ВІСНИК ПРИАЗОВСЬКОГО ДЕРЖАВНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
2025р. Серія: Технічні науки Вип. 52
p-ISSN: 2225-6733; e-ISSN: 2519-271X

УДК 004.9 DOI: 10.31498/2225-6733.52.2025.350997

ЗАХИСТ ДАНИХ І БЕЗПЕКА МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ В РИНКОВО-НЕЙТРАЛЬНИХ СТРАТЕГІЯХ КРИПТОТРЕЙДИНГУ

Левицька Т.О. *канд. техн. наук, доцент, ДВНЗ «Приазовський державний технічний університет», м. Дніпро, ORCID: https://orcid.org/0000-0003-3359-1313, e-mail: levitskaya_t_a@pstu.edu;*

Копійка О.С. *студент, ДВНЗ «Приазовський державний технічний університет», м. Дніпро, ORCID: https://orcid.org/0009-0004-4117-4899, e-mail: kopiika_o_s@students.pstu.edu;*

Пилипенко Б.В. *студент, ДВНЗ «Приазовський державний технічний університет», м. Дніпро, ORCID: https://orcid.org/0009-0000-4968-8190, e-mail: pylypenko_b_v@pstu.edu*

Криптовалютні ринки та алгоритмічний криптотрейдинг активно переходять до використання моделей глибинного навчання й ринково-нейтральних стратегій, що підсилює вимоги до захисту даних і безпеки моделей. Стаття пропонує цілісний підхід до end-to-end захисту даних у хмарній системі алгоритмічного криптотрейдингу, яка реалізує ринково-нейтральні стратегії на основі моделей машинного навчання. Розглянуто криптографічні механізми протоколів Bitcoin та Ethereum і їхній внесок у забезпечення цілісності, незаперечності та стійкості транзакцій до повторного відтворення. Проаналізовано типові загрози DeFi-протоколів та біржових API, зокрема реентрантні атаки, маніпуляції оракулами, flash-кредити, MEV-атаки та зловживання API-ключами. Систематизовано патерни захисту даних і секретів у хмарній інфраструктурі Azure, AWS і GCP з використанням служб керування ключами та секретами, шифрування даних у транзиті та на спокої, принципів мінімальних привілеїв і сегментації мережі. Окрему увагу приділено загрозам для моделей машинного навчання у задачах прогнозування фінансових часових рядів, включно з отруєнням даних, адверсаріальними впливами та витоком моделей, а також їхньому зв'язку з вимогами регуляторів до алгоритмічного трейдингу й фреймворком NIST AI RMF. На прикладі прототипу ринково-нейтральної системи криптотрейдингу на основі LSTM/GRU-моделей побудовано матрицю «загроза–мітигація» та запропоновано практичні рекомендації щодо архітектури захисту. Додатково наведено мініексперимент із HMAC-SHA256-підписом і часовим вікном для запитів до біржового API, що демонструє виявлення та блокування спроб повторного відтворення запитів.

Ключові слова: *захист даних, криптотрейдинг, ринково-нейтральні стратегії, машинне навчання, глибинне навчання, хмарна інфраструктура, інформаційна безпека, DeFi, HMAC, kill-switch.*

Постановка проблеми

Активний розвиток ринку криптовалют і децентралізованих фінансів призвів до появи великої кількості алгоритмічних торгових систем, які використовують глибинні нейронні мережі для прогнозування часових рядів цін та формування ринково-нейтральних стратегій. У більшості публікацій основна увага приділяється якості прогнозу та доходності портфеля, тоді як питання захисту даних і ключів у повному життєвому циклі системи розглядаються фрагментарно або взагалі ігноруються.

На практиці ML-стек алгоритмічного трейдингу працює з чутливими даними й обліковими даними: API-ключами централізованих і децентралізованих бірж, історією котирувань та ордерів, наборами ознак для навчання моделей, снапшотами натренованих моделей, журналами операцій і бек-тестів. Компрометація будь-якого з цих елементів, цілеспрямоване спотворення вхідних даних або захоплення моделі атакувальником можуть призвести до прямих фінансових втрат, порушення регуляторних вимог до управління ризиками алгоритмічного трейдингу та втрати довіри до системи.

Проблема полягає в тому, що відсутня цілісна методика проєктування й експлуатації ML-орієнтованих криптовалютних торгових систем, у якій засоби криптографічного захисту, хмарна інфраструктура управління секретами, протокольні механізми аутентифікації біржових API та практики безпеки моделей машинного навчання були б інтегровані в єдину архітектуру ринково-нейтральної стратегії з контрольованим ризиком. Саме заповненню цієї прогалини й присвячена стаття.

Аналіз останніх досліджень та публікацій

У працях з прогнозування криптовалютних часових рядів переважають моделі глибинного навчання. Автори порівнюють моделі типу LSTM, GRU та двонапрямні LSTM за точністю прогнозу і показниками умовного трейдингу. Показано, що ці архітектури краще відтворюють нелінійні залежності й довгу пам'ять, ніж лінійні моделі, що зменшує похибку прогнозу і покращує прості стратегії купівлі-продажу [1] . При цьому джерела даних, цілісність часового ряду та модель загроз для самої моделі майже не аналізуються. Більшість робіт просто приймає, що вхідні дані коректні, а торгове середовище не є ворожим.

Криптографічні властивості протоколів Bitcoin і Ethereum опрацьовані набагато глибше. Оригінальні специфікації описують використання цифрових підписів на еліптичних кривих, побудову дерев Меркла та моделі обліку, які забезпечують незмінність журналу

транзакцій і зв'язок між витраченими та отриманими монетами [2-4] . Стандарти NIST і IETF для хеш-функцій, HMAC та протоколу TLS 1.3 визначають набір стійких примітивів для автентифікації й захисту трафіку у фінансових застосунках [5-8] . Це створює надійну базу для побудови безпечних каналів і підпису запитів до біржових API, однак питання інтеграції цих примітивів у повний ML-стек зазвичай залишається на розсуд розробника.

