПУМБ, поширення набуло шахрайство з використанням програм відділеного доступу (AnyDesk або TeamViewer) [13]. Особливим випадком у вітчизняній банківській системі за останні роки є поширення мереж «дропів» (у міжнародній практиці більш поширений термін «грошовий мул» – money mule; це люди, які надають шахраям за певну плату доступ до своїх рахунків та здійснення операцій з використанням мобільного банкінгу), проблема набула такого масштабу, що привернула увагу регулятора, який був змушений вводити додаткові обмеження для боротьби з нею.

У таблиці 2 наведено дані по кількості дропів за даними ЄМА (Українська міжбанківська асоціація членів платіжних систем ЄМА) за період з 2023 по 2024 роки. Як бачимо, кількість дропів у 2023 році порівняно з 2021 збільшилася майже в 6 разів. Хоча аналогічні дані за 2024 рік ще не оприлюднено, але за даними НБУ [14] за 8 місяців 2024 року банками було припинено відносини з більш ніж 80 тисячами клієнтів через участь у мережах дропів, що набагато перевищує показники попередніх років. Втім, такий приріст може частково пояснюватися більшою увагою регулятора та банків до проблеми починаючи з 2024 року, і як наслідок значно більшою кількістю ідентифікованих випадків.

Таблиця 1

Динаміка кількості електронних платіжних засобів

Показник	01.12.2024	01.12.2023	01.12.2022	01.12.2021	01.12.2020
ЕПЗ, термін дії яких не закінчився (в обігу)	127 853 882	114 348 392	109 622 858	79 991 775	72 950 959
ЕПЗ, за якими протягом звітнього періоду була здійснена хоча б одна видаткова транзакція	55 697 664	51 322 029	45 335 152	43 809 555	39 232 291
приріст кількості ЕПЗ, термін дії яких не закінчився (в обігу)	13 505 490	4 725 534	29 631 083	7 040 816	-
приріст к-ті ЕПЗ, за якими була здійснена хоча б одна видаткова транзакція	4 375 635	5 986 877	1 525 597	4 577 264	-

Джерело: побудовано на основі даних НБУ [11]

Таблиця 2

Динаміка кількості ідентифікованих дропів

Показник	2021	2022	2023
К-ть ідентифікованих грошових мулів ("дропів")	1850	3734	10820
Абсолютний приріст (рік до року)	-	1884	7086
Відносний приріст (рік до року)	-	101.84%	189.77%
Відносний приріст (за період)	-	101.84%	383.03%

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [13; 15]

Проблема також посилюється тим, що припиненнях банком відносин з дропом не є вирішенням проблеми, адже такий клієнт може перейти до іншого банку – тобто не існує обміну між банками даними про високоризикових клієнтів. На етапі відкриття клієнта ризикових ознак цілком може і не бути (особливо враховуючи існування так званих «сплячих дропів»), лише маючи історію операцій по клієнту можливо зробити більш обґрунтований висновок, а це вимагає часу та певний час обслуговування клієнта. Водночас і повна заборона користуватися банківськими послугами незалежно від банку для клієнтів з високим рівнем ризику та історією участі в мережах дропів також не є бажаним результатом, адже сприятиме фактично «випадінню» таких людей з банківської системи і як наслідок зменшенню фінансової інклюзії. Варто також відзначити, що раннє виявлення дропів має і важливу соціальну функцію, бо саме дропи, які свідомо чи несвідомо є учасниками шахрайських схем, водночас є і одними з постраждалих, адже надаючи шахраям повний доступ до своїх рахунків та мобільного додатку вони, окрім юридичної відповідальності, також отримують неможливість обслуговування в банку (як HBP – клієнти з неприйнятно високим рівнем ризику), податкові зобов'язання (сплата податків з доходів, отриманих від третіх осіб), та потенційно оформлений на них та виведений кредит в межах максимального кредитного ліміту, який було надано банком такому клієнту.

Діяльність державного регулятора в напрямі боротьби з шахрайством поєднує як просвітницьку діяльність, так і посилення вимог до надавачів платіжних послуг, та, в окремих випадках, запровадження заборон та обмежень. Зокрема за останні роки було:

1) запроваджену посилену автентифікацію надавачами платіжних послуг [16];

2) поновлено Всеукраїнську інформаційну кампанію з платіжної безпеки #ШахрайГудбай (перша така кампанія була в 2020 році) [12];

3) розпочато проєкт протидії кібершахрайству у фінансовому секторі спільно з найбільшими провайдерами з основним акцентом на протидію фінансовому фішингу [17];

4) спільно з ДССЗЗІ запущено Всеукраїнську кампанію з платіжної безпеки #КібербезпекаФінансів [18];

5) встановлено тимчасовий ліміт на суму P2P-переказів [14];

6) за сприяння НБУ, НАБУ, АУБ найбільші банки підписали Меморандум про забезпечення прозорості функціонування ринку платіжних послуг, що зокрема запроваджує диференційовані ліміти на суму переказів залежно від рівня ризику клієнта, також задекларовано створення реєстру сумнівних клієнтів, дані з якого мають враховуватися банками при відкритті клієнта [19].

