УДК: 004.056.55 https://doi.org/10.15407/pp2025.02.028

І.О. Шахматов, І.В. Замрій

ІНТЕГРОВАНА СИСТЕМА БЕЗПЕКИ ДЛЯ ЗАХИСТУ СИНХРОНІЗАЦІЇ ПЛАТЕЖІВ ВІД MITM-АТАК

У статті вирішується проблема захисту синхронізації платежів від MITM-атак у багатоканальних платіжних системах, де готівкові, карткові та онлайн-платежі інтегровані з CRM і бухгалтерськими платформами. Розглянуто сценарії атак «людина посередині» та їхній вплив на цілісність транзакцій. Запропоновано багаторівневу систему захисту з використанням методів штучного інтелекту, криптографії (цифрові підписи й часові мітки) та додаткової верифікації клієнтів. Модель підвищує стійкість до фальсифікацій, повторних атак і підміни даних, забезпечуючи високу надійність і масштабованість у системах, що працюють із електронними транзакціями.
Ключові слова: Захист платежів, MITM-атака, безпека фінансових транзакцій, штучний інтелект у кібербезпеці.

I.O. Shakhmatov, I.V. Zamrii

INTEGRATED SECURITY SYSTEM FOR PROTECTING PAYMENT SYNCHRONIZATION FROM MITM ATTACKS

The article addresses the challenge of securing payment synchronization against Man-in-the-Middle (MITM) attacks in multichannel payment systems, where cash, card, and online transactions are integrated with CRM and accounting platforms. It examines MITM attack scenarios and their impact on transaction integrity. A multi-layered security framework is proposed, leveraging artificial intelligence techniques, cryptographic methods (digital signatures and timestamps), and additional client verification mechanisms. The model enhances resilience against fraud, replay attacks, and data substitution, ensuring high reliability and scalability across electronic transaction systems.
Keywords: Payment security, MITM attack, financial transaction security, artificial intelligence in cybersecurity.

Вступ

Електронні платежі стали невід'ємною частиною фінансових операцій, забезпечуючи зручність, швидкість і широку географічну доступність транзакцій. Інтеграція CRM-систем та автоматизованих бухгалтерських платформ значно підвищує ефективність і прозорість обробки платежів, дозволяючи відстежувати кожен етап транзакції, автоматизувати розподіл коштів і спрощувати фінансову звітність. Однак разом із розвитком інноваційних платіжних рішень зростає й ризик кібератак, серед яких особливо небезпечними є атаки типу «людина посередині» (Man-in-the-Middle, MITM). Вони становлять загрозу не лише для конфіденційності, а й для цілісності фінансових даних та репутації компаній, що обробляють великі обсяги платежів.

Значну вразливість виявляють складні платіжні системи, що поєднують кілька способів оплати (готівка, банківські картки, онлайн-платежі), а також використовують реєстрацію чеків через ПРРО (Checkbox) та зовнішні сервіси на кшталт Portmone. Через інтеграцію між платіжними пристроями, серверами, CRM-модулями та бухгалтерськими системами утворюється комплексна інфраструктура обміну даними, яка може стати привабливою ціллю для кіберзловмисників. Зокрема, несанкціоноване перехоплення та модифікація платіжної інформації в реальному часі може призвести до фінансових втрат, витоку конфіденційних даних чи порушення цілісності всієї системи (Рис. 1). MITM-атаки характеризуються здатністю зловмисника непомітно «встава-

ти» між учасниками платіжної комунікації, підмінюючи або перехоплюючи дані без прямого виявлення. Ця проблема стає особливо актуальною в умовах, коли традиційні засоби автентифікації (наприклад, базові протоколи шифрування чи цифрові підписи) не завжди забезпечують належний рівень захисту від витончених методів атак, що можуть використовувати динамічну модифікацію трафіку, повторне відтворення (Replay) транзакцій та маніпуляції часовими мітками.

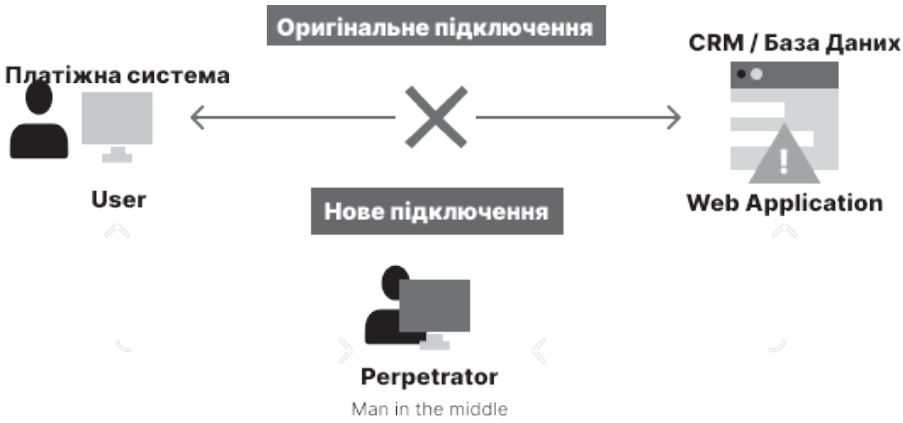

Рис. 1. Схема потенційної MITM-атаки в платіжній системі

У зв'язку з цим зростає потреба у створенні багаторівневих та адаптивних механізмів захисту, здатних ефективно протидіяти MITM-атакам. Важливу роль у забезпеченні безпеки відіграють засоби криптографічного захисту, зокрема продумані протоколи шифрування, цифровий підпис і маркери часу, що ускладнюють маніпуляції з боку зловмисників.

