

РЕЗИЛЬЄНТНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ЕКОНОМІЧНИХ СУБ'ЄКТІВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Глушко А. Д.

*кандидат економічних наук, доцент,
доцент кафедри фінансів, банківського бізнесу та оподаткування
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
м. Полтава, Україна*

Янко А. С.

*кандидат технічних наук, доцент,
доцент кафедри комп'ютерних та інформаційних технологій і систем
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
м. Полтава, Україна*

В умовах цифрової трансформації економіки резильєнтність інформаційних систем економічних суб'єктів доцільно розглядати як одну з базових передумов забезпечення їх стабільного, безперервного та безпечного функціонування. Посилення залежності підприємств від цифрових технологій об'єктивно актуалізує не лише проблематику інформаційної безпеки, пов'язану із запобіганням втраті, викривленню чи несанкціонованому використанню даних, а й питання формування здатності інформаційних систем зберігати функціональність, підтримувати критично важливі процеси та відновлювати працездатність за умов деструктивного впливу [1].

У сучасному науковому дискурсі резильєнтність інформаційних систем доцільно трактувати як інтегральну системну властивість, що відображає їхню спроможність передбачати потенційні загрози, протидіяти деструктивним впливам, забезпечувати виконання критично важливих функцій за умов порушення штатного режиму роботи, відновлювати функціональність після інцидентів та адаптуватися до змін цифрового середовища [2, 3]. Принципово важливо, що резильєнтність не зводиться лише до наявності технічних засобів кіберзахисту, а формується як результат системного поєднання архітектурних, технологічних, організаційних, управлінських і поведінкових рішень, спрямованих на зменшення вразливості інформаційної інфраструктури та забезпечення стійкості функціонування економічного суб'єкта.

Відповідно, резильєнтність інформаційних систем охоплює комплекс взаємопов'язаних характеристик, а саме: надійність, що забезпечує стабільне функціонування системи в межах визначених параметрів; відмовостійкість, яка дає змогу зберігати критично важливі функції у разі збоїв або пошкодження окремих елементів [4]; адаптивність як здатність системи реагувати на нові загрози й зміни технологічного середовища; відновлюваність, що характеризує швидкість і повноту повернення системи до працездатного стану після інциденту; а також керованість ризиками, яка передбачає систематичне виявлення, оцінювання, моніторинг і мінімізацію загроз цифрового середовища. Саме поєднання зазначених характеристик дозволяє розглядати резильєнтність не як окремих технічний параметр, а як комплексну умову забезпечення функціональної стійкості інформаційних систем економічних суб'єктів.

Досліджуючи резильєнтність інформаційних систем, доцільно враховувати її багаторівневу природу. На рівні окремих цифрових ресурсів вона проявляється у захисті даних, програмного забезпечення, мережних елементів та апаратної інфраструктури. На рівні бізнес-процесів резильєнтність забезпечує здатність економічного суб'єкта продовжувати виконання ключових операцій навіть за умов часткової втрати функціональності інформаційної системи. На організаційному рівні вона пов'язана з наявністю процедур реагування на інциденти, резервного копіювання, планів безперервності діяльності, розподілу відповідальності та підготовки персоналу до роботи в умовах цифрових загроз. На стратегічному рівні резильєнтність інформаційних систем виступає чинником зниження вразливості економічного суб'єкта до зовнішніх і внутрішніх ризиків, підтримання його операційної спроможності та зміцнення конкурентних позицій у цифровізованому середовищі.

В умовах цифрової трансформації економіки зростає кількість загроз, що можуть порушувати функціонування інформаційних систем [5]. Особливо небезпечним є те, що цифрові загрози характеризуються високою швидкістю поширення, латентністю, складністю ідентифікації та значним потенціалом мультиплікативного впливу. Саме тому формування резильєнтності інформаційних систем економічних суб'єктів потребує переходу від реактивної моделі кіберзахисту до проактивної та адаптивної моделі управління цифровими ризиками. Реактивний підхід, орієнтований переважно на усунення наслідків інцидентів після їх виникнення, є недостатнім в умовах високої динаміки цифрових загроз. Натомість проактивний підхід передбачає постійне прогнозування потенційних загроз, моделювання сценаріїв порушення роботи інформаційних систем, тестування їхньої стійкості, формування резервних механізмів функціонування та вдосконалення процедур відновлення [6]. За такого підходу резильєнтність набуває ознак не лише захисного, а й превентивно-

адаптивного механізму, спрямованого на забезпечення безперервності діяльності економічного суб'єкта в умовах невизначеності.

