МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ
(зимовий форум)

Одеса, Україна, 14 листопада 2025 р.

Одеса
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL UNIVERSITY

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025)

Odesa, Ukraine, November 14, 2025

Conference Proceedings
(winter forum)

Odesa
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції
(зимовий форум)

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 101 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 101 с.

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.
ПЕДЯШ В.В. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.
ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ЗМІСТ

— Ефективне зберігання даних: Застосування циклічних буферів для зберігання часових рядів дозволяє уникнути постійного перерозподілу пам'яті та забезпечує швидкий доступ до даних для розрахунків ковзних вікон.

— Динамічна обробка списку монет: Система автоматично відстежує делістинг монет (DelistedCoinHandler), видаляючи їх зі сховищ, що запобігає накопиченню неактуальних даних.

— Персистентність: Реалізовано механізм періодичного збереження стану Metrics Storage на диск (SaverHandler), що дозволяє відновлювати роботу системи після перезапуску без втрати накопичених даних.

Розроблений програмний комплекс охоплює повний цикл збору, обробки та візуалізації ринкових даних, включаючи інтеграцію з API провідних бірж, механізми кешування, а також систему сповіщень про аномальні події. Особливу увагу приділено аналітичному модулю, який надає користувачеві розширений набір метрик для оцінки ринкової динаміки, серед яких — унікальний рейтинг ліквідності, що враховує як обсяг торгів, так і глибину ордербуку.

Висновки

У ході виконання роботи було спроєктовано та реалізовано багатокомпонентну програмну систему, призначену для глибокого аналізу криптовалютних ринків у режимі реального часу. Архітектура рішення передбачає чітке розділення функціональних модулів, що забезпечує високу масштабованість, гнучкість та зручність супроводу. Ключовим технологічним вибором стала мова програмування Rust, яка завдяки своїй безпечній моделі пам’яті, високій продуктивності та підтримці паралельних обчислень, дозволила реалізувати ефективну обробку великих обсягів даних із мінімальними затримками.

Система спроєктована з урахуванням перспективи подальшого розвитку: її модульна структура дозволяє легко інтегрувати нові алгоритми, підключати додаткові джерела даних, а також адаптувати функціонал під потреби конкретних сценаріїв — від побудови складних аналітичних панелей до реалізації алгоритмічних торгових стратегій та систем автоматизованого моніторингу. Таким чином, створене рішення не лише задовольняє поточні вимоги до аналізу криптовалютних ринків, а й формує надійну основу для подальших досліджень і розробок у сфері фінансових технологій.

Література

1. Hintjens P. ZeroMQ: Messaging for Many Applications. O'Reilly Media, 2013. – 502 p.
2. Polars User Guide [Electronic resource] // Polars Documentation. – Mode of access: access:https://pola-rs.github.io/polars-book/user-guide/.
3. Rust Documentation [Electronic resource] // The Rust Programming Language. – Mode of access: https://rust-lang.org/learn.
4. Binance API Documentation access:https://www.binance.com/en/binance-api

Тімофєєв Олександр Олександрович
бакалавр, спеціальність 125
«Кібербезпека та захист інформації»
Міжнародний університет
timofeev.kraken@gmail.com

Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент
Міжнародний університет
yonalarisa66@gmail.com

ФОРМАЛЬНІ МЕТОДИ АНАЛІЗУ ВРАЗЛИВОСТЕЙ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

***Анотація**. У роботі досліджено вразливості систем електронного документообігу (СЕД) з використанням формальних методів моделювання. Запропоновано методику аналізу на основі моделі загроз STRIDE та інструментів формальної верифікації NuSMV і TLA+. Виявлено та усунуто логічні помилки в протоколах документообігу. Показано, що формальна верифікація досягає 100% ефективності у виявленні критичних вразливостей, що підтверджує доцільність її застосування в критичних системах.*

Системи електронного документообігу є критично важливими компонентами сучасної цифрової інфраструктури, які забезпечують управління документами, автоматизацію бізнес-процесів та захист інформації. Однак із розширенням функціональності СЕД зростають і вимоги до їх інформаційної безпеки. Документи часто містять конфіденційні дані, що робить ці системи привабливою ціллю для кіберзлочинців [1, 2].

