PROCEEDINGS

1ST INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «RESILIENT SYSTEMS: SECURE DIGITAL TECHNOLOGIES AND CRITICAL INFRASTRUCTURE» (RS-2025)

June 27, 2025

Drohobych, 2025

UDC 004.56/004.08/519.6
DOI: 10.5281/ZENODO.15775240

CONFERENCE ORGANIZING:

Donetsk National Technical University
G. E. Pukhov Institute for Modeling Problems in Energy Engineering, NAS of Ukraine
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Cherkasy State Technological University
Ternopil Ivan Puluj National Technical University
State University "Zhytomyr Polytechnic"
Lviv State University of Life Safety
National Aerospace University "Kharkiv Aviation Institute"
Berdyansk State Pedagogical University
Odesa National University of Economics
State Service for Special Communications and Information Protection of Ukraine
National Bank of Ukraine
University of Zielona Góra (Poland)
Academy of Silesia (Poland)
State University of Western Paraná (Brazil)
Copenhagen Business School (Denmark)

Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. 184 pp.

The proceeding contains materials of the conference on theoretical and practical problems of AI, cybersecurity and critical infrastructures.

Recommended for publication by the Academic Council of the State Higher Educational Institution 'Donetsk National Technical University'

The materials are submitted in the author's edition

© Donetsk National Technical University, 2025

ORGANIZING COMMITTEE

Chair of the Organizing Committee:

Iaroslav DOROHYI – DSc, Professor, Head of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Deputy Chair of the Organizing Committee:

Mykyta ALEKSANDROV – PhD**,** Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Members of the Organizing Committee:

Yevhen BASHKOV – DSc, Professor, Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Tetiana ALTUKHOVA – CSc, Associate Professor, Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Iryna NAZAROVA – CSc, Associate Professor, Associate Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Yelyzaveta YEZHOVA – Assistant Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Dmytro KHOMA – Assistant Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

PROGRAM COMMITTEE

Chair of the Program Committee:

Yaroslav DOROHYI – DSc, Professor, Head of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Deputy Chair of the Program Committee:

Yevhen BASHKOV – DSc, Professor, Professor of the Department of Applied Mathematics and Informatics, DonNTU (Ukraine).

Members of the Program Committee:

Volodymyr MOKHOR – Corresponding Member of NASU, DSc, Professor, Director, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Oleksandr CHEMERYS – DSc, Professor, Deputy Director for Research, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Serhii HILHURT – DSc, Senior Researcher, Head of the Department of Mathematical and Econometric Modeling, G.E. Pukhov Institute for Modeling in Energy Engineering NASU (Ukraine).

Dmytro LANDE – DSc, Professor, Head of the Department of Information Security, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Ukraine).

Anatolii CHEPYNOHA – CSc, Associate Professor, Dean of the Faculty of Information Technologies and Systems, Cherkasy State Technological University (Ukraine).

Roman PROSKUROVSKYI – CSc, Associate Professor, Head of the Critical Infrastructure Protection Division, National Bank of Ukraine (Ukraine).

Oleksandr BAKALYNSKYI – CSc, Senior Researcher, Senior Specialist of the Critical Infrastructure Protection Department, National Bank of Ukraine (Ukraine).

Serhii MARTSENKO – CSc, Associate Professor, Associate Professor of the Department of Computer Science, Ternopil Ivan Puluj National Technical University (Ukraine).

Andrii YEFIMENKO – CSc, Associate Professor, Head of the Department of Computer Engineering and Cybersecurity, State University "Zhytomyr Polytechnic" (Ukraine).

Maryna HRAF – PhD, Associate Professor, Head of the Department of Computer Science, State University "Zhytomyr Polytechnic" (Ukraine).

Nataliia MASLOVA – CSc, Associate Professor, Department of Information Security Management, Lviv State University of Life Safety (Ukraine).

Vitalii BEZSHTANKO – CSc, Deputy Head of the Unit of Cyber Protection, Administration of the State Service of Special Communications and Information Protection of Ukraine (Ukraine).

Maryna KOLISNYK – CSc, Associate Professor, Associate Professor of the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute" (Ukraine).

Viktoriia HUROCHKINA – Dr. hab., Professor UZ, Department of International Economics and Market Analysis, Institute of Economics and Finance, University of Zielona Góra (Poland).

Olha DEHTIAREVA – DSc, Professor, Odesa National University of Economics (Ukraine), Copenhagen Business School (Denmark).

Tetiana NESTORENKO – PhD, Professor AS, Academy of Silesia (Poland).

