Тетяна НІКІТІНА,
кандидат технічних наук,
доцент кафедри кібербезпеки та інтелектуальних
інформаційних технологій Національного аерокосмічного
університету «Харківський авіаційний інститут»,
ORCID: https://orcid.org/0009-0000-7549-1017,
e-mail: t.nikitina@khai.edu

Ольга МОРОЗОВА,
доктор технічних наук,
професор кафедри кібербезпеки та інтелектуальних
інформаційних технологій Національного аерокосмічного
університету «Харківський авіаційний інститут»,
ORCID: https://orcid.org/0000-0001-7706-3155,
e-mail: o.morozova@khai.edu

Вячеслав ХАРЧЕНКО,
доктор технічних наук,
професор, завідувач кафедри кібербезпеки та інтелектуальних
інформаційних технологій Національного аерокосмічного
університету «Харківський авіаційний інститут»,
ORCID: https://orcid.org/0000-0001-5352-077X,
e-mail: v.kharchenko@csn.khai.edu

DOI: https://doi.org/10.32620/pls.2025.8.62

РЕЗИЛЬЄНТНІСТЬ ІНФРАСТРУКТУРИ УНІВЕРСИТЕТУ В УМОВАХ ВІЙНИ: СИСТЕМНА МОДЕЛЬ ТА ЇЇ КОМПОНЕНТИ

Анотація. *Університети, що працюють в умовах підвищених ризиків, потребують стійких інформаційних інфраструктур для підтримання діяльності під час гібридних загроз. У статті представлено багаторівневу модель резильєнтності інфраструктури університету, яка поєднує кіберзахист, ситуаційну обізнаність, управління ризиками, інфраструктурну стійкість, цифровий двійник та AI-підтримку рішень. Людиноцентричний шар взаємодії на основі аватара забезпечує персоналізовану комунікацію, сповіщення про небезпеку та адаптивні реакції. Модель інтегрує зовнішні цифрові дані для підвищення обізнаності та створює основу для практичної реалізації і подальших досліджень щодо резильєнтності університетів у воєнний час.*

Ключові слова: *Критична інфраструктура, резильєнтність, цифрова стійкість, гібридні загрози, цифровий двійник, кібербезпека, ситуаційна обізнаність, AI-підтримка рішень, управління ризиками, людиноцентричні системи.*

Резильєнтність освітніх інституцій у період війни є одним з ключових елементів загальної суспільної стійкості. Університети виконують функції підготовки фахівців, проведення наукових досліджень та підтримання безперервного розвитку держави. Умови гібридних загроз створюють суттєві обмеження для фізичної, цифрової та соціальної інфраструктури, що підсилює потребу у побудові адаптивних цифрових екосистем. У цьому дослідженні представлено теоретичну модель цифрової екосистеми резильєнтного університету, яка поєднує багаторівневий моніторинг, цифровий двійник, модуль управління університетом та людиноцентричний підхід.

Мета дослідження полягає у формуванні моделі цифрової екосистеми університету, здатної підтримувати освітні та адміністративні процеси у періоди гібридних загроз. У межах цієї мети визначено такі завдання: сформувати структуру моделі, описати взаємодію між її компонентами, обґрунтувати роль системи управління університетом як центрального інструмента адаптивного управління, а також визначити критерій резильєнтності цифрової екосистеми університету.

Огляд сучасних підходів та аналіз кейсу України в умовах гібридних загроз. Цифрова екосистема України, зокрема застосунок «Дія» [1], забезпечила безперервний доступ громадян до

ключових документів, освітніх записів та державних сервісів навіть у період масових переміщень та воєнних загроз. Завдяки попередній десятирічній цифровізації та впровадженню хмарних технологій, держава зберегла функціональність критичних процесів, що стало фундаментом цифрової резильєнтності в умовах війни.

