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.

і навіть розподілом ролей. У деяких випадках зловмисники пропонують послуги «фішинг як сервіс» (Phishing-as-a-Service), коли будь-хто може купити доступ до готових інструментів атаки.

Окрім фінансових втрат, наслідками фішингу є витік критично важливої інформації, зокрема даних облікових записів, конфіденційної кореспонденції, внутрішніх документів. Такі атаки часто є початковою ланкою для масових заражень шкідливим ПЗ, включно з бекдорами, кейлогерами та інструментами для повного контролю над інфраструктурою [2].

Таким чином, одна фішингова атака може відкрити ворота до повномасштабної компрометації системи. У разі втрати корпоративного доступу — це загрожує зривом операцій, фінансовими штрафами, репутаційними втратами та навіть кримінальною відповідальністю за порушення законодавства у сфері захисту персональних даних.

Урядова команда CERT-UA постійно фіксує нові фішингові сайти, які імітують державні портали. Наприклад, підроблений сайт portal.nazk.org.ua маскувався під офіційний реєстр декларацій portal.nazk.gov.ua. Громадянам рекомендується звертати увагу на домен .gov.ua, уникати відкриття підозрілих листів і не вводити дані без перевірки сайту [1].

Цей приклад ще раз доводить, наскільки легко зловмисники можуть імітувати навіть офіційні ресурси, якщо користувачі не звикли уважно перевіряти адреси сторінок. Саме тому особливої ваги набуває просвіта та цифрова гігієна населення.

Фішинг — це не просто технічний виклик, а глибоко психологічна та соціальна загроза, що базується на довірі, неуважності або стресі. В умовах гібридної війни він перетворюється на ефективну зброю в руках супротивника, здатну паралізувати роботу цілих установ чи підрозділів. Успішна протидія цій загрозі можлива лише за умов поєднання технологічних рішень (фільтрів, антивірусів, моніторингових систем) та людського чинника — навчання, пильності, обізнаності. Особливої важливості набуває тісна взаємодія між державними органами, приватними компаніями та громадянським суспільством, адже тільки спільними зусиллями можна забезпечити реальний захист у цифровій війні, що точиться сьогодні на кіберфронті України.

Література:

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

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

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

4. Аналітичний звіт з питань кібербезпеки в Україні: загрози та протидія. – ХНТУ, 2024. – С. 330–345.

УДК: 004.056 : 004.4

Царенко Євгеній Валентинович
Здобувач другого (магістерського) рівня вищої освіти факультету кібербезпеки, програмної інженерії та комп'ютерних наук, спеціальність «Кібербезпека та захист інформації»
Міжнародний Гуманітарний Університет
i.am.zhenya.tsarenko@gmail.com
Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент

Міжнародний гуманітарний університет
yonalarisa66@gmail.com

ВПЛИВ МІКРОСЕРВІСНОЇ ТА МОНОЛІТНОЇ АРХІТЕКТУРИ НА КІБЕРБЕЗПЕКУ СУЧАСНИХ ДОДАТКІВ

Анотація. *У роботі розглядається вплив вибору архітектурного підходу - монолітного або мікросервісного на кібербезпеку сучасних програмних систем. Проаналізовано ключові відмінності між цими моделями з точки зору захисту даних, контролю доступу, вразливостей та засобів безпеки. Увага приділяється практикам, таким як використання JWT, API Gateway та secrets management, що дозволяють знизити ризики незалежно від обраної архітектури. У висновках підкреслюється необхідність інтеграції безпекових рішень на етапі проєктування архітектури, адже саме від неї значною мірою залежить стійкість додатка до кіберзагроз.*

У сучасній розробці програмного забезпечення дедалі частіше постає вибір між монолітною та мікросервісною архітектурою. Монолітна модель передбачає створення єдиної цілісної системи, тоді як мікросервіси розділяють додаток на незалежні модулі, кожен з яких виконує окрему функцію. Вибір між цими підходами впливає не лише на гнучкість і масштабованість системи, а й на її захищеність. Кібербезпека відіграє ключову роль у забезпеченні стійкості додатків до атак: архітектурні рішення визначають площу атаки, шляхи доступу, способи автентифікації та захисту даних.