Дослідження DeFi та смарт-контрактів зосереджені на аналізі конкретних вразливостей і сценаріїв атак. Узагальнюючі огляди виділяють повторні виклики, помилки у валідації стану, небезпечні зовнішні виклики та слабкі механізми оновлення як основні джерела критичних помилок у смарт-контрактах Ethereum [9, 10]. Роботи з безпеки DeFi показують, що flash-кредити дають змогу атакувальнику швидко нарощувати позицію, зміщувати ціни в оракулах та виводити кошти з протоколів, якщо цінові механізми побудовані на коротких вікнах спостереження [11, 12]. Аналіз MEV-активності демонструє, що доступ до упорядкування транзакцій у mempool дозволяє цілеспрямовано погіршувати ціну виконання заявок інших учасників через front-running та sandwich-атаки [13]. Для алгоритмічних стратегій це означає, що навіть коректний сигнал моделі може реалізовуватися на ринку зі стійким зсувом проти трейдера.

У сфері безпеки машинного навчання сформовано класи атак, які безпосередньо стосуються торгових моделей. Базові огляди виділяють отруєння навчальних вибірок, маніпуляції на етапі експлуатації через спеціально сконструйовані приклади, а також атаки на конфіденційність навчальних даних і параметрів моделі [14, 15]. Роботи щодо крадіжки моделей показують, що доступ до API прогнозування дозволяє відтворювати модель або її частину з достатньою точністю, щоб використовувати її логіку у власних стратегіях [16]. Атаки інверсії моделі демонструють можливість відновлення чутливих характеристик навчальних даних із вихідних ймовірностей [17]. Для фінансових моделей це створює два напрями ризику: спотворення сигналів через маніпуляцію даними і витік торгового ноу-хау через несекурні API та журнали.

Регуляторні органи описують безпеку алгоритмічного трейдингу з позицій ринкової стабільності та керованості. Стаття 17 MiFID II та звіти ESMA вимагають від учасників ринку наявності стрес-тестування алгоритмів, обмежень за обсягом і ціною ордерів, журналювання всіх рішень і можливості негайно припинити роботу алгоритму при збої [18, 19]. Документи HKMA та PRA конкретизують вимоги до корпоративного управління, незалежного контролю ризиків і технічного kill-switch, який повинен бути прив'язаний до чітких процедур і регулярно тестуватися [20, 21]. Звіти BIS і FMSB показують, що відсутність таких механізмів у поєднанні з алгоритмічними стратегіями призводить до різких рухів ринку та самопідсилюючих каскадів угод [22, 23]. Це безпосередньо стосується ML-орієнтованих стратегій, де швидкість ухвалення рішень висока, а помилка моделі може швидко масштабуватися.

Окремий огляд Ради з фінансової стабільності узагальнює вплив широкого використання систем штучного інтелекту та машинного навчання у фінансових послугах на ринкову й системну стабільність та підкреслює необхідність вбудовування таких систем у вже наявні рамки управління ризиками [24].

Фреймворки ризик-менеджменту штучного інтелекту пропонують більш загальний рівень опису. NIST AI RMF вводить функції Govern, Map, Measure і Manage, які задають вимоги до ролей, процесів, оцінки ризиків і механізмів реагування для AI-систем [25] . Ці функції дають основу для опису життєвого циклу моделей у фінансових застосунках, але не деталізують, як пов'язати вимоги до управління моделями з криптографічними засобами, DeFi-загрозами та хмарними сервісами керування секретами.

Питання захисту секретів і даних у хмарі описані в основному в документації провайдерів і практичних гайдах. Microsoft, Amazon Web Services та Google Cloud рекомендують використовувати спеціалізовані служби керування секретами та ключами, напряму не зберігати API-ключі в коді й конфігураційних файлах, застосовувати принцип найменших привілеїв, приватні мережеві точки доступу та централізований аудит операцій з секретами [26-28]. Біржі та брокери у своїх рекомендаціях описують вимоги до HMAC-підпису запитів, обмежених вікон часу, жорстких rate-limit і прив'язки ключів до конкретних IP-адрес [29-31]. Ці документи дають чіткі вимоги до окремих компонентів торгової системи, але не розглядають їх як частину єдиного стеку, в якому дані проходять шлях від блокчейн-протоколу до моделі глибинного навчання та модуля виконання ринково-нейтральної стратегії.

Мета статті

Метою статті є розроблення та обґрунтування цілісного підходу до захисту даних у хмарній системі алгоритмічного криптотрейдингу, що реалізує ринково-нейтральні стратегії на основі моделей глибинного навчання. Для цього аналізуються криптографічні властивості протоколів Bitcoin та Ethereum, класи загроз для DeFi та біржових API, патерни керування секретами й шифрування даних у хмарній інфраструктурі, а також загрози для моделей машинного навчання, після чого формується узгоджена архітектура захисту та матриця «загроза–мітигація» з прикладом технічної реалізації.

Матеріали та методи

Об'єктом дослідження є прототип хмарної системи алгоритмічного криптотрейдингу, що використовує біржові дані централізованої платформи, ознаковий конвеєр для агрегованих OHLCV-рядів, двошарові моделі типу LSTM/GRU для прогнозування відносних

p-ISSN: 2225-6733; e-ISSN: 2519-271X

дохідностей та ринково-нейтральну стратегію з виконанням ордерів через біржові API. У дослідженні застосовано аналіз специфікацій блокчейн-протоколів, оглядів вразливостей DeFi та біржових API, документів регуляторів щодо алгоритмічного трейдингу, а також рекомендацій хмарних провайдерів щодо керування секретами; на основі цих джерел побудовано модель загроз для всієї системи, сформовано матрицю «загроза–мітигація» та реалізовано демонстраційний приклад із HMAC-підписом і часовим вікном для захисту запитів до API.

Виклад основного матеріалу

Розглянута система алгоритмічного криптотрейдингу побудована як багаторівневий конвеєр. Зовнішні джерела даних включають централізовану біржу Binance для спотових котирувань, DeFi-протоколи та ончейн-дані, а також деривативну платформу dYdX для виконання ринково-нейтральних стратегій. Потік ринкової інформації надходить до модуля збору даних, далі до конвеєра ознак, який агрегує OHLCV-ряди, обчислює технічні індикатори та нормалізує ознаки. На наступному етапі працює сервіс моделі, де багатовалютна LSTM або GRU формує вектор прогнозів для групи активів. Ці прогнози обробляє стратегічний модуль, що формує ринково-нейтральні позиції, накладає ліміти ризику і генерує сигнали для шлюзу виконання ордерів, який взаємодіє з API бірж.