У публікації [2] досліджено особливості цифрової трансформації українських організацій у період війни та визначено ключові функції цифрової резильєнтності. Автори встановили, що критично важливим механізмом є режим "freeze-mode", який дозволяє тимчасово зупиняти процеси для збереження безпеки персоналу. Дослідники також підкреслюють значення багатоканальної взаємодії та психологічної підтримки, що забезпечуються цифровими системами комунікації в умовах гібридних загроз.

У монографії [3] подано узагальнений огляд цифрової резильєнтності України у воєнний період, заснований на міжнародних стандартах кібербезпеки, серед яких NIST Cybersecurity Framework, директива Європейського Союзу (ЄС) NIS2 та індекси GCI, NCSI, що застосовуються для оцінювання національної стійкості. У монографії підкреслено, що партнерські мережі ЄС та міжнародні академічні інституції сприяють модернізації українських цифрових сервісів, зокрема платформи «Дія», яка підтримує неперервність державних послуг під час інфраструктурних атак. Автори роблять висновок, що взаємодія державних структур, міжнародних організацій та приватного сектору формує багаторівневу модель цифрової безпеки, яку нині розглядають як перспективний приклад глобальної кіберкооперації.

У нещодавньому дослідженні автори [4] проаналізували як сучасні регуляції у сфері кібербезпеки формують резилієнтність цифрових систем, порівнюючи підходи США та ЄС. Робота демонструє, що обидві моделі відходять від виключно технічного розуміння безпеки і розглядають її як елемент суспільної стійкості та довіри. Дослідники підкреслюють що європейський підхід приділяє більше уваги інклюзивності та захисту вразливих користувачів, а американський – фокусується на прозорості ланцюгів постачання та відповідальності виробників програмного забезпечення.

У відповідь на триваючу кризу Фінляндія посилила свою комплексну стратегію безпеки, організовуючи регулярні національні навчання та симуляції для підготовки до гібридних загроз у тісній співпраці з ЄС та НАТО. Університет прикладних наук JAMK через свій центр кібербезпеки, Центр технологій безпеки Jyväskylä, активно бере участь у цих симуляціях, зосереджуючись як на цифрових, так і на фізичних загрозах критичній інфраструктурі [5].

Під час війни Україна розробила надійну модель цифрової стійкості, перемістивши критичну інфраструктуру до багатохмарних та транскордонних центрів обробки даних і цей підхід був підтриманий Естонією, яка започаткувала концепцію data embassy та запропонувала допомогу Україні у забезпеченні цифрової безперервності під час конфлікту [6]. Такі стратегії також можуть бути ефективно впроваджені прикордонними університетами для забезпечення безперервності освіти в умовах гібридних загроз.

Результати аналізу показують, що сучасна цифрова резилієнтність формується як багатокомпонентна система, яка охоплює кібербезпеку, міжнародну взаємодію, безперервність цифрових сервісів, захист критичної інфраструктури та здатність інституцій адаптуватися до гібридних загроз. Досвід Фінляндії, України та Естонії демонструє, що ключову роль відіграють як технічні рішення, так і стратегічні партнерства, включно з транскордонним зберіганням даних та участю у національних і міжнародних навчаннях. Для університетів в кризових умовах така багаторівнева модель може стати основою забезпечення стійкої та безперервної освіти під час криз. Концепція цифрового двійника [7, 8] додатково посилює цю модель, оскільки дозволяє інтегрувати моніторинг, прогнозування та підтримку рішень у єдину адаптивну екосистему резильєнтності.

Практичний досвід функціонування українських університетів у періоди гібридних загроз продемонстрував значний вплив цифрових інструментів на забезпечення безперервності освітнього процесу. Навіть за умов обмеженого доступу до ресурсів академічні інституції змогли підтримувати навчання та адміністративну діяльність завдяки мобільним пристроям, хмарним платформам [9] і гнучким інформаційним системам. Український кейс показав, що університети з розвиненими цифровими системами [10] зберігають вищий рівень стійкості, а також спроможність адаптуватися до швидких змін середовища.

