

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.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

Співголови

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.

Члени організаційного комітету

БЕРКМАН Л.Н. – д.т.н., проф., Державний університет телекомунікацій, м.Київ, Україна.

КЛИМАШ М.М. – д.т.н., проф., Національний університет «Львівська політехніка», м.Львів, Україна.

ЛЕМЕШКО А. В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РИХЛІК А. – к.т.н., Лодзький технічний університет, м.Лодзь, Польща

СЕМЕНКО А.І. – д.т.н., проф., Національний авіаційний університет, Київ, Україна.

СІМЕНС Е. – д.т.н., проф., Анхальтський університет прикладних наук, м.Кетен, Німеччина.

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

СУНДУЧКОВ К.С. – д.т.н., проф., Національний авіаційний університет, м. Київ, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

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

РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

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.

ЛЕМЕСЬКО 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.

Khniunin S.H.
PhD in Technical Sciences, Associate Professor,
Department of Information Technologies,
International Humanitarian University,
Odessa, Ukraine
sergii.khniunin@gmail.com

Shvedu M.I.
2nd-year Master's student in Cybersecurity and Information Protection,
International Humanitarian University,
Odessa, Ukraine
blackangel2657@gmail.com

AN ANALYSIS OF ENTERPRISE OPERATIONAL STABILITY IN RELATION TO COMMUNICATION AND ENERGY SYSTEMS

Abstract: *This paper examines key global incidents involving damage to both power and communication lines between 2023 and 2025. It analyses their impact not only on transnational distributed enterprises, but also on entire nations, affecting critical infrastructure, economic activity, social stability, and national security. A classification of equipment failures is presented, distinguishing between natural (environmental) and intentional causes. These disruptions influence not only private entities but also state-level operations. With society undergoing complete digitalisation, such events now result in severe economic losses and casualties. The once-reliable practice of communication line redundancy has recently failed to deliver the expected level of resilience.*

Keywords: *distributed enterprises, communication networks, power outages, economic losses*

The modern world is inextricably linked to distributed enterprises—organisations that no longer operate within a single office but rely on integrated information platforms spanning multiple regions, nations, or even continents. These entities are heavily dependent on uninterrupted access to databases, communication channels, and energy systems. Disruptions in these infrastructures pose more than just technical inconveniences—they have the potential to halt supply chains, cripple infrastructure, and cause economic damage on a global scale [1].

A classification of distributed enterprises is presented in Fig. 1.

Organisations of this kind include:

- Banks – reliant on global transactions, distributed processing centres, and financial gateways.
- Pharmacies – requiring real-time data on stock availability, prices, and logistics.
- Postal and logistics services (such as UkrPoshta, Nova Poshta) – dependent on routing, tracking, and electronic documentation.
- Taxi and transport platforms (Uber, Bolt, DHL) – entirely reliant on servers, GPS systems, and route optimization.

Equally critical, though often overlooked, are sectors such as:

- Mining and oil & gas companies – employing remote sensors and offshore drilling platforms, with data centralised at headquarters.
- Chemical and metallurgical plants – frequently structured as distributed systems, where safety metrics, temperatures, and chemical reactions are monitored from a central server.

- Shipping and freight enterprises (e.g., Maersk, MSC) – dependent on global navigation systems, customs databases, and real-time cargo tracking. Any disruption in IT infrastructure can bring an entire fleet to a standstill worldwide.

Distributed enterprises

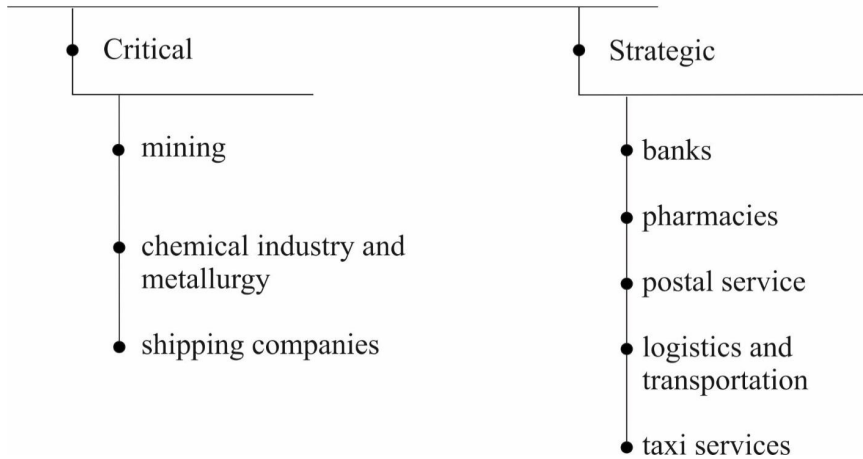


Figure 1 - Classification of distributed enterprise types

These enterprises cannot function in isolation—they are nodes in a global network. This means that a single point of failure, such as a power outage or communication breakdown in one country, can trigger cascading consequences in another.

Hence, increasing emphasis is placed on the reliability of communication and energy systems, as these underpin the uninterrupted operation of global business. Real-world case studies reveal that faults in information and power networks are not anomalies—they are part of an escalating pattern of systemic risk.

Historically, such failures received scant attention. Threats were perceived as abstract and their consequences exaggerated. Disruptions were primarily discussed within technical communities [2] and viewed more as localised mishaps [3] than as global warning signs.

Today, however, society's growing dependence on stable energy and communication infrastructure renders each new incident a cause of tangible economic, social, and political damage. Among the most significant cases in recent years are:

- Widespread power outage in Chile (February 2025) – over 70% of the country was left without electricity, affecting major hospitals and transport hubs [4].

- National blackout in Kenya (December 2024) – the entire country was plunged into darkness for several hours. The main airport ceased operations, trains halted, and communication networks largely collapsed [5].

- Complete communication loss in Gaza (October 2023) – amid military conflict, residents lost access to mobile and internet services, making emergency response and humanitarian coordination impossible [6].

- Telecommunication blackout in Libya following floods (September 2022) – after severe flooding, several regions near Derna became entirely cut off from the outside world [7].

These catastrophes can be categorised as either natural—resulting from environmental events and associated equipment failure—or intentional, including terrorism and military action. In cases of natural disaster, enterprises can mitigate risk through technical innovation and

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).

Срьоменко 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