Архітектура зберігання даних містить окремі сховища для історичних ринкових рядів, наборів ознак, реєстру моделей та журналів торгів. Навколо обчислювальних компонентів розташовано хмарні сервіси безпеки: сховище секретів і ключів, служби керування ідентичностями та моніторинг. Саме через ці сервіси проходять усі операції читання API-ключів бірж, ключів шифрування та критичних параметрів стратегії. Таке розділення дозволяє чітко виділити зони довіри й визначити, які компоненти потрібно захищати від компрометації в першу чергу. Архітектуру системи та взаємодію між основними компонентами показано на рис. 1.

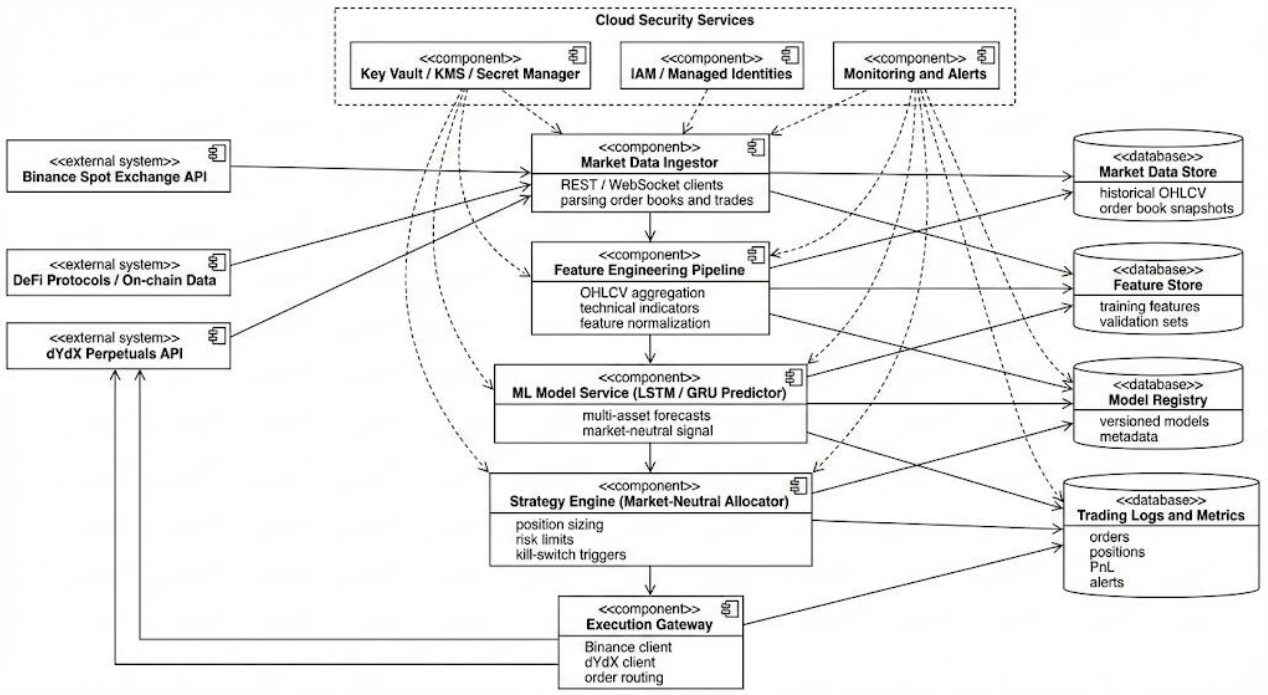

Рис. 1 – Архітектура хмарної системи алгоритмічного криптотрейдингу та її основні компоненти захисту даних

На вході конвеєра система отримує потоки котирувань, книг заявок і торгової активності зі спотових і деривативних бірж, а також цінові ряди та стани позицій із DeFi-протоколів. Ці дані вже містять перший рівень ризиків. Якщо API біржі або DeFi-протоколу піддається атакам типу re-entrancy, flash-кредитів чи маніпуляції ціною, то окремі часові фрагменти ринку суттєво спотворюються. У такому випадку модель, яка тренується на цих даних, вчиться на аномальних режимах і може відтворювати поведінку, вигідну атакувальнику. Навіть якщо сам блокчейн зберігає цілісність журналу транзакцій, інтерфейс API стає точкою, де формується спотворений погляд на ринок.

Другий рівень ризику виникає всередині системи збору та підготовки даних. Якщо модуль завантаження працює без чітких правил щодо джерел, інтервалів та часових зон, то в історію потрапляють дублікати, прогалини й шматки даних, отримані через нестабільні мережеві з’єднання. За відсутності валідації і логування ці артефакти непомітно проходять до конвеєра ознак і

p-ISSN: 2225-6733; e-ISSN: 2519-271X

далі до моделі. Отруєння тренувального набору може відбутися як через цілеспрямовану підміну файлів, так і через неконтрольоване змішування різних режимів роботи біржі, коли, наприклад, у часі кластери високої волатильності поєднуються з періодами низької ліквідності.

Третій рівень стосується самого ML-сервісу та стратегічного модуля. Якщо доступ до моделі здійснюється через загальний REST-ендпойнт без чітких політик автентифікації, зловмисник може надсилати спеціально сформовані вектори ознак, спостерігати відповіді й відтворити логіку стратегії [16, 17]. Журнали, що містять повні вектори входів і виходів моделі, створюють додаткову площу атаки. Компрометація цих журналів дозволяє відновити структуру ознак, діапазони значень та реакцію стратегії на різні сценарії ринку. Для ринково-нейтральної стратегії це особливо небезпечно, оскільки конкурент отримує можливість створити дзеркальну або контр-стратегію з використанням тих самих сигналів.

Четвертий рівень загроз пов’язаний із модулем виконання ордерів. Компрометація API-ключів, відсутність обмежень за IP-адресами та нечітке розділення прав доступу призводять до того, що сторонній користувач може не лише прочитати історію угод, а й відкривати нові позиції на повний ліміт, змінювати параметри ризику та вимикати механізми контролю. Якщо разом із цим відсутній централізований kill-switch, то навіть коректна модель і чисті дані не захистять від серії небажаних ордерів, які виконуються від імені системи. Саме тому подальші підрозділи присвячені побудові хмарного контуру безпеки та контролю моделі й стратегії.