Аналіз літературних даних

Зростання безготівкових платежів супроводжується ризиками атак MITM, що загрожують цілісності та безпеці фінансових транзакцій. Основні уразливості мобільних платіжних систем пов'язані з недостатнім рівнем автентифікації, слабким шифруванням даних та можливістю перехоплення інформації під час синхронізації платежів. Інтегрована система безпеки, яка поєднує шифрування, механізми виявлення аномалій та динамічні протоколи перевірки даних, мінімізує ризик атак MITM та підвищує стійкість платіжних платформ [1].

Для захисту платіжних транзакцій широко застосовуються методи шифрування та автентифікації. Використання багаторівневих механізмів, зокрема багатофакторної автентифікації та наскрізного шифрування, забезпечує значне зниження ризиків компрометації даних [2]. Одним із ефективних рішень є використання зашифрованих систем керування, які не лише забезпечують конфіденційність, а й виявляють аномалії, що можуть свідчити про можливу атаку. Дослідження показують, що ефективність таких систем залежить від типу шифрування, параметрів його налаштування та механізмів перевірки цілісності даних [3].

Традиційні методи захисту не завжди ефективні проти сучасних атак, які використовують алгоритми машинного навчання для обходу класичних систем безпеки. Впровадження адаптивних та самонавчальних систем дозволяє оперативно реагувати на загрози та передбачати потенційні вразливості. Інтеграція ШІ в мобільні платіжні системи сприяє аналізу поведінкових патернів, виявленню аномального трафіку та покращеному шифруванню, що суттєво знижує ризик атак MITM [4]. Дослідження показують, що використання алгоритмів класифікації, таких як Random Forest та глибоке навчання, дозволяє ефективно розрізняти нормальну та

аномальну поведінку в платіжних системах, що удосконалює виявлення загроз у режимі реального часу [5].

Одним із перспективних напрямків у сфері кібербезпеки є застосування технології блокчейну для захисту синхронізації платежів. Завдяки своїй децентралізованій природі, блокчейн гарантує незмінність записів і прозорість операцій, що значно ускладнює підробку або модифікацію даних [6]. Поєднання технологій федеративного навчання та блокчейну дозволяє ідентифікувати шахрайські транзакції без передачі конфіденційних даних між фінансовими установами. Використання смарт-контрактів забезпечує автоматичну перевірку платіжних запитів, що значно підвищує рівень безпеки [7]. Крім того, нові виклики в кібербезпеці вимагають розгляду технологій, стійких до квантових атак. Квантова криптографія забезпечує захист фінансових даних завдяки механізмам, що залишаються безпечними навіть у разі появи квантових комп'ютерів [11]. Інтеграція цієї технології разом із технологією розподіленого реєстру (DLT) дозволяє створити децентралізовану систему, що гарантує незмінність історії транзакцій та захищає їх від підробки.

Оптимальний рівень захисту забезпечується завдяки поєднанню кількох методів, таких як штучний інтелект, блокчейн та адаптивні алгоритми аналізу мережевого трафіку. Наприклад, комбінація методів XGBoost і Random Forest дозволяє ефективно класифікувати та блокувати атакуючі запити, а використання алгоритмів градієнтного бустингу покращує ідентифікацію аномальних операцій у фінансових потоках [8, 12]. Додатково білінійний протокол транзакцій із подвійною автентифікацією підсилює безпеку за рахунок двоетапного підтвердження операцій, унеможливлюючи компрометацію платежів навіть у разі витоку облікових даних [12]. Інтеграція штучного інтелекту в систему безпеки платіжних операцій забезпечує динамічну адаптацію до нових загроз, аналізуючи мережевий трафік та відстежуючи шахрайські схеми в режимі реального часу [13]. Використання ймовірнісних нейронних мереж (PNN) значно підвищує ефективність виявлення MITM-атак, оскільки дозволяє зменшити кількість хибнопозитивних спрацьовувань та підвищити швидкість реакції на загрози [14]. Застосування алгоритмів машинного навчання для аналізу транзакцій у режимі реального часу забезпечує ефективний захист від складних шахрайських схем. Використання GBDT для аналізу фінансових потоків дозволяє знаходити приховані патерни шахрайства та блокувати потенційно шкідливі запити до їх виконання [15]. Поєднання блокчейну з механізмами моніторингу транзакцій створює додатковий рівень прозорості операцій та забезпечує захист від атак MITM [16, 17].

Атаки MITM залишаються серйозною загрозою для синхронізації платежів, однак сучасні технології дозволяють ефективно їм протидіяти. Поєднання методів шифрування, машинного навчання, квантової криптографії та блокчейну забезпечує комплексний захист фінансових транзакцій. Впровадження децентралізованих систем перевірки транзакцій, механізмів виявлення аномалій та розширених криптографічних протоколів дозволяє мінімізувати ризик атак MITM та забезпечити високу стійкість платіжних платформ [10, 17].

Навіть за умови значної кількості досліджень та впровадження різноманітних криптографічних і блокчейн-рішень, наявні напрацювання залишають відкритими кілька ключових питань. Перш за все, не має єдиної цілісної методики, яка б одночасно охоплювала всі рівні платіжної інфраструктури – від фізичних пристроїв прийому платежів до інтегрованих CRM-рішень. Окремі методи машинного навчання або блокчейн-технології використовуються переважно як самостійні модулі, не завжди забезпечуючи узгоджену взаємодію між етапами опрацювання транзакцій. Додатковою проблемою є адаптивність систем безпеки до нових форм MITM-атак. Більшість наявних рішень передбачає виключно реагування на типові загрози, не враховуючи еволюцію шахрайських схем і можливість складних комбінацій атак (наприклад, одночасне використання фішингових методів і перехоплення

трафіку). Попри високий потенціал нейромережевих моделей і технологій квантового шифрування, їх практичне впровадження у фінансових платформах усе ще обмежується великою кількістю конфігураційних параметрів та вимогами до обчислювальних ресурсів.