Olena TSVIRKO – DSc, Professor, Western Paraná State University (Brazil).

CONTENTS

SECTION 1: ARTIFICIAL INTELLIGENCE

SECTION 2: CYBERSECURITY AND CRITICAL INFRASTRUCTURE

SECTION 3: INFORMATION TECHNOLOGIES

SECTION 4: COMPUTER AND MATHEMATICAL MODELING

SECTION 5: DIGITAL SYSTEMS

CRITERIA FOR ORGANIZATIONAL RESILIENCE TO EMERGENT INFORMATION SECURITY RISKS

Volodymyr Mokhor, Oleksandr Bakalynskyi, Vitalii Bezshtanko, Iaroslav Dorohyi, Vasyl Tsurkan

КРИТЕРІЇ РЕЗИЛЬЄНТНОСТІ ОРГАНІЗАЦІЙ ДО ЕМЕРДЖЕНТНИХ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мохор В.В.[1], Бакалинський О.О.[1], Безштанько В.М.[2], Дорогий Я.Ю.[3], Цуркан В.В.[1,4]
[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова
Національної академії наук України,
[2]Донецький національний технічний університет,
[3]Державна служба спеціального зв’язку та захисту інформації України,
[4]Національний технічний університет України «Київський політехнічний інститут»

Анотація. Проаналізовано передумови обробляння емерджентних ризиків інформаційної безпеки. Встановлено їхню обумовленість наявністю перевіреної інформації і, сформованих на її основі, знань. Цим визначено критерії резильєнтності організацій до мінливих внутрішніх і зовнішніх обставин діяльності.

Вступ. Нині однією з типових особливостей діяльності організацій є мінливість як внутрішніх, так і зовнішніх обставин. Зазначена специфіка може призводити до недостатності або відсутності перевіреної інформації. Потреба у ній пов’язана з необхідністю приймання обґрунтованих рішень про обробляння насамперед емерджентних (нових) ризиків інформаційної безпеки (наприклад, кібербезпеки, використання хмарних технологій і, зокрема, штучного інтелекту) [1, 2]. Тож наявністю перевірної інформації і, як наслідок, сформованих на її основі, знань обумовлюється здатність організацій до сприймання, відновлювання і адаптування з урахуванням мінливості внутрішніх і зовнішніх обставин діяльності. Така здатність тлумачиться як резильєнтність організацій або організаційна резильєнтність (англ. organizational resilience) [1].

Результати. З огляду на сформульовану здатність організацій визначаються критерії її резильєнтності. Серед них виокремлюються [1]:

1) передбачення (англ. anticipation) – здатність організацій готуватися до проявляння неочікуваних або маловірогідних подій. Це може досягатися завдяки впроваджуванню або розвиванню відповідних можливостей реагування. Наприклад, завдяки систематичному перегляданню обставин діяльності організацій;
2) протидіяння та відновлювання (англ. resistance, recovery) – здатність організацій протидіяти реалізуванням емерджентних загроз інформаційній безпеки. До того ж відновлюватися після їх реалізування і, зокрема, настання негативних наслідків. Унаслідок цього організації повертаються до нормального стану їхньої діяльності;
3) адаптування (англ. adaptation) – здатність організацій ефективно обробляти емерджентні ризики інформаційної безпеки шляхом обирання відповідних заходів і засобів. Крім того, адаптуватися до проявляння руйнівних подій (насамперед асоційованих з емерджентими загрозами) і для запобігання їхнім проявам трансформовувати їхню діяльність.

Висновки. Отже, визначання критеріїв резильєнтності організацій дозволяє встановлювати їхню здатність до сприймання, відновлювання і адаптування з урахуванням мінливості внутрішніх і зовнішніх обставин діяльності. Як наслідок, виокремлювати серед них ті, що обробляють емерджентні ризики інформаційної безпеки на основі перевіреної інформації і сформованих на її основі знань.

ЛІТЕРАТУРА

1. ISO/TS 31050:2023. Risk management. Guidelines for managing an emerging risk to enhance resilience. [Valid from 2023-10-27]. URL: https://www.iso.org/standard/54224.html (accessed on: 10.06.2025).
2. Мохор В.В., Бакалинський О.О., Дорогий Я.Ю., Цуркан В.В. Парадигма нових ризиків кібербезпеки. Кібербезпека енергетики : матеріали науково-практичної конференції : КБЕ-2024 (Київ, 29 травня 2024 р.). Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2024. С. 116–117. DOI: https://doi.org/10.5281/zenodo.14601760.