Розглянемо детальніше деякі з існуючих методів міжбанківської взаємодії для попередження та виявлення шахрайських операцій на прикладі EMA Anti Fraud Hub (окрім розглянутих проєктів ЄМА також має сервіси Mobile Check, CrimeCheck online, CardCheck Online, та займається просвітницькою діяльністю: воркшопи, посібники, гра «Здолай шахрая», Школа кібербезпеки) [20; 21]:

1) Cardholder Verification – сервіс для перевірки приналежності картки тій особі, якій призначається платіж на основі ІПН та маски картки [22]. На рис. 1 зображено динаміку кількості виявлених невідповідностей власника картки документів (тобто коли у клієнта з вказаним ІПН відсутня карта з відповідною маскою), та розрахункову суму попереджених втрат від шахрайства. Збільшення кількості перевірок з невідповідностями та розрахункової суми пояснюється в першу чергу підключення додаткових банків до сервісу про-

тягом періоду. Загальна розрахункова сума попереджених таким чином втрат за період з 01.01.2023 по 15.01.2025 (без врахування періоду з 01.07.2024 по 15.07.2024), оскільки за цей проміжок ЄМА не оприлюднила статистику використання сервісу) становить майже 53 мільйони грн.

2) Fraud Payments Tracker – сервіс, завданням якого є сприяння відстеженню та блокуванню шахрайських операцій, передбачає відправку банком жертви шахрайства після повідомлення від клієнта про шахрайство повідомлення (алерту) банку отримувачу такого переказу [25].

Як бачимо на основі рис. 3 та рис. 4, основним типом шахрайських операцій є соціальна інженерія (57% випадків), на 2-му місці – несанкціонований платіж (майже 33%), і на останньому – ненадання товару/послуги (майже 10%).

3) БД Інциденти – база даних з даними про інциденти платіжного та кредитного шахрайства [26]. На рисунку 5 наведено динаміку кількості інцидентів та кількості організацій, що повідомляли про інциденти (за період з 01.01.2023 по 15.01.2025, окрім періодів 01.07.2024-15.07.2024, 16.08.2024-31.08.2024 за які дані відсутні або неповні, та без врахування періоду 01.02.2024-15.02.2024, оскільки в цей період відбулася реєстрація історичних даних Монобанку за період з 2020 по 2024 роки, і як наслідок кількість інцидентів за період становила майже 20 тисяч). Протягом розглянутого періоду банки доєднувалися або розширювали роботу з сервісом, що частково пояснює зростання кількості інцидентів.

Автори статті вбачають доцільними такі рекомендації для боротьби з протиправним використанням платіжної інфраструктури:

1) Посилення міжбанківської взаємодії та створення реєстру дропів за сприяння НБУ – перспективним вважаємо створення єдиного реєстру для аналізу шахрайських схем у масштабах усієї платіжної системи. Така структура могла б виконувати роль аналітичного хаба, що акумулюватиме дані від усіх банків і сприятиме протидії шахрайству в режимі реального часу. Це дозволить виявляти складні шахрайські мережі, які можуть охоплювати декілька фінансових установ одночасно. Хоча частково схожий функціонал і реалізовано ЄМА, але він охоплює лише частину банків та не дозволяє повноцінно вирішити проблему.

2) Активне використання методів машинного навчання та мережевого аналізу (зокрема графової аналітики) для раннього виявлення мереж «дропів» зокрема та для автоматизації і пришвидшення процесів фінансового моні-

