УДК 338.23:004.056(100)

DOI: https://doi.org/10.32782/2413-2675/2024-61-5

Буряк А.А.
кандидат економічних наук, доцент,
доцент кафедри міжнародних економічних відносин та туризму,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0002-0814-7459
Buriak Alona
National University "Yuri Kondratyuk Poltava Polytechnic"

Маслій О.А.
кандидат економічних наук, доцент,
доцент кафедри фінансів, банківського бізнесу та оподаткування,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0003-2184-968X
Maslii Oleksandra
National University "Yuri Kondratyuk Poltava Polytechnic"

Кудінова А.О.
кандидат економічних наук, доцент,
доцент кафедри менеджменту і логістики,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0003-3821-2079
Kudinova Alina
National University "Yuri Kondratyuk Poltava Polytechnic"

ІДЕНТИФІКАЦІЯ ТРИГЕРНИХ ТОЧОК ВПЛИВУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ЕКОНОМІЧНУ В УМОВАХ МІЖНАРОДНОЇ НЕСТАБІЛЬНОСТІ

IDENTIFICATION OF TRIGGER POINTS IN THE IMPACT OF INFORMATION SECURITY ON ECONOMIC STABILITY UNDER CONDITIONS OF INTERNATIONAL INSTABILITY

Анотація. У статті досліджено актуальні підходи до ідентифікації тригерних точок впливу інформаційної безпеки на економічну в умовах міжнародної нестабільності. Визначено основні загрози цифрового простору, які впливають на критичні елементи економічної системи та здатність адаптації до глобальних викликів. Розглянуто механізми інформаційної війни та їх наслідки для національної економіки, акцентуючи на важливості захисту цифрових ресурсів державного управління. На основі методології FMEA ідентифіковано тригерні точки, які мають найбільший вплив на економічну безпеку. Запропоновано підходи до оцінки ризиків та методи мінімізації загроз, зокрема через аналіз тригерних точок. Результати дослідження дозволяють сформувати безпекоорієнтоване інформаційне середовище для підвищення економічної стійкості країни.

Ключові слова: інформаційна безпека, загрози цифрового простору, економічна безпека, міжнародна нестабільність, безпекоорієнтоване інформаційне середовище.

Постановка проблеми. Сучасна цифрова трансформація стала потужним рушієм економічного зростання, створюючи нові можливості для підвищення ефективності бізнес-процесів, покращення доступу до інформації та оптимізації управлінських рішень. Проте, зростаюча залежність від цифрових технологій в