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

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Русу О.П., Цуркан Л.Л. Програмне забезпечення для розрахунку перетворювачів напруги комп'ютерного обладнання 10

Жигулін О.А., Шестаков М.М. Інформаційні технології у забезпеченні сталого розвитку бізнесу 12

Азовський А.І. Педяш В.В. Програмна реалізація нейромережевих моделей для автоматизованого аналізу текстових даних 14

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

Стрелковська І.В., Салоїд В.О. Сплайн-апроксимація розпізнавання жестів рук на базі OpenCV 18

Стрелковська І.В., Стоянов І.А. Дослідження мережевого трафіку хмарних сервісів та CDN-платформ 22

Баранюк Е.О. Розробка ігрового застосунку в жанрі city builder 27

Беседа О.Д. Розробка інтелектуальної мобільної платформи з функцією відстеження об'єктів 28

Дудко І.А. Дослідження системи розпізнавання жестів з використанням Mobilenet для задач комп'ютерного зору 30

Нікольський В.В., Лорткіпанідзе Р. Розподілена система моніторингу навколишнього середовища на базі LoRaWAN 34

Колесник О.В. Розробка інтелектуальної системи детекції зображень 37

Крупецький К.А., Русу О.П. Цифрове керування імпульсними перетворювачами напруги в комп'ютерному обладнанні 39

Горбачов В.Е., Яровий Д.О. Дослідження параметрів датчиків температури у цифрових сенсорних мережах 42

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Перчеклій Д.В. Дослідження інтеграції технології блокчейн у платіжні системи 45

Петков Є.І. Принципи роботи DoS, DDoS атак та засоби захисту проти них 48

Бєліков Д.В. Дослідження методів захисту від соціально-інженерних загроз 51

Чебанюк О.Д., Динін Б.І. Розробка та реалізація високопродуктивної системи для агрегації та аналізу метрик криптовалютних ринків у реальному часі 53

Тімофєєв О.О. Формальні методи аналізу вразливостей систем електронного документообігу 56

Головатюк К.В., Григор'єва Т.І. Оптимізація процесів інформаційних технологій при атаках фішингу із застосуванням нечіткої логіки 60

Проценко М.М. Порівняльне дослідження методів тестування безпеки LLM-коду: SAST, DAST, graph-based та синтез гібридного підходу 63

Лавров А.В. Стан та перспективи розвитку електронних платежів в Україні 66

Onatskyi Oleksii, Zharova Oksana. Comparative analysis of homomorphic properties of asymmetric cryptosystems RSA and Paillier 68

пошта, SMS, соціальні мережі та телефонні дзвінки, які поєднують технічні прийоми зі способами психологічного впливу на користувача.

2. Запропоновано підхід до оцінювання ризику фішингових атак із використанням нечіткої логіки, який дозволяє гнучко враховувати такі параметри, як схожість домену, рівень персоналізації повідомлення, історія реакцій користувача та канал доставки. Це дає можливість системам кібербезпеки адаптувати реакцію до рівня загрози, зменшуючи навантаження на аналітиків і підвищуючи точність виявлення атак.

3. В роботі побудовано математичну модель із застосуванням нечіткої логіки, яка дозволяє оцінити ризик загрози та адаптувати реакцію системи кібербезпеки відповідно до ступеня ризику.

4. Реалізація нечіткої моделі в процесах моніторингу та реагування сприятиме оптимізації використання ресурсів, скороченню часу реагування на інциденти й зниженню кількості успішних атак. Поєднання технологічних засобів, обміну даними між установами та підвищення цифрової грамотності користувачів є ключовими умовами ефективної протидії фішингу в умовах сучасної кібервійни.

Література.

1. Бурячок А. І. Інформаційна безпека в умовах гібридної війни: фішинг як інструмент соціальної інженерії. // Науково-аналітичний вісник. – 2023. – №4. – С. 110–140.

2. Інформаційна безпека: проблеми правового забезпечення та технологічного супроводу. – К.: Інститут інформації, безпеки і права, 2022. – 358 с.

3. CERT-UA. Як убезпечитися від фішингового сайта? [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/article/2808

Проценко М.М.

здобувач вищої освіти третього (аспірантського рівня)

спеціальності 123 – Комп'ютерна інженерія

Науковий керівник: Мірошник М. А.

