КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.215228
УДК 004.056:338.46

Хавікова Юлія Ігорівна
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0003-1017-3602
y.khavikova@knute.edu.ua

ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ПОСЛУГАХ

Анотація. У публікації досліджується проблема захисту інформації в контексті швидкого розвитку електронних послуг і зростаючих вимог до їх безпеки. Зазначено, що інтенсивне впровадження сучасних технологій у фінансові та інші інформаційно-комунікаційні системи призводить до збільшення обсягів електронних транзакцій та інформаційного обміну, що активізує потребу у високоефективних методах захисту. Основний акцент робиться на важливості використання багатофакторної автентифікації та сучасних криптографічних методів для запобігання несанкціонованому доступу до конфіденційної інформації та маніпуляцій з електронними транзакціями. Дослідження відзначає, що успішність сучасних інформаційно-комунікаційних систем значною мірою залежить від здатності їхніх компонентів ефективно захищати дані та забезпечувати надійність операцій для користувачів. Стаття досліджує сучасні підходи до захисту інформації при наданні електронних послуг, акцентуючи увагу на інноваційних рішеннях та технологіях, спрямованих на забезпечення конфіденційності, цілісності та доступності даних. Розглянуті аспекти включають впровадження машинного навчання для виявлення загроз, використання біометричних методів для автентифікації та застосування блокчейн-технологій для забезпечення безпеки транзакцій. Актуальність дослідження підкріплюється зростаючими вимогами до захисту персональних даних і фінансових операцій у віртуальному просторі, що вимагає постійного удосконалення інформаційної безпеки та впровадження передових заходів захисту.

Ключові слова: захист інформації; електронні послуги; електронні транзакції; багатофакторна автентифікація; криптографічні методи; безпека даних; інформаційно-комунікаційні системи; конфіденційність інформації.

ВСТУП

Аналізуючи та обробляючи безпекові аспекти електронних послуг, неможливо оминути актуальну проблему захисту інформації в цифрову епоху. Швидкий розвиток електронних технологій і зростання обсягів електронних транзакцій вимагають надзвичайної уваги до забезпечення конфіденційності та цілісності персональних даних користувачів. В умовах, коли електронні платіжні системи стають неодмінною складовою фінансового життя, важливо забезпечити надійний захист від кіберзагроз і злочинних втручань. Стаття присвячена аналізу сучасних методів і технологій захисту інформації, що використовуються в електронних послугах. Розглядаються виклики, які виникають у контексті збільшення обсягів електронних транзакцій і розширення сфери застосування цифрових сервісів. Особлива увага приділяється новітнім підходам у кібербезпеці, таким як багатофакторна аутентифікація, криптографічне шифрування та використання штучного інтелекту для виявлення та запобігання кіберзагрозам.

Постановка проблеми. Проблематика підходів до захисту інформації в електронних послугах, зокрема у сфері електронних платіжних систем та інших цифрових сервісів, в контексті стрімкого розвитку цифрових технологій і зростання

кількості електронних транзакцій, полягає в необхідності забезпечення високого рівня кібербезпеки та захисту конфіденційної інформації користувачів. Проблема виникає через недостатню захищеність багатьох сучасних електронних платіжних систем і сервісів від кібератак і зловживань, що може призвести до крадіжок фінансових даних, несанкціонованого доступу до особистої інформації та інших серйозних наслідків для користувачів та компаній. Проблематика підходів до захисту полягає в тому, що існуючі методи не завжди успішно впораються зі сучасними загрозами, такими як атаки з використанням шкідливих програм, соціального інжинірингу та використання застарілих методів аутентифікації та шифрування, що збільшує ризик несанкціонованого доступу, зокрема через використання криптографічних атак. Деякі системи використовують застарілі методи аутентифікації та шифрування, що збільшує ризик несанкціонованого доступу. Для вирішення цих проблем необхідно розвивати новітні технології кібербезпеки, такі як багатофакторна аутентифікація, аналіз поведінки користувачів, використання блокчейн-технологій та штучного інтелекту для автоматизації виявлення та реагування на загрози в реальному часі.

Аналіз останніх досліджень і публікацій. У роботах [1] – [4] висвітлюються проблеми та виклики, пов’язані із захистом інформації в електронних послугах. Актуальні дослідження зосереджуються на дослідженні сучасних методів захисту, ідентифікації та автентифікації в електронних платіжних системах та цифрових сервісах. Однією з головних проблем, яка висвітлюється у дослідженнях, є недостатній рівень безпеки інформації в електронних платіжних системах. Виявлено, що багато систем використовують застарілі методи шифрування та аутентифікації, що робить їх уразливими перед сучасними кіберзагрозами. Наприклад, атаки з використанням соціального інжинірингу або шкідливих програм можуть легко обійти захист, який базується на старих технологіях. Дослідження також акцентують увагу на необхідності впровадження новітніх технологій кібербезпеки, таких як багатофакторна аутентифікація, аналіз поведінки користувачів та інтелектуальні системи для виявлення аномальних активностей. Впровадження таких технологій дозволяє покращити відповідь на загрози та забезпечити високий рівень захисту конфіденційної інформації в реальному часі [2] – [6], [9]. Крім того, дослідження вказують на важливість вдосконалення правового регулювання та стандартів у сфері кібербезпеки, що дозволить зменшити вразливість інформаційно-комунікаційних систем перед кібератаками та забезпечити безпеку та довіру користувачів до електронних послуг. Останні дослідження підкреслюють необхідність комплексного підходу до захисту інформації в електронних сервісах, що включає як технічні інновації, так і вдосконалення правових механізмів, що регулюють цю сферу.

