МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

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

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

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.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

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

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний 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 гуманітарний 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 гуманітарний університет, м.Одеса, Україна.

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

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний 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 гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний 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 гуманітарний 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 гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

modernisation. However, when damage is deliberate, both governments and businesses must act in unison. The effectiveness of their collaboration will determine the capacity of modern civilisation to adapt and survive in a deeply interdependent global landscape.

While such incidents were once treated with indifference, today they represent a pressing threat. With widespread digitalisation, their consequences are more profound than ever—incurring both economic losses and loss of life. Moreover, where a single backup communication line once offered sufficient protection, recent years have shown that even fibre optics and certain satellites are vulnerable to repeated damage.

In light of these developments, we must conclude that distributed enterprises operating on centralised databases are now highly exposed to emerging global risks. This vulnerability results in extensive labour hours spent on manually restoring and resynchronising data following network outages. Therefore, any organisation operating within a distributed model must integrate the following into its core strategy: preventive risk management, cybersecurity, system redundancy, and robust architectural planning. The rapid advancement of artificial intelligence offers a promising avenue to streamline and partially automate these vital processes in the near future.

References:

1. Khniunin S.H., Shvedu M.I. Ensuring the Security of Information Systems in Distributed Enterprises in Conditions of Unstable Communication System Operations // Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку: Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь: Liha-Pres, 2025. – Ч. 2. – С. 144 - 146. DOI: 10.36059/978-966-397-491-0-42

2. The US Grid Attack Looming on the Horizon. URL: https://www.wired.com/story/youre-not-ready-for-a-grid-attack/?utm_source=chatgpt.com (date of access: 06.06.2025).

3. Power Outages, Communication Failures & Healthcare. URL: https://www.domprep.com/articles/power-outages-communication-failures-healthcare?utm_source=chatgpt.com (date of access: 06.06.2025).

4. Empresario del área metalúrgica: Quién es Rudy Basualdo, el hombre secuestrado en Rancagua (February 2025). URL: https://www.emol.com/noticias/Nacional/2025/02/18/1112344/Corte-de-luz-nacional-en-Chile.html (date of access: 06.06.2025).

5. Power supply restored after major outage hits Kenya, affects internet access (December 2024). URL: https://www.reuters.com/world/africa/major-power-outage-hits-kenya-affects-internet-access-2024-12-18/?utm_source=chatgpt.com (date of access: 06.06.2025).

6. Chile declares emergency as power outage plunges country into darkness (October 2023). URL: https://www.aljazeera.com/news/2025/2/26/chile-declares-state-of-emergency-as-blackout-plunges-country-into-darkness?utm_source=chatgpt.com (date of access: 06.06.2025).

7. Communication outage hits flood-stricken city in Libya, further complicating search efforts (September 2022). URL: https://apnews.com/article/libya-derna-floods-069adb76afc3c4ec92956ee4141ad872 (date of access: 06.06.2025).

Єрьоменко Анастасія Русланівна
Студент факультету Кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність: Електронні комунікації та радіотехніка (172)
Міжнародний гуманітарний університет
ananastya1330@gmail.com
Керівник: к.т.н.,доцент Йона Лариса Григорівна,
yonalarisa66@gmail.com

МЕТОДИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

***Анотація*.** Розглянуто сучасні підходи до захисту цілісності електронних документів, зокрема новітні криптографічні методи, інтеграцію штучного інтелекту, використання блокчейну та перспективи впровадження постквантових технологій. Підкреслено необхідність переходу від класичних централізованих моделей до децентралізованих систем із високим рівнем довіри. Проаналізовано внутрішні дослідження та практичні приклади впровадження.

1. Вступ

У сучасному цифровому середовищі передача, зберігання та обробка документів часто здійснюються без використання паперових носіїв. Це вимагає створення механізмів захисту, які не лише гарантують цілісність документів, але й дозволяють безсумнівно встановити їхнє походження [4].

Сучасні виклики — зростання кіберзагроз, юридичні конфлікти, розвиток квантових обчислень — потребують інноваційних рішень, що виходять за межі класичних цифрових підписів і сертифікатів [1], [3].

2. Теоретичні основи цілісності та автентифікації

Цілісність документа — це властивість, яка гарантує незмінність даних. Автентифікація засвідчує, що джерело документа відповідає очікуваному. Класичні інструменти — геш-функції, цифрові підписи, PKI (інфраструктура відкритих ключів) — залишаються актуальними, проте потребують доповнення у зв'язку зі зростанням складності загроз [3].

Основні загрози(та сучастні протидії їм):

- Модифікація або знищення даних зловмисником (Цифрові підписи для верифікації незмінності. Резервне копіювання у захищених сховищах.[4]).
- Фальсифікація джерела походження документа (PKI-сертифікати для перевірки особи відправника. Цифрові підписи з перевіркою по відкритому ключу.[3]).
- Несанкціонований доступ до конфіденційної інформації(Шифрування даних (AES, RSA). Аудит доступу та журналювання дій користувачів.[4]).
- Підміна або підробка електронного документа (Блокчейн для фіксації автентичних копій. \ Водяні знаки або метадані з шифруванням. Штучний інтелект для виявлення аномалій у структурі документа[2],[5].).

3. Механізми програмного забезпечення цілісності

Блокчейн та децентралізація

Розподілені реєстри дозволяють фіксувати кожен факт взаємодії з документом у незмінному вигляді. Геш документа зберігається в блокчейні, що дозволяє перевірити його справжність у будь-який момент [4]. Наприклад, нотаріальні блокчейн-сервіси вже використовуються у правових процесах.