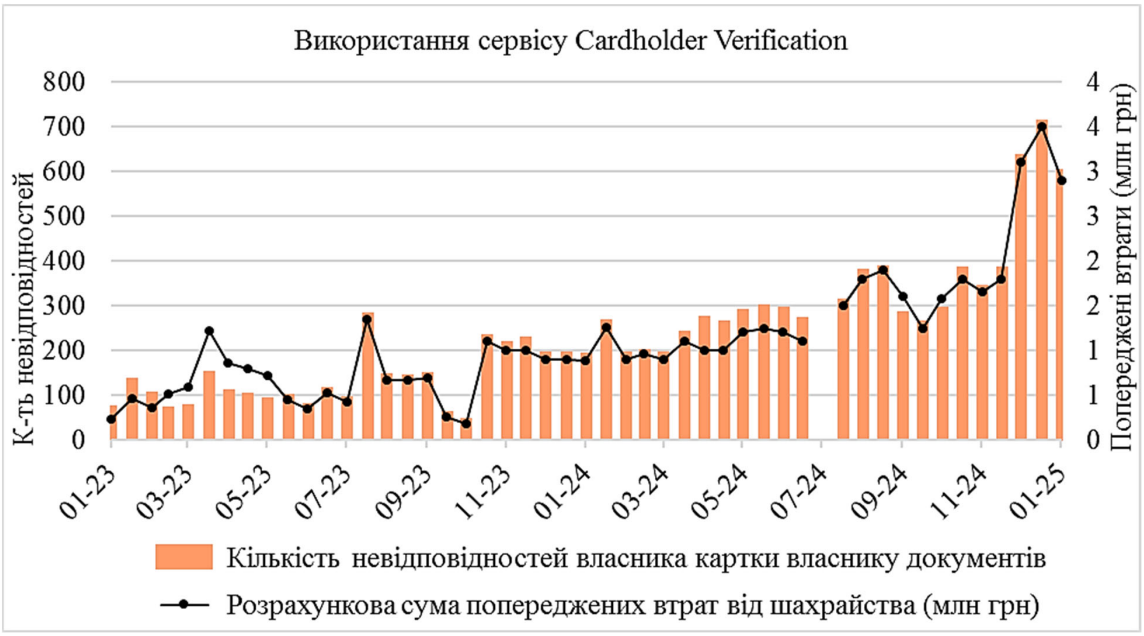

Рис. 1. Використання сервісу Cardholder Verification: кількість невідповідностей власника картки власнику документа та розрахункова сума попереджених втрат від шахрайства

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [23; 24]

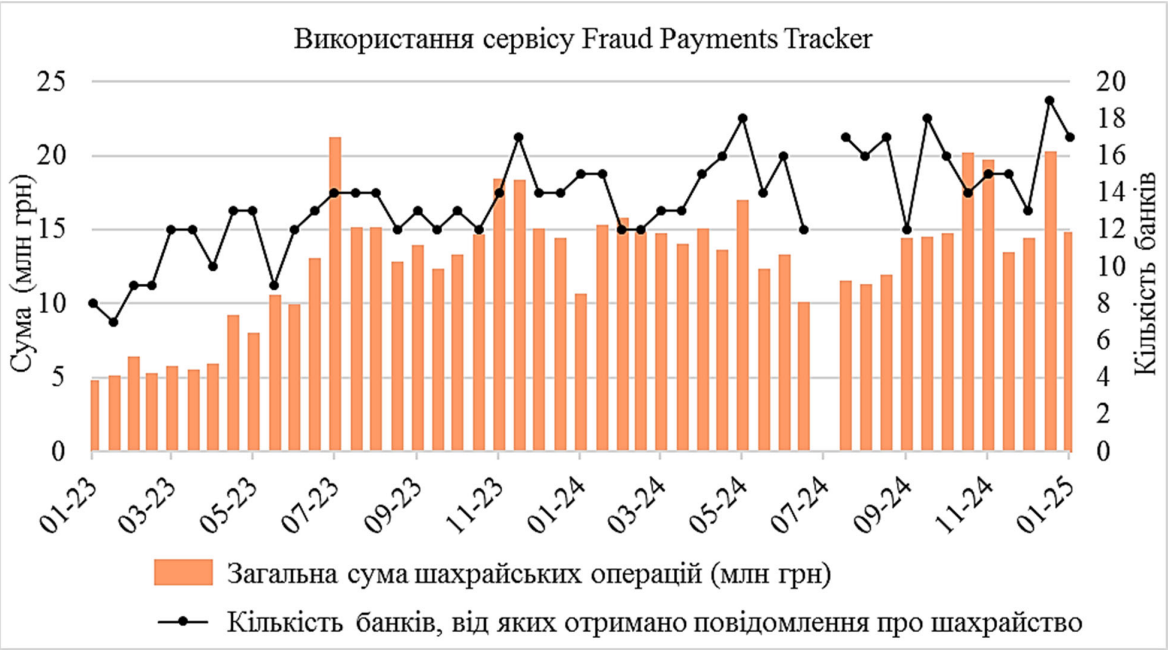

Рис. 2. Загальна сума попереджених операцій за алертами та кількість банків, які про них повідомляли, за даними сервісу Fraud Payments Tracker

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [23; 24]