Для розміщення системи використовується захищене хмарне середовище з виділеною віртуальною мережею. Всередині цієї мережі працюють обчислювальні вузли з контейнерами або функціями, де розгорнуті модулі збору даних, сервіс моделі та стратегічно-виконавчий модуль. Жоден з цих компонентів не зберігає API-ключі або інші секрети локально. Доступ до секретів здійснюється лише через служби керування ключами та секретами, такі як Key Vault або KMS, з використанням керованих ідентичностей і ролей з мінімальними привілеями. Усі з’єднання між компонентами та сховищами проходять через внутрішні адреси в межах віртуальної мережі, а вихід до публічного інтернету дозволено лише з виконувальних модулів і тільки до доменів бірж.

Сховища даних розділені за призначенням: окремо зберігаються історичні ринкові ряди, набори ознак і снапшоти моделей, окремо журнали торгів і метрики ризику. Для цих сховищ вмикається шифрування на спокої з використанням ключів, якими керує KMS, а доступ контролюється як на рівні ролей, так і на рівні мережевих правил. Журнали доступу до секретів і ключів, а також усі виняткові події безпеки надсилаються до системи моніторингу, де налаштовано сповіщення про підозрілі патерни. Взаємодію між обчислювальними вузлами, сервісами безпеки, сховищами даних і зовнішніми біржами у межах хмарного периметра показано на рис. 2.

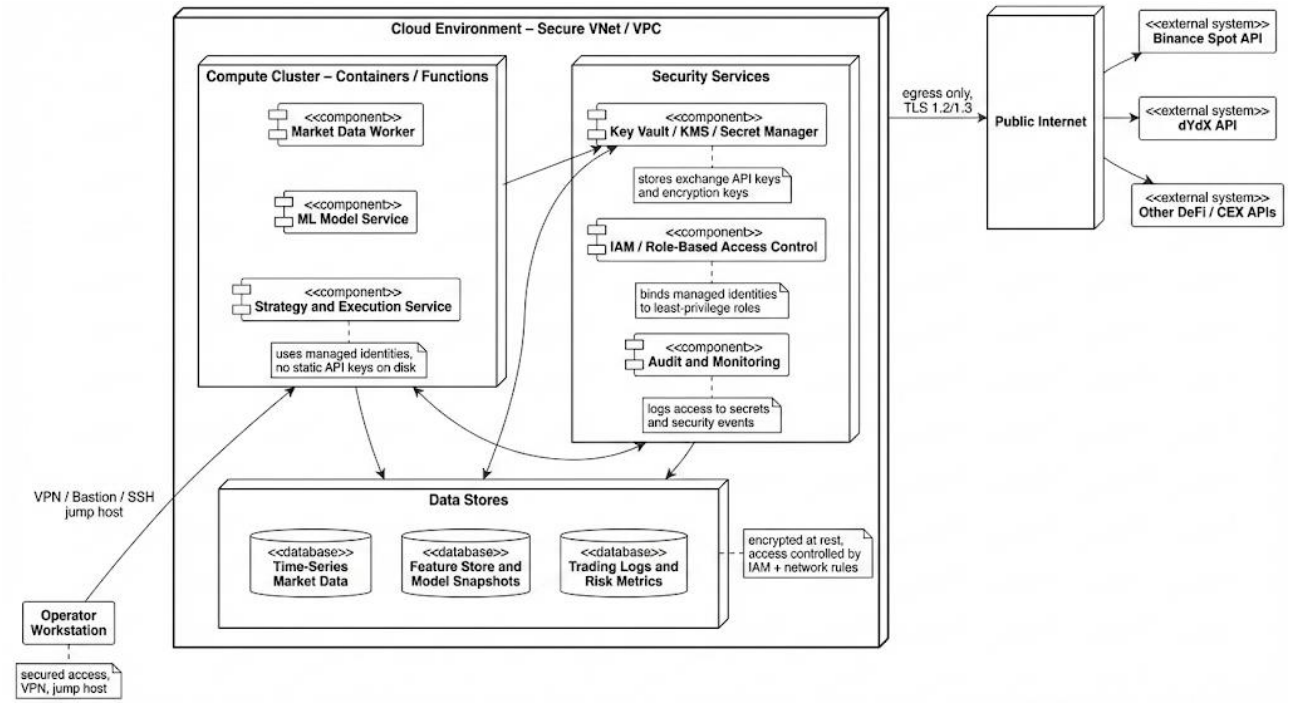

Рис. 2 – Розгортання компонентів торгової системи в межах захищеного хмарного середовища

p-ISSN: 2225-6733; e-ISSN: 2519-271X

Окремо проектується процедура аварійного відкликання. У разі підозри на компрометацію ключів або некоректну активність у журналах система автоматично відкликає або перевипускає секрети у сховищі, зупиняє контейнери з торговими стратегіями та блокує вихідний трафік до бірж до завершення розслідування. Такий сценарій реалізує технічний варіант kill-switch на рівні інфраструктури й узгоджується з рекомендаціями Azure, AWS та Google щодо реагування на інциденти безпеки.

Модель глибинного навчання навчається на історичних даних Binance з урахуванням комісій та обмежень ліквідності, а стратегія формує ринково-нейтральні портфелі з кількох активів. Для зменшення ризиків отруєння й перенавчання тренувальний набір формується з неперекривних часових відрізків, а перевірка проводиться за схемою покрокового просування у часі. Вхідні ряди проходять попередній контроль: видаляються дні з аномальною кількістю відключень, підозрілими сплесками обсягів та суттєвими розбіжностями між біржами. Для поточної роботи моделі вводиться моніторинг розподілів ознак та виходів, щоб фіксувати відхилення від історичних профілів.

Стратегічний модуль має власний контур контролю. На кожному циклі оновлення позицій обчислюються ключові метрики ризику: поточний розмір плеча, концентрація позицій за окремими активами, добовий прибуток або збиток, а також ознаки деградації якості даних. Якщо одна або кілька метрик виходять за встановлені межі, спрацьовують локальні обмежувачі, які поступово знижують розмір позицій, і вмикається логіка kill-switch. Її ключові кроки такі: зупинка генерації нових ордерів, скасування активних заявок і тимчасове відкликання API-ключів у сховищі секретів. Після цього система переходить у стан, де відновлення можливо лише після ручної перевірки оператором. Послідовність дій у контурі kill-switch подано на рис. 3. Такий підхід відповідає вимогам регуляторів щодо можливості негайного припинення роботи алгоритмічної стратегії та повернення керування людині.

