

Отже, застосування об'єктно-орієнтованого підходу до проєктування архітектури взаємодії з LLM надає можливість трансформувати лінійні процедурні виклики у високорівневу систему з багаторівневою оптимізацією. Завдяки впровадженню інтелектуальних шарів кешування та менеджменту контексту, стає можливим не лише суттєво знизити експлуатаційні витрати, а й забезпечити цілісність даних та стійкість системи до зовнішніх затримок. Також слід зазначити, що запропонована модель створює фундамент для автономного накопичення валідованих даних, що дозволяє працювати над покращенням якості відповідей у динамічному форматі, вказуючи на те, що такий метод може бути використаний як для негайного масштабування стартап-проєктів, так і для стратегічного переходу до використання локальних спеціалізованих моделей.

Список використаних джерел

1. Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1994). *Design patterns: Elements of reusable object-oriented software*. Addison-Wesley.
2. Pinecone Systems. (2024). *Semantic search and vector databases: A guide to latency optimization*. <https://www.pinecone.io/learn/>
3. Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M.-A., Lacroix, T., Rozière, B., Goyal, N., Hambro, E., Azhar, F., Rodriguez, A., Joulin, A., Grave, E., & Lample, G. (2023). *LLaMA: Open and efficient foundation language models*. arXiv. <https://arxiv.org/abs/2302.13971>

Будник М.О.,
здобувачка першого (бакалаврського) рівня вищої освіти,
Чугаєва О.В.,
старший викладач,
Київський національний економічний університет імені Вадима Гетьмана

БУЛЕВІ ФУНКЦІЇ ТА ЛОГІЧНІ МАТРИЦІ У СИСТЕМАХ АВТОМАТИЧНОГО ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ

Аналізуючи підсумкові дані НБУ за 2025 рік, можна зробити висновок, що обсяг безготівкових операцій в Україні становив 9 083,5 млн. на суму 4 684,3 млрд. грн, показавши зростання на 11% та 10,4% відповідно. Безготівковий сегмент охопив 95,5% від загальної кількості всіх карткових транзакцій, зокрема розрахунки в інтернеті перевищили 1,2 млрд операцій на суму майже 770 млрд. грн. Проте маємо зворотний бік такої цифровізації — збільшення кількості кібератак та фінансового шахрайства, що зумовлює необхідність розробки та впровадження автоматизованих систем захисту електронних переказів. [1]

Дослідження актуальних фінансових ризиків фіксує зміну стратегії кіберзлочинців, які компенсують кількісне зменшення атак вищим рівнем їхньої успішності. За підсумками 2025 року загальна кількість шахрайських операцій з платіжними картками в Україні знизилася на 5% до 256 тис. випадків, проте сумарні фінансові втрати громадян зросли на 24%, досягнувши 1,4 млрд грн. Головним чинником такої динаміки стало збільшення середнього чека однієї

незаконної транзакції на 30% – з 4 247 грн до 5 536 грн. [2] Водночас повномасштабна збройна агресія з боку РФ призвела до суттєвого зростання попиту на соціальну допомогу та гуманітарні товари, що стало підґрунтям для активізації кіберзлочинців, які адаптують свої методи під воєнні реалії. Абсолютна більшість таких правопорушень реалізується у цифровому середовищі через механізми соціальної інженерії та фішингу, які є ключовими інструментами атак у цифровому середовищі [3].

Висока активізація фінансової діяльності в інтернеті зумовлює рух величезних потоків конфіденційних даних каналами зв'язку, що провокує появу нових глобальних схем кібератак. Процес протидії шахрайству в електронному банкінгу є безперервним процесом: спочатку зловмисники створюють нові типи атак, а вже потім банки розробляють інструменти для боротьби з ними. Головним недоліком класичних методів захисту є те, що вони діють із запізненням. Поки банківська система аналізує нову загрозу, шахраї встигають викрасти кошти, оскільки традиційна перевірка операцій забирає забагато часу. Організація миттєвого автоматизованого контролю ускладнюється ще й тим, що реальна статистика кібератак є закритою для зовнішнього світу. Це актуалізує пошук нових теоретичних і математичних підходів до розробки систем швидкого реагування. [4]