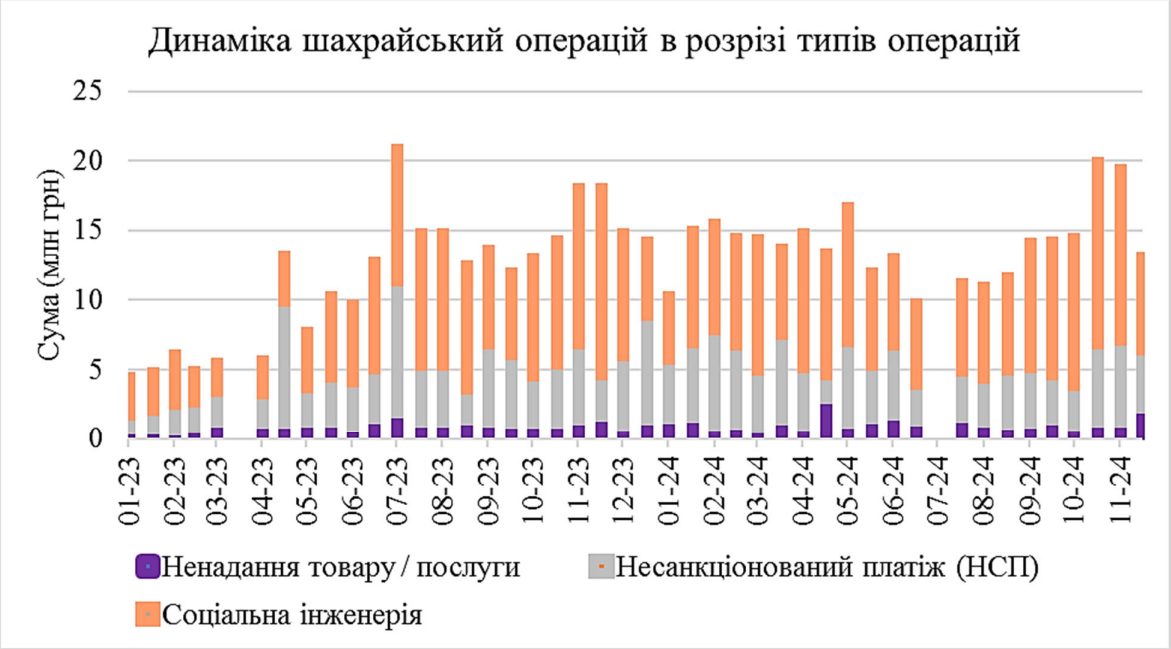

Рис. 3. Динаміка шахрайський операцій в розрізі типів операцій за даними сервісу Fraud Payments Tracker

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [23; 24]

торингу в цілому. Традиційні методи фінансового моніторингу вже не здатні ефективно впоратися з новими викликами у сфері шахрайства, оскільки зловмисники постійно змінюють свої підходи та розробляють складніші схеми. У зв'язку з цим використання методів

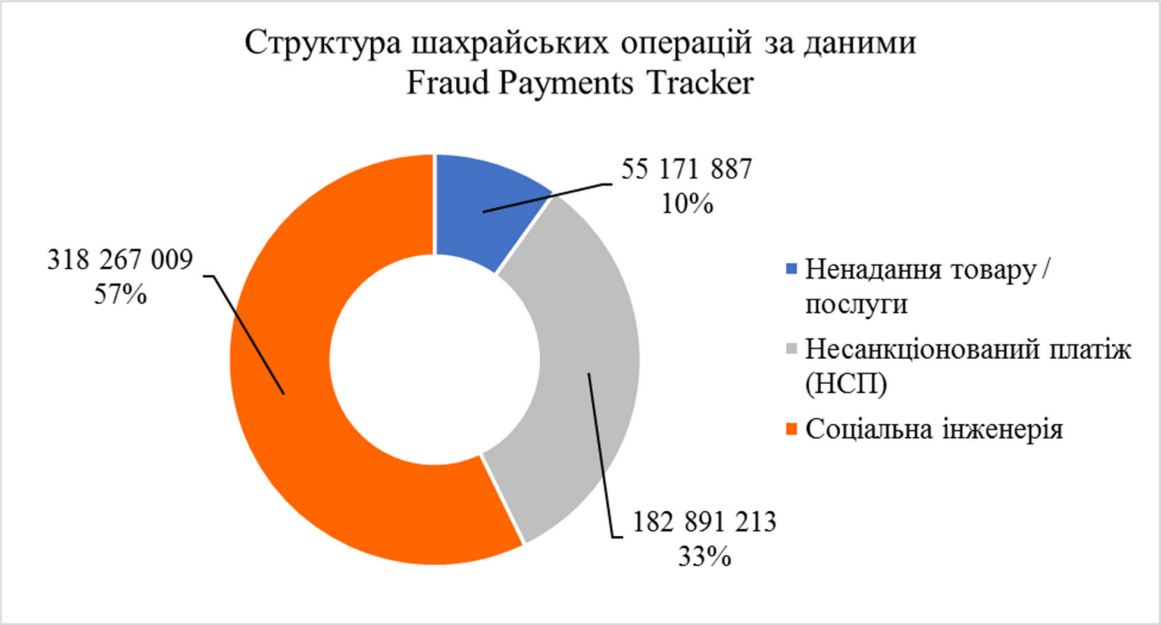

Рис. 4. Структура суми шахрайських операцій в розрізі типів за даними сервісу Fraud Payments Tracker