Мета статті. Метою дослідження є аналіз сучасних підходів до захисту інформації в електронних послугах з урахуванням використання криптографічних методів, штучного інтелекту для виявлення кіберзагроз, інтеграції багатофакторної автентифікації та біометричних технологій у системах безпеки, спрямованих на підвищення рівня кібербезпеки та надійності електронних транзакцій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Грошові відносини з використанням електронних засобів наразі переживають період бурхливого розвитку, що обумовлено активним впровадженням новітніх електронних пристроїв та методів обміну інформацією, які передбачають наявність

платних інформаційних та інших залежних від інформації послуг [1] – [3], [5]. Фінансові організації стабільно збільшують ринок електронних платіжних засобів, проте захист інформації в електронних послугах, зокрема захист користувацьких платіжних інструментів (КПІ) в електронних платіжно-грошових системах (ЕПГС), залишається на низькому рівні і покладається в основному на користувачів, що зумовлює часті випадки крадіжок електронних засобів.

У зв'язку з цим, виникає нагальна потреба у створенні універсального КПІ, здатного переміщати грошову вартість з високою швидкістю (бажано миттєво) та при цьому забезпечувати максимальний, в ідеалі непереборний, захист як від підробки, так і від викрадення одиниць вартості [1], [4] – [7]. Важливим аспектом є те, щоб захист інформації та КПІ здійснювався не особисто користувачем, а автоматично, що дозволить залучити до електронного товарообміну не лише професіоналів комп'ютерної техніки, але й осіб, які не мають спеціальних технічних знань і не вміють самостійно організувати захист своїх електронних фінансів. Високою залишається також вартість самого переміщення, адже враховуючи, що в мережі Інтернет застосовуються одні платіжні інструменти, а в повсякденному житті інші, слід враховувати і вартість конверсії. Більше того, операція конверсії може зайняти деякий час і часто слабо піддається автоматизації.

Вищезазначене, безсумнівно, гальмує розвиток інформаційної економіки, тому сучасні тенденції включають розвиток блокчейн-технологій та впровадження криптовалют, які пропонують потенційно високий рівень безпеки та швидкість транзакцій. Крім того, розвиток штучного інтелекту та машинного навчання може значно підвищити рівень автоматизації та безпеки електронних послуг, забезпечуючи надійний захист інформації в сучасних електронних системах.

Сучасні методи захисту інформації включають використання багатофакторної автентифікації, біометричних даних та систем на основі машинного навчання, які виявляють та запобігають підозрілим діям у реальному часі, що критично важливо для підтримання довіри користувачів до електронних послуг [2], [6]. Крім того, впровадження криптографічних методів шифрування забезпечує високий рівень захисту даних під час передачі та зберігання.

Інтеграція штучного інтелекту в системи безпеки дозволяє автоматично ідентифікувати та реагувати на загрози, мінімізуючи людський фактор і зменшуючи ймовірність успішних кібератак. Тому інновації у сфері захисту інформації є невід'ємною частиною розвитку електронних послуг, сприяючи побудові безпечного та ефективного цифрового середовища для користувачів і бізнесів.

Таким чином, актуальність теми полягає у розвитку електронних сервісів представлення товарів, розширенні ринку інформаційних товарів та інформаційної економіки в цілому; зростанні вартості використання паперових грошових коштів у міру становлення інформаційного суспільства; слабкій переміщуваності та ліквідності існуючих електронних еквівалентів грошей; відсутності електронних платіжно-грошових систем (ЕПГС), що мають функціональність готівкових грошей, і потребі в таких системах, які дозволяють проводити фінансові операції між платником та отримувачем без посередників банківської системи.

Актуальність також обумовлена відсутністю електронних користувацьких платіжних інструментів (КПІ), які забезпечують електронні взаєморозрахунки між учасниками в режимі реального часу з використанням електронних аналогів грошей без залучення будь-яких центрів авторизації, крім учасників розрахунків індивідуальних електронних грошових модулів (ЕГМ). Ці модулі, подібно до паперових грошових коштів, захищені декількома ступенями захисту, і їх підробка можлива лише при

зламуванні всіх цих ступенів. Необхідність забезпечення повернення грошових коштів власнику ЕГМ у разі його втрати або крадіжки, а також потреба у забезпеченні повернення коштів власнику у випадку виходу з ладу його КПІ (ЕГМ), є ще однією важливою складовою. Актуальність зазначеної теми підкріплюється розвитком сучасних технологій захисту інформації, включаючи блокчейн-технології та впровадження криптовалют, які пропонують потенційно високий рівень безпеки та швидкість транзакцій [1] – [2], [5] – [7]. Крім того, застосування штучного інтелекту та машинного навчання може значно підвищити рівень автоматизації та безпеки електронних послуг, забезпечуючи надійний захист даних користувачів.

Сучасні методи захисту інформації включають використання багатофакторної автентифікації, біометричних даних та систем на основі машинного навчання, які здатні виявляти та запобігати підозрілим діям у реальному часі, що є критично важливим для підтримання довіри користувачів до електронних послуг. Впровадження криптографічних методів шифрування забезпечує високий рівень захисту даних під час їх передачі та зберігання [6], [8]. Інтеграція штучного інтелекту в системи безпеки дозволяє автоматично ідентифікувати та реагувати на загрози, мінімізуючи людський фактор і зменшуючи ймовірність успішних кібератак.

Таким чином, інновації у сфері захисту інформації є невід'ємною частиною розвитку електронних послуг, сприяючи побудові безпечного та ефективного цифрового середовища для користувачів і бізнесів.

Аналіз існуючих форм, методів та систем електронних грошових розрахунків показав, що на сьогодні не існує електронних систем управління грошовим обігом, які б гарантували стабільне функціонування. Порівняльний аналіз електронних платіжно-грошових систем (ЕПГС) виявив, що сучасні системи мають характеристики, які позитивно відрізняють їх від паперових грошових коштів, однак вони також мають ряд недоліків, таких як залежність від постійних каналів зв'язку, відсутність гарантованого захисту робочих місць клієнтів або користувацьких платіжних інструментів (КПІ), висока вартість таких систем та відсутність можливості повернення втрачених грошових коштів.