Традиційні методи тестування не завжди здатні виявити приховані логічні вади в протоколах документообігу, що може призвести до порушення конфіденційності, цілісності або доступності інформації. У зв'язку з цим актуальним є застосування формальних методів моделювання та верифікації для математично обґрунтованої перевірки властивостей безпеки СЕД [3, 4]. Метою дослідження було розробити методику аналізу вразливостей систем електронного документообігу з використанням формальних методів, провести моделювання типових загроз і оцінити ефективність захисних механізмів.

На основі аналізу сучасних СЕД було розроблено матричну модель загроз, що класифікує загрози за рівнями (глобальні, організаційні, технічні, операційні, користувацькі) та типами активів (документи, користувачі, канали зв'язку, сервери, програмне забезпечення). Такий підхід забезпечує багатовимірне представлення ризиків і дозволяє точніше ідентифікувати вразливі компоненти СЕД.

Результати дослідження засвідчили, що найбільшу небезпеку для функціонування СЕД становлять саме технічні загрози, які мають потенціал спричинити критичні порушення конфіденційності, цілісності та доступності інформації. До найпоширеніших і найнебезпечніших технічних загроз віднесено несанкціонований доступ до документів, що може призвести до витоку або модифікації чутливої інформації; крадіжку облікових даних, яка відкриває шлях до компрометації облікових записів користувачів; атаки типу «людина посередині» (MITM) та фішингові кампанії, що спрямовані на перехоплення або підробку автентифікаційних даних; розподілені атаки на відмову в обслуговуванні (DDoS), які здатні паралізувати роботу системи; а також використання шкідливого програмного забезпечення, включно з експлуатацією вразливостей і наявністю бекдорів у програмному коді. Усі ці загрози потребують особливої уваги при проєктуванні, впровадженні та аудиті СЕД, оскільки вони можуть мати як безпосередні, так і відкладені наслідки для інформаційної безпеки організації.

Для систематизації загроз застосовано модель **STRIDE**, яка охоплює шість категорій [5]:

— **S**poofing (підміна особи);

— **T**ampering (порушення цілісності);

— **R**epudiation (відмова від дій);

— **I**nformation Disclosure (розголошення інформації);

— **D**enial of Service (порушення доступності);

— **E**levation of Privilege (ескалація привілеїв).

У межах дослідження було здійснено формальне моделювання протоколу обробки платіжного документа в електронній банківській системі. Як приклад було обрано типовий протокол, що охоплює послідовність етапів: створення документа, підпис бухгалтера, підпис керівника, передача до банку та архівування.

[Створення] → [Підпис бухгалтера] → [Підпис керівника] → [Передача до банку] → [Архів]

Для формалізації цього процесу застосовано підхід скінченного автомата, в якому кожен етап обробки представлено як окремий стан, а дії користувачів — як переходи між станами. Така модель дозволяє чітко описати логіку документообігу, виявити потенційні вразливості та забезпечити основу для подальшої формальної верифікації властивостей безпеки протоколу.

Для перевірки коректності протоколу сформульовано властивості у логіці LTL (Linear Temporal Logic):

Цілісність маршруту: документ не може бути переданий до банку без підпису керівника:

$$G\ (\neg(status = \text{"sent\_to\_bank"}) \vee signed\_by(\text{"manager"}))$$

Повна автентифікація: архівування можливе лише після підписання обома особами:

$$G\ (status = \text{"archived"} \rightarrow signed\_by(\text{"accountant"}) \wedge signed\_by(\text{"manager"}))$$

Контроль доступу**:** лише уповноважені користувачі можуть виконувати відповідні дії:

$$G\ (\neg(user.role \neq \text{"accountant"} \wedge action = \text{"sign"}))$$

Для верифікації використано інструменти **NuSMV** та **TLA+**. NuSMV дозволяє виконати символьну перевірку моделей, а TLA+ — описати дії та перевірити інваріанти системи [6, 7].

Виявлена вразливість: у результаті формальної перевірки було виявлено логічну неоднозначність у переході між станами «підпис керівника» та «передача до банку», яка дозволяла обійти перевірку підпису бухгалтера.

До виправлення:

```
next(docStatus) := case
  docStatus = "signed_by_manager" : "sent_to_bank";
  ...
esac;
```

Після виправлення:

```
next(docStatus) := case
  docStatus = "signed_by_manager" & signed_by_accountant = TRUE :
    "sent_to_bank";
  ...
esac;
```

Після усунення вади модель успішно пройшла верифікацію для всіх сформульованих властивостей безпеки.

Для оцінки ефективності захисних механізмів застосовано кількісні критерії у відсотках:

— Висока ефективність: 85–100%

— Середня ефективність: 60–84%

— Низька ефективність: <60%

Результати оцінки представлено у Табл.1.