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [23; 24]

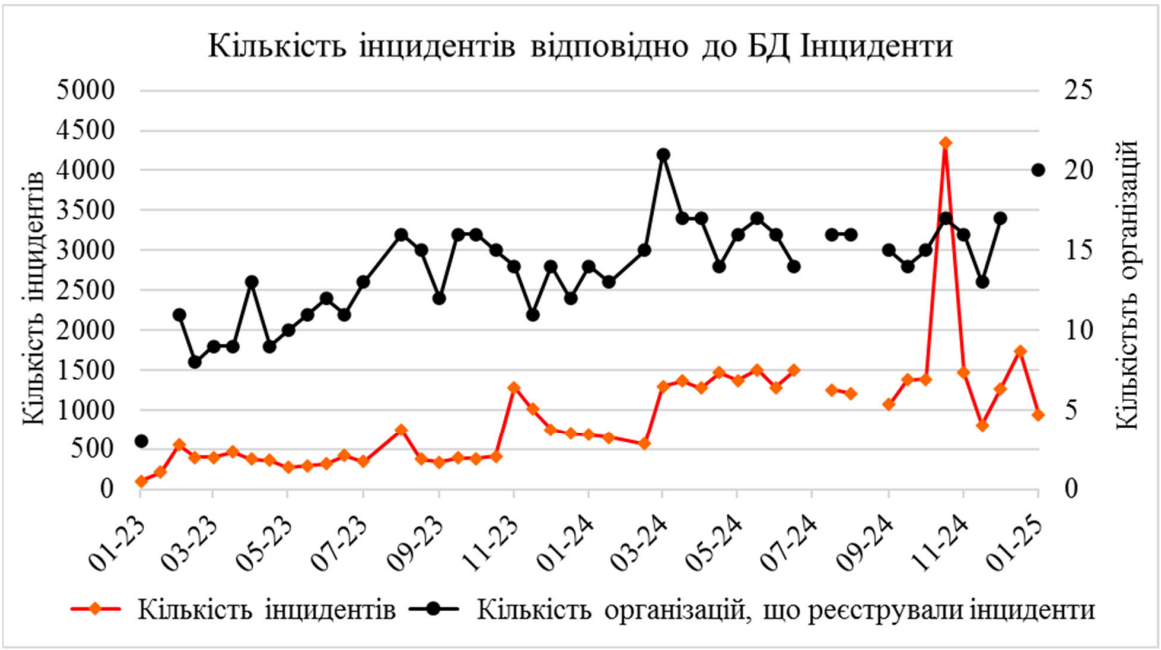

Рис. 5. Кількість інцидентів та кількість організацій, що реєстрували інциденти, в БД Інциденти

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [23; 24]

машинного навчання та мережевого аналізу стає невід'ємною частиною сучасних систем фінансової безпеки. Показовим є кейс одного з українських банків – ПУМБ, який інтегрував в процес фінансового моніторингу методи машинного навчання, що дозволило покращити процес та позбутися недоліків та затримок (серед яких ручний аналіз вибірок

та звітів, неможливість ефективно обробляти вручну мільйони клієнтів та транзакцій, відсутність можливості оперативно відслідковувати тенденцію «ускладнення» ризикових клієнтів) [27]. Алгоритми машинного навчання дозволяють на основі великих масивів транзакційних даних виявляти аномалії та прогнозувати ризикові операції ще до того, як вони призведуть до фінансових втрат. Графова аналітика дає змогу ідентифікувати шахрайські мережі, відслідковуючи зв'язки між учасниками схем на основі їхніх фінансових операцій. Це дозволяє не лише блокувати окремі підозрілі транзакції, а й виявляти ключові вузли в шахрайських схемах, що суттєво ускладнює діяльність злочинних груп. Інтеграція таких технологій банками України допоможе суттєво знизити рівень шахрайства та підвищити загальний рівень фінансової безпеки.