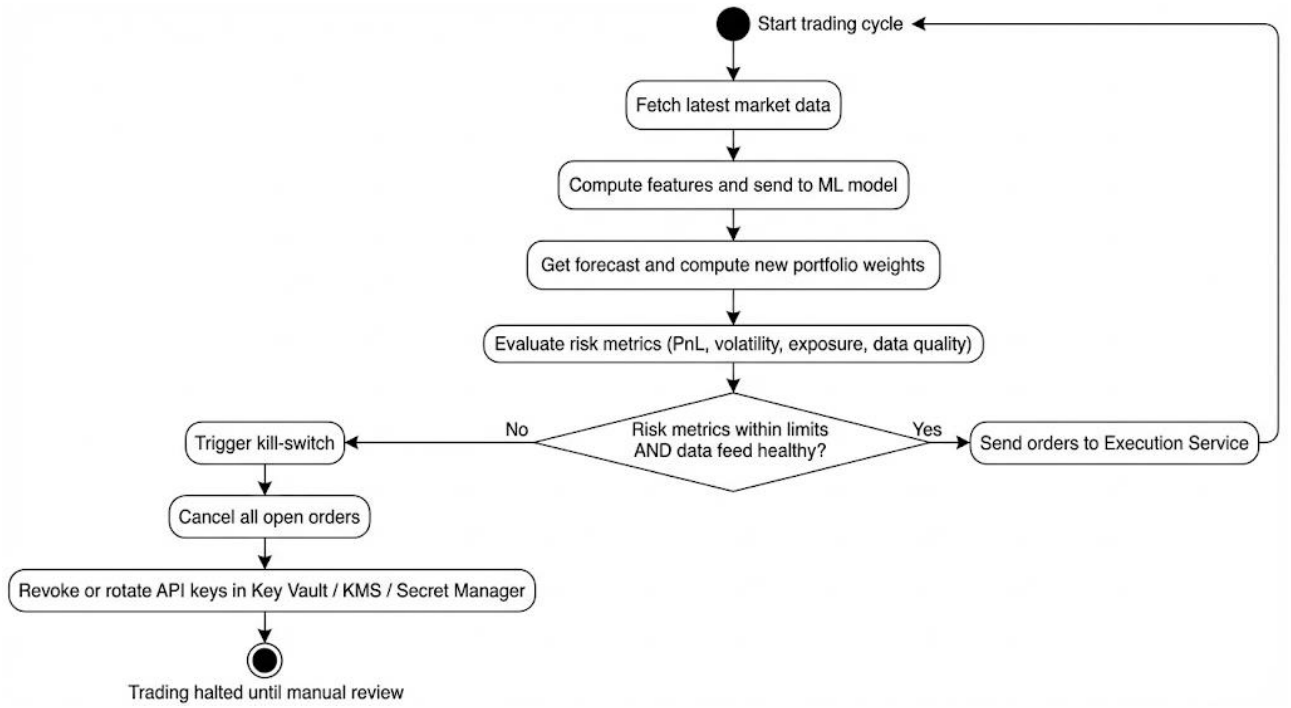

Рис. 3 – Логіка ризик-орієнтованого kill-switch для ринково-нейтральної торгової стратегії

Для ілюстрації впливу класичних механізмів захисту на рівні API проведено мініексперимент. Згенеровано послідовність зі 200 законних запитів до умовного торгового сервісу, кожен з яких містить метод, шлях, тіло запиту та мітку часу. Далі сформовано 120 повторних запитів, які імітують поведінку атакувальника, що перехопив законні повідомлення і намагається відтворювати їх із випадковою затримкою. Розглянуто два варіанти сервера. У першому варіанті сервер приймає всі запити без перевірки часу, nonce та HMAC, отже кожен повтор вважається успішним. У другому варіанті сервер перевіряє коректність HMAC-SHA256, обмежує прийнятний часовий зсув до тридцяти секунд і не приймає один і той самий nonce двічі.

Результати показано на рис. 4. У сценарії без захисту кумулятивна кількість успішних повторних запитів зростає майже лінійно та досягає значення, близького до кількості спроб. У сценарії з HMAC-підписом і часовим вікном більшість повторів відхиляється: крива швидко виходить на плато, оскільки однакові запити з простроченими мітками часу або повторним nonce не проходять перевірку.

p-ISSN: 2225-6733; e-ISSN: 2519-271X

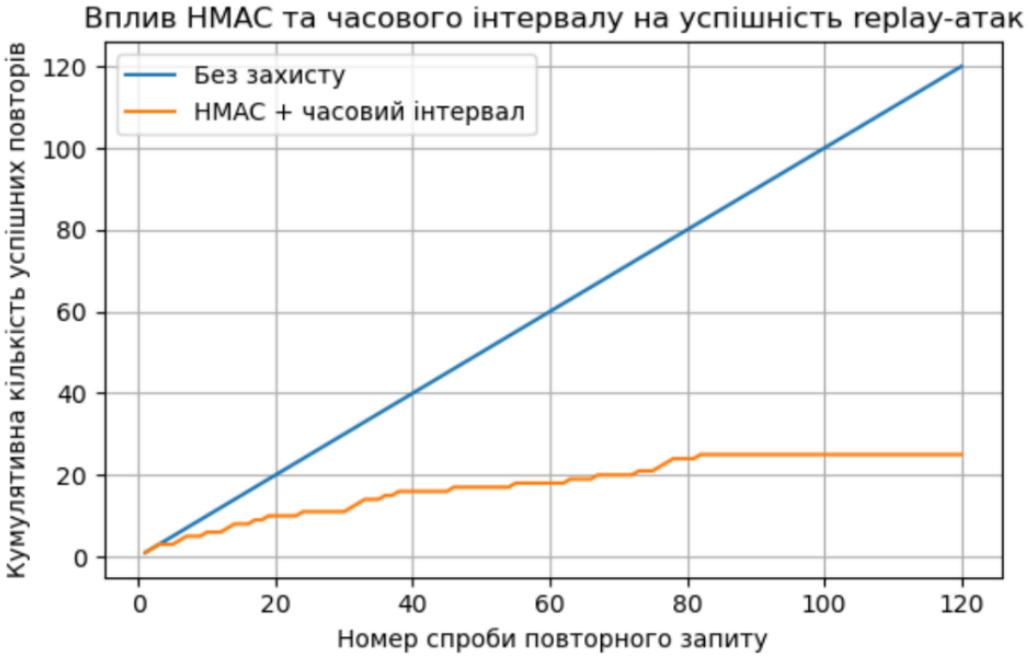

Рис. 4 – Вплив HMAC-підпису та часового інтервалу на успішність replay-атак на торговий API