Модель цифрової екосистеми резильєнтного університету. На основі проведеного аналізу досліджень цифрової резильєнтності та практик реагування на гібридні загрози в Україні пропонується модель резильєнтності університету (рис. 1), орієнтована на безперервність освітніх процесів і захист користувачів в умовах підвищеного ризику. Запропонована архітектура поєднує технічні, організаційні та людиноцентричні компоненти, що разом формують інтегровану систему адаптації та стійкості університету.

В українському кейсі гібридної війни визначено три базові домени загроз: фізичні загрози, пов'язані з руйнуванням інфраструктури та небезпекою для життя; цифрові загрози, що стосуються атак на інформаційні системи та критичні сервіси; людські загрози, що включають психологічний стрес, втрату зв'язку та неможливість взаємодії з інституціями.

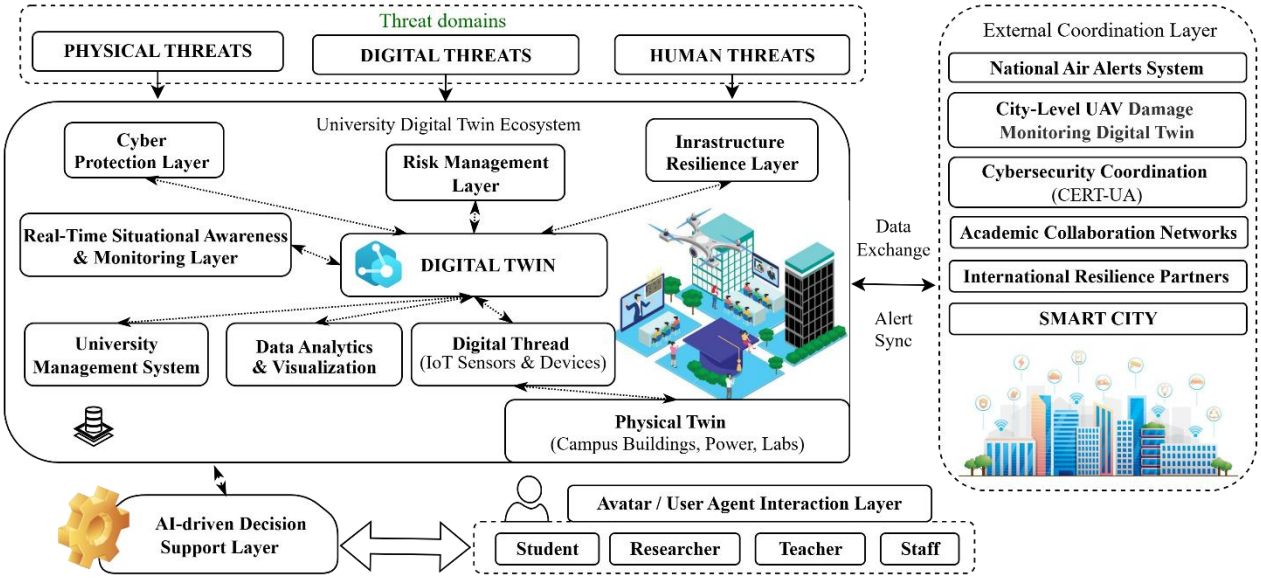

Рис. 1. Системна модель резильєнтності інфраструктури університету в умовах гібридних загроз

Запропонована модель університетської резильєнтності включає такі ключові компоненти:

Cyber Protection Layer. Спрямований на забезпечення кіберзахисту, виявлення атак, запобігання вторгненням та підтримку цілісності цифрової інфраструктури університету;

Real-Time Situational Awareness and Monitoring Layer. Забезпечує моніторинг загроз у режимі реального часу, включно з даними від сенсорів та зовнішніх джерел, для формування актуальної картини ризиків;

Risk Management Layer. Містить механізми оцінки та прогнозування ризиків, підтримує прийняття рішень і дозволяє університету адаптуватися до змінних умов;