Актуальність створення таких систем підкріплюється розвитком технологій захисту інформації в електронних послугах, що стає критично важливим у контексті зростаючої кількості електронних транзакцій та необхідності забезпечення безпеки даних користувачів. Використання багатофакторної автентифікації, криптографічних методів шифрування, а також систем на основі штучного інтелекту дозволяє значно підвищити рівень захисту електронних фінансових операцій та мінімізувати ризики кібератак [4], [7].

З розвитком блокчейн-технологій, які забезпечують високий рівень прозорості та безпеки транзакцій, стає можливим створення більш досконалих електронних платіжних систем, які не лише гарантують високу швидкість і надійність переказів, але й забезпечують надійний захист інформації користувачів. Такі технології, як штучний інтелект та машинне навчання, можуть бути інтегровані в системи безпеки для автоматичного виявлення та реагування на потенційні загрози в режимі реального часу, що є критично важливим для підтримання довіри користувачів до електронних послуг [5].

Таким чином, інновації у сфері захисту інформації є невід'ємною частиною розвитку електронних послуг, сприяючи побудові безпечного та ефективного цифрового середовища для користувачів і бізнесів.

Електронна платіжна система (ЕПС), призначена для виконання фінансових операцій з використанням електронних грошових модулів (ЕГМ), включає центральний

ISSN 2663 - 4023

елемент (ЦЕ) та сукупність ЕГМ. Основу захисту грошових транзакцій складає використання електронного підпису, а також наявність декількох мікропроцесорних пристроїв з захистом від зломів, що працюють паралельно в одному користувацькому платіжному інструменті. Метод розподілу ключової інформації та метод передачі повідомлень створені з метою виключити можливість впровадження і використання фальшивих повідомлень, а також повторного використання повідомлень, які раніше вже були оброблені [1], [3], [6] – [7]. У функції ЦЕ входять емісія ЕГМ та електронної готівки, генерація, супровід і зберігання ключів шифрування та електронних підписів (ЕП) ЦЕ та ЕГМ, а також підтримка стійкості системи до злому та управління ситуаціями, пов'язаними з виходом з ладу ЕГМ. ЦЕ включає електронну базу відкритих компонентів ЕП, емітованих ЕГМ, та ЕП ЦЕ. ЕГМ є пристроями, що зберігають свою грошову вартість, мають унікальні ідентифікатори і призначені для взаємодії та проведення платежів зі зміною своєї внутрішньої вартості безпосередньо один з одним (без участі ЦЕ), а також за участю ЦЕ. Організація запропонованої електронної грошової системи представлена на рис. 1 та 2.

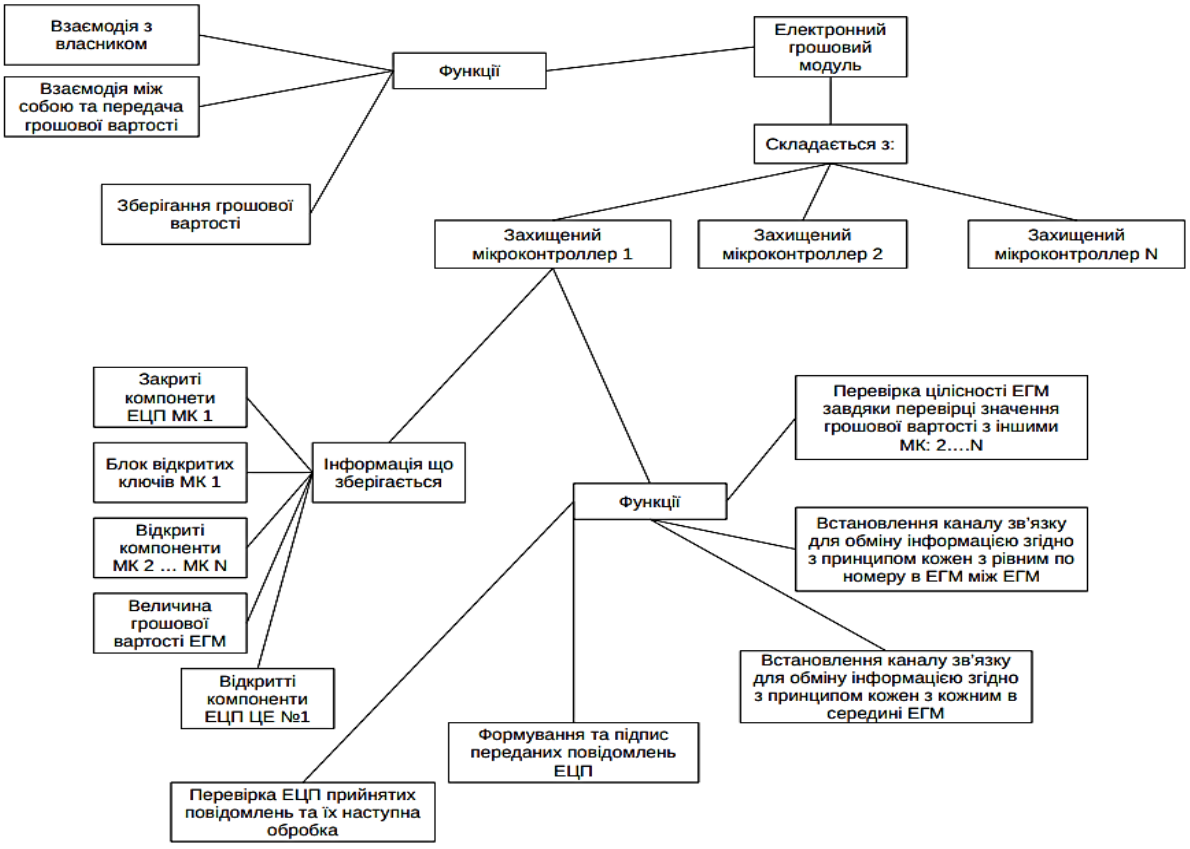

Рис. 1. Електронний грошовий модуль ЕПС
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

