DOI: https://doi.org/10.32782/2524-0072/2026-84-101

УДК 004.8:004.056:338.5

НЕЙРОМЕРЕЖЕВІ ТЕХНОЛОГІЇ ЯК КЛЮЧОВИЙ ФАКТОР ПРОГНОЗУВАННЯ ФІНАНСОВИХ ВТРАТ ВІД КІБЕРЗАГРОЗ

NEURAL NETWORK TECHNOLOGIES AS A KEY DETERMINANT OF FORECASTING ACCURACY OF FINANCIAL LOSSES FROM CYBER THREATS

Бойко Антон Олександрович
доктор економічних наук, професор,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-1784-9364

Кушнерьов Олександр Сергійович
доктор філософії,
Сумський державний університет
ORCID: https://orcid.org/0000-0001-8253-5698

Ліхолєтов Дмитро Олександрович
аспірант,
Сумський державний університет
ORCID: https://orcid.org/0009-0004-4872-5868

Boiko Anton, Kushnerov Oleksandr, Likholietov Dmytro
Sumy State University

Стаття присвячена дослідженню нейромережевих технологій як ключового фактору прогнозування фінансових втрат від кіберзагроз в умовах цифровізації та гібридної агресії проти України. Обґрунтовано обмеженість традиційних методів прогнозування через їхню неспроможність враховувати нелінійність і динамічність кіберсередовища. Проаналізовано вплив розвитку архітектур нейронних мереж, зокрема LSTM та Transformer, а також якості даних, обчислювальних ресурсів і експертизи на точність прогнозів. Визначено, що нейромережі забезпечують виявлення прихованих закономірностей та підвищують ефективність оцінки фінансових втрат. Доведено необхідність комплексного підходу до впровадження таких технологій в Україні.

Ключові слова: прогнозування, нейромержі, фінансові втрати, кіберзагрози, стійкість, штучний інтелект, цифровізація.

The article examines the key factors determining the accuracy of forecasting financial losses from cyber threats using neural network technologies. In the context of rapid digitalization and ongoing hybrid aggression against Ukraine, the problem of reliable assessment and forecasting of financial losses has gained strategic importance for national security. The study aims to provide a comprehensive analysis of how the evolution of neural network architectures, data availability and quality, computational resources, and domain expertise influence the performance and reliability of predictive models. The research is based on the analysis of scientific literature and official CERT-UA reports for 2021-2024, which highlight the limitations of traditional forecasting approaches. A theoretical and methodological framework is employed to identify the relationships between key factors affecting forecasting accuracy. The findings indicate that predictive performance is driven by the synergy of three core components: data quality and volume, computational capacity, and expert knowledge. It is demonstrated that modern neural network architectures, including LSTM and Transformer models, significantly outperform traditional methods in capturing nonlinear dependencies and latent patterns. The study substantiates that the effective implementation of neural network-based forecasting systems in Ukraine requires a comprehensive approach, including the development of a national data infrastructure, investment in high-performance computing, and the advancement of specialized expertise. The proposed recommendations take into account the specific threat landscape and structural characteristics of the Ukrainian economy. Enhancing model transparency and interpretability, as well as strengthening international cooperation, are identified as critical prerequisites for increasing trust in forecasting results and their practical application.

Keywords: forecasting, neural networks, financial losses, cyber threats, resilience, artificial intelligence, digitalization.

Постановка проблеми. Стрімка цифрова трансформація сучасного суспільного життя та економічної діяльності суб'єктів господарювання, попри беззаперечні переваги, несе в собі й суттєві ризики, серед яких дедалі загрозливіших масштабів набувають кібератаки, які призводять до значних фінансових втрат. Глобальна економіка щороку зазнає колосальних фінансових збитків від зловмисної діяльності у кіберпросторі, і за деякими прогнозами, в 2025 року ці втрати сягнули 10,5 трильйонів доларів США [1], а в 2026 році можуть збільшитись ще на 10-15% від значення попереднього року. Ця цифра, регулярно оновлюється провідними аналітичними центрами, та відображає не лише прямі фінансові втрати, але й значно ширший спектр економічних наслідків, які важко піддаються точній кількісній оцінці [2]. Для України, яка вже понад десятиліття перебуває в стані гібридної війни, невід'ємною складовою якої є цілеспрямована та систематична агресія в кіберпросторі, ця проблема стоїть особливо гостро та набуває рис екзистенційної загрози для стабільності держави та фінансової стійкості економічних агентів [3]. Національна система кібербезпеки, зокрема Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України та його Оперативний центр реагування на кіберінциденти, відомий як CERT-UA, щоденно фіксує та опрацьовує величезну кількість кіберзагроз та кіберінцидентів, спрямованих на державні органи, об'єкти критичної інфраструктури, фінансовий сектор, оборонні підприємства та інші важливі елементи національної економіки [3].

Звіти CERT-UA за останні роки яскраво ілюструють цю невпинну ескалацію та адаптацію загроз [3]. Ця зростаюча статистика, що відображає лише верхівку айсберга реальної активності у кіберпросторі, підкреслює нагальну потребу в ефективних інструментах прогнозування потенційних фінансових втрат як окремо для кожного суб'єкта господарювання, так і для економіки вцілому. Такі прогнози необхідні для стратегічного планування заходів кіберзахисту, адекватного розподілу ресурсів та формування національної політики кіберстійкості. Проте саме прогнозування є надзвичайно складним завданням, адже кібератаки, як зазначає CERT-UA, стають дедалі складнішими, зловмисники використовують легітимні сервіси та інструменти для маскування своєї діяльності, що значно ускладнює їх своєчасне виявлення та ефективну нейтралізацію [3].