Хоча модель експерименту спрощена, вона демонструє, що навіть базові засоби захисту на рівні API істотно зменшують площу атаки. У реальній системі ці механізми доповнюються IP-обмеженнями, розділенням прав доступу для читання й торгівлі та моніторингом спроб автентифікації, що разом формує завершений контур захисту даних і операцій.

Висновки

В роботі сформовано цілісний погляд на захист даних у хмарній системі алгоритмічного криптотрейдингу з ринково-нейтральними стратегіями на основі моделей глибинного навчання. Показано, що криптографічні механізми блокчейн-протоколів самі по собі не гарантують безпеки торгових даних, оскільки основна площа атаки зміщується на рівні біржових і DeFi API, хмарної інфраструктури та ML-пайплайна.

Запропоновано архітектуру, у якій всі секрети та ключі централізовано зберігаються у хмарних службах керування ключами, доступ до них надається лише через керовані ідентичності з мінімальними привілеями, а сховища ринкових даних, ознак, моделей і журналів працюють у межах ізольованого мережевого периметра із шифруванням на спокої та в транзиті. Для моделі та стратегії описано окремий контур контролю, що включає фільтрацію даних, покрокову валідацію у часі, моніторинг розподілів ознак і виходів, обмеження на зміну позицій і ризик-орієнтований kill-switch, який зупиняє торгівлю та ініціює відкликання ключів у разі відхилень.

Мініексперимент з HMAC-підписом і часовим інтервалом показав, що навіть базові механізми автентифікації й захисту від повторного відтворення запитів суттєво зменшують кількість успішних атак на торговий API. Це підтверджує доцільність поєднання класичних криптографічних засобів з інженерними практиками ротації ключів, обмеженням мережевого доступу та централізованим моніторингом. Подальший розвиток роботи може включати формальне моделювання загроз для складніших багатоступеневих стратегій з кількома горизонтами прогнозу, а також експериментальну перевірку стійкості моделей до цілеспрямованого отруєння даних на реальних потоках крипторинку.

Перелік використаних джерел

[1] Cryptocurrency price forecasting – A comparative analysis of ensemble learning and deep learning methods / Bouteska A., Abedin M. Z., Hajek P., Yuan K. *International Review of Financial Analysis*. 2024. Vol. 92. Article 103055. DOI: https://doi.org/10.1016/j.irfa.2023.103055.

[2] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN Electronic Journal*. 2008. Pp. 1-9. DOI: https://doi.org/10.2139/ssrn.3440802.

[3] Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Whitepaper, 2014. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 10.10.2025).

[4] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper, 2014. URL: https://ethereum.github.io/yellowpaper/paper.pdf (дата звернення: 10.10.2025).

[5] FIPS PUB 180-4: Secure Hash Standard (SHS). Gaithersburg : National Institute of Standards and Technology, 2015.
[6] FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Gaithersburg : National Institute of Standards and Technology, 2015.
[7] Krawczyk H., Bellare M., Canetti R. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, Internet Engineering Task Force, 1997. DOI: https://doi.org/10.17487/RFC2104.
[8] Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force, 2018. DOI: https://doi.org/10.17487/RFC8446.
[9] Atzei N., Bartoletti M., Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). *Principles of Security and Trust*: Proceedings of the 6th International Conference, Uppsala, Sweden, 22-29 April 2017. 2017. Vol. 10204. Pp. 164-186. DOI: https://doi.org/10.1007/978-3-662-54455-6_8.
[10] SoK: Decentralized Finance (DeFi) Attacks / L. Zhou et al. *IEEE Symposium on Security and Privacy*, San Francisco, USA, 21-25 May 2023. Pp. 2444-2461. DOI: https://doi.org/10.1109/SP46215.2023.10179435.
[11] SoK: Decentralized Finance (DeFi) / S. Werner et al. *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, Cambridge, USA, 19-21 September 2022. Pp. 30-46. DOI: https://doi.org/10.1145/3558535.3559780.
[12] Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges / Hasan R., Crandall D., Fritz M., Kapadia A. IEEE Symposium on Security and Privacy, San Francisco, USA, 18-21 May 2020. Pp. 318-335. DOI: https://doi.org/10.1109/SP40000.2020.00097.
[13] Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit / Qin K., Zhou L., Livshits B., Gervais A. *Financial Cryptography and Data Security* : 25th International Conference, virtual Event, 1-5 March 2021. 2021. Pp. 3-32. DOI: https://doi.org/10.1007/978-3-662-64322-8_1.
[14] Yerlikaya F. A., Bahtiyar Ş. Data poisoning attacks against machine learning algorithms. *Expert Systems with Applications*. 2022. Vol. 208. Article 118101. DOI: https://doi.org/10.1016/j.eswa.2022.118101.
[15] Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning / M. Jagielski et al. *IEEE Symposium on Security and Privacy*, San Francisco, USA, 20-24 May 2018. Pp. 19-35. DOI: https://doi.org/10.1109/SP.2018.00057.
[16] Time series adversarial attacks: An investigation of smooth perturbations and defense approaches / G. Pialla et al. *International Journal of Data Science and Analytics*. 2025. Vol. 19. Pp. 129-139. DOI: https://doi.org/10.1007/s41060-023-00438-0.
[17] Rigaki M., Garcia S. A survey of privacy attacks in machine learning. *ACM Computing Surveys*. 2023. Vol. 56(4). Article 101. Pp. 1-34. DOI: https://doi.org/10.1145/3624010.
[18] European Securities and Markets Authority. Article 17 Algorithmic Trading. ESMA, 2014. URL: https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mifid-ii/article-17-algorithmic-trading (дата звернення: 10.10.2025).
[19] European Securities and Markets Authority. MiFID II Review Report on Algorithmic Trading. ESMA70-156-4572, 2021. 170 p.
[20] Hong Kong Monetary Authority. Sound risk management practices for algorithmic trading. Circular, 06.03.2020. URL: https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20200306-4-EN/20200306-4-EN.pdf (дата звернення: 10.10.2025).
[21] Prudential Regulation Authority, Bank of England. Supervisory Statement SS5/18: Algorithmic trading. London, 2018. URL: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/algorithmic-trading-ss (дата звернення: 10.10.2025).
[22] Markets Committee, Bank for International Settlements. FX execution algorithms and market functioning. BIS, 2020. URL: https://www.bis.org/publ/mktc13.pdf (дата звернення: 10.10.2025).
[23] FICC Markets Standards Board. Emerging themes and challenges in algorithmic trading and machine learning. Spotlight Review, 2020. URL: https://fmsb.com/wp-content/uploads/2020/04/FMSB-Spotlight-Review-Emerging-themes-and-challenges-in-algorithmic-trading-and-machine-learning.pdf (дата звернення: 10.10.2025).
[24] Financial Stability Board. Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Basel, 2017. URL: https://www.fsb.org/wp-content/uploads/P011117.pdf (дата звернення: 10.10.2025).
[25] Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg : National Institute of Standards and Technology, 2023. 42 p. DOI: https://doi.org/10.6028/NIST.AI.100-1.
[26] Microsoft Corporation. Best practices for secrets management in Azure Key Vault. Microsoft Learn, 2023. URL: https://learn.microsoft.com/azure/key-vault/secrets/secrets-best-practices (дата звернення: 10.10.2025).
[27] Amazon Web Services. AWS Secrets Manager best practices. AWS Documentation, 2024. URL: https://docs.aws.amazon.com/secretsmanager/latest/userguide/best-practices.html (дата звернення: 10.10.2025).
[28] Google Cloud. Secret Manager best practices. Google Cloud Documentation, 2024. URL: https://cloud.google.com/secret-manager/docs/best-practices (дата звернення: 10.10.2025).
[29] Binance. Signed endpoint security. Binance API Documentation, 2024. URL: https://binance-docs.github.io/apidocs/spot/en/#signed-trade-