ISSN 2663 - 4023

Рис. 2. Центр емісії ЕПС
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

У контексті захисту інформації в електронних послугах, сучасні технології шифрування та управління ключами забезпечують надійний захист персональних даних та фінансових транзакцій [5], [8], [9]. Використання блокчейн-технологій може значно підвищити безпеку систем, забезпечуючи прозорість та непідробність транзакцій. Інтеграція штучного інтелекту дозволяє автоматизувати виявлення та відповідь на потенційні загрози кібербезпеки в режимі реального часу, що є критично важливим для підтримання безпеки електронних фінансових операцій та збільшення довіри користувачів до цифрових платіжних систем. Електронні грошові модулі (ЕГМ), що складаються з двох або більше електронних пристроїв — мікроконтролерів (МК), захищених від несанкціонованого доступу на читання та запис інформації, представляють собою складні системи, спроектовані для забезпечення безпеки та надійності фінансових транзакцій. Кожен МК має унікальний внутрішній номер в межах кожного ЕГМ, що дозволяє однозначно ідентифікувати його в системі. Для забезпечення безпеки операцій, кожен МК зберігає важливі дані, такі як грошова вартість, відкриті ключі ЕП, унікальні закриті ключі ЕП та інші компоненти, які необхідні для підтвердження автентичності та цілісності транзакцій.

Мікроконтролери в ЕГМ можуть встановлювати канали зв’язку та обмінюватися інформацією як всередині одного модуля, так і між різними модулями з однаковими номерами МК. При обміні повідомленнями між МК ЕГМ, кожне повідомлення підписується ЕП відправника і перевіряється на відкритих компонентах ЕП у приймаючого МК. Тільки після успішної перевірки ЕП повідомлення приймаються для подальшої обробки. Це забезпечує високий рівень безпеки та надійності фінансових операцій, зменшуючи ризики несанкціонованого доступу та маніпуляцій з даними.

За сучасних умов актуальність захисту інформації в електронних послугах підкріплюється використанням передових технологій криптографії та механізмів перевірки автентичності, що дозволяє ефективно запобігати кібератакам та забезпечувати безпеку фінансових операцій.

Спосіб передачі повідомлень між електронними грошовими модулями (ЕГМ) є ключовим елементом забезпечення безпеки в електронних платіжних системах (ЕПС). Цей метод передбачає обмін відкритими компонентами електронного підпису (ЕП) та ідентифікаційними даними, які підписані ЕЦП центрального елемента (ЦЕ). Після цього

ISSN 2663 - 4023

мікроконтролери обох взаємодіючих ЕГМ використовують отримані відкриті компоненти для перевірки цілісності вхідних повідомлень під час поточного сеансу. Це дозволяє забезпечити високий рівень автентифікації і гарантує, що всі передані дані є достовірними і не були змінені під час передачі [6], [9] – [10]. Для додаткового підвищення безпеки, сучасні ЕПС використовують багатофакторну аутентифікацію, яка включає не лише ЕП, а й біометричні дані користувача, такі як відбитки пальців або розпізнавання обличчя. Це робить процес авторизації більш надійним і менш вразливим до шахрайства. Крім того, метод розподілу ключової інформації та метод передачі повідомлень створені з метою виключити можливість впровадження і використання фальшивих повідомлень, а також повторного використання повідомлень, які раніше вже були оброблені. Ці методи допомагають запобігти атакам типу «людина посередині» (Man-in-the-Middle) та іншим формам перехоплення даних.

Метод переміщення грошових коштів між ЕГМ забезпечує можливість переміщення грошових коштів без зв’язку з централізованою базою даних або авторизуючим центром. Це досягається за рахунок використання децентралізованих технологій, таких як блокчейн, що дозволяють проводити транзакції безпосередньо між учасниками мережі, забезпечуючи при цьому високу прозорість і безпеку.

Спосіб захисту від зломів ЕГМ полягає у поступовому обміні ЕГМ або їх складових мікроконтролерів. Цей спосіб дозволяє проводити обмін не одночасно для всіх учасників, а поетапно, що виключає ймовірність зупинки проведення платежів в ЕПС і водночас не знижує захищеність системи [2], [4], [9], [10]. Такий підхід також дозволяє виявляти і локалізувати можливі вразливості на ранніх етапах, запобігаючи їх поширенню в системі. На рис. 3 і 4 представлена структура основних повідомлень, які циркулюють між ЕГМ: на рис. 3 показано ідентифікаційний блок з відкритими ключами МК ЕГМ та ідентифікаційною інформацією, на рис. 4 — фінансовий блок, за допомогою якого здійснюється передача грошової вартості від одного ЕГМ до іншого.

Рис. 3. Блок відкритих ключів
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

ISSN 2663 - 4023

Рис. 4. Фінансовий блок
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

На прикладі методу передачі повідомлень, як показано на рис. 5 і 6, демонструється сучасний підхід до захисту передаваних даних. Перед тим як відправити повідомлення, відправник ЕГМ здійснює електронний підпис (ЕП) і проводить внутрішню перевірку повідомлення між своїми мікроконтролерами. Якщо результат перевірки позитивний, повідомлення приймається до обробки. Додатково він відправляє свої відкриті компоненти ЕП на ЕГМ отримувача. ЕГМ отримувач спочатку приймає ці відкриті компоненти, перевіряє їх ЕП ЦЕ і реєструє ключі взаємодіючої ЕГМ. Потім отримує саме повідомлення, перевіряє його ЕП з використанням зареєстрованих відкритих компонентів ЕП і проводить внутрішню перевірку повідомлення між своїми мікроконтролерами. Якщо ця перевірка також є позитивною, то повідомлення приймається для подальшої обробки.