Також залишається недостатньо дослідженим питання динамічної корекції системи в реальному часі. Більшість систем виявлення аномалій вимагає попереднього навчання на значному наборі історичних даних, що ускладнює миттєву адаптацію до нових сценаріїв атак. Водночас комплексна інтеграція блокчейну, квантових протоколів і машинного навчання перебуває на стадії концептуальних чи пілотних проєктів. Немає статистично верифікованих оцінок ефективності цих підходів у середовищах із високим навантаженням і великим обсягом транзакцій, що є типовим для комерційних платіжних систем. З урахуванням наведених обмежень та викликів, подальші дослідження мають зосередитися на розробці інтегрованих, масштабованих і динамічно адаптивних рішень, здатних оперативно реагувати на нетипові сценарії атак MITM. Це підкреслює актуальність і нагальну потребу у комплексних системах захисту, які будуть не лише вчасно виявляти, а й ефективно блокувати спроби перехоплення, підміни або повторного відтворення платіжних даних у різних каналах обробки фінансових транзакцій.

Зважаючи на необхідність постійно розвивати системи захисту MITM атак, необхідно впроваджувати методи поведінкового аналізу, які дозволяють виявляти аномальні транзакції та підозрілі запити, використовуючи інтелектуальні алгоритми для аналізу закономірностей взаємодії користувачів із системою. Додатковим рівнем безпеки стає багатоетапна верифікація, яка передбачає повторну ідентифікацію користувача у разі виявлення підозрілої активності, що мінімізує ризик несанкціонованого доступу. Важливою складовою є також система моніторингу та логування, яка забезпечує детальний запис усіх ключових дій, дозволяючи оперативно виявляти нові вектори атак і регулярно оновлювати протоколи безпеки.

Дослідження спрямоване на створення комплексної моделі захисту синхронізації платежів, здатної оперативно виявляти та блокувати MITM-атаки в режимі реального часу. Основна мета полягає у розробці гнучкої системи безпеки, яка відповідала б вимогам як малих, так і великих фінансових та CRM-платформ. Важливим аспектом такої системи є механізм виявлення аномальних транзакцій, що базується на методах аналізу даних та алгоритмах штучного інтелекту. Ефективний захист від повторних атак забезпечується впровадженням криптографічних часових маркерів, що унеможливлюють їх використання. Динамічний пороговий аналіз дозволяє швидко ідентифікувати загрози та своєчасно на них реагувати, що підвищує загальний рівень безпеки системи. Додатковим рівнем захисту стає інтеграція багаторівневих механізмів перевірки автентичності, які зміцнюють стійкість фінансових платформ до потенційних загроз.

Запропонований підхід у межах цього дослідження, може бути застосований як у вже існуючих багатофункціональних платіжних системах, так і в нових розробках фінансових сервісів, де безпека даних та безперервність процесів є пріоритетом. Крім того, запропонована модель стане основою для розробки універсальних рішень у галузі кібербезпеки, спрямованих на ефективну детекцію й нейтралізацію складних MITM-атак у платіжних та CRM-середовищах.

Опис системи

Платіжна система, що розглядається, поєднує кілька каналів проведення транзакцій, інтегрованих між собою для підвищення швидкості та зручності обробки платежів. Одним із ключових компонентів є пристрій сплати, який підтримує різні способи оплати, включаючи готівкові розрахунки, безготівкові платежі через POS-термінал та онлайн-оплату за допомогою QR-коду через платформу Portmone. Ку-

пюроприймач автоматично фіксує внесену суму та перевіряє непідробність банкнот, а POS-термінал забезпечує проведення операцій за допомогою магнітної стрічки, чипа або безконтактної NFC-технології. Під час використання онлайн-оплати на екрані пристрою генерується QR-код, який клієнт сканує для переходу до платіжного сервісу та підтвердження транзакції. Важливу роль у функціонуванні системи відіграє сервіс реєстрації чеків Checkbox. Після успішної оплати автоматично створюється електронний чек, який реєструється у програмному реєстраторі розрахункових операцій (ПРРО) відповідно до вимог законодавства. Користувач отримує посилання на чек через SMS або E-mail, що дозволяє переглядати зареєстрований документ у зручний спосіб.

CRM-система забезпечує інтеграцію платіжного процесу з бухгалтерським обліком та додатковими механізмами верифікації. Вона отримує дані про транзакції від пристрою сплати та Checkbox, автоматично передаючи їх до бухгалтерської системи для формування звітів, рахунків і закриття фінансових періодів. Для підвищення рівня безпеки можливе підтвердження особи платника через SMS-код, що вводиться у відповідне поле під час проведення операції. Додатково CRM дозволяє швидко знаходити деталі платежу за номером чека, що значно спрощує ідентифікацію клієнта, обробку повернень коштів та коригування платежів. Згаданий комплекс взаємодії між купюроприймачем, POS-терміналом, онлайн-платіжним сервісом Portmone, Checkbox та CRM-системою створює складне багатоканальне середовище. Кожний канал водночас є потенційним вектором атаки, тому забезпечення надійної взаємодії між усіма компонентами є пріоритетом.