Оскільки традиційні системи захисту запізнюються і не встигають за швидкістю нових шахрайських схем, то актуальним науково-практичним завданням є розробка алгоритмів миттєвої верифікації транзакцій. Для цього доцільно застосувати апарат дискретної математики, зокрема булеві функції та логічні матриці. Запропонований підхід дозволяє формалізувати параметри операції (наприклад, нетипову суму платежу, новий пристрій, тощо) у вигляді булевих змінних, де «1» позначає наявність ризику, а «0» – його відсутність. Логічні матриці (таблиці істинності) обробляються процесором паралельно за долі мілісекунди [4]. Водночас закони мінімізації булевих функцій дозволяють максимально спростити правила перевірки та прибрати зайві кроки. Це гарантує миттєве прийняття чіткого бінарного рішення (дозвіл або блокування платежу) в режимі реального часу, запобігаючи втраті коштів до моменту їх списання.

Об'єктом дослідження є процес автоматизованого моніторингу та виявлення шахрайських транзакцій у сучасних електронних платіжних системах.

Предметом дослідження є математичні моделі, алгоритми та методи швидкої перевірки операцій, побудовані на основі апарату булевих функцій та логічних матриць ризиків.

Для прийняття рішень у системах антифрод-моніторингу використовується n -місна булева (логічна) функція $y = f(x_1, x_2, \dots, x_n)$, де аргументи x_i ($i = 1, \dots, n$) і значення функції y , набувають значень з множини $B = \{0, 1\}$. Якщо обчислене значення $y = 0$, то транзакція вважається законною і система дозволяє її проведення; тоді як результат $y = 1$ вказує на виявлення шахрайства та ініціює автоматичне блокування платежу.

Вхідні змінні x_i описують параметри платежу. Кожна ознака потенційного шахрайства (зміна пристрою, нічний час проведення операції, нетиповий обсяг коштів, тощо) формалізується у вигляді двійкової змінної. Значення $x_i = 0$ означає відсутність загрози, а $x_i = 1$ – фіксує наявність підозрілого фактору. [6]

Математичною основою обробки таких матриць є апарат булевої алгебри [7]. Процес перевірки безпекових правил базується на використанні логічних операцій – кон'юнкції (I), диз'юнкції (АБО) та заперечення (Не). Це дозволяє подати складні критерії перевірки чітких бінарних кодів.

Завдяки представленню правил безпеки у вигляді матриць стає можливою їх паралельна обробка на апаратному рівні. Замість послідовної перевірки процесор виконує групові побітові операції над векторами даних, що забезпечує ухвалення рішення за долі мілісекунди. [4]

Основою для побудови системи моніторингу стала класифікація ризиків, представлена на Рис.1. Серед наведених видів для онлайн-операцій найбільш критичними є шахрайство, пов'язане з крадіжкою (зокрема, компрометація даних та дистанційне використання реквізитів), а також поведінковий обман (соціальна інженерія).



Рис. 1. Види шахрайства

Джерело: розраховано авторами на основі [5]

На основі цих видів виокремлено три ознаки ризику та формалізовано їх у логічні змінні:

- x_1 — пристрій/геолокація (0 — звичний, 1 — новий);
- x_2 — час операції (0 — день, 1 — ніч);
- x_3 — сума переказу (0 — стандартна, 1 — нетипова).

Вихідна функція y визначає рішення системи: $y = 0$ — дозволити платіж, $y = 1$ — заблокувати операцію через фрод.

Матриця ризиків (таблиця істинності) будується для правила, згідно з яким рішення про блокування ($y = 1$) ухвалюється за наявності хоча б двох будь-яких підозрілих ознак:

Таблиця 1

Матриця ризиків

№	x_1	x_2	x_3	y	Конституенти 1
0	0	0	0	0	
1	0	0	1	0	
2	0	1	0	0	
3	0	1	1	1	$\bar{x}_1 \wedge x_2 \wedge x_3$
4	1	0	0	0	
5	1	0	1	1	$x_1 \wedge \bar{x}_2 \wedge x_3$
6	1	1	0	1	$x_1 \wedge x_2 \wedge \bar{x}_3$
7	1	1	1	1	$x_1 \wedge x_2 \wedge x_3$

Джерело: розраховано авторами

На основі комбінацій вхідних змінних, за яких транзакція підлягає обов'язковому блокуванню ($y = 1$) формуються відповідні конституенти одиниці та записується досконала диз'юнктивна нормальна форма (ДДНФ), що об'єднує визначені логічні добутки операцією диз'юнкції. Проте варто враховувати, що безпосередній програмний розрахунок повної форми ДДНФ створює додаткове обчислювальне навантаження. Для забезпечення максимальної швидкодії системи та ухвалення рішення за частки мілісекунди проводиться мінімізація отриманої функції на основі законів булевої алгебри.