Спосіб повернення втрачених або викрадених грошових коштів дозволяє, використовуючи проміжні ЕГМ, передавати інформацію про втрачений і заблокований баланс у ЦЕ та, як наслідок, повертати кошти власнику. Пошкоджену паперову купюру можна обміняти на нову, але електронні гроші при пошкодженні платіжного інструменту можуть бути втрачені безповоротно. Завдяки запропонованій організації ЕГМ, інформація дублюється у декількох його мікроконтролерних блоках. Це дозволяє уникнути втрати даних при пошкодженні одного з мікроконтролерів ЕГМ і забезпечує безперервність роботи системи та подальше повернення коштів. Програмна частина електронної грошової системи складається з програми управління мікроконтролером ЕГМ та програми управління ЦЕ [6] – [8]. Програма управління мікроконтролером є основною одиницею в побудові ЕГМ і реалізує всі його функції. Програма ЦЕ призначена для організації емісії ЕГМ, а також для організації взаємодії з ними, відповідно до запропонованих принципів роботи.

ISSN 2663 - 4023

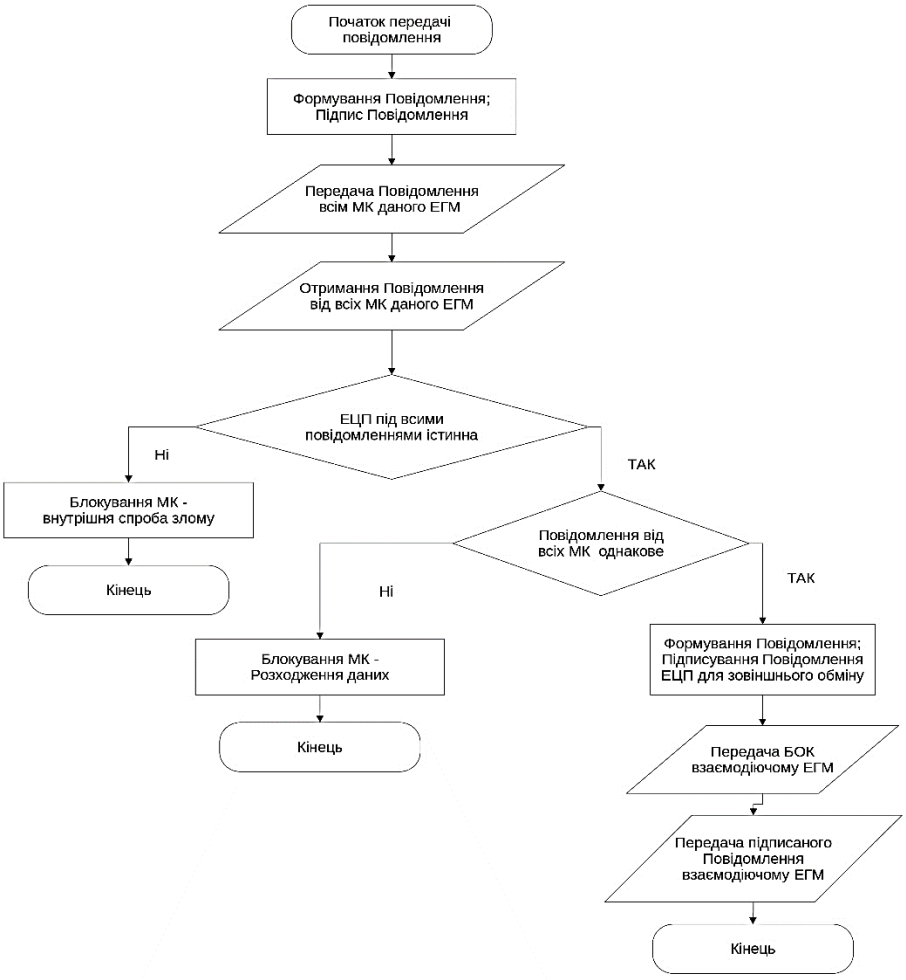

Рис. 5. Алгоритм передачі зовнішніх повідомлень на МК ЕГ
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Спосіб здійснення платежу, що базується на методі передачі повідомлень та використовує спеціальні інформаційні повідомлення для повної ідентифікації платежу, представлений на рис. 4, активно застосовується в сучасних електронних фінансових системах. Метод повернення втрачених фінансових коштів у електронній платіжній системі (ЕПС) забезпечує високу ступінь безпеки і надійності, що особливо важливо в умовах сучасних кіберзагроз [5], [7], [8], [10]. Згідно з цим методом, спроба розблокувати втрачений або викрадений електронний грошовий модуль (ЕГМ) призводить до формування основної частини збереженої вартості у вигляді коду інкасації. Цей код передається через систему ЕГМ до центрального елемента (ЦЕ), де він конвертується в суму на рахунку власника. Це дозволяє швидко і ефективно повертати кошти власникам, мінімізуючи ризики втрат.

Важливо зазначити, що метод переміщення повідомлень через ЕГМ в ЕПС має свої обмеження. Кожен викрадений ЕГМ може передати лише три коди інкасації: перші два коди передаються по ланцюжку, а наступні — по одному. Подальші коди інкасації не передаються між ЕГМ і можуть зберігатися тільки у ЦЕ. Це обмеження забезпечує додатковий рівень захисту, запобігаючи можливості масових атак на систему і забезпечуючи захист фінансових транзакцій. Окрім цього, технологія використання електронного цифрового підпису (ЕЦП) в електронних платіжних системах також

відіграє ключову роль у забезпеченні безпеки. Відкриті компоненти ЕЦП та ідентифікаційні дані, підписані ЕЦП ЦЕ, обмінюються між взаємодіючими ЕГМ. Після цього мікроконтролери обох ЕГМ використовують отримані відкриті компоненти для перевірки цілісності вхідних повідомлень під час поточного сеансу. Це гарантує, що всі передані дані є автентичними і не були змінені під час передачі, що забезпечує високий рівень захисту від можливих кіберзагроз [2], [5], [8] – [10].