Атаки типу «людина посередині» (Man-in-the-Middle, MITM) становлять серйозну загрозу для платіжних сервісів, оскільки дозволяють зловмиснику перехоплювати або змінювати дані, що передаються між різними компонентами системи, залишаючись непомітними для учасників транзакції. Одним із небезпечних сценаріїв є фальсифікація транзакцій, коли змінюються сума платежу, реквізити отримувача або призначення платежу. У таких випадках реальний платіж може бути перенаправлений на інший рахунок, а відображені дані у бухгалтерському обліку та CRM можуть не відповідати дійсності, що створює ризики шахрайства та фінансових втрат.

Ще одним поширеним методом є повторна атака, коли зловмисник перехоплює дані успішної платіжної операції, наприклад, пакет із підтвердженням оплати, і повторно відтворює його, щоб знову списати кошти або отримати доступ до вже оплаченої послуги. Такі атаки особливо небезпечні в системах, які не перевіряють унікальність і «свіжість» транзакцій, зокрема в разі відсутності механізмів перевірки одноразових маркерів чи часових міток. Окрему загрозу становить перехоплення SMS-коду, який використовується для аутентифікації або підтвердження платежу. Якщо зловмисник отримує доступ до мобільного пристрою жертви або використовує вразливості мережі (як-от, у протоколі SS7) чи шкідливі програми, він може несанкціоновано підтвердити транзакцію від імені користувача. Це дає можливість отримати контроль над фінансовими операціями без відома власника облікового запису. Ще одним способом маніпуляції є підміна відповіді від сервісів платіжного шлюзу або системи реєстрації чеків, таких як Checkbox чи Portmone. У цьому випадку злочинець модифікує відповідь сервера, надсилаючи підроблену інформацію про нібито успішне проведення платежу. Як наслідок, CRM-система чи бухгалтерський модуль можуть зберегти некоректні дані про оплату, що відкриває можливості для шахрайських дій, неправильного формування звітності та спотворення фінансових операцій. Усі зазначені загрози вимагають комплексного підходу до безпеки платіжних систем, що включає різнопланові механізми захисту, такі як криптографічні методи шифрування, багатофакторна автентифікація, поведінковий аналіз транзакцій та моніторинг мережевого трафіку.

У рамках дослідження основна увага зосереджена на протидії атакам типу «людина посередині» (MITM), оскільки

вони становлять особливу небезпеку для платіжних сервісів, дозволяючи зловмисникам втручатися у процес передачі даних та змінювати фінансову інформацію без відома учасників транзакції. Ефективний захист від MITM є одним із ключових аспектів безпеки всієї системи, адже його відсутність може зробити вразливими навіть найбільш захищені компоненти інфраструктури, зокрема, CRM та бухгалтерські модулі, які обробляють фінансові операції. Для мінімізації ризиків була запропонована багаторівнева система захисту, що включає механізми формування платіжного запиту, верифікації транзакцій, детекції атак та підтвердження платежу перед його передачею в CRM та бухгалтерську систему (Рис. 2). Такий підхід дозволяє забезпечити комплексну безпеку на кожному етапі обробки транзакцій, мінімізуючи можливості для несанкціонованого втручання.

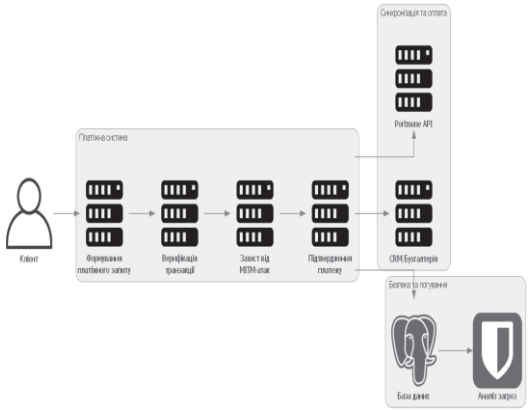

Рис. 2. Діаграма розгортання системи захисту

Модель та методологія дослідження

Запропонована модель виявлення аномалій у платіжних операціях та механізмів протидії атакам MITM поєднує пороговий метод детектування, статистичний аналіз та алгоритми машинного навчання, що забезпечує надійний захист від шахрайських дій. В основі системи лежить набір вхідних параметрів, які використовуються для ідентифікації та аналізу кожної транзакції. Для кожної операції формується унікальний ідентифікатор, що однозначно визначає платіж у системі. Платіжні реквізити містять дані про суму операції, момент її ініціалізації у секундах та спосіб оплати, що може включати готівковий розрахунок, використання банківської картки або онлайн-платіж. Інформація про електронний чек включає його унікальний номер, що дозволяє відстежувати операцію, а також ідентифікатор ПРРО, який генерується системою Checkbox і має фіксовану довжину. Верифікаційні дані містять номер телефону, представлений у міжнародному форматі, та SMS-код, який використовується для підтвердження транзакції. Код може бути чотири- або шестизначним, залежно від визначеного формату безпеки. Відповідь від сервісів Portmone або Checkbox використовується для верифікації результату операції та містить ключові параметри. Статус відповіді представлений булевою змінною, що сигналізує про успішне або невдале виконання платежу. Додатково передається текстове повідомлення, яке уточнює причину успіху чи помилки, надаючи системі можливість аналізу потенційних загроз та коригування механізмів безпеки.

Повний набір даних X_i для i-ї транзакції:

$$X_i = \{T_i, P_i, C_i, V_i, R_i\}$$

Кожен елемент X_i є категоріальним, що дає змогу детально аналізувати платіж та визначати аномальні відхилення. T_i – ідентифікатор i-ї транзакції, унікальне ціле число в діапазоні $[1, 10^{12}]$, що однозначно визначає платіж у системі. P_i– платіжні реквізити, а саме: сума операції, час ініціалізації, спосіб оплати. C_i, – дані електронного чека: номер чека, ідентифікатор ПРРО. V_i – верифікаційні дані: номер телефону, SMS-код. R_i – відповідь від сервісу Portmone або Checkbox: статус відповіді, текстовий код.