доктор технічних наук, професор

Міжнародний університет

місто Одеса, Україна

ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДІВ ТЕСТУВАННЯ БЕЗПЕКИ LLM-КОДУ: SAST, DAST, GRAPH-BASED ТА СИНТЕЗ ГІБРИДНОГО ПІДХОДУ

Анотація. *У сучасному програмуванні великі мовні моделі (LLM) широко застосовуються для автоматичної генерації коду, однак дослідження 2025 року показують, що такий код нерідко містить вразливості безпеки [1]. Традиційні методи тестування – статичний аналіз безпеки (SAST) та динамічне тестування (DAST) – не завжди справляються з цими викликами. SAST-інструменти сканують вихідний код до його виконання, але генерують багато хибних спрацювань і не розуміють повної семантики застосунку. DAST-підходи перевіряють програму під час роботи, виявляючи лише явні проблеми та пропускаючи приховані дефекти, особливо у складних системах.*

LLM відкривають нові можливості для аналізу коду. Моделі здатні розуміти семантику і помічати небезпечні патерни, які складно формалізувати правилами. GPT-4 успішно розпізнав близько 94% тестових уразливостей, тоді як провідний SAST-сканер виявив лише ~34% [2]. Водночас LLM можуть генерувати некоректні висновки (галюцинації), тому напряму довіряти їм ризиковано. Це зумовило появу гібридних систем, що поєднують строгість статичного аналізу з семантичним міркуванням LLM. Інструмент SAST-Genius, який інтегрує LLM у конвеєр статичного сканування, досягає точності понад 90% при повноті ~95%, тоді як типовий аналізатор демонструє лише ~60% через хибні спрацювання [3]. Експеримент показав зменшення хибних попереджень на ~91% (з 225 до 20) при використанні LLM як постфільтра [3]. Таким чином, симбіоз SAST та LLM дає суттєвий виграш у точності виявлення вразливостей.

LLM також підвищують ефективність динамічного тестування. LLM-асистовані системи генерують цілеспрямовані тестові вектори замість випадкового фаззингу. Система HGFuzzer, керована мовною моделлю, спровокувала 85% відомих уразливостей менш ніж за хвилину, що у 24+ рази швидше за традиційні фаззери, і виявила 9 нових уразливостей з CVE-ідентифікаторами [4]. У пентестингу LLM-агенти самостійно планують і здійснюють атаки, знаходячи в декілька разів більше шляхів експлуатації завдяки розумінню коду й документації.

Для великих кодових баз перспективним є графовий аналіз. Подання програми як графа властивостей коду (CPG), що поєднує синтаксичне дерево, граф потоку управління та граф потоків даних, дозволяє відстежувати складні взаємозв'язки. Модель Hound з підходом "relation-first" підвищила повноту виявлення з 8.3% до 31.2% (чотирикратне зростання) порівняно з базовим LLM-сканером [6]. Граф знань дає ширший контекст: агент простежує шлях від зовнішнього вводу через функції до критичної точки, знаходячи логічні уразливості. Підхід GRASP інтегрує граф правил безпечного кодування в процес генерації, підвищуючи частку безпечних рішень на ~16–20% для різних LLM [3].

На основі аналізу літератури пропонується синтезований гібридний фреймворк, що об'єднує SAST, DAST і графовий аналіз під керуванням LLM-агента. Архітектура включає шість ключових компонентів: Одноагентний модуль – єдиний LLM-агент для статичного й поверхневого динамічного аналізу невеликих проєктів. Багатоагентний модуль – група спеціалізованих агентів (сканер, фаззер, аналізатор залежностей), що паралельно перевіряють різні аспекти безпеки у великих базах. Ієрархічний модуль – багаторівнева структура: верхній агент-планувальник визначає стратегію, підлеглі детально аналізують компоненти. Корективний модуль – механізм самоперевірки: після кожного етапу LLM переглядає

висновки, виявляє помилки й повторює аналіз. Адаптивний модуль – автоматично підлаштовує глибину аналізу під складність проєкту, оптимізуючи швидкість і повноту. Графовий модуль – представляє кодову базу як граф (CPG), забезпечуючи контекст про структуру та потоки даних.