У цьому багатогранному та динамічному контексті технології штучного інтелекту, зокрема різні архітектури нейронних мереж, розглядаються світовою спільнотою як один із найперспективніших інструментів, здатних якісно покращити аналіз великих масивів даних, виявляти складні та неочевидні закономірності, а отже, і прогнозувати комплексні економічні явища, пов'язані з кіберзагрозами [4; 5]. Однак, ефективність такого прогнозування, його точність, надійність та, зрештою, практична придатність для прийняття управлінських рішень залежать від поточного рівня розвитку самих нейромережевих технологій. Розуміння цих складних взаємозв'язків та існуючих обмежень є критично важливим для розробки адекватних національних стратегій кібербезпеки [6], формування науково обґрунтованої політики у сфері розвитку та застосування штучного інтелекту, а також для прийняття зважених рішень щодо інвестицій у захисні технології та наукові дослідження, особливо для країн, що, подібно до України, перебувають на вістрі глобальної боротьби з кібератрегресією та потребують інноваційних підходів для забезпечення своєї фінансової стійкості.

Аналіз останніх досліджень і публікацій. Сучасні дослідження проблеми прогнозування фінансових втрат від кіберзагроз формуються на перетині трьох наукових напрямів: кібербезпеки, фінансової аналітики та штучного інтелекту. Аналіз існуючих наукових публікацій дозволяє виокремити певні напрямки сучасних досліджень. Так, вітчизняні наукові роботи, присвячені в своїй більшості, аналізу кіберризиків та забезпеченню кіберстійкості фінансового сектору. Зокрема, у роботах В. Боженка, О. Пахненка, Г. Яровенка та В. Койбічука [7] обґрунтовано застосування інструментів аналізу даних для оцінювання кіберризиків у фінансових послугах, що створює підґрунтя для подальшого розвитку прогнозних моделей. Дослідження І. Гончаренка [8] акцентує увагу на зростанні кіберзагроз у фінансовому секторі в умовах війни, підкреслюючи їх системний вплив на економічну безпеку держави. Аналогічно, О. Криклій [9] та Н. Трусова з І. Чканом [10] розглядають питання кіберстійкості банківської системи, визначаючи її як ключовий елемент стабільності фінансової інфраструктури.

Окремий напрям становлять дослідження, присвячені моделюванню кіберризиків.

Так, С. Тищенко, О. Пархоменко та В. Дармосюк [11] застосовують методи математичної статистики та інструменти Python для аналізу ризиків кібератак, що свідчить про активне впровадження кількісних підходів у цій сфері. Водночас у роботі В. Фаріона та інші [12] доведено ефективність використання штучного інтелекту для прогнозування фінансових показників, що підтверджує потенціал адаптації таких методів до задач оцінювання втрат від кіберзагроз.

У міжнародних дослідженнях спостерігається більш глибока інтеграція методів машинного навчання у фінансову аналітику. Зокрема, роботи Д. Хоанг та К. Вігратц [13], а також Г. Джаваїд [14] демонструють широкі можливості застосування алгоритмів машинного навчання для оцінювання ризиків і підтримки фінансових рішень. Систематичний огляд С. Аль-Емарі, Й. Санджалаве, та А. Аль-Емарі [15] підтверджує, що штучний інтелект суттєво підвищує ефективність управління фінансовими процесами.

Особливу увагу в сучасній науці приділено нейромережевим підходам до прогнозування. Дослідження К. Сако, Б. Мпінда та П. Родрігес [16] доводить високу ефективність нейронних мереж у прогнозуванні фінансових часових рядів, зокрема завдяки їх здатності виявляти нелінійні залежності. Подальший розвиток цього напряму пов’язаний із використанням квантових обчислень: роботи О. Тіво [17], С. Таккар та інші [18], а також З. Сюй та інші [19] демонструють потенціал квантового машинного навчання у підвищенні точності прогнозів і стійкості до кіберзагроз.

Водночас дослідження О. Обіоха-Вал та інші [20] акцентує увагу на ризиках застосування штучного інтелекту в моделюванні кіберзагроз, зокрема на проблемах безпеки даних і можливих вразливостях самих моделей, що підкреслює необхідність комплексного підходу до їх використання.

Незважаючи на значну кількість наукових напрацювань, слід відзначити відсутність комплексних досліджень, спрямованих саме на прогнозування фінансових втрат від кіберзагроз із використанням нейромережевих технологій. Більшість існуючих робіт зосереджена або на оцінюванні кіберризиків, або на прогнозуванні фінансових показників без урахування специфіки кіберінцидентів.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість досліджень, присвячених кіберзагрозам та їх економічним наслідкам, проблема точного прогнозування фінансових втрат залишається недостатньо вирішеною, особливо в умовах високої динамічності та нелінійності кіберсередовища. Традиційні підходи до оцінювання збитків, що базуються на статистичних методах, експертних оцінках та ретроспективному аналізі, демонструють обмежену здатність враховувати складні взаємозв’язки між технічними характеристиками кібератак і їх фінансовими наслідками.