Для додаткового підвищення рівня безпеки сучасні ЕПС інтегрують багатофакторну аутентифікацію, що включає не лише ЕЦП, а й біометричні дані користувача, такі як відбитки пальців або розпізнавання обличчя. Цей підхід робить процес авторизації більш надійним і менш вразливим до шахрайства, забезпечуючи максимальний захист фінансових даних користувачів.

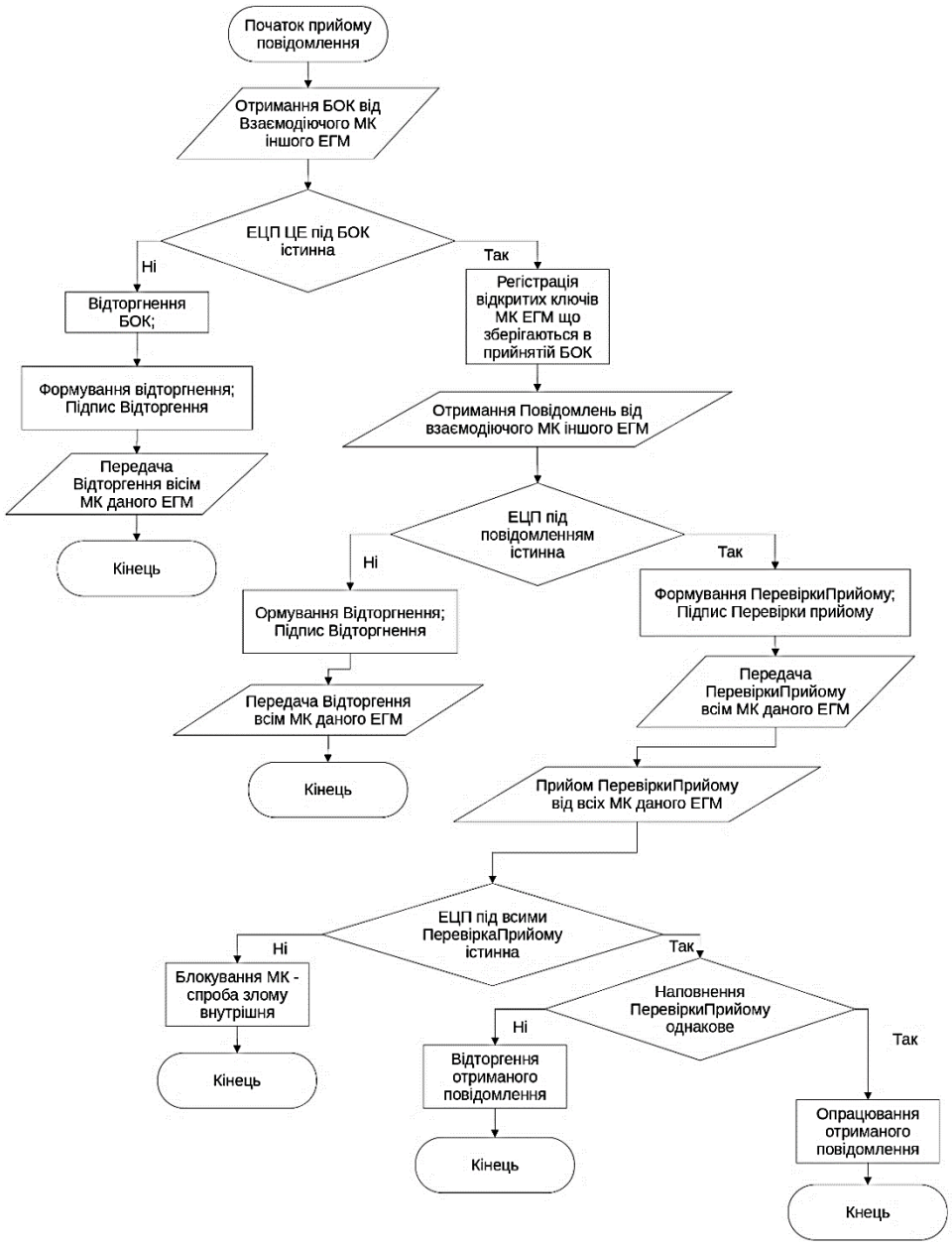

Рис. 6. Алгоритм прийому зовнішніх повідомлень на МК ЕГМ
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

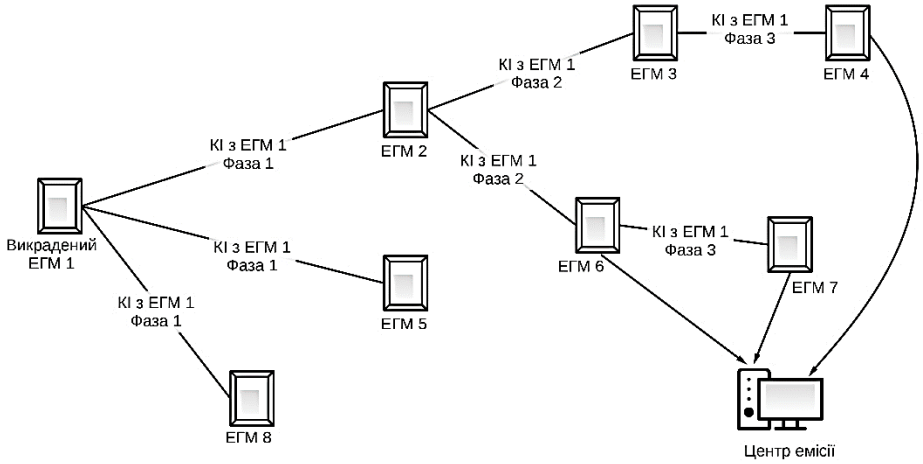

Рис. 7. Передача коду інкасації в центр емісії
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