Таблиця 1 — Ефективність захисних механізмів

Критерій оцінювання	**Результат перевірки**	**Ефективність, (%)**	**Рівень**
Цілісність маршруту документа	Виявлено та усунуто логічну ваду	95	Висока
Контроль доступу	Дії обмежені відповідно до ролей	90	Висока
Незаперечність дій	Підтверджено формально	100	Висока
Стійкість до загроз (STRIDE)	Виявлено потенційні сценарії	80	Середня→ Висока
Відповідність ISO/IEC 27001	Властивості узгоджено з вимогами	90	Висока
Формальна перевірка властивостей	Виконуються в усіх сценаріях	100	Висока

Найвищу ефективність — на рівні 100% — продемонстрували механізми незаперечності дій та формальної верифікації, що було підтверджено інструментальним аналізом із використанням засобів моделювання та перевірки властивостей системи. Застосування формальних методів дозволило не лише виявити приховані логічні вади, недоступні для традиційного тестування, але й забезпечити гарантії виконання критичних вимог безпеки, зокрема цілісності, автентичності та незаперечності дій користувачів у межах протоколу документообігу. Такий результат свідчить про високу надійність обраного підходу в контексті

критичних інформаційних систем, де помилки можуть мати значні правові та фінансові наслідки. Водночас, механізм стійкості до загроз, хоча й продемонстрував базову ефективність у загальних сценаріях, потребує подальшого уточнення логіки реагування для специфічних випадків, зокрема при нестандартних послідовностях дій, змінених ролях користувачів або умовах часткової компрометації каналів зв'язку. Це вимагає розширення моделі загроз, деталізації сценаріїв атаки та адаптації механізмів захисту до динамічного середовища функціонування СЕД. Подальші дослідження мають бути спрямовані на інтеграцію адаптивних механізмів реагування та контекстно-орієнтованої логіки перевірки, що дозволить підвищити загальну стійкість системи до складних і комбінованих типів загроз.

Висновки

У межах проведеного дослідження було розроблено методику аналізу вразливостей систем електронного документообігу (СЕД), що поєднує модель загроз STRIDE із формальними методами верифікації, зокрема NuSMV та TLA+. Застосування формальної верифікації дозволило виявити критичну логічну ваду в протоколі документообігу, яка залишалася непоміченою під час традиційного тестування та могла спричинити порушення регламенту обробки документів. Експериментальні результати підтвердили ефективність формальних методів і механізмів незаперечності, які забезпечили 100% виявлення порушень, що свідчить про їхню доцільність у критичних СЕД. Комбіноване використання STRIDE та формальної верифікації забезпечує багаторівневий захист і гарантує виконання властивостей безпеки в усіх можливих сценаріях функціонування системи. Отримані результати мають практичну цінність і можуть бути використані при розробці, аудиті та вдосконаленні СЕД у банківському секторі, державних установах і корпоративних середовищах.

Література

1. Гриценко О. В. Інформаційна безпека в електронному документообігі: теорія і практика. Харків: Фоліо, 2021. 256 с.

2. Ковальов С. В. Класифікація загроз інформаційній безпеці в системах електронного документообігу // Інформаційна безпека. 2023. № 2. С. 45–52.

3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO, 2013. 30 p.

4. Коваленко А. А., Куценко Т. Г., Шаповал А. С., Ситник О. В., Ні Я. С. Огляд методів аналізу безпечного програмного забезпечення // Системи управління, навігації та зв'язку. 2025. №1. С. 156–161.

5. STRIDE Threat Modeling / Microsoft. URL: https://learn.microsoft.com/en-us/security/compass/stride-threat-modeling (дата звернення: 10.11.2025).

6. Cimatti A., Clarke E., Giunchiglia F., Roveri M. NuSMV: A New Symbolic Model Verifier // International Journal on Software Tools for Technology Transfer. 2002. Vol. 2, No. 4. URL: https://nusmv.fbk.eu

7. Lamport L. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers. Boston: Addison-Wesley, 2002. 384 с.

8. Йона Е. О., Йона Л. Г., Терешко В. С. Криптографічний захист електронного документообігу // Цифрові технології. 2013. № 13. С. 142–146.

УДК 004.056.53 : 004.89

Головатюк К.В.
студент факультету Кібербезпека, спеціальність 125
Міжнародний університет
kostya93.06@gmail.com