Якісні архітектурні рішення сприяють кібербезпеці через впровадження таких принципів як розмежування доступу, шифрування даних та багатошаровий захист. Вдала архітектура також допомагає усувати вразливості завдяки спрощенню тестування. [1]

Наприклад, у класичній веб-програмі з монолітною структурою реалізація механізму єдиної автентифікації (Single Sign-On) можлива централізовано, через єдину точку обробки запитів. Це знижує ризик розбіжностей у логіці контролю доступу та полегшує аудит безпеки. На Рис. 1 представлено приклад монолітної архітектури.

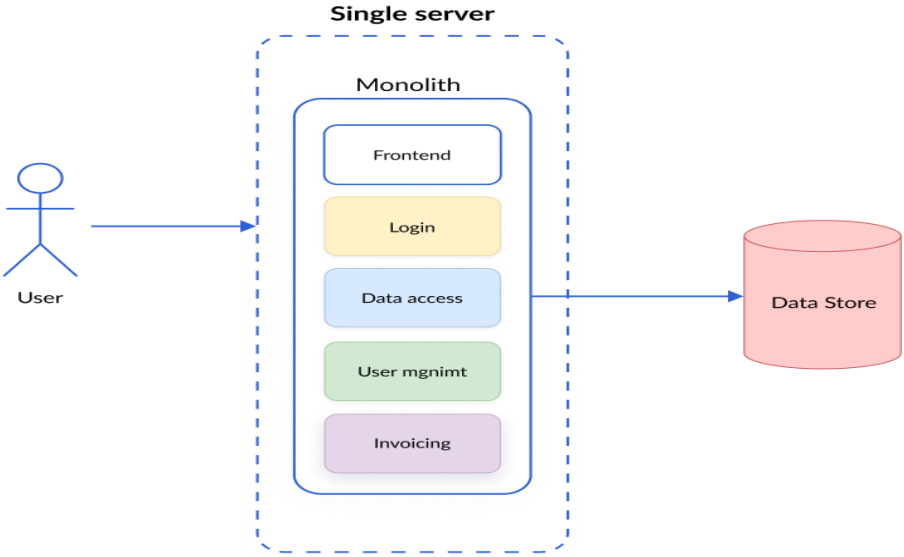

Рисунок 1 – Приклад монолітної архітектури

У мікросервісних системах збільшується кількість взаємодій між сервісами, що потребує додаткових зусиль для забезпечення автентифікації, авторизації, шифрування трафіку й моніторингу безпеки на міжсервісному рівні.

Безпека більше не може бути другорядною, коли справа стосується проектування програмного забезпечення. Кожен розробник повинен дивитися свій код через призму кібербезпеки. Жодна з архітектур не ідеальна, але розробники повинні зважити їхні переваги та недоліки, щоб забезпечити безпеку застосування [3].

В мікросервісній архітектурі одна з головних причин, чому виникають проблеми з безпекою, полягає в тому, що вона має більш складну структуру порівняно з традиційними монолітними програмами. У монолітних програмах усі компоненти знаходяться в одній кодовій базі та зазвичай працюють на одному сервері. Це полегшує впровадження заходів безпеки в центральній точці. Однак у мікросервісах кожна служба розробляється, розгортається та масштабується незалежно. Це означає, що кожна служба має власні вимоги до безпеки та має бути захищена окремо [2]. На Рис. 2 представлено приклад мікросервісної архітектури.