Ключовою невирішеною частиною проблеми є недостатній рівень інтеграції нейромережевих технологій у процеси прогнозування фінансових втрат від кіберзагроз. Хоча сучасні нейронні мережі мають доведену здатність ефективно працювати з великими обсягами різнорідних даних та виявляти приховані закономірності, їх потенціал у сфері прогнозування кіберризиків використовується фрагментарно та несистемно. Зокрема, відсутні комплексні моделі, що поєднують дані про кіберінциденти, фінансові втрати та макроекономічні показники в єдиній аналітичній системі.

Додатковою проблемою є обмеженість якісних і стандартизованих даних для навчання нейромережевих моделей. Недостатня репрезентативність інформації про реальні фінансові втрати, особливо непрямі, значно знижує точність прогнозів та стримує розвиток відповідних технологічних рішень. У випадку України ця проблема ускладнюється специфікою кіберзагроз, зумовлених гібридною війною, що формує унікальний та слабо формалізований масив даних.

Водночас залишається відкритим питання визначення того, якою мірою саме рівень розвитку нейромережевих технологій – включаючи архітектуру моделей, якість даних, обчислювальні ресурси та рівень підготовки фахівців – впливає на точність і надійність прогнозування фінансових втрат. Недостатньо досліджено також питання адаптації сучасних нейромережевих архітектур до специфіки задач прогнозування кіберризиків та їх економічних наслідків.

Окремою невирішеною проблемою є низький рівень інтерпретованості результатів нейромережевого моделювання, що обмежує їх використання у практиці прийняття управлінських рішень. Відсутність прозорих механізмів пояснення прогнозів знижує довіру до таких технологій з боку державних органів та бізнесу.

Таким чином, існує потреба у поглибленому дослідженні нейромережевих техноло-

гій як ключового фактору підвищення точності прогнозування фінансових втрат від кіберзагроз, а також у розробці комплексних підходів до їх ефективного впровадження в умовах сучасних безпекових викликів.

Мета статті: ідентифікація та теоретико-методичне обґрунтування ролі нейромережевих технологій як ключового фактору підвищення точності прогнозування фінансових втрат від кіберзагроз на основі аналізу впливу архітектур нейронних мереж, якості та репрезентативності даних, обчислювальних ресурсів і рівня експертного забезпечення на ефективність прогнозних моделей.

Виклад основного матеріалу дослідження. Кіберзагрози охоплюють надзвичайно широкий спектр деструктивних дій, що здійснюються у глобальному та національному кіберпросторі та спрямовані на порушення штатного функціонування економічних суб'єктів усіх форм власності, а також об'єктів критичної інфраструктури таких як енергетика, транспорт, зв'язок, фінанси, охорона здоров'я тощо. Згідно з переліком категорій кіберінцидентів, який було схвалено Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України та використовується CERT-UA для класифікації, основними категоріями є шкідливий вміст, що включає спам, і шкідливий програмний код, який охоплює зараження шкідливим програмним забезпеченням, його розповсюдження, активність командно-контрольних центрів та шкідливі підключення. До переліку також входять збір інформації зловмисником, що передбачає сканування мереж, сніфінг та фішинг, а також спроби втручання, такі як спроби експлуатації вразливостей та несанкціонованої авторизації. Інші категорії включають втручання, що означає компрометацію облікового запису або системи. Крім цього, виділяють порушення властивостей інформації як несанкціонований доступ до інформації та її модифікацію, шахрайство через шахрайські вебсайти. Завершує список категорія інше, до якої відносять невизначені інциденти [3].

Фінансові втрати від таких цілеспрямованих та масштабних кіберзагроз поділяються на прямі та непрямі [2]. Прямі збитки – це безпосередні, легко ідентифіковані фінансові збитки, що виникають як негайний наслідок кіберінциденту. До них належать витрати на технічне відновлення працездатності інформаційних систем та даних, закупівля нового серверного або мережевого обладнання, ліцензій на програмне забезпечення, оплата послуг зовнішніх IT-фахівців та консультантів з кібербезпеки. Втрачений дохід через вимушені простої в роботі підприємств та організацій, порушення ключових бізнес-процесів, наприклад, зупинка виробничих ліній, неможливість обробки замовлень чи надання онлайн-послуг, недоотриманий прибуток. Виплати викупів зловмисникам у разі успішних атак програм-вимагачів, хоча державні органи та більшість експертів не рекомендують цього робити, а також витрати на проведення розслідування інциденту, юридичні послуги, повідомлення клієнтів та регуляторних органів про витік даних, та можливі адміністративні штрафи за порушення законодавства про захист персональних даних чи інформаційної безпеки. У той же час, непрямі збитки, хоча їх значно складніше кількісно оцінити та часто важко безпосередньо пов'язати з конкретним кіберінцидентом, у довгостроковій перспективі можуть значно перевищувати прямі фінансові втрати і мати більш руйнівний вплив на економіку [21]. До цієї категорії належать репутаційні збитки та втрата довіри з боку громадян, клієнтів, ділових партнерів та потенційних інвесторів, що може призвести до відтоку клієнтської бази, зниження обсягів продажів та лояльності, втрати ринкової частки та значного ускладнення процесу залучення нового фінансування чи інвестицій. Також сюди відносяться втрата чутливої інформації, такої як інтелектуальна власність, комерційна таємниця, стратегічні плани розвитку, що може надати конкурентам нечесні переваги [2]. Крім того, масштабні кібератаки, особливо на об'єкти критичної інфраструктури, можуть мати серйозні соціальні наслідки, такі як порушення надання життєво важливих суспільних послуг, що може призвести до соціальної напруженості, паніки, а в екстремальних випадках – навіть до загрози здоров'ю та життю людей.