Функція аномальності $\mathrm{D}(X_i)$ відображає наскільки характеристики поточної транзакції X_i відхиляються від «нормальної» поведінки, зафіксованої у системі.

$$\mathrm{D}(X_i) = \sigma(X_i),$$

де $\sigma(X_i) \geq 0$, це алгоритмічна операція, що повертає невід'ємне число і відображає ступінь «відхилення» транзакції X_i. Чим вище $\mathrm{D}(X_i)$, тим більша ймовірність, що операція містить аномальні чи потенційно небезпечні характеристики. На

цій основі встановлюється динамічний поріг δ ($\delta \geq 0$), що визначає межу допустимого відхилення:

$$u(T_i) = \begin{cases} 1, \text{якщо } \left|\mathrm{D}(X_i) - \breve{D}\right| < \delta, \\ 0, \text{якщо } \left|\mathrm{D}(X_i) - \breve{D}\right| \geq \delta . \end{cases}$$

У даному формулюванні:

$u(T_i) = 1$ свідчить про те, що транзакція не перевищує встановлений поріг аномальності й вважається умовно безпечною (однак може бути перевірена додатково).

$u(T_i) = 0$ позначає, що рівень аномальності надто високий і платежу присвоюється статус «підозрілий» із подальшим застосуванням механізмів блокування або додаткової верифікації.

Оскільки атака MITM змінює принаймні один із параметрів транзакції (наприклад, суму або чекові дані), імовірність потрапляння такої зміненої транзакції за межі порогу δ є високою, за умови належного налаштування $\mathrm{D}(X_i)$. Рівень детектування атаки визначається показником P_d у межах [0,1]:

$$P_d = 1 - (P_f)^N,$$

де P_f – імовірність хибного негативу $\in$ [0,1], тобто вірогідність, що система не виявить справжню атаку. N – кількість перевірок, $\in N$, $N \geq 1$, під час яких аналізуються різні складові транзакції (верифікаційний код, відповідь від платіжного сервісу, часові мітки). Із зростанням N і покращенням якості оцінки аномальності (зменшення P_f), величина P_d наближається до 1, що означає майже гарантовану детекцію спроби фальсифікації даних.

Для підвищення точності виявлення складних видів шахрайства запроваджується нейромережева модель f_θ, що оперує вектором X_i. Результатом обчислень є ризик-функція $R(T_i)$, значення якої лежить в інтервалі [0,1]:

$$R(T_i) = f_\theta(X_i),$$

значення якої лежить в інтервалі [0,1]. $R(T_i)$ відображає ймовірність того, що транзакція T_i є атакованою. Тут f_θ – функція нейромережі, параметризована векторами вагами θ, Ваги θ це числові коефіцієнти (вектори та матриці), які визначають зв'язки між нейронами на суміжних шарах мережі. Під час навчання мережі ці ваги коригуються так, щоб мінімізувати обрану функцію втрат і забезпечити найбільш точну класифікацію транзакцій (виявлення атак).

Для оцінки загрози встановлюється порогове значення $\tau \in [0,1]$. Якщо

$$R(T_i) > \tau,$$

то транзакція вважається потенційно атакованою. На відміну від статичного δ, поріг τ може динамічно переоцінюватися залежно від змін у платіжному потоці та появи нових сценаріїв зловмисних дій.

Запропонована модель складається з п'яти шарів, що послідовно обробляють вхідний вектор ознак X_i і формують вихідну оцінку ризику $R(T_i)$. Вхідний шар (Input Layer) отримує вектор ознак розмірності d, який утворюється після попередньої підготовки даних (масштабування числових параметрів, кодування категоріальних ознак). Усі елементи вектора X_i надходять до наступного шару без додаткової обробки. Прихований щільний шар (Dense Layer 1) містить 128 нейронів, кожен з яких обчислює лінійну комбінацію вхідних сигналів із вектором ваг. Така конфігурація дозволяє відсікати від'ємні значення та підвищує здатність моделі виявляти складні залежності. Прихований щільний шар (Dense Layer 2) містить 64 нейрони, зменшення кількості нейронів порівняно з попереднім шаром допомагає мережі узагальнювати дані та уникати перенавчання. Прихований щільний шар (Dense Layer 3) містить 32 нейрони, застосування третього щільного шару підвищує глибину моделі та дає змогу виявляти більш витончені патерни шахрайства, характерні для MITM-атак. Вихідний шар (Output Layer) складається з одного нейрона із сигмоїдною активацією, яка обмежує вихідне значення в інтервалі [0,1]. Цей вихід трактується як імовірність атаки (ризик-функція $R(T_i)$), де значення, близькі до 1, свідчать про високу вірогідність MITM-атаки.

Під час навчання мережі вагові коефіцієнти θ усіх шарів коригуються методом зворотного поширення помилки (backpropagation). Застосовується функція втрат (наприклад, бінарна крос-ентропія)

та оптимізатор (наприклад, Adam) із заданими гіперпараметрами швидкості навчання. У результаті зменшується різниця між фактичною міткою (атака або нормальна транзакція) та виходом моделі $R(T_i)$. Після завершення процесу навчання мережа здатна з високою точністю розрізняти транзакції, які містять ознаки MITM-атак, і нормальні операції.