Висновки. Таким чином, паралельно з поширенням безготівкових розрахунків та діджиталізацією економіки відбувається і збільшення кількості шахрайських операцій. Активне використання шахраями сучасних технологій та залучення великої кількості клієнтів банків у якості посередників суттєво ускладнює боротьбу з ними, особливо якщо йдеться про раннє виявлення. Враховуючи можливість одночасного використання шахраями різних банків для створення розгалуджених мереж, надзвичайно важливим є питання міжбанківської взаємодії та взаємодії з регулятором. Окрім того, важливою є просвітницька робота (як з боку регулятора, так і з боку міжбанківської асоціації та окремих банків) з клієнтами, адже соціальна інженерія залишається найбільш поширеним методом шахрайства. Перспективним напрямом подальших досліджень вважаємо перевірку доцільності використання методів машинного навчання та мережевого аналізу для попередження та виявлення сучасних методів шахрайства, зокрема мереж розгалуджених мереж «дропів», та аналіз міжнародного досвіду боротьби з «грошовими мулами».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Рисін В. В, Карпець А. Р. Особливості новітніх способів відмивання грошей з використанням фінансових установ. *Бізнес Інформ*. 2021. № 3. С. 132–140. DOI: https://doi.org/10.32983/2222-4459-2021-3-132-140

2. Рисін В. В., Корначук О. Ю. Ризики залучення банків до схем відмивання грошей. *Ефективна економіка.* 2020. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=7853 (дата звернення: 20.01.2025). DOI: https://doi.org/10.32702/2307-2105-2020.5.2

3. Вишивана Б. М., Козак Д. А. Платіжне шахрайство в Україні: види та методи боротьби. *Грааль науки.* 2021. № 9. С. 72–76. DOI: https://doi.org/10.36074/grail-of-science.22.10.2021.10

4. Чуницька І. І. Заходи запобігання фінансовому шахрайству та легалізації коштів, зароблених злочинним шляхом. *Проблеми економіки.* 2017. № 2. С. 282–291.

5. Маршук Л. М., Складанюк М. С. Фінансове шахрайство з банківськими рахунками в Україні. *Економіка та суспільство.* 2021. № 32. URL: https://economyandsociety.in.ua/index.php/journal/article/view/797/764 (дата звернення: 22.01.2025). DOI: https://doi.org/10.32782/2524-0072/2021-32-55

6. Васильченко З. М., Пилипенко А. М. Аналіз ринку платіжних карток та платіжної інфраструктури. *Економіка та суспільство.* 2022. № 37. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1181/1138 (дата звернення: 22.01.2025). DOI: https://doi.org/10.32782/2524-0072/2022-37-8

7. Сизоненко В. Ю., Кисельов А. О. Особливості протидії підрозділами Національної поліції України шахрайству за допомогою громадськості. *Universum.* 2024. № 13. С. 89–96.

8. EBA Opinion on new types of payment fraud and possible mitigants. URL: https://surl.li/jyfddi (дата звернення: 23.01.2025).

9. 2023 Payment threats and European Payments Council (EPC) fraud trends report. URL: https://surl.li/sbfflv (дата звернення: 23.01.2025).

10. Fraud risks in fast payments. International Bank for Reconstruction and Development. URL: https://surl.li/lrildt (дата звернення: 23.01.2025).

11. Дані у розрізі учасників платіжних систем щодо кількості платіжних карток та інфраструктури їх обслуговування на 01.12.2024. НБУ. URL: https://bank.gov.ua/ua/payments (дата звернення: 26.01.2025).

12. Стартувала інформаційна кампанія #ШахрайГудбай: нагадуємо про важливі правила платіжної безпеки. НБУ. URL: https://bank.gov.ua/ua/news/all/startuvala-informatsiyna-kampaniya-shahraygudbay-nagaduyemo-pro-vajlivi-pravila-platijnoyi-bezpeki (дата звернення: 28.01.2025).

13. Підсумки платіжного та банкоматного шахрайства у 2021 році в Україні. Ukraine Media Center. URL: https://surl.li/ncdwpn (дата звернення: 28.01.2025).

14. Тимчасовий ліміт на суму переказів з "карти на карту" запобігатиме використанню платіжної інфраструктури в протиправних цілях. НБУ. URL: https://bank.gov.ua/ua/news/all/timchasoviy-limit-na-sumu-perekaziv-z-karti-na-kartu-zapobigatime-vikoristannyu-platijnoyi-infrastrukturi-v-protipravnih-tsilyah-ta-ne-vpline-na-diyalnist-volonteriv (дата звернення: 29.01.2025).

15. Підсумки платіжного шахрайства у 2023 році в Україні. Ukraine Media Center. URL: https://surl.li/crntdj (дата звернення: 01.02.2025).

16. З метою зниження ризиків шахрайства надавачі платіжних послуг застосуватимуть посилену автентифікацію. НБУ. URL: https://bank.gov.ua/ua/news/all/z-metoyu-znijennya-rizikiv-shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500 (дата звернення: 02.02.2025).

17. Стартував проєкт із протидії кібершахрайству у фінансовому секторі. НБУ. URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori (дата звернення: 02.02.2025).