Infrastructure Resilience Layer. Спрямований на підтримання функціонування енергетичних, комунікаційних та інших систем університету за умов руйнувань або перебоїв;

Digital Twin Ecosystem. Інтегрує цифровий двійник університету з фізичними об'єктами campus-інфраструктури, забезпечує цифрове моделювання загроз і прогнозування сценаріїв розвитку подій;

Digital Thread (IoT Sensors & Devices). Збирає, передає та синхронізує дані між фізичним та цифровим середовищем для підтримки аналітики, моніторингу та керування;

Data Analytics and Visualization Layer. Обробляє великі обсяги даних, надає візуалізацію стану системи, генерує рекомендації та формує основу AI-підтримки рішень;

AI-driven Decision Support Layer. Автоматизує аналіз ризиків, пропонує варіанти реагування, може активувати режими пріоритизації або "freeze-mode" для зупинки небезпечних процесів;

University Management System. Функціонує як ядро адміністративних сервісів, забезпечує безперервність освітніх і управлінських процесів навіть у разі евакуації персоналу чи втрати доступу до комп'ютерів;

Avatar (User Agent Interaction Layer). Людиноцентричний інтерфейс взаємодії, який забезпечує персоналізовану комунікацію зі студентами, викладачами, дослідниками та персоналом, включно з психологічною підтримкою, сповіщеннями та рекомендаціями.

Окрім внутрішніх механізмів стійкості, модель передбачає інтеграцію з зовнішніми системами, що критично важливо для університетів, розташованих у прикордонних регіонах. Така взаємодія охоплює системи оповіщення про небезпеку, національні й муніципальні цифрові сервіси, мережі академічної кооперації, міжнародних resilience-партнерів та смарт-міські платформи. Ці системи забезпечують доступ до даних про загрози, інструменти комунікації, додаткові ресурси та канали підтримки, посилюючи загальну резильєнтність університету.

Запропонована архітектура є людино-центричною, оскільки в її основі лежить захист, підтримка та цифрова взаємодія з користувачем. Поєднання Digital Twin, AI, багаторівневого моніторингу та міжнародної взаємодії формує інтегровану модель, здатну забезпечити високу стійкість університету в умовах гібридних загроз.

Висновки. Запропонована модель резильєнтності університету демонструє потенціал інтеграції цифрових технологій, моніторингу загроз та людиноцентричних механізмів взаємодії для забезпечення безперервності освітніх процесів у період гібридних загроз. Разом з тим модель потребує подальшого доопрацювання і практичної реалізації, що особливо актуально для університетів та закладів освіти, які функціонують у зонах підвищеного ризику.

Подальший розвиток запропонованої моделі базуватиметься на результатах попередніх

досліджень авторів [10-12], у яких сформовано концептуальні основи цифрової стійкості університетської інфраструктури в умовах війни, принципи керування резильєнтність для кіберфізичних систем, а також окреслено підходи до інтелектуальної обробки та моніторингу великих потоків даних, необхідних для підтримки цифрового двійника та системи ситуаційної обізнаності.

Таким чином, подальше дослідження зосереджуватиметься на інтеграції методів обробки великих даних, системної аналітики та моделювання загроз у цифровому двійнику університету. Це дозволить розширити запропоновану модель та забезпечити її практичну застосовність у реальних умовах гібридних загроз.