user_data-and-margin-endpoint-security (дата звернення: 10.10.2025).
[30] dYdX Trading Inc. API Keys and Authentication. dYdX Documentation, 2023. URL: https://docs.dydx.exchange (дата звернення: 10.10.2025).
[31] Interactive Brokers. Secure Your Trading Algorithms and Servers: General Guide. IBKR Quant News, 2020. URL: https://www.interactivebrokers.com/campus/ibkr-quant-news/secure-your-trading-algorithms-and-servers-general-guide/ (дата звернення: 10.10.2025).

DATA PROTECTION AND SECURITY OF MACHINE LEARNING MODELS IN MARKET-NEUTRAL CRYPTOCURRENCY TRADING STRATEGIES

Levytska T.O. *PhD (Engineering), associate professor, SHEI «Priazovskyi state technical university», Dnipro, ORCID: https://orcid.org/0000-0003-3359-1313, e-mail: levitskaya_t_a@pstu.edu;*

Kopiika O.S. *student, SHEI «Priazovskyi state technical university», Dnipro, ORCID: https://orcid.org/0009-0004-4117-4899, e-mail: kopiika_o_s@students.pstu.edu;*

Pylypenko B.V. *student, SHEI «Priazovskyi state technical university», Dnipro, ORCID: https://orcid.org/0009-0000-4968-8190, e-mail: pylypenko_b_v@pstu.edu*

Cryptocurrency markets and algorithmic crypto trading are increasingly relying on deep learning models and market-neutral strategies, which amplifies the requirements for data protection and model security. This paper presents an end-to-end approach to data protection in a cloud-based algorithmic cryptocurrency trading system that implements market-neutral strategies using machine learning models. We examine the cryptographic mechanisms of the Bitcoin and Ethereum protocols and their contribution to transaction integrity, non-repudiation, and resistance to replay. We then show how these guarantees interact with higher-level data flows in exchanges and DeFi protocols. We analyse typical threats in DeFi protocols and exchange APIs, including re-entrancy attacks, oracle manipulation, flash loans, MEV attacks, and abuse of API keys, and we highlight how these threats can distort training data, backtests, and live execution. We systematise data and secret protection patterns in Azure, AWS, and GCP cloud infrastructures, focusing on key and secret management services, encryption of data in transit and at rest, least-privilege access, network segmentation, and incident-driven key revocation. Special attention is paid to machine learning security threats in financial time-series forecasting, including data poisoning, adversarial perturbations, model extraction, and model inversion, and to their relationship with regulatory requirements for algorithmic trading and the NIST AI RMF framework. Using a prototype market-neutral crypto trading system based on LSTM/GRU models as a case study, we derive a threat–mitigation matrix, outline a risk-based kill-switch design that links portfolio risk metrics with technical controls, and propose practical architectural recommendations for data protection along the entire pipeline. In addition, we provide a small experiment with HMAC-SHA256 signing and a timestamp window for exchange API requests, demonstrating the detection and blocking of replay attempts and showing how standard cryptographic tools can be embedded into the trading stack without changing the economic logic of the strategy.

Keywords: *data protection, cryptocurrency trading, market-neutral strategies, machine learning, deep learning, cloud infrastructure, information security, DeFi, HMAC, kill-switch.*

References

[1] A. Bouteska, M.Z. Abedin, P. Hajek, and K.Yuan, “Cryptocurrency price forecasting – A comparative analysis of ensemble learning and deep learning methods,” *International Review of Financial Analysis*, vol. 92, article 103055, 2024. **doi: 10.1016/j.irfa.2023.103055**
[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *SSRN Electronic Journal*, pp. 1-9, 2008. **doi: 10.2139/ssrn.3440802**.
[3] V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”. 2014. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 10.10.2025).
[4] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf. Accessed on: October 10, 2025.
[5] *Secure Hash Standard (SHS)*, FIPS PUB 180-4, National Institute of Standards and Technology, Gaithersburg, 2015.
[6] Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202: SHA-3 Standard, National Institute of Standards and Technology, Gaithersburg, 2015.
[7] H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104, Internet Engineering Task Force, 1997. **doi: 10.17487/RFC2104**.