На прикладі методу відшкодування коштів з несправних електронних грошових модулів (ЕГМ), де використовується надмірність збереженої інформації для визначення збереженої вартості на підставі даних, отриманих від працюючих мікроконтролерів несправного ЕГМ під час аналізу у центральному елементі (ЦЕ), демонструється ефективність інформаційного зв'язку між системними компонентами для відновлення фінансової цілісності [1] – [3], [8] – [10]. На основі програмної реалізації електронних грошових модулів (ЕГМ) і центру емісії (ЦЕ) реалізовані компоненти, що написані мовою програмування С++. Програма роботи мікроконтролера ЕГМ створена шляхом складання трьох копій програми, кожна з яких має власні дані та ключі електронних підписів (ЕП), тим самим формуючи ЕГМ. Отриманий екземпляр координує всі свої операції, підписує пакети даних ЕП та перевіряє їх коректність в прийнятій інформації. Під час обміну фінансовими блоками змінюється його грошова вартість. Реалізовані ЕГМ можуть використовувати різні формати ЕП як зовнішні підключувані модулі. Центр емісії реалізований як сукупність модифікованих програмних модулів мікроконтролера ЕГМ та бази даних ключової інформації про емітовані ЕГМ.

Технологія електронних грошей дозволяє досягти високого ступеня захисту від зломів платіжних інструментів. Основу захисту грошових транзакцій складає використання електронного цифрового підпису, а також наявність декількох мікропроцесорних пристроїв з захистом від зломів, що працюють паралельно в одному користувацькому платіжному інструменті. Метод розподілу ключової інформації та метод передачі повідомлень створені з метою виключити можливість впровадження і використання фальшивих повідомлень, а також повторного використання повідомлень, які раніше вже були оброблені. Сучасний метод переміщення грошових коштів полягає в забезпеченні можливості переміщення грошових коштів між електронними грошовими модулями (ЕГМ) без зв'язку з централізованою базою даних або авторизуючим центром. Спосіб захисту від зломів ЕГМ, що полягає у поступовому обміні ЕГМ або їх складових мікроконтролерів, дозволяє проводити обмін не одночасно для всіх учасників, а поетапно, що виключає ймовірність зупинки проведення платежів в електронній платіжній системі (ЕПС) і водночас не знижує захищеність системи [4] – [6], [10]. Методи повернення втрачених або викрадених грошових коштів дозволяють, використовуючи проміжні ЕГМ, передавати інформацію про втрачений і заблокований баланс у Центр емісії (ЦЕ) та, як наслідок, повертати кошти власнику. Пошкоджену

паперову купюру можна обміняти на нову, але електронні гроші при пошкодженні платіжного інструменту можуть бути втрачені безповоротно. Завдяки сучасній організації ЕГМ, інформація дублюється у декількох його мікроконтролерних блоках, що дозволяє уникнути втрати даних при пошкодженні одного з мікроконтролерів ЕГМ і забезпечує безперервність роботи системи та подальше повернення коштів. Програмна частина електронної грошової системи складається з програми управління мікроконтролером ЕГМ та програми управління Центром емісії [2], [7], [9], [10]. Програма управління мікроконтролером є основною одиницею в побудові ЕГМ і реалізує всі його функції. Програма ЦЕ призначена для організації емісії ЕГМ, а також для організації взаємодії з ними, відповідно до запропонованих принципів роботи.

Запропонована методика оцінки ефективності ЕПС як системи заміни паперових грошових коштів має високий потенціал у порівнянні з аналогами. Сучасні тенденції включають інтеграцію біометричних технологій, аналіз поведінки користувачів та впровадження штучного інтелекту для автоматизації процесів виявлення та усунення кіберзагроз в реальному часі, що значно підвищує рівень безпеки електронних платіжних систем.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Електронні грошові відносини перебувають у періоді активного розвитку, що вимагає постійного вдосконалення систем захисту інформації в електронних платіжних системах (ЕПГС). Недоліки у сучасних системах захисту, такі як низький рівень захисту користувацьких платіжних інструментів (КПІ), не лише обмежують розвиток електронних фінансових послуг, але й підносять питання щодо необхідності та ефективності застосування вже існуючих технологій. Важливою стає потреба у створенні універсальних КПІ, які забезпечать високу швидкість та надійний захист інформації, не вимагаючи від користувачів спеціалізованих технічних знань. Крім того, розвиток блокчейн-технологій, криптовалют і інтеграція штучного інтелекту мають потенціал значно підвищити безпеку та ефективність електронних фінансових транзакцій, створюючи нові можливості для інновацій у цій сфері.

Електронні платіжні системи (ЕПС) демонструють високі показники ефективності завдяки своїм властивостям, які дозволяють використовувати їх не лише як додаткову систему до існуючих, заснованих на паперових готівкових коштах, але й як повноцінну заміну, що повністю витісняє паперову готівку її електронними еквівалентами. Інші відомі та аналізовані електронні платіжно-грошові системи (ЕПДС) не мають здатності настільки ефективно інтегруватися в сучасну економіку, залишаючись залежними від традиційних паперових грошових коштів. З розвитком технологій захисту інформації в електронних послугах, зокрема застосуванням біометричних технологій, аналізу поведінки користувачів, а також штучного інтелекту, що автоматизує процеси виявлення та усунення кіберзагроз в реальному часі, забезпечується високий рівень безпеки та надійності ЕПС. Вдосконалення криптографічних методів шифрування для забезпечення непереборного захисту даних під час їх передачі та зберігання є критично важливим для збереження довіри користувачів до електронних фінансових операцій.

Властивості сучасних ЕПС включають інтеграцію новітніх технологій, таких як блокчейн та криптовалюти, які підвищують прозорість та безпеку транзакцій, забезпечуючи надійний захист від підробок та зловживань. Розробка і впровадження нових стандартів безпеки, спрямованих на підвищення стійкості та надійності електронних фінансових

операцій, стає необхідністю у контексті стрімкого зростання кількості електронних транзакцій.