Зважаючи на потенційний обсяг фінансових втрат, які можуть бути заподіянні кіберзагрозами процес прогнозування набуває значної актуальності. У той же час, традиційні методи прогнозування фінансових втрат, що включають експертні оцінки, аналіз історичних даних та екстраполяцію трендів, регресійний аналіз та сценарний аналіз, хоча й мають свою певну цінність та застосовуються в різних сферах управління ризиками, демонструють суттєві обмеження при спробі їхнього застосування до такого динамічного, складного та часто нелінійного середовища, яким

є кіберзагрози та їхні економічні наслідки [4]. Експертні оцінки, хоч і можуть бути корисними для якісного аналізу та оцінки непрямих або репутаційних збитків, за своєю природою є суб'єктивними, залежать від кваліфікації та досвіду конкретних експертів, і їх складно формалізувати, масштабувати та використовувати для отримання послідовних та відтворюваних кількісних прогнозів. Аналіз історичних даних та екстраполяція виявлених трендів у майбутнє стикаються з фундаментальною проблемою швидкої та непередбачуваної еволюції кіберзагроз: постійно з'являються нові типи атак, нові вектори проникнення, змінюються тактики, техніки та процедури зловмисників, а також їхні інструменти та мотивації. Це означає, що минулі дані про інциденти та пов'язані з ними фінансові збитки можуть швидко втрачати свою релевантність для адекватного прогнозування майбутніх подій, особливо тих, що пов'язані з новими, раніше невідомими загрозами.

Регресійний аналіз, який намагається встановити статистично значущу залежність між розміром фінансових втрат та різними потенційними факторами впливу, тип атаки, уражена галузь, розмір компанії, рівень її захищеності тощо, часто спирається на припущення про лінійність цих взаємозв'язків, що рідко відповідає дійсності у випадку складних кібернетичних систем та їхніх економічних наслідків, які часто характеризуються нелінійними залежностями, пороговими ефектами та каскадними збоями. Крім того, побудова адекватної регресійної моделі потребує ідентифікації та включення всіх значущих змінних, що є складним завданням, а самі моделі можуть бути досить чутливими до «викидів» у даних, що може спотворювати оцінки коефіцієнтів та загальну прогнозну точність. Сценарний аналіз, хоч і є корисним інструментом для оцінки потенційних наслідків екстремальних сценаріїв кібератак та для стрес-тестування систем захисту, значною мірою залежить від суб'єктивного вибору цих сценаріїв, визначення їхніх ключових параметрів та експертної оцінки їхньої ймовірності реалізації, що також вносить значний елемент невизначеності та суб'єктивізму у прогнозні оцінки. Головними системними недоліками цих традиційних підходів є їхня обмежена здатність ефективно обробляти великі обсяги різнорідних, часто неструктурованих або «зашумлених» даних, текстові звіти про інциденти, дані з відкритих джерел розвідки загроз, інформацію з соціальних мереж чи форумів у даркнеті, адекватно враховувати складні нелінійні та динамічні взаємозв'язки між численними факторами, а також швидко адаптуватися до нових, раніше невідомих типів загроз.

На противагу традиційним методам, нейронні мережі, як один з ключових напрямків розвитку штучного інтелекту, пропонують значно більший потенціал та гнучкість для прогнозування фінансових втрат від кіберзагроз. Фундаментальна сила та відмінність цих методів полягає у здатності навчатися безпосередньо на великих обсягах даних, автоматично, без явного програмування конкретних правил чи залежностей, виявляючи складні, нелінійні та приховані закономірності, які можуть бути неочевидними для людського аналітика або занадто складними для точної формалізації у вигляді традиційних статистичних моделей [22]. Нейронні мережі здатні обробляти величезні обсяги різнорідних даних, включаючи структуровані числові часові ряди, категоріальні дані, неструктуровану текстову інформацію та навіть зображення чи відео, що дозволяє створювати більш комплексні, багатофакторні та інформативні прогнозні моделі. Важливою перевагою сучасних нейромережевих підходів є їхня адаптивність: після початкового навчання нейронні мережі можуть бути донавчені на нових даних, що постійно надходять, таким чином оновлюючи свої внутрішні представлення знань про загрози та їхні наслідки, і, відповідно, покращуючи точність своїх прогнозів у мінливому та динамічному середовищі кіберзагроз [23].

Серед усього різноманіття існуючих архітектур нейронних мереж, особливу увагу в контексті прогнозування фінансових наслідків кібератак та аналізу пов'язаних з ними часових рядів привертають ті, що спеціально розроблені для ефективної роботи з послідовними даними, де порядок елементів та часові залежності мають критичне значення. До таких архітектур насамперед належать рекурентні нейронні мережі та їхні більш просунуті та широко використовувані варіанти, такі як нейронні мережі довгої короткострокової пам'яті (LSTM) та вентильні рекурентні нейрони (GRU) [24]. Ці архітектури містять у своїй структурі зворотні зв'язки, що дозволяє їм зберігати інформацію про попередні стани послідовності та використовувати її для обробки поточних даних. Спеціальні механізми, такі як вентилі та комірки пам'яті, дозволяють цим мережам ефективно навчатися на довгих послідовностях та моделю-

вати довгострокові залежності, уникаючи класичних проблем простих рекурентних мереж, таких як швидке згасання або вибух градієнта під час навчання. Ця здатність «пам'ятати» важливу інформацію з минулих спостережень на тривалих часових проміжках є критично важливою для виявлення складних часових тенденцій у частоті, типах та серйозності кіберінцидентів, або для моделювання затяжних, відкладених та каскадних фінансових втрат від масштабних кібератак, які можуть проявлятися не одразу, а протягом кількох місяців або навіть років.