З урахуванням вищезазначеного, до основних напрямів посилення резильєнтності інформаційних систем економічних суб'єктів доцільно віднести: впровадження ризик-орієнтованого підходу до управління цифровою інфраструктурою; формування багаторівневої системи кіберзахисту; забезпечення резервування критично важливих даних і сервісів; розроблення планів безперервності діяльності та аварійного відновлення; регулярне проведення аудиту інформаційної безпеки; підвищення цифрової грамотності персоналу; запровадження систем моніторингу кіберінцидентів; посилення контролю за доступом до інформаційних ресурсів; диверсифікацію цифрових сервісів і постачальників ІТ-рішень; інтеграцію принципів безпеки та стійкості на етапі проєктування інформаційних систем. Реалізація зазначених напрямів дає змогу сформувати більш цілісну систему управління цифровими ризиками, у межах якої технологічні рішення поєднуються з організаційними регламентами, управлінськими процедурами та розвитком культури цифрової безпеки.

Таким чином, резильєнтність інформаційних систем економічних суб'єктів в умовах цифрової трансформації слід розглядати як комплексну системну характеристику, що поєднує здатність до захисту, протидії, відновлення, адаптації і розвитку, та визначає спроможність економічних суб'єктів ефективно функціонувати, зберігати керованість бізнес-процесів і підтримувати конкурентоспроможність у цифровізованому, ризикогенному та висококонкурентному середовищі.

Література:

1. R Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems. *NIST Special Publication 800-160*. Vol. 2. Rev. 1. 2021. DOI: <https://doi.org/10.6028/NIST.SP.800-160v2r1>
2. Лисенко С.М., Харченко В.С., Бобровнікова К.Ю., Щука Р.В. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія. *Радіoeлектронні і комп'ютерні системи*. 2020. № 1. С. 17–28. DOI: <https://doi.org/10.32620/reks.2020.1.02>
3. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. № 5. P. 136–142. DOI: <https://doi.org/10.33271/nvngu/2024-5/136>
4. Yanko A., Mychailichenko O., Hlushko A. Modern methods for protecting and storing data in computer systems to ensure their fault tolerance. *Theoretical and Applied Cyber Security*. 2024. Vol. 6, № 1. P. 72–80. DOI: <https://doi.org/10.20535/tacs.2664-29132024.1.315086>

5. Линда І.С. Нові виклики та загрози цифрової трансформації економіки для системи фінансово-економічної безпеки підприємництва. *Академічні візії*. 2025. № 50. URL: <https://academy-vision.org/index.php/av/article/view/2483>

6. Глушко А.Д., Янко А.С., Білько С.С. Цифрова трансформація бізнес-процесів: безпековий аспект. *Цифрова економіка та економічна безпека*. 2025. № 2(17). DOI: <https://doi.org/10.32782/dees.17-26>

DOI <https://doi.org/10.36059/978-966-397-614-3-1-47>

РОЛЬ ПРЯМИХ ІНОЗЕМНИХ ІНВЕСТИЦІЙ У РОЗВИТКУ ЕКОНОМІКИ УКРАЇНИ

Глюзицька Є. В.

здобувачка 2 курсу

спеціальності 292 «Міжнародні економічні відносини»

Міжнародний університет

м. Одеса, Україна

Зеркіна О. О.

кандидат економічних наук,

доцент кафедри економіки та міжнародних економічних відносин

Міжнародний університет

м. Одеса, Україна

В умовах обмеженості внутрішніх фінансових ресурсів та необхідності відновлення економіки України особливого значення набувають прямі іноземні інвестиції (ПІІ) як джерело капіталу, технологій та управлінського досвіду. Вони виступають важливим фактором економічного зростання, структурної модернізації та інтеграції України у світову економіку [6].

Прямі іноземні інвестиції є формою міжнародного руху капіталу, що передбачає довгострокове вкладення ресурсів з метою отримання контролю над підприємством або участі в його діяльності [4]. Їх залучення сприяє розвитку виробництва, впровадженню інновацій та підвищенню конкурентоспроможності національної економіки [1].

ПІІ позитивно впливають на економічне зростання через створення нових робочих місць, розвиток інфраструктури та збільшення обсягів експорту. Зокрема, дослідження показують, що іноземні інвестиції стимулюють підвищення доходів населення та розвиток регіонів [5]. Крім