ДДНФ:

$$\begin{aligned} y &= (\bar{x}_1 x_2 x_3) \vee (x_1 \bar{x}_2 x_3) \vee (x_1 x_2 \bar{x}_3) \vee (x_1 x_2 x_3) \equiv ((\bar{x}_1 x_2 x_3) \vee (x_1 x_2 x_3)) \vee \\ &((x_1 \bar{x}_2 x_3) \vee (x_1 x_2 x_3)) \vee ((x_1 x_2 \bar{x}_3) \vee (x_1 x_2 x_3)) \equiv (x_2 x_3)(\bar{x}_1 \vee x_1) \vee (x_1 x_3)(\bar{x}_2 \vee x_2) \vee \\ &(x_1 x_2)(\bar{x}_3 \vee x_3) \equiv (x_2 x_3) \vee (x_1 x_3) \vee (x_1 x_2), \end{aligned}$$

Отримана логічна функція значно спрощує алгоритм антифрод-перевірки: транзакція блокується, якщо виконується хоча б одна пара ризикованих умов.

Процес перевірки зводиться до обчислення спрощеного виразу

$$y = (x_2 x_3) \vee (x_1 x_3) \vee (x_1 x_2)$$

на основі вхідного вектора ознак.

Замість складного послідовного перебору умов, програма виконує прямі побітові операції на рівні процесора. Оскільки обчислення відбуваються лінійно і потребують лише трьох операцій кон'юнкції та двох диз'юнкцій, алгоритм працює з мінімальним залученням пам'яті, що максимально прискорює антифрод-моніторинг.

Емпірична оцінка розробленого матричного алгоритму показує його високу ефективність за двома ключовими критеріями:

1) Швидкість обчислень: Завдяки переходу від символьних обчислень до паралельної обробки булевих матриць, швидкість роботи системи зростає на 1–4 порядки порівняно зі стандартними підходами. Це дозволяє здійснювати повноцінний моніторинг інтенсивних потоків транзакцій у режимі реального часу без відчутних затримок для клієнтів.

2) Точність реагування: Чітка математична логіка унеможливорює суб'єктивні помилки під час ухвалення рішень. Система безпомилково блокує операції лише за наявності критичного збігу факторів ризику, мінімізуючи відсоток помилкових спрацювань.

Список використаних джерел

1. Національний банк України. (2026, 16 лютого). Операції з платіжними картками у 2025 році: Більшість – безготівкові. <https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist-bezgotivkovi>
2. Національний банк України. (2026, 17 квітня). Шахрайство з платіжними картками у 2025 році: Кількість випадків знизилася, сума збитків – зросла. <https://bank.gov.ua/ua/news/all/shahraystvo-z-platijnimi-kartkami-u-2025-rotsi-kilkist-vipadkiv-znizilasya-suma-zbitkiv-zroslo>
3. Департамент кіберполіції Національної поліції України. (2026, 16 лютого). Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік. <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/>
4. Леонов, С. В., Кузьменко, О. В., & Яровенко, Г. М. (2018). Сучасні інструменти боротьби з кібершахрайствами у банках: Монографія (за заг. ред. О. В. Кузьменко, Г. М. Яровенко). Суми: Ярославна. <https://essuir.sumdu.edu.ua/server/api/core/bitstreams/84c3a8fd-6733-439d-92dc-5463b7d27c4b/content>
5. Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, 4(2), 57–68.
6. Темнікова, О. Л. (2019). Дискретна математика: Конспект лекцій (Частина 2): Навч. посіб. Київ: КПІ ім. Ігоря Сікорського.