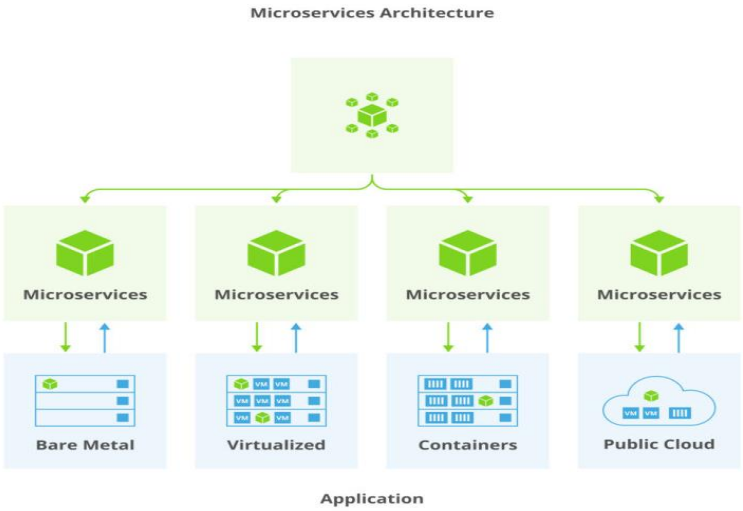

Рисунок 2 – Приклад мікросервісної архітектури

Відтак перевірка безпеки програмного забезпечення стає в розробці пріоритетом №1. Сьогодні добре продумана архітектура має бути відповіддю на загрози кібербезпеки. Вдалі патерни проєктування можуть мінімізувати вразливість системи, забезпечити захист даних та гарантувати надійність роботи ПЗ [1].

Приклади захисту додатків при різній архітектурі:

1) Використання JWT (JSON Web Tokens).

Алгоритм роботи передбачає, що один сервіс (auth) видає підписаний токен, а інші сервіси перевіряють його без звернення до auth.

У мікросервісній архітектурі JWT дозволяє безпечно передавати підтвердження ідентичності між сервісами без централізованого зберігання сесій.

2) API Gateway як захисний бар'єр.

Призначення:

— Аутентифікація та авторизація запитів
— Трафік-фільтрація (rate limiting, IP whitelist/blacklist)
— Захист від типових атак (наприклад, brute-force)

API Gateway — це перший рівень захисту мікросервісної архітектури, що знижує ризик прямого доступу до внутрішніх сервісів.

3) Secrets Management (Vault, AWS Secrets Manager)

Застосовується у CI/CD, при з'єднанні з БД, API

Призначенням є забезпечення безпечного зберігання токенів, паролів, ключів та ротація ключів без зміни коду.

Централізоване управління секретами допомагає уникнути витоку критичних даних з коду чи середовища.

Вибір між монолітною та мікросервісною архітектурою повинен враховувати не лише технічні та бізнесові потреби, а й потенційні ризики для кібербезпеки. Моноліт забезпечує

централізований контроль і меншу кількість точок входу, але вразливість в одній частині може поставити під загрозу всю систему. Натомість мікросервіси дають гнучкість та ізоляцію компонентів, проте вимагають ретельного підходу до захисту міжсервісної комунікації, автентифікації та моніторингу. У результаті, ефективна безпека додатку значною мірою залежить від правильного балансу між архітектурним підходом і впровадженими механізмами захисту.

Література:

1. Архітектура програмного забезпечення: як правильне проєктування забезпечує ефективність та безпеку. Березень 2025 року. [Електронний ресурс] URL: https://wezom.com.ua/ua/blog/arhitektura-programnogo-zabezpechennya (дата звернення 30.06.2025)

2. The Importance of Microservices Architecture and Security Challenges. Березень 2025 року. [Електронний ресурс] URL: https://www.hostragons.com/en/blog/security-challenges-in-microservices-architecture (дата звернення: 30.06.2025).

3. Microservices vs. Monoliths: Why Every Developer Must Also Be a Cybersecurity Professional. Березень 2023 року. [Електронний ресурс] URL: https://vfunction.com/blog/microservices-vs-monoliths-why-every-developer-must-be-cybersecurity-professional (дата звернення: 30.06.2025).

Пахолюк Олег Ігорович
Аспірант, спеціальність 125 «Кібербезпека та захист інформації»,
Науковий керівник
Йона Лариса Григорівна, к.т.н., доцент
Міжнародний гуманітарний університет
yonalarisa66@gmail.com

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ОПТИМІЗАЦІЇ ПРОЦЕДУР ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Анотація*. У статті запропоновано підхід до виявлення вразливостей інформаційних систем, що базується на вдосконаленні процедур ідентифікації та автентифікації. Розглянуто основні недоліки існуючих методів захисту, які можуть призводити до компрометації безпеки. Наведено математичну модель, яка дозволяє прогнозувати потенційні вразливості на ранніх етапах і забезпечувати високий рівень кіберзахисту.*

Вступ

Інформаційні системи є основою багатьох бізнесових, адміністративних і технологічних процесів та охоплюють етапи збереження, оброблення, видалення та передавання даних.

Проте кіберзлочинці постійно вдосконалюють свої методи атак та здатні обходити традиційні заходи безпеки, тобто загрози розвиваються так само швидко, як і технології