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

Бєліков Дмитро
Вячеславович
Міжнародний університет

iriska3434dima@gmail.com
Науковий керівник: Йона Лариса Григорівна зав.каф. КІmaIT, доцент, к.т.н.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ ЗАГРОЗ

Анотація. *Соціальна інженерія (СІ) є домінуючим вектором кібератак, посиленим генеративним ШІ (GenAI). Дослідження аналізує ландшафт загроз 2024-2025 років та обґрунтовує необхідність переходу від фокусування на 'Click Rate' до 'Reporting Rate' як ключової метрики стійкості. На основі аналізу запропоновано комплексну, багаторівневу стратегію 'Defense-in-Depth', що поєднує технічні (DMARC), адміністративні (PoLP, IR Plan) та інноваційні людські методи.*

1. Психологічна парадигма сучасної кіберзагрози

Сучасний ландшафт кібербезпеки демонструє тривожний парадокс. Організації інвестують мільярдні кошти в технологічні засоби захисту, проте переважна більшість успішних кібератак — до 98% — покладаються не на технічні експлойти, а на маніпуляцію. Соціальна інженерія (СІ) оминає технологічні бар'єри, націлюючись безпосередньо на "людський фактор".

Ефективність СІ ґрунтується на експлуатації фундаментальних психологічних механізмів та когнітивних попереджень, які є невід'ємною частиною людської поведінки. Зловмисники цілеспрямовано використовують принципи переконання, ідентифіковані Робертом Чалдіні, такі як Авторитет (імперсонація керівництва), Терміновість (вимога негайної дії) та Соціальний доказ. Це перетворює загрозу із суто технічної на психологічну, роблячи традиційні методи захисту недостатньо ефективними.

2. Новий каталізатор: Вплив Генеративного ШІ (GenAI)

Якщо СІ завжди було ефективним, то поява генеративного ШІ (GenAI) у 2024-2025 роках стала потужним «підсилювачем загрози». GenAI докорінно змінює економіку та ефективність атак, руйнуючи традиційний компроміс зловмисників між масштабом та якістю. Це призвело до появи нового класу загроз: «масово-персоналізованих атак».

Ключові вектори посилення атак за допомогою GenAI:

Бездоганні фішингові приманки: GenAI дозволяє масово створювати ідеально написані, контекстуально обізнані листи на будь-якому мові, що імітують стиль спілкування конкретної особи.

Клонування голосу та Deepfakes: Технології GenAI використовують для створення переконливих атак Vishing (голосовий фішинг), де зловмисник говоритиме голосом керівника або колеги.

Інтерактивні атаки в реальному часі: ШІ-агенти можуть підтримувати "живу" взаємодію з жертвою, миттєво генеруючи переконливі відповіді на її запитання та розвіюючи сумніви.

3. Вимірювання стійкості: Перехід від Click Rate до Reporting Rate

Для протидії новим загрозам потрібна адекватна система вимірювання. Традиційні симуляції фішингу (наприклад, за допомогою Gophish) є дієвим методом кількісної оцінки вразливості персоналу, що вимірює «Phish-prone Percentage» (Click Rate). Цей показник фіксує відсоток співробітників, які натиснули на шкідливе посилання.

Однак, фокусування лише на цій метриці є помилкою, оскільки вона вимірює виключно невдачу. Зріла програма безпеки повинна вимірювати стійкість (Resilience). Набагато ціннішою метрикою є Reporting Rate (коефіцієнт звітування) — відсоток співробітників, які розпізнали загрозу та повідомили про неї у службу безпеки. Ефективна програма захисту має демонструвати чітку динаміку: одночасно зниження Click Rate при зростанні Reporting Rate.

4. Комплексна багаторівнева стратегія захисту (Defense-in-Depth)

Результати аналізу доводять, що покладатися лише на один рівень захисту (технології чи тренінги) — недостатньо. Ефективний захист вимагає інтегрованої, багаторівневої стратегії "Defense-in-Depth", що діє на трьох ключових рівнях.

4.1. Рівень 1: Технічний захист (DMARC)

Перший рівень має на меті автоматично блокувати якомога більше загроз. У контексті CI, що покладається на спуфінг (підробку) email-адреси, ключовим є впровадження протоколів автентифікації пошти. Тільки DMARC з коректно налаштованим "вирівнюванням" (Alignment) та політикою p=reject є найефективнішим технічним контрзаходом. Він вимагає, щоб домен, який бачить користувач у полі `From:`, збігався з доменом, що пройшов автентифікацію SPF/DKIM, блокуючи найпоширеніші тактики обману.

4.2. Рівень 2: Адміністративний захист (PoLP та IR Plan)

Цей рівень діє як "обмежувач шкоди".

Принцип найменших привілеїв (PoLP): Ця концепція вимагає, щоб користувачам надавався лише мінімально необхідний рівень доступу. PoLP не запобігає успішному фішингу, але драматично обмежує шкоду, блокуючи швидке латеральне переміщення та ескалацію привілеїв.

План реагування на інциденти (IR Plan): Наявність задокументованого та відрепетованого IR Plan є критичною. Найважливішими є те, що найшвидшим тригером для цього плану є не лише технічні засоби (SIEM/EDR), а й сам співробітник, який негайно повідомляє про інцидент.

4.3. Рівень 3: Людський захист ("Людський брандмауер")

Це фінальний рівень захисту. "Людський брандмауер" - це не пасивна стіна, а активна система виявлення. Проте традиційні щорічні тренінги є неефективними. Для побудови дієвого "людського брандмауера" потрібний перехід до безперервного, гейміфікованого мікронавчання. Цей підхід, заснований на поведінковій науці (напр., модель B=MAP Фогга) та гейміфікації (балі, значки, лідерборди), використовує позитивні психологічні стимули для боротьби з негативними маніпуляціями зловмисників.

Висновки

Соціальна інженерія залишається домінуючою та найбільш небезпечною загрозою, оскільки вона націлена на незмінну людську психологію. Поява GenAI лише посилює цю загрозу, демократизуючи складні, персоналізовані атаки.

Дослідження стверджує, що ефективна захист не може бути досягнута жодним окремим рішенням. Він вимагає побудови глибоко інтегрованої системи Defense-in-Depth, де кожен рівень підтримує інший:

1. Технічні засоби (DMARC) відсіюють 99% автоматизованих атак.
2. Адміністративні політики (PoLP, IR Plan) стримують та обмежують шкоду від тих атак, що пройшли.
3. Людський брандмауер, навчений через безперервну гейміфікацію, слугує найдосконалішим сенсором, що виявляє цільові, згенеровані ШІ атаки, та негайно активує План реагування на інциденти.

Лише така синергетична стратегія здатна забезпечити реальну стійкість організації в умовах сучасного ландшафту кіберзагроз.

Література

1. Cost of a Data Breach Report 2024/IBM Security; Ponemon Institute. 2024. URL: https://www.ibm.com/reports/data-breach.

2. 2024 Data Breach Investigations Report (DBIR) / Verizon. 2024. URL: https://www.verizon.com/business/resources/reports/dbir/.

3. 2024 Phishing by Industry Benchmarking Report / KnowBe4. 2024. URL: https://www.knowbe4.com/hubfs/final_2024_phishing_benchmark_report.pdf.

4. Чалдіні Р. Психологія впливу. Упевнюйте та досягайте успіху!. Харків: КОД, 2024. 608 с.

5. Computer Security Incident Handling Guide : NIST Special Publication 800-61 Rev. 3/National Institute of Standards and Technology. 2025. URL: https://csrc.nist.gov/pubs/sp/800-61/r3/final.

Чебанюк Олексій Дмитрович
бакалавр, спеціальність
014«Середня освіта (Інформатика та програмування)»
Міжнародний університет
chebanuk@gmail.com
Динін Борис Іванович
бакалавр, спеціальність
121 «Інженерія програмного забезпечення»
Міжнародний університет
borisdynin757@gmail.com
Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент
Міжнародний університет
yonalarisa66@gmail.com

РОЗРОБКА ТА РЕАЛІЗАЦІЯ ВИСОКОПРОДУКТИВНОЇ СИСТЕМИ ДЛЯ АГРЕГАЦІЇ ТА АНАЛІЗУ МЕТРИК КРИПТОВАЛЮТНИХ РИНКІВ У РЕАЛЬНОМУ ЧАСІ

Анотація. *У роботі представлено архітектуру та реалізацію програмного комплексу для збору, обробки та аналізу високочастотних даних із криптовалютних бірж. Система, розроблена мовою програмування Rust, використовує асинхронну модель, багатопотокову обробку та обмін повідомленнями через ZMQ для досягнення високої продуктивності. Описано ключові модулі: обробник потоку угод, калькулятор метрик, система розрахунку рейтингу ліквідності та механізми інтеграції із зовнішніми аналітичними сервісами. Отримані результати демонструють ефективність системи для моніторингу ринку в реальному часі.*

Криптовалютні ринки характеризуються високою волатильністю та величезним обсягом торгових даних, що генеруються щомиті. Для ефективного аналізу, моніторингу та ухвалення торгових рішень необхідні інструменти, здатні обробляти ці потоки інформації в режимі реального часу з мінімальними затримками. Метою даної роботи є розробка високопродуктивної системи, здатної агрегувати необролені дані про угоди з різних бірж і на їх основі розраховувати комплексні аналітичні метрики. В якості основного інструменту розробки було обрано мову Rust завдяки її фокусу на безпеці, конкурентності та продуктивності**.**

Розроблена система побудована на модульній архітектурі, що передбачає чітке розмежування функціональності між окремими компонентами. Кожен модуль виконує