Якщо в результаті перевірки транзакція визначається як аномальна або потенційно шахрайська, система активує механізми додаткової верифікації та захисту. Це може включати повторне надсилання SMS-коду автентифікації, що вимагає від користувача підтвердження своєї особи. У деяких випадках потрібне втручання адміністратора, а система тимчасово блокується. За необхідності транзакція може бути повністю скасована, а клієнт негайно отримує відповідне повідомлення про причину відмови. Додатковим захисним заходом є створення нового платіжного середовища, що унеможливлює повторне використання скомпрометованих даних. Для цього система генерує новий QR-код або унікальне платіжне посилання для сервісу Portmone, що дозволяє безпечно повторити спробу оплати. Паралельно з цими заходами адміністратор отримує сповіщення про спробу атаки. Всі подібні випадки фіксуються у журналах моніторингу, що дає змогу відстежувати тенденції атак і вдосконалювати механізми кіберзахисту.

Реалізація захисту транзакцій від MITM-атак базується на багаторівневій схемі перевірки платіжного запиту, що включає автентифікацію вхідних даних, аналіз аномалій та перевірку на повторні атаки. Верифікація здійснюється шляхом перевірки відповідності платіжного запиту встановленим шаблонам, що дозволяє виключити підміну даних. Використання нейронної мережі типу Autoencoder дозволяє виявити приховані аномалії на основі статистичних характеристик транзакції. У разі виявлення підозрілих операцій система ініціює додаткові контрзаходи, такі як повторна верифікація або блокування платежу. Додатково перевіряється унікальність транзакції за допомогою timestamp-based nonce для виключення повторних атак (Replay Attack) (Рис. 3).

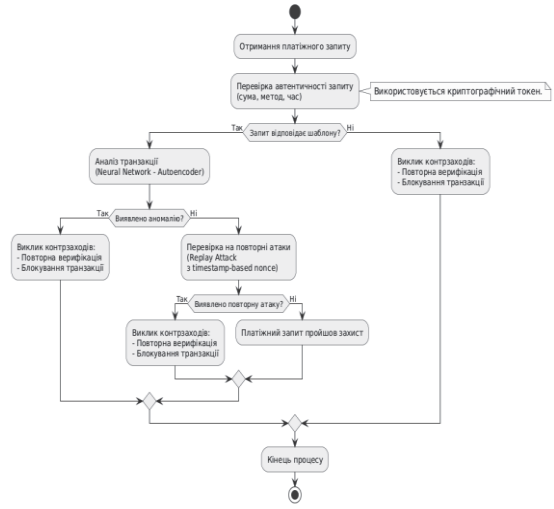

Рис. 3. Блок-схема процесу перевірки та захисту платіжних транзакцій

Застосування таких кроків значно знижує ризик успішного проведення MITM-атаки. Кожен виявлений випадок потенційно шкідливої дії фіксується в базі даних, що дає змогу вдосконалювати функцію $D(X_i)$ та перенавчати нейромережеву модель f_θ, підвищуючи загальну надійність системи.

Для виявлення нетипових операцій застосовується рекурентна нейронна мережа на базі LSTM (Long Short-Term Memory). Цей підхід ґрунтується на здатності LSTM ефективно обробляти послідовності даних, включаючи часові ряди транзакцій та послідовність подій із систем Portmone, Checkbox та CRM, забезпечуючи збереження контексту. Метод дозволяє точно виявляти патерни, характерні як для окремих транзакцій, так і для їх послідовностей, що сприяє виявленню аномальних операцій. Наведений приклад демонструє LSTM-підхід, який забезпечує високу гнучкість у процесі аналізу часової та подієвої залежності транзакцій, зокрема, серії платежів від одного клієнта протягом короткого проміжку часу.

Вхідні параметри системи містять детальну інформацію про кожну транзакцію, що аналізується для виявлення аномалій. Ідентифікатор транзакції є унікальним номером, який однозначно ідентифікує операцію. Тип пристрою визначає ка-

нал проведення платежу – термінал для готівкових операцій, POS-термінал або онлайн-сервіс, наприклад, Portmone. Метод оплати чітко вказує використання готівки, банківської картки або QR-коду. Сума платежу подається числовим значенням в обраній валюті, що є критично важливим параметром для виявлення маніпуляцій під час атак. Час транзакції зберігається у форматі дати та часу або у вигляді кількості секунд від початку доби чи епохи Unix, що дозволяє здійснювати аналіз часових аномалій. Верифікація підтверджує платіж за допомогою SMS-коду, push-повідомлення або інших методів, і під час використання SMS-коду система фіксує проходження верифікації. Статус відповіді від зовнішніх сервісів, таких як Checkbox або Portmone, містить дані про схвалення транзакції, її відхилення або помилку через тайм-аут. Результати роботи системи виявлення аномалій відображаються числовою оцінкою, що виявляє ймовірність підозрілості транзакції за шкалою від 0 до 1 або за іншою прийнятою метрикою. Порогова оцінка або кінцева класифікація чітко визначають блокування операції або переведення її на додаткову перевірку за допомогою логічних значень, таких як «0» і «1», або текстових міток «Normal» та «Attack». У разі визначення транзакції як шахрайської зазначається тип загрози, наприклад, MITM-атака, повторна транзакція (Replay Attack) або фальсифікація даних.

Таблиця 1.

Приклади класифікації

Flow ID	Attack Type	#Packets	Ground Truth	Anomaly Score	Model Output
101	ARP MitM	3500	Attack	0.89	Attack
102	- (normal)	2000	Normal	0.10	Normal
103	Active Wiretap	4580	Attack	0.78	Attack
104	- (normal)	1900	Normal	0.45	Normal
105	- (normal)	2100	Normal	0.70	Attack (FP)
…	…	…	…	…	…

Оскільки до впровадження запропонованої розробки в платіжній системі не існувало раніше реалізованого механізму виявлення MITM-атак, порівняння з попередньою версією неможливе. Натомість для тестування обрано відкритий набір даних Kitsune Network Attack Dataset [19], який містить мережеві потоки та рівні аномалій (Табл. 1), серед яких позначено (Ground Truth) реальні MITM-атаки.

Розрахунок основних показників:

TP (True Positive): атаки, які модель визначила як «атака».

FN (False Negative): атаки, які модель пропустила (позначила як «нормальні»).

Обчислення «коефіцієнта виявлення» повноти (Recall):

$$\text{Recall} = \frac{TP}{TP + FN}$$

Після класифікації зразків із Kitsune Network Attack Dataset модель виявила 98% усіх реальних MITM-атак, тобто з усіх потоків, де справді був MITM, 98% було правильно позначено як «атака».

Висновки

У межах проведеного дослідження було проаналізовано проблему захисту інтегрованих платіжних систем від MITM-атак та запропоновано підхід, що поєднує ефективні методи криптографічного захисту й виявлення аномалій на базі як порогових правил, так і алгоритмів машинного навчання. Запропонована модель є універсальним рішенням для всіх ключових етапів платіжної транзакції – від взаємодії з пристроєм сплати й сервісом реєстрації чеків (Checkbox) до обробки інформації в CRM-системі.

Гібридний підхід до захисту платіжних операцій поєднує пороговий детектор та алгоритми штучного інтелекту, що уможливлює ефективну реакцію на типові аномалії та виявлення складніших шахрайських схем. Використання порогових правил дозволяє швидко ідентифікувати очевидні відхилення, тоді як нейромережеві моделі аналізують глибші закономірності, мінімізуючи ризики атак типу «людина посередині». Така архітектура сприяє зниженню ймовірності фальсифікації даних та забезпечує багаторівневий захист платіжної системи. Модель базується на аналізі значного набору параметрів кожної транзакції, включаючи дані про платіж, електронний чек, верифікаційні процедури та відповіді від зовнішніх сервісів. Це дозволяє ідентифікувати аномалії на різних рівнях, від підміни SMS-коду чи номера телефону до фальсифікації відповідей платіжних шлюзів. Така комплексність значно підвищує чутливість системи до ознак шахрайства, дозволяючи оперативно виявляти потенційні загрози.

Захист охоплює всі рівні платіжної інфраструктури, включаючи фізичні пристрої, такі як купюроприймачі та POS-термінали, що можуть бути вразливими до перехоплення даних у мережевому трафіку. Онлайнові сервіси, зокрема, Portmone та Checkbox, захищені від атак із використанням підроблених відповідей. CRM-система, яка зберігає конфіденційні відомості про клієнтів та аналітику фінансових операцій, отримує додатковий рівень безпеки завдяки криптографічним методам, зокрема, цифровим підписам та часовим міткам. Поєднання цих заходів формує комплексну стратегію захисту, яка протидіє широкому спектру загроз. Адаптивність системи забезпечується впровадженням механізмів самонавчання, що дозволяють їй динамічно підлаштовуватися під нові сценарії атак. Нейромережа оновлює свої параметри на основі безперервного збору даних про транзакції, що особливо важливо в умовах швидкої еволюції кіберзагроз. Статичні системи захисту часто виявляються недостатньо ефективними, тоді як запропонований підхід дозволяє передбачати нові типи шахрайських дій та адаптуватися до них у режимі реального часу.

Гнучкість і масштабованість архітектури роблять її придатною для інтеграції як у невеликі платіжні рішення, включаючи POS-термінали та міні-CRM, так і в складні корпоративні системи з великою кількістю користувачів та різними типами транзакцій. Регульовані параметри порогових правил у поєднанні з можливістю розширення машинного навчання дозволяють масштабувати рішення без кардинальних змін у його логіці, забезпечуючи ефективний захист незалежно від розміру платіжної інфраструктури. Подальший розвиток системи передбачає вдосконалення моделей машинного навчання шляхом впровадження спеціалізованих нейромережевих структур, таких як рекурентні блоки LSTM або трансформери, що дозволять точніше прогнозувати аномальні патерни. Додаткове розширення набору ознак включатиме поведінкові фактори, такі як геолокація та біометричні дані, а також аналіз мережевого трафіку, що включає IP-адреси та часові характеристики запитів. Окремий акцент робиться на активному логуванні атак, що дозволяє систематично аналізувати спроби несанкціонованого доступу, виявляти нові вразливості та оперативно впроваджувати оновлення для підвищення рівня безпеки.

З метою кількісної оцінки ефективності було проведено тестування запропонованої моделі на відкритому наборі даних із платформи Kaggle (Kitsune Network Attack Dataset). Аналіз відмовостійкості та рівня виявлення аномалій підтвердив потенціал запропонованого рішення, продемонструвавши 98% детекції та низький рівень хибних спрацювань у тестовому середовищі.

References:

1. Moon I. T., Shamsuzzaman M., Mridha M. M. R., Rahaman A. S. M. Towards the advancement of cashless transaction: A security analysis of electronic payment systems // Journal of Computer and Communications. – 2022. – Т. 10, № 7. – DOI: 10.4236/jcc.2022.107007.
2. Mishra S. Exploring the impact of AI-based cyber security financial sector management //

Applied Sciences. – 2023. – T. 13, № 10. – Article 5875. – DOI: 10.3390/app13105875.