Фреймворк працює як адаптивний конвеєр. Спочатку статичний аналізатор сканує код, LLM відсіює хибні спрацювання та додає пояснення. Динамічний модуль генерує цільові тести або експлойти для підтвердження уразливостей. Паралельно графовий модуль будує карту компонентів і потоків, виявляючи комплексні логічні вразливості. LLM-агент формує консолідований звіт з доказами та рекомендаціями. Коригувальний цикл генерує патчі, після чого аналіз повторюється до досягнення критеріїв безпеки.

Дослідження підтверджують ефективність компонентів підходу. LLM-підсилений статичний аналіз досягає F1-міри 0.93 проти 0.55 у класичних сканерів [3]. GPT-4 знаходить утричі більше уразливостей, ніж звичайний SAST [2]. Агент SecureFixAgent підвищив точність виправлень на 13.5% і знизив хибні спрацювання на 11% [5]. Графовий аналіз (Hound) виявляє у чотири рази більше уразливостей на рівні програми [6]. Таким чином, поєднання методів з логікою LLM забезпечує більш повне тестування безпеки.

Адаптивний гібридний фреймворк тестування безпеки LLM-коду поєднує сильні сторони SAST, DAST і графового аналізу, долаючи їхні обмеження. Завдяки LLM агенти глибоко аналізують код, відсівають помилкові попередження, генерують сценарії атак та пропонують виправлення автоматично. Оглянуті дослідження показують, що такі системи виявляють більше реальних уразливостей, швидше підтверджують експлуатацію і генерують якісніші патчі, ніж традиційні підходи. Це робить гібридні LLM-методи перспективним напрямком для DevSecOps. Подальші розробки зосередяться на покращенні узгодженості LLM, зниженні витрат і тіснішій інтеграції з інструментами розробки для промислового масштабування. Поєднання штучного інтелекту з класичними методами безпеки здатне суттєво підвищити стійкість програмного забезпечення до кіберзагроз.

Література

1. Sabra A., Schmitt O., Tyler J. Assessing the Quality and Security of AI-Generated Code: A Quantitative Analysis. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2508.14727 (дата звернення: 04.11.2025).

2. Tehrani M.G., Sultanow E., Buchanan W.J., Houmani M., Fodja C.H.D. LLM vs. SAST: A Technical Analysis on Detecting Coding Bugs of GPT-4 Advanced Data Analysis. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2506.15212 (дата звернення: 04.11.2025).

3. Agrawal V., Ahi K. LLM-Driven SAST-Genius: A Hybrid Static Analysis Framework for Comprehensive and Actionable Security. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2509.15433 (дата звернення: 04.11.2025).

4. Xu H., Zhao Y., Wang H. Directed Greybox Fuzzing via Large Language Model. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2505.03425 (дата звернення: 04.11.2025).

5. Gajjar J., Subramaniakuppusamy K., Puthal R., Ranaware K. SecureFixAgent: A Hybrid LLM Agent for Automated Python Static Vulnerability Repair. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2509.16275 (дата звернення: 04.11.2025).

6. Mueller B. Hound: Relation-First Knowledge Graphs for Complex-System Reasoning in Security Audits. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2510.09633 (дата звернення: 04.11.2025).

Лавров Андрій Вікторович
Здобувач факультету кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність 122 Комп'ютерні науки
Міжнародний університет
lavrs6nh@gmail.com
Керівник: д.т.н., професор кафедри Радівілова Т.А.

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЕЛЕКТРОННИХ ПЛАТЕЖІВ В УКРАЇНІ

Анотація. *У роботі проаналізовано сучасний стан розвитку електронних платежів в Україні, а також визначено основні тенденції, виклики та перспективи подальшого зростання галузі. Розглянуто вплив цифровізації фінансового сектору, появу нових платіжних технологій та впровадження державних ініціатив, спрямованих на підвищення безпеки електронних транзакцій. Особливу увагу приділено розвитку мобільного банкінгу, платіжних сервісів на базі NFC та цифрових гаманців.*

Ключові слова: електронні платежі, фінтех, цифровізація, банківські технології, кібербезпека, платіжні системи, мобільний банкінг.

Стрімкий розвиток інформаційних технологій і фінансових сервісів в Україні за останнє десятиліття суттєво змінив підхід до здійснення фінансових операцій. Якщо раніше більшість платежів відбувалася через банківські каси або термінали, то сьогодні понад 75% транзакцій здійснюється в електронному форматі. Такі зміни стали можливими завдяки розвитку фінансових технологій (FinTech), появі інноваційних рішень для мобільних і