Подальше удосконалення технологій захисту інформації в електронних платіжних системах включає застосування біометричних технологій та аналізу поведінки користувачів. Дослідження продовжують вивчати вплив штучного інтелекту на автоматизацію процесів виявлення та усунення кіберзагроз у реальному часі. Вдосконалення криптографічних методів шифрування націлене на забезпечення неперебoрного захисту даних під час їх передачі та зберігання. Також відбувається активна розробка і впровадження нових стандартів безпеки з метою забезпечення стійкості і надійності електронних фінансових операцій, що відповідає сучасним викликам і вимогам цифрової економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gadetska, Z. M., Omelchuk, D. G., & Lytvyn, R. V. (2013). Identification and authentication - methods of protection from unauthorized access. *Eastern-European Journal of Enterprise Technologies, 2(2(62),* 8–10. https://doi.org/10.15587/1729-4061.2013.12347
2. Muminova, S. Sh., & Asatov, M. A. (2021). Issues of information security in EDMS. Issues of information security in EDI. *International scientific-online conference on "Innovation in the modern education system". Part-3. Collections of scientific works. Washington*, 204–207.
3. Pucket, C. (2009). The Story of the Social Security Number. *Social Security Bulletin, 69,* 55–74.
4. Muminova, S. Sh. (2022). Protection of information in electronic document management systems from the point of view of data leakage. *International scientific journal «Science and innovation», 3,* 215–220.
5. Monajemi, M. (2018). Privacy regulation in the age of biometrics deal with a new world order of information. *University of Miami International & Comparative Law Review, 25 (2),* 371–408.
6. Feldman, R. (2003). Considerations on the emerging implementation of biometric technology. *Hastings Communications and Entertainment Journal, 25(3),* 653–682.
7. Toliupa, S., Buchyk, S., Kulinich, O., & Buchyk, O. (2022) Protection of state management of critical infrastructure facilities under the influence of cyber attacks. *Infocommunication Technologies and Electronic Engineering, 2,* 33–41.
8. Slokenberga, S. (2021). Setting the Foundations: Individual Rights, Public Interest, Scientific Research, and Biobanking. In *LGTS, 43,* 11–30.
9. Salnyk, S. V., Storchak, A. S., & Mykytyuk, A. V. (2019). Model of violation of the security of information resources of communication systems. *Information Technology And Security, 7(1),* 25–34.
10. Jain, A. K., Nandakumar, K., & Nagar, A.(2008) Biometric template security. *EURASIP Journal on advances in signal processing,* 1–17.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Yuliia Khavikova
PhD student of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-1017-3602
y.khavikova@knute.edu.ua

PROTECTION OF INFORMATION IN ELECTRONIC SERVICESAND

Abstract. The publication explores the problem of information security in the context of the rapid development of electronic services and growing requirements for their security. It is noted that the intensive introduction of modern technologies into financial and other electronic systems leads to an increase in the volume of electronic transactions and information exchange, which intensifies the need for highly effective security methods. The main emphasis is placed on the importance of using multi-factor authentication and modern cryptographic methods to prevent unauthorized access to confidential information and manipulation of electronic transactions. The study notes that the success of modern electronic systems largely depends on the ability of their components to effectively protect data and ensure the reliability of operations for users. The article explores modern approaches to information security in electronic systems, focusing on innovative solutions and technologies aimed at ensuring the confidentiality, integrity and availability of data. The aspects considered include the introduction of machine learning for threat detection, the use of biometric methods for authentication, and the use of blockchain technologies to ensure transaction security. The relevance of the study is reinforced by the growing requirements for the protection of personal data and financial transactions in the virtual space, which requires continuous improvement of information security and implementation of advanced protection measures.

Keywords: information security; electronic services; electronic transactions; multi-factor authentication; cryptographic methods; data security; electronic systems; information privacy.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Gadetska, Z. M., Omelchuk, D. G., & Lytvyn, R. V. (2013). Identification and authentication - methods of protection from unauthorized access. *Eastern-European Journal of Enterprise Technologies, 2(2(62),* 8–10. https://doi.org/10.15587/1729-4061.2013.12347
2. Muminova, S. Sh., & Asatov, M. A. (2021). Issues of information security in EDMS. Issues of information security in EDI. *International scientific-online conference on "Innovation in the modern education system". Part-3. Collections of scientific works. Washington,* 204–207.
3. Pucket, C. (2009). The Story of the Social Security Number. *Social Security Bulletin, 69,* 55–74.
4. Muminova, S. Sh. (2022). Protection of information in electronic document management systems from the point of view of data leakage. *International scientific journal «Science and innovation», 3,* 215–220.
5. Monajemi, M. (2018). Privacy regulation in the age of biometrics deal with a new world order of information. *University of Miami International & Comparative Law Review, 25 (2),* 371–408.
6. Feldman, R. (2003). Considerations on the emerging implementation of biometric technology. *Hastings Communications and Entertainment Journal, 25(3),* 653–682.
7. Toliupa, S., Buchyk, S., Kulinich, O., & Buchyk, O. (2022) Protection of state management of critical infrastructure facilities under the influence of cyber attacks. *Infocommunication Technologies and Electronic Engineering, 2,* 33–41.
8. Slokenberga, S. (2021). Setting the Foundations: Individual Rights, Public Interest, Scientific Research, and Biobanking. In *LGTS, 43,* 11–30.
9. Salnyk, S. V., Storchak, A. S., & Mykytyuk, A. V. (2019). Model of violation of the security of information resources of communication systems. *Information Technology And Security, 7(1),* 25–34.
10. Jain, A. K., Nandakumar, K., & Nagar, A.(2008) Biometric template security. *EURASIP Journal on advances in signal processing,* 1–17.