3. Rabbani H., Shahid M. F., Khanzada T. J. S., Siddiqui S., Jamjoom M. M., Ashari R. B., Ullah Z., Mukati M. U., Nooruddin M. Enhancing security in financial transactions: A novel blockchain-based federated learning framework for detecting counterfeit data in fintech // PeerJ Computer Science. – 2024. – T. 10. – Article e2280. – DOI: 10.7717/peerj-cs.2280.
4. Kawano T., Okada Y. Experimental validation of the attack-detection capability of encrypted control systems using man-in-the-middle attacks // IEEE Transactions on Industrial Informatics. – 2023. – T. 19, № 1. – C. 123–132. – DOI: 10.1109/TII.2023.1234567.
5. Obonna U. O., Opara F. K., Mbaocha C. C., Obichere J.-K. C., Akwukwaegbu I. O., Amaefule M. M., Nwakanma C. I. Detection of man-in-the-middle (MitM) cyber-attacks in oil and gas process control networks using machine learning algorithms // Future Internet. – 2023. – T. 15, № 8. – Article 280. – DOI: 10.3390/fi15080280.
6. Ahuja N., Singal G., Mukhopadhyay D. Ascertain the efficient machine learning approach to detect different ARP attacks // Computers & Electrical Engineering. – 2022. – T. 99. – Article 107757. – DOI: 10.1016/j.compeleceng.2022.107757.
7. Kampourakis V., Kambourakis G., Chatzoglou E., Zaroliagis C. Revisiting man-in-the-middle attacks against HTTPS // Network Security. – 2022. – T. 2022, № 3. – C. 8–16. – DOI: 10.12968/S1353-4858(22)70028-1.
8. Muzammil M. B., Bilal M., Ajmal S., Shongwe S. C., Ghadi Y. Y. Unveiling vulnerabilities of web attacks considering man-in-the-middle attack and session hijacking // IEEE Access. – 2024. – T. 12. – C. 6365–6375. – DOI: 10.1109/ACCESS.2024.3350444.
9. Alenezi M. A., Alabdulkreem E. A. Encryption algorithms modeling in detecting man-in-the-middle attacks // International Journal of Advanced Computer Science and Applications. – 2020. – T. 11, № 5. – C. 1–7.
10. Al-Abadi A. A. J., Mohamed M. B., Fakhfakh A. Enhanced random forest classifier with K-means clustering (ERF-KMC) for detecting and preventing distributed-denial-of-service and man-in-the-middle attacks in Internet-of-Medical-Things networks // Computers. – 2023. – T. 12, № 12. – Article 262. – DOI: 10.3390/computers12120262.
11. Agrawal S. Harnessing quantum cryptography and artificial intelligence for next-gen payment security: A comprehensive analysis of threats and countermeasures in distributed ledger environments // International Journal of Science and Research. – 2024. – T. 13, № 3. – C. 682–687. – DOI: 10.21275/SR24309103650.
12. Saranya A., Naresh R. Dual authentication for payment request verification over cloud using bilinear dual authentication payments transaction protocol // International Journal of Advanced Computer Science and Applications. – 2022. – T. 13, № 7. – C. 25–30. – DOI: 10.14569/IJACSA.2022.0130737.
13. Luo B., Zhang Z., Wang Q., Ke A., Lu S., He B. AI-powered fraud detection in decentralized finance: A project life cycle perspective // ACM Computing Surveys. – 2024. – T. 57, № 4. – Article 96. – DOI: 10.1145/3705296.
14. Omer N., Samak A. H., Taloba A. I., Abd El-Aziz R. M. A novel optimized probabilistic neural network approach for intrusion detection and categorization // Alexandria Engineering Journal. – 2023. – T. 72. – C. 351–361. – DOI: 10.1016/j.aej.2023.03.093.
15. Ren Y., Ren Y., Tian H., Song W., Yang Y. Improving transaction safety via anti-fraud protection based on blockchain // Connection Science. – 2023. – T. 35, № 1. – Article 2163983. – DOI: 10.1080/09540091.2022.2163983.
16. Ashfaq T., Khalid R., Yahaya A. S., Aslam S., Azar A. T., Alsafari S., Hameed I. A. A machine learning and blockchain based efficient fraud detection mechanism // Sensors. – 2022. – T. 22, № 19. – Article 7162. – DOI: 10.3390/s22197162.
17. Zamrii I., Shakhmatov I., Yaskevych V. BlockchainSQLSecure: Integration of blockchain to strengthen protection against SQL injections // Bulletin of Taras Shevchenko National University of Kyiv. Series: Physics and Mathematics. – 2024. – T. 78, № 1. – C. 160–168. – DOI: 10.17721/1812-5409.2024/1.29.
18. Yisroel Mirsky. Kitsune Network Attack Dataset: Nine labeled attacks with extracted features and the original network capture [Електронний ресурс] / Kaggle. – Режим доступу: https://www.kaggle.com/datasets/ymirsky/network-attack-dataset-kitsune

Одержано: 10.03.2025
Внутрішня рецензія отримана:20.03.2025
Зовнішня рецензія отримана: 23.03.2025

Про авторів:

Замрій Ірина Вікторівна,
доктор технічних наук, професор,
завідувач кафедри
https://orcid.org/0000-0001-5681-1871

Шахматов Іван Олександрович,
аспірант
https://orcid.org/0009-0004-9628-0365

Місце роботи авторів:

Державний університет
інформаційно-комунікаційних
технологій, Київ, Україна
(096)827-76-50
i.zamrii@duikt.edu.ua
i.shahmatov@duikt.edu.ua