Останнім часом справжню революцію в багатьох галузях штучного інтелекту, включно з обробкою природної мови, комп'ютерним зором та аналізом складних часових рядів, здійснили моделі, засновані на архітектурі Transformer [25; 26]. Ключовою інновацією трансформерів є механізм уваги, зокрема його варіант під назвою само-увага, який дозволяє моделі динамічно оцінювати та зважувати важливість різних частин вхідної послідовності або навіть різних вхідних послідовностей при формуванні вихідного представлення або кінцевого прогнозу. Це дає змогу ефективно моделювати глобальні залежності між будь-якими, навіть дуже віддаленими один від одного елементами послідовності, що може бути проблематичним для традиційних рекурентних архітектур, які обробляють дані переважно послідовно. Крім того, архітектура трансформерів, на відміну від рекурентних мереж, значно краще піддається паралелізації обчислень під час навчання, що дозволяє ефективно тренувати дуже великі моделі з сотнями мільйонів або навіть мільярдами параметрів на величезних обсягах даних. У контексті прогнозування фінансових втрат від кіберзагроз, трансформери потенційно можуть одночасно аналізувати різні типи вхідних даних – наприклад, часові ряди детальної статистики кіберінцидентів включаючи технічні індикатори, макроекономічні показники країни та окремих галузей, неструктуровані текстові дані зі звітів про нові загрози та вразливості, новини про геополітичну ситуацію – виявляючи складні та неочевидні взаємозв'язки між ними та формуючи більш точні та обґрунтовані прогнози.

Існуючі дослідження в суміжних галузях неодноразово демонстрували практичну перевагу нейромережевих підходів над традиційними методами. Наприклад, деякі роботи вказують, що моделі на основі LSTM можуть знижувати середньоквадратичну помилку прогнозування на 84-87% порівняно з класичними статистичними моделями типу ARIMA при аналізі часових рядів, пов'язаних з частотою або характеристиками кібератак [24]. Моделі Transformer також демонструють надзвичайно високу точність у таких задачах, як класифікація мережевого трафіку, виявлення шкідливого програмного забезпечення або детектування аномальної активності, часто перевершуючи за показниками точності та повноти інші популярні архітектури, такі як згорткові нейронні мережі (CNN) або ті ж LSTM, особливо при роботі з великими та складними наборами даних [25].

Ключовим фактором, що визначає точність, надійність та, зрештою, практичну цінність прогнозів фінансових втрат від кіберзагроз, отриманих за допомогою нейронних мереж, є так званий «рівень розвитку нейромережевих технологій». Це не статична характеристика, а динамічний комплексний параметр, що охоплює декілька взаємопов'язаних та взаємозалежних складових, кожна з яких робить свій вирішальний внесок у кінцевий результат роботи прогнозної моделі.

По-перше, фундаментальне значення має досконаліть та адекватність архітектур нейронних мереж обраній задачі. Вибір оптимального рівня складності та адекватної архітектури, яка найкраще відповідає специфіці наявних даних та особливостям прогнозованого явища, є важливим дослідницьким завданням. Це може включати ретельне експериментування з різними конфігураціями існуючих архітектур, застосування методів регуляризації для запобігання перенавчанню, або навіть розробку нових гібридних моделей, що поєднують переваги різних підходів, наприклад, LSTM та Transformer [26], та їхню спеціалізовану адаптацію до специфіки економічних даних України та характеру кіберзагроз, що спостерігаються в країні [27].

По-друге, вирішальним фактором, від якого залежить успіх будь-якої моделі машинного навчання, є доступність, обсяг, якість та репрезентативність даних для навчання. Нейронні мережі, особливо глибокі та складні архітектури, є надзвичайно «голодними» до даних [23]. Для ефективного навчання, виявлення стійких та статистично значущих закономірностей, а також для уникнення перенавчання та забезпечення високої узагальнюючої здатності моделі, їм потрібні великі масиви релевантних, точних, повних та репрезентативних таких, що адекватно відо-

бражають всю сукупність можливих ситуацій та варіацій даних.

По-третє, невід'ємним компонентом рівня розвитку нейромережевих технологій є наявність відповідних обчислювальних ресурсів та ефективність використовуваних алгоритмів навчання та оптимізації. Окрім власне апаратного забезпечення, надзвичайно важливу роль відіграють ефективність самих алгоритмів навчання, методи оптимізації гіперпараметрів моделі, а також використання ефективних технік регуляризації, що дозволяють запобігати швидкому перенавчанню моделі, прискорювати процес її збіжності до оптимального рішення та покращувати її узагальнюючу здатність на нових даних [23].

По-четверте, неможливо переоцінити вирішальну роль кваліфікованих фахівців та нагальної проблеми інтерпретованості розроблених моделей. Навіть за наявності технічно досконалих та формально точних моделей, їхня практична цінність для прийняття обґрунтованих управлінських рішень може бути суттєво обмежена, якщо результати їхньої роботи та внутрішні механізми прийняття рішень залишаються непрозорими та незрозумілими для кінцевих користувачів. Проблема «чорної скриньки», яка тією чи іншою мірою властива багатьом складним нейромережевим архітектурам, полягає саме у цій непрозорості. Тому активний розвиток та практичне застосування методів так званого пояснювального штучного інтелекту, таких як SHAP, LIME, аналіз карт уваги для трансформерів та інших технік, які дозволяють візуалізувати важливість вхідних ознак, аналізувати внесок окремих компонентів моделі у фінальний результат та загалом підвищити прозорість, зрозумілість та інтерпретованість роботи складних нейронних мереж, є надзвичайно актуальним та важливим напрямком сучасних досліджень та практичних розробок у цій галузі [5]. Отже, виходячи з вище зазначено можна формалізувати за допомогою рисунку 1.

Рис. 1. Взаємозв'язок ключових факторів рівня розвитку нейромережевих технологій та точності прогнозування фінансових втрат

Джерело: сформовано авторами на основі [23; 24; 25; 26]

У той же час, справедливо зазначити, що незважаючи на значний теоретичний потенціал та певні практичні успіхи, застосування нейронних мереж для прогнозування фінансових втрат від кіберзагроз, стикається з низкою серйозних викликів та об'єктивних обмежень. Окрім вже детально розглянутих фундаментальних проблем, пов'язаних з досконалістю та адекватністю архітектур, якістю та доступністю необхідних даних, наявністю достатніх обчислювальних ресурсів та гострою потребою в кваліфікованих кадрах і прозорих, інтерпретованих моделях, специфічні умови, в яких функціонує Україна, накладають додаткові значні ускладнення. Постійні, масовані, цілеспрямовані та часто відверто спонсоровані державою-агресором кібератаки на об'єкти критичної інфраструктури, державні установи, фінансову систему та оборонний комплекс створюють унікальний та надзвичайно динамічний ландшафт загроз.

Висновки. Зауважимо, що сучасні нейромережеві підходи, безперечно, відкривають значні та раніше недосяжні перспективи для вирішення завдання з прогнозування фінансових втрат від кіберзагроз. Однак їхній повний потенціал може бути реалізований лише за умови системного, цілеспрямованого та ресурсного подолання існуючих об'єктивних викликів та обмежень, насамперед у сфері збору, підготовки, стандартизації та управління даними, а також у сфері забезпечення необхідними технологічними та, що найважливіше, людськими ресурсами. Важливо чітко усвідомлювати, що прогрес лише в одній з цих взаємозалежних областей, наприклад, у розробці все нових і нових архітектур нейронних мереж, без відповідного паралельного розвитку національної інфраструктури даних, без підготовки достатньої кількості кваліфікованих фахівців або без забезпечення доступу до необхідних обчислювальних потужностей, не призведе до кардинального та сталого покращення загальної прогнозної спроможності та практичної ефективності таких систем. Успішна реалізація комплексного підходу до вирішення зазначених проблем дозволить не лише значно підвищити точність та обґрунтованість оцінки потенційних фінансових втрат від кібератак, але й сприятиме більш ефективному та раціональному розподілу обмежених державних та приватних ресурсів на превентивні заходи захисту, посилить загальну стійкість національної економіки та її критичних секторів до деструктивних впливів у кіберпросторі та, зрештою, забезпечить необхідні умови для безпечного та сталого цифрового розвитку країни навіть в умовах тривалої та виснажливої гібридної агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Полігенько О. Кібератака на Україну: від держреєстрів до Monobank. Як бізнесу захиститися, не втратити дані і працездатність. *Forbes.ua*. 2025. URL: https://forbes.ua/innovations/kiberriziki-na-ponad-10-trln-zbitkiv-yaki-galuzi-biznesu-naybilshe-atakuyut-kiberzlochintsi-ta-yak-minimizuvati-naslidki-instruktsiya-vid-eksperta-u-sferi-kiberbezpeki-olega-poligenko-23012025-26534

2. World Bank. A review of the economic costs of cyber incidents. 2024. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099092324164536687/p17876919ffee4079180e81701969ad0a18

3. CERT-UA. 2025. URL: https://cert.gov.ua/

4. World Economic Forum. Global cybersecurity outlook 2025. 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

5. Department for Science, Innovation and Technology. Research on the cyber security of AI. 2024. URL: https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai

6. European Union Agency for Cybersecurity (ENISA). Risk management. URL: https://www.enisa.europa.eu/topics/risk-management

7. Боженко В. В., Пахненко О. М., Яровенко Г. М., Койбічук В. В. Інструменти аналізу даних для оцінки кіберризиків у фінансових послугах. *Здобутки економіки: перспективи та інновації*. 2025. № 20. DOI: https://doi.org/10.5281/zenodo.16509500

8. Гончаренко І. Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство*. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-82

9. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: https://doi.org/10.32702/2307-2105-2020.10.504

10. Трусова Н. В., Чкан І. О. Кіберзахист банківської системи України в умовах цифрових трансформацій. *Збірник наукових праць ТДАТУ*. 2023. № 1(47). С. 151-163. DOI: https://doi.org/10.31388/2519-884X-2023-47-151-163

11. Тищенко С. І., Пархоменко О. Ю., Дармосюк В. М. Моделювання та аналіз ризиків кібератак на фінансові установи з використанням методів математичної статистики та Python. *Modern Economics*. 2024. № 48. С. 130-136. DOI: https://doi.org/10.31521/modecon.V48(2024)-166

12. Фаріон В., Гомотюк А., Назар Р., Турчин С. Використання штучного інтелекту для прогнозування фінансових показників. *Економічний аналіз*. 2024. Т. 34. № 2. С. 327–337. DOI: https://doi.org/10.35774/econa2024.02.327

13. Hoang D., Wiegratz K. Machine learning methods in finance: Recent applications and prospects. *European Financial Management*. 2023. Vol. 29, No. 5. DOI: https://doi.org/10.1111/eufm.12408

14. Javaid H. A. AI-driven predictive analytics in finance: Transforming risk assessment and decision-making. *Advances in Computer Sciences*. 2024. Vol. 7, No. 1. URL: https://acadexpinnara.com/index.php/acs/article/view/204

15. Al-E'mari S., Sanjalawe Y., Al-E'mari A. The role of artificial intelligence in enhancing financial decision-making and administrative efficiency: A systematic review. *Al-Basaer Journal of Business Research*. 2025. Vol. 1, No. 1. DOI: https://doi.org/10.71202/paper21

16. Sako K., Mpinda B. N., Rodrigues P. C. Neural networks for financial time series forecasting. *Entropy*. 2022. Vol. 24, No. 5. Art. 657. DOI: https://doi.org/10.3390/e24050657

17. Tiwo O. J. Quantum machine learning for secure financial forecasting: Mitigating data breaches and adversarial exploits. *Asian Journal of Research in Computer Science*. 2025. Vol. 18, No. 4. P. 154-175. DOI: https://doi.org/10.9734/ajrcos/2025/v18i4613

18. Thakkar S., Kazdaghli S., Mathur N., et al. Improved financial forecasting via quantum machine learning. *Quantum Machine Intelligence*. 2024. Vol. 6, No. 1. DOI: https://doi.org/10.1007/s42484-024-00157-0

19. Xu Z., Wang Y., Feng X., et al. Quantum-enhanced forecasting: Leveraging quantum gramian angular field and CNNs for stock return predictions. *Finance Research Letters*. 2024. Vol. 67. Art. 105840. DOI: https://doi.org/10.1016/j.frl.2024.105840

20. Obioha-Val O. A., Lawal T. I., Olaniyi O. O., et al. Investigating the feasibility and risks of leveraging artificial intelligence and open source intelligence to manage predictive cyber threat models. *Journal of Engineering Research and Reports*. 2025. Vol. 27, No. 2. P. 10-28. DOI: https://doi.org/10.9734/jerr/2025/v27i21390

21. Eling M., Elvedi M., Falco G. The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*. 2022. Vol. 27, No. 3. P. 429–443. DOI: https://doi.org/10.1080/10920277.2022.2034507

22. Kyivstar Business Hub. Microsoft digital defense report 2024: Ключові інсайти у глобальній індустрії кібербезпеки. 2024. URL: https://hub.kyivstar.ua/articles/microsoft-digital-defense-report-2024-klyuchovi-insajti-u-globalnij-industriyi-kiberbezpeki

23. Субботін С. О. *Нейронні мережі: теорія та практика*: навч. посіб. Житомир : Вид. О. О. Євенок, 2020. 184 с.

24. Hakim L., Wulandhari L. A. Cyber security threat prediction using time-series data with LSTM algorithms. *Indonesian Journal of Electrical Engineering and Informatics*. 2024. Vol. 12, No. 4. P. 1111-1133. DOI: https://doi.org/10.52549/ijeei.v12i4.5648

25. Santoso J., Hartono B., Silalahi F., Muthohir M. Transformers in cybersecurity: Advancing threat detection and response through machine learning architectures. *Journal of Technology Informatics and Engineering*. 2024. Vol. 3, No. 3. P. 382-396. DOI: https://doi.org/10.51903/jtie.v3i3.211

26. Kabir M. R., Bhadra D., Ridoy M., Milanova M. LSTM-Transformer-based robust hybrid deep learning model for financial time series forecasting. *Sci*. 2024. Vol. 7, No. 1. Art. 7. DOI: https://doi.org/10.3390/sci7010007

27. Бебешко Б. Т. Навчання штучної нейронної мережі на основі даних оцінювання результативності та ризиків інвестування в цифрові активи. *Кібербезпека: освіта, наука, техніка*. 2023. № 3(19). С. 135-145. DOI: https://doi.org/10.28925/2663-4023.2023.19.135145

REFERENCES:

1. Polihenko, O. (2025). Cyberattack on Ukraine: From state registers to Monobank. How businesses can protect themselves, avoid losing data and efficiency. *Forbes.ua*. Available at: https://forbes.ua/innovations/kiberriziki-na-ponad-10-trln-zbitkiv-yaki-galuzi-biznesu-naybilshe-atakuyut-kiberzlochintsi-ta-yak-minimizuvati-naslidki-instruktsiya-vid-eksperta-u-sferi-kiberbezpeki-olega-poligenko-23012025-26534

2. World Bank. (2024). *A review of the economic costs of cyber incidents*. Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099092324164536687/p17876919ffee4079180e81701969ad0a18

3. CERT-UA. (2025). *cert.gov.ua*. Available at: https://cert.gov.ua/

4. World Economic Forum. (2025). *Global cybersecurity outlook 2025*. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

5. Department for Science, Innovation and Technology. (2024). *Research on the cyber security of AI*. GOV.UK. Available at: https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai

6. European Union Agency for Cybersecurity. (n.d.). *Risk management*. Available at: https://www.enisa.europa.eu/topics/risk-management

7. Bozhenko, V. V., Pakhnenko, O. M., Yarovenko, H. M., & Koibichuk, V. V. (2025). Data mining tools for cyber risk assessment in financial services. *Economic achievements: prospects and innovations*, 20. DOI: https://doi.org/10.5281/zenodo.16509500

8. Honcharenko, I. (2023). Cyber threats of the financial sector in the conditions of war. *Economy and Society*, 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-82

9. Kryklii, O. A. (2020). Theory and practice of ensuring cyber resilience of banks. *Efficient economy*, 10. DOI: https://doi.org/10.32702/2307-2105-2020.10.504

10. Trusova, N. V., & Chkan, I. O. (2023). Cyber protection of the banking system of Ukraine in conditions of digital transformations. *Scientific bulletin of the Tavria State Agrotechnological University, 1*(47), 151-163. DOI: https://doi.org/10.31388/2519-884X-2023-47-151-163

11. Tyshchenko, S. I., Parkhomenko, O. Yu., & Darmosyuk, V. M. (2024). Modeling and analysis of risks of cyberattacks on financial institutions using methods of mathematical statistics and Python. *Modern Economics*, 48, 130-136. DOI: https://doi.org/10.31521/modecon.V48(2024)-166

12. Farion, V., Homotiuk, A., Nazar, R., & Turchyn, S. (2024). Use of artificial intelligence for forecasting financial indicators. *Economic analysis, 34*(2), 327-337. DOI: https://doi.org/10.35774/econa2024.02.327

13. Hoang, D., & Wiegratz, K. (2023). Machine learning methods in finance: Recent applications and prospects. *European Financial Management, 29*(5). DOI: https://doi.org/10.1111/eufm.12408

14. Javaid, H. A. (2024). AI-driven predictive analytics in finance: Transforming risk assessment and decision-making. *Advances in Computer Sciences, 7*(1). Available at: https://acadexpinnara.com/index.php/acs/article/view/204

15. Al-E'mari, S., Sanjalawe, Y., & Al-E'mari, A. (2025). The role of artificial intelligence in enhancing financial decision-making and administrative efficiency: A systematic review. *Al-Basaer Journal of Business Research, 1*(1). DOI: https://doi.org/10.71202/paper21

16. Sako, K., Mpinda, B. N., & Rodrigues, P. C. (2022). Neural networks for financial time series forecasting. *Entropy, 24*(5), 657. DOI: https://doi.org/10.3390/e24050657

17. Tiwo, O. J. (2025). Quantum machine learning for secure financial forecasting: Mitigating data breaches and adversarial exploits. *Asian Journal of Research in Computer Science, 18*(4), 154-175. DOI: https://doi.org/10.9734/ajrcos/2025/v18i4613

18. Thakkar, S., Kazdaghli, S., Mathur, N., Kerenidis, I., Ferreira-Martins, A. J., & Brito, S. (2024). Improved financial forecasting via quantum machine learning. *Quantum Machine Intelligence, 6*(1). DOI: https://doi.org/10.1007/s42484-024-00157-0

19. Xu, Z., Wang, Y., Feng, X., Wang, Y., Li, Y., & Lin, H. (2024). Quantum-enhanced forecasting: Leveraging quantum gramian angular field and CNNs for stock return predictions. *Finance Research Letters, 67*, 105840. DOI: https://doi.org/10.1016/j.frl.2024.105840

20. Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the feasibility and risks of leveraging artificial intelligence and open source intelligence to manage predictive cyber threat models. *Journal of Engineering Research and Reports, 27*(2), 10-28. DOI: https://doi.org/10.9734/jerr/2025/v27i21390

21. Eling, M., Elvedi, M., & Falco, G. (2022). The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal, 27*(3), 429-443. DOI: https://doi.org/10.1080/10920277.2022.2034507

22. Kyivstar Business Hub. (2024). *Microsoft digital defense report 2024: Key insights into the global cybersecurity industry*. Available at: https://hub.kyivstar.ua/articles/microsoft-digital-defense-report-2024-klyuchovi-insajti-u-globalnij-industriyi-kiberbezpeki

23. Subbotin, S. O. (2020). Neural networks: theory and practice. Zhytomyr: Publishing house O. O. Evenok.

24. Hakim, L., & Wulandhari, L. A. (2024). Cyber security threat prediction using time-series data with LSTM algorithms. *Indonesian Journal of Electrical Engineering and Informatics, 12*(4), 1111-1133. DOI: https://doi.org/10.52549/ijeei.v12i4.5648

25. Santoso, J., Hartono, B., Silalahi, F., & Muthohir, M. (2024). Transformers in cybersecurity: Advancing threat detection and response through machine learning architectures. *Journal of Technology Informatics and Engineering, 3*(3), 382-396. DOI: https://doi.org/10.51903/jtie.v3i3.211

26. Kabir, M. R., Bhadra, D., Ridoy, M., & Milanova, M. (2024). LSTM-Transformer-based robust hybrid deep learning model for financial time series forecasting. *Sci, 7*(1), 7. DOI: https://doi.org/10.3390/sci7010007

27. Bebeshko, B. (2023). Artificial neural network training based on performance and risks assessment data of the investment in digital assets. *Cybersecurity: Education, Science, Technique, 3*(19), 135-145. DOI: https://doi.org/10.28925/2663-4023.2023.19.135145

Дата надходження статті: 13.03.2026
Дата прийняття статті: 02.04.2026
Дата публікації статті: 06.04.2026