18. Стартує Всеукраїнська інформаційна кампанія з платіжної безпеки #КібербезпекаФінансів. НБУ. URL: https://bank.gov.ua/ua/news/all/startuye-vseukrayinska-informatsiyna-kampaniya-z-platijnoyi-bezpeki-kiberbezpekafinansiv (дата звернення: 02.02.2025).

19. Українські банки за координації банківських асоціацій підписали Меморандум про забезпечення прозорості функціонування ринку платіжних послуг. НБУ. URL: https://bank.gov.ua/ua/news/all/ukrayinski-banki-za-koordinatsiyi-bankivskih-asotsiatsiy-pidpisali-memorandum-pro-zabezpechennya-prozorosti-funktsionuvannya-rinku-platijnih-poslug (дата звернення: 03.02.2025).

20. Проєкти ЄМА. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/about/projects/ (дата звернення: 05.02.2025).

21. BlackList ЕМА. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/citizens/blacklist/ (дата звернення: 05.02.2025).

22. Cardholder Verification. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/business/antifraud-hub/cardholder-verification/ (дата звернення: 05.02.2025).

23. Новини платіжного ринку від ЄМА. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/news/ (дата звернення: 10.02.2025).

24. Дайджест новин ЄМА – 2023 рік. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/news/27621/ (дата звернення: 13.02.2025).

25. Fraud Payments Tracker. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/business/antifraud-hub/fraud-payments-tracker/ (дата звернення: 13.02.2025).

26. БД Інциденти. Українська міжбанківська асоціація членів платіжних систем ЄМА. URL: https://www.ema.com.ua/about/projects/bd-incidenty/ (дата звернення: 15.02.2025).

27. Data Science на сторожі закону: як ми автоматизували фінансовий моніторинг в ПУМБ. DOU. URL: https://dou.ua/forums/topic/34631/ (дата звернення: 20.02.2025).

REFERENCES:

1. Rysin V. V., Karpets A. R. (2021) Osoblyvosti novitnikh sposobiv vidmyvannya groshei z vykorystannyam finansovykh ustanov [Features of the latest money laundering methods using financial institutions]. *Biznes Inform*, no. 3, pp. 132–140. DOI: https://doi.org/10.32983/2222-4459-2021-3-132-140

2. Rysin V. V., Kornachuk O. Y. (2020) Ryzyky zaluchennya bankiv do skhem vidmyvannya groshei [Risks of banks' involvement in money laundering schemes]. *Efektyvna ekonomika*, no. 5. Available at: http://www.economy.nayka.com.ua/?op=1&z=7853 (accessed January 20, 2025). DOI: https://doi.org/10.32702/2307-2105-2020.5.2

3. Vyshyvana B. M., Kozak D. A. (2021) Platyzhne shakhraistvo v Ukraini: vydy ta metody borotby [Payment fraud in Ukraine: types and methods of counteraction]. *Graal nauky*, no. 9, pp. 72–76. DOI: https://doi.org/10.36074/grail-of-science.22.10.2021.10

4. Chunytska I. I. (2017) Zakhody zapobihannya finansovomu shakhraistvu ta lehalizatsii koshtiv, zaroblenykh zlochynnym shlyakhom [Measures to prevent financial fraud and money laundering]. *Problemy ekonomiky*, no. 2, pp. 282–291.

5. Marshuk L. M., Skladanyuk M. S. (2021) Finansove shakhraistvo z bankivskymy rakhunkamy v Ukraini [Financial fraud with bank accounts in Ukraine]. *Ekonomika ta suspilstvo*, no. 32. Available at: https://economyandsociety.in.ua/index.php/journal/article/view/797/764 (accessed January 22, 2025). DOI: https://doi.org/10.32782/2524-0072/2021-32-55

6. Vasylchenko Z. M., Pylypenko A. M. (2022) Analiz rynku platyzhnykh kartok ta platyzhnoi infrastruktury [Analysis of the payment card market and payment infrastructure]. *Ekonomika ta suspilstvo*, no. 37. Available at:

https://economyandsociety.in.ua/index.php/journal/article/view/1181/1138 (accessed January 22, 2025). DOI: https://doi.org/10.32782/2524-0072/2022-37-8

7. Sysonenko V. Yu., Kyseliov A. O. (2024) Osoblyvosti protydii pidrozdilamy Natsionalnoi politsii Ukrainy shakhraistvu za dopomohoiu hromadskosti [Peculiarities of counteracting fraud by the National Police of Ukraine with public assistance]. *Universum*, no. 13, pp. 89–96.

8. EBA Opinion on new types of payment fraud and possible mitigants. Available at: https://surl.li/jyfddi (accessed January 23, 2025).

9. 2023 Payment threats and European Payments Council (EPC) fraud trends report. Available at: https://surl.li/sbfflv (accessed January 23, 2025).

10. Fraud risks in fast payments. International Bank for Reconstruction and Development. Available at: https://surl.li/lrildt (accessed January 23, 2025).