[8] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446*, Internet Engineering Task Force, 2018. **doi: 10.17487/rfc8446**.

[9] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in Proc. of the 6th Int. Conf. «Principles of Security and Trust», Uppsala, Sweden, April 22-29, 2017, vol. 10204, pp. 164-186. **doi: 10.1007/978-3-662-54455-6_8**.

[10] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, and Y. Wang, "SoK: Decentralized Finance (DeFi) Attacks," in *Proc. of the IEEE Symposium on Security and Privacy*, San Francisco, USA, May 21-25, 2023, pp. 2444-2461. **doi: 10.1109/SP46215.2023.10179435**.

[11] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, "SoK: Decentralized Finance (DeFi)," in *Proc. of the 4th ACM Conf. on Advances in Financial Technologies*, Cambridge, USA, Sept. 19-21, 2022, pp. 30-46. **doi: 10.1145/3558535.3559780**.

[12] R. Hasan, D. Crandall, M. Fritz, and A. Kapadia, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," in *Proc. of the IEEE Symposium on Security and Privacy*, San Francisco, USA, May 18-21, 2020, pp. 318-335. **doi: 10.1109/SP40000.2020.00097**.

[13] K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," in *Proc. of the 25th Int. Conf. «Financial Cryptography and Data Security»*, virtual event, March 1-5, pp. 3-32. **doi: 10.1007/978-3-662-64322-8_1**.

[14] F.A. Yerlikaya, and Ş. Bahtiyar, "Data poisoning attacks against machine learning algorithms," *Expert Systems with Applications*, vol. 208, article 118101, 2022. **doi: 10.1016/j.eswa.2022.118101**.

[15] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning," in *Proc. of the IEEE Symposium on Security and Privacy*, San Francisco, USA, May 20-24, 2018, pp. 19-35. **doi: 10.1109/SP.2018.00057**.

[16] G. Pialla et al., "Time series adversarial attacks: An investigation of smooth perturbations and defense approaches," *International Journal of Data Science and Analytics*, vol. 19, pp. 129-139, 2025. **doi: 10.1007/s41060-023-00438-0**.

[17] M. Rigaki, and S. Garcia, "A survey of privacy attacks in machine learning," *ACM Computing Surveys*, vol. 56(4), article 101, pp. 1-34, 2023. **doi: 10.1145/3624010**.

[18] European Securities and Markets Authority. Article 17 Algorithmic Trading. ESMA, 2014. [Online]. Available: https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mifid-ii/article-17-algorithmic-trading. Accessed on: October 10, 2025.

[19] "MiFID II Review Report on Algorithmic Trading ESMA70-156-4572," European Securities and Markets Authority, 2021.

[20] Hong Kong Monetary Authority. Sound risk management practices for algorithmic trading. Circular, 06.03.2020. [Online]. Available: https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20200306-4-EN/20200306-4-EN.pdf. Accessed on: October 10, 2025.

[21] Prudential Regulation Authority, Bank of England. Supervisory Statement SS5/18: Algorithmic trading. London, 2018. [Online]. Available: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/algorithmic-trading-ss. Accessed on: October 10, 2025.

[22] Markets Committee, Bank for International Settlements. FX execution algorithms and market functioning. BIS, 2020. [Online]. Available: https://www.bis.org/publ/mktc13.pdf. Accessed on: October 10, 2025.

[23] FICC Markets Standards Board. Emerging themes and challenges in algorithmic trading and machine learning. Spotlight Review, 2020. [Online]. Available: https://fmsb.com/wp-content/uploads/2020/04/FMSB-Spotlight-Review-Emerging-themes-and-challenges-in-algorithmic-trading-and-machine-learning.pdf. Accessed on: October 10, 2025.

[24] Financial Stability Board. Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Basel, 2017. [Online]. Available: https://www.fsb.org/wp-content/uploads/P011117.pdf. Accessed on: October 10, 2025.

[25] *Artificial Intelligence Risk Management Framework*, AI RMF 1.0, National Institute of Standards and Technology, Gaithersburg, USA, 2023. **doi: 10.6028/NIST.AI.100-1**.

[26] Microsoft Corporation. Best practices for secrets management in Azure Key Vault. Microsoft Learn, 2023. [Online]. Available: https://learn.microsoft.com/azure/key-vault/secrets/secrets-best-practices. Accessed on: October 10, 2025.

[27] Amazon Web Services. AWS Secrets Manager best practices. AWS Documentation, 2024. [Online]. Available: https://docs.aws.amazon.com/secretsmanager/latest/userguide/best-practices.html. Accessed on: October 10, 2025.

[28] Google Cloud. Secret Manager best practices. Google Cloud Documentation, 2024. [Online]. Available: https://cloud.google.com/secret-manager/docs/best-practices. Accessed on: October 10, 2025.

[29] Binance. Signed endpoint security. Binance API Documentation, 2024. [Online]. Available: https://binance-docs.github.io/apidocs/spot/en/#signed-trade-user_data-and-margin-endpoint-security. Accessed on: October 10, 2025.

[30] dYdX Trading Inc. API Keys and Authentication. dYdX Documentation, 2023. [Online]. Available:

https://docs.dydx.exchange. Accessed on: October 10, 2025.

[31] Interactive Brokers. Secure Your Trading Algorithms and Servers: General Guide. IBKR Quant News, 2020. [Online]. Available: https://www.interactivebrokers.com/campus/ibkr-quant-news/secure-your-trading-algorithms-and-servers-general-guide/. Accessed on: October 10, 2025.

Стаття надійшла 10.11.2025
Стаття прийнята 02.12.2025
Стаття опублікована 29.12.2025

Цитуйте цю статтю як: Левицька Т. О., Копійка О. С., Пилипенко Б. В. Захист даних і безпека моделей машинного навчання в ринково-нейтральних стратегіях криптотрейдингу. *Вісник Приазовського державного технічного університету. Серія: Технічні науки*. 2025. Вип. 52. С. 83-92. DOI: https://doi.org/10.31498/2225-6733.52.2025.350997.