Бібліографічні посилання

1. Ingram G., Vora P. Ukraine: Digital resilience in a time of war. The Brookings Institution, 2024. URL: https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/

2. Berbyuk Lindström N., Razmerita L., Prokopenko S., Popovich N. Building Digital Resilience in Major Shocks: How Ukrainian Organizations Enact Digital Transformation in Times of War. Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS), 3–6 January 2024, Honolulu. Honolulu, 2024. DOI: https://doi.org/10.24251/HICSS.2024.816

3. Vasylieva T., Zakharkin O., Yarovenko H. Digital transformations of Ukraine's cybersecurity system in wartime. Hamburg: The Academic Research and Publishing UG, 2025. 163 p. DOI: https://doi.org/10.61093/978-3-911748-05-6/2025

4. Kelemen R., Squillace J., Medvácz Á., Cappella J., Bucko B., Mazuch M. Cybersecurity Regulations and Software Resilience: Strengthening Awareness and Societal Stability. Social Sciences, 2025, 14(10), 578. Available at: https://doi.org/10.3390/socsci14100578

5. Edvardsen, A.: Finland Strengthens Cybersecurity in the North with Extensive Exercising. High North News, February 12 (2025). [Online]. https://www.highnorthnews.com/en/finland-strengthens-cybersecurity-north-extensive-exercising

6. Mamediieva G., Moynihan D. Digital Resilience in Wartime: The Case of Ukraine. Public Administration Review, 2023, 83(5). Available at: https://doi.org/10.1111/puar.13742

7. Abarnikov, Y., Kharchenko, V., & Morozova, O. "Equipment Monitoring System with Use of Digital Twins and Internet of Things: Algorithms, Architecting and Experiments." In: Proc. 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Cracow, Poland, Sept. 22–25, 2021, pp. 75–80. https://doi.org/10.1109/IDAACS53288.2021.9661033

8. Kharchenko, V., Morozova, O., Illiashenko, O., & Sokolov, S. "Combination of Digital Twin and Artificial Intelligence in Manufacturing Using Industrial IoT". In: Proc. 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, May 14–18, 2020, pp. 196–201.https://doi.org/10.1109/DESSERT50317.2020.9125038

9. Tarasenko, S., Vorontsova, A., Régent, V., Soss, J., & Mylenkova, R. Science mapping analysis of challenges surrounding cloud universities and their impact on the resilience of higher education. Knowledge and Performance Management, 9(2), 2025, 1–17 pp. https://doi.org/10.21511/kpm.09(2).2025.01

10. Nikitina, T. Kharchenko V., & Morozova, O. "A Resilience Model for Borderline University Infrastructure in Wartime". In Proceedings of the 20th Conference on ICT Technologies in Education, Research, and Industrial Applications (ICTERI 2025), Nice, France, September 1-4, 2025. Available online: https://link.springer.com/book/9783032104762

11. Zaika V., Chuiev O., Morozova O., Nikitina T. Intelligent Web Systems for Automation of Processing and Monitoring of Information Flows. Scientific Journal "Systems of Control, Navigation and Communication", 2025, No. 3. Available at: https://doi.org/10.26906/SUNZ.2025.3.087

12. Поночовний, Ю., & Харченко, В. (2020). Dependability assurance methodology of information and control systems using multipurpose service strategies. Radioelectronic and Computer Systems, 3, pp. 43-58. DOI: https://doi.org/10.32620/reks.2020.3.05.

T. Nikitina, O. Morozova, V. Kharchenko

A resilience of university infrastructure in wartime: system model and its components.

Abstract: Universities operating in high-risk environments require resilient information infrastructures to sustain operations during hybrid threats. The article presents a multi-level model of university infrastructure resilience that combines cyber defense, situational awareness, risk management, infrastructure resilience, digital twin, and AI-enabled solutions. A human-centric avatar-based interaction layer enables personalized communication, hazard alerts, and adaptive responses. The model integrates external digital data to increase awareness and provides a foundation for practical implementation and further research on university resilience in wartime.

Keywords: Critical infrastructure, resilience, hybrid threats, digital twin, cybersecurity, situational awareness, AI decision support, freeze-mode, risk management, human-centric systems.

Зразок для цитування:

Нікітіна Т., Морозова О., Харченко В. Резильєнтність інфраструктури університету в умовах війни: системна модель та її компоненти. Пропілеї права та безпеки, 2025. №8. С. 243-246. DOI: https://doi.org/10.32620/pls.2025.8.62.