11. Dani u rozrizi uchasnykiv platyzhnykh system shchodo kilkosti platyzhnykh kartok ta infrastruktury yikh obsluhovuvannya na 01.12.2024 [Data on payment system participants regarding the number of payment cards and service infrastructure as of 01.12.2024]. NBU. Available at: https://bank.gov.ua/ua/payments (accessed January 26, 2025).

12. Startuvala informatsiina kampaniya #ShakhrayHudbay: nahaduemo pro vazhlyvi pravyla platyzhnoi bezpeky [The information campaign #ShakhrayHudbay has started: reminding about important payment security rules]. NBU. Available at: https://bank.gov.ua/ua/news/all/startuvala-informatsiyna-kampaniya-shahraygudbay-nagaduyemo-pro-vajlivi-pravila-platijnoyi-bezpeki (accessed January 28, 2025).

13. Pidsumky platyzhnoho ta bankomatnoho shakhraistva u 2021 rotsi v Ukraini [Summary of payment and ATM fraud in Ukraine in 2021].Ukraine Media Center. Available at: https://surl.li/ncdwpn (accessed January 28, 2025).

14. Tymchasovyi limit na sumu perekaziv z "karty na kartu" zapobigatyme vykorystannyu platyzhnoi infrastruktury v protypravnykh tsilyakh [The temporary limit on "card-to-card" transfers will prevent the misuse of payment infrastructure for illegal purposes]. NBU. Available at: https://bank.gov.ua/ua/news/all/timchasoviy-limit-na-sumu-perekaziv-z-karti-na-kartu-zapobigatime-vikoristannyu-platijnoyi-infrastrukturi-v-protipravnih-tsilyah-ta-ne-vpline-na-diyalnist-volonteriv (accessed January 29, 2025).

15. Pidsumky platyzhnoho shakhraistva u 2023 rotsi v Ukraini [Summary of payment fraud in Ukraine in 2023]. Ukraine Media Center. Available at: https://surl.li/crntdj (accessed February 1, 2025).

16. Z metoyu znyzhennya ryzykiv shakhraistva nadavachi platyzhnykh posluh zastosuvatymut posylenu avtentyfikatsiyu [To reduce fraud risks, payment service providers will apply strong authentication]. NBU. Available at: https://bank.gov.ua/ua/news/all/z-metoyu-znijennya-rizikiv-shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500 (accessed February 2, 2025).

17. Startuvav proiekt iz protydii kibershakhraistvu u finansovomu sektori [A project to combat cyber fraud in the financial sector has been launched]. NBU. Available at: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori (accessed February 2, 2025).

18. Startuie Vseukrainska informatsiina kampaniya z platyzhnoi bezpeky #KiberbezpekaFinansiv [The nationwide information campaign on payment security #CyberSecurityFinance is launching]. NBU. Available at: https://bank.gov.ua/ua/news/all/startuye-vseukrayinska-informatsiyna-kampaniya-z-platijnoyi-bezpeki-kiberbezpekafinansiv (accessed February 2, 2025).

19. Ukrayinski banky za koordynatsii bankivskykh asotsiatsii pidpysaly Memorandum pro zabezpechennya prozorosti funktsionuvannya rynku platyzhnykh posluh [Ukrainian banks, coordinated by banking associations, signed a Memorandum on ensuring transparency in the functioning of the payment services market]. NBU. Available at: https://bank.gov.ua/ua/news/all/ukrayinski-banki-za-koordinatsiyi-bankivskih-asotsiatsiy-pidpisali-memorandum-pro-zabezpechennya-prozorosti-funktsionuvannya-rinku-platijnih-poslug (accessed February 3, 2025).

20. Proiekty YEMA [EMA Projects]. Ukrainian Interbank Payment Systems Member Association "EMA". Available at: https://www.ema.com.ua/about/projects/ (accessed February 5, 2025).

21. BlackList EMA. Ukrainian Interbank Payment Systems Member Association "EMA". Available at: https://www.ema.com.ua/citizens/blacklist/ (accessed February 5, 2025).

22. Cardholder Verification. Ukrainian Interbank Payment Systems Member Association "EMA". Available at: https://www.ema.com.ua/business/antifraud-hub/cardholder-verification/ (accessed February 5, 2025).

23. Novyny platyzhnoho rynku vid YEMA [Payment market news from EMA]. Ukrainian Interbank Payment Systems Member Association "EMA". Available at: https://www.ema.com.ua/news/ (accessed February 10, 2025).

24. Daidzhest novyn YEMA – 2023 rik [EMA News Digest – 2023]. Ukrainian Interbank Payment Systems Member Association "EMA". Available at: https://www.ema.com.ua/news/27621/ (accessed February 13, 2025).