Пропонується створити міжвідомчий державний блокчейн для реєстрації дій із публічними цифровими документами, який працюватиме в режимі реального часу та надаватиме публічний API для перевірки цілісності документа будь-яким громадянином/громадянкою.

Штучний інтелект / машинне навчання (AI/ML) для верифікації

Штучний інтелект може виявляти зміни у структурі документа, які не виявляються звичайними криптографічними засобами[2]. Наприклад, аналізуючи стилістику тексту або метадані PDF-файлів. Це особливо актуально для виявлення фальсифікацій офіційних документів.

Можливе створення інтелектуальної системи фільтрів для державних установ, яка автоматично класифікуватиме та маркуватиме документи з ознаками фальсифікації на основі нейромережевого аналізу структури й стилю [2], [5].

Гомоморфне шифрування

Це підхід, що дозволяє обробляти зашифровані документи без їхнього розшифрування [1], [6]. Завдяки цьому забезпечується перевірка та обробка з повною конфіденційністю.

Переваги:

- Дані залишаються зашифрованими під час обробки.
- Мінімізується ризик витоку інформації.

Недоліки:

- Повністю гомоморфне шифрування залишається обчислювально складним і ресурсоємним.
- Ще не є практичним для всіх сценаріїв використання.

Приклад: впровадження пілотної платформи для обміну медичними даними між установами, де інформація обробляється виключно у зашифрованому вигляді з можливістю аналітики без доступу до персональних даних пацієнтів.

Постквантова криптографія

Класичні алгоритми (RSA, ECC) вразливі до квантових атак. Сучасні дослідження зосереджені на створенні стійкої до квантового зламу криптографії[3]. Розглядаються нові геш-функції (SPHINCS+, Picnic), здатні гарантувати цілісність у довгостроковій перспективі.

Напрямок — розвиток гібридних систем захисту цифрових архівів, що поєднують класичні алгоритми з постквантовими протоколами, дозволяючи поступовий перехід до нових стандартів без втрати сумісності.

4. Практичне застосування в Україні

У рамках цифровізації держави сервіси як Дія, Електронний суд, eHealth інтегрують цифрові підписи. Зростає інтерес до нових підходів: деякі стартапи працюють над верифікацією дипломів і медичних карток через блокчейн. КПІ ім. І. Сікорського досліджує багатофакторну автентифікацію на основі нейромереж [2], [5].

5. Висновки

Автентифікація та захист цілісності документів є ключовими елементами інформаційної безпеки в умовах цифрової трансформації. Інновації у сфері цілісності та автентифікації документів мають вирішальне значення для безпечного інформаційного середовища. Впровадження ШІ, блокчейну, гомоморфного шифрування та постквантових методів створює підґрунтя для нової архітектури довіри. Водночас необхідні стандартизація, нормативне забезпечення та етичне осмислення.

Література

1. Вікіпедія. Гомоморфне шифрування. URL: https://uk.wikipedia.org/wiki/Гомоморфне_шифрування

2. С. Славінський, «Застосування методів машинного навчання для виявлення фальсифікацій у цифрових документах», КПІ ім. І. Сікорського, магістерська дисертація, 2021. URL: https://ai.kpi.ua/ua/masters/thesis/28521smai-slavinskyi_magistr.pdf

3. CoinMarketCap. Повне гомоморфне шифрування (FHE). URL: https://coinmarketcap.com/academy/uk/glossary/fully-homomorphic-encryption

4. bip.net.ua. «Як підприємцю організувати електронний документообіг». URL: https://bip.net.ua/articles/yak-pidpryyemczyu-organizuvaty-elektronnyj-dokumentoobig/

5. І. М. Шевченко, С. Ю. Смоляр, «Блокчейн у забезпеченні цілісності електронних документів», Журнал якісних моделей та технологій, №2, 2023. URL: https://jqmth.donnu.edu.ua/article/download/14956/14862

6. Національний департамент інформатизації. «Сучасні загрози цифровим даним та методи захисту», Електронний репозиторій НДІПППП. URL: https://repository.ndippp.gov.ua/handle/765432198/1050

Петков Євген Ігорович.
Аспірант, спеціальність 125
“Кібербезпека та захист інформації”,
Міжнародний гуманітарний університет
yepetkov@gmail.com
Науковий керівник
Йона Лариса Григорівна, к.т.н.,
Завідувач, доцент кафедри Комп’ютерної інженерії та інноваційних технологій
Факультету Кібербезпеки, програмної інженерії та комп’ютерних наук
Міжнародного гуманітарного університету
yonalarisa66@gmail.com

ТИПИ СПУФІНГ АТАК ТА ЗАСОБІВ ЗАХИСТУ В ЛОКАЛЬНИХ МЕРЕЖАХ

Анотація. *Дослідження розглядає типи Spoofing-атак та засобів боротьби з ними в мережі рівня доступу.*

Атаки типу спуфінг (spoofing) — це категорія кібератак, у яких зловмисник маскується під іншу особу або пристрій, щоб обдурити користувача, систему або мережу. Основна мета таких атак — отримати несанкціонований доступ, перехопити конфіденційні дані або ввести в оману.

MAC Spoofing атаки. Як правило, мережевий коммутатор L2 рівня за замовчуванням динамічно вивчає MAC-адресу пристроя підключеного до порту, та не контролює кількість MAC-адрес, які він може вивчити на одному порту, і не блокує записи в CAM-таблиці. Зловмисник може використати ці вразливості декількома способами.

- По-перше, підробити (продублювати) MAC-адресу іншого легітимного хоста в локальній мережі. Хакер відправляє Ethernet кадр з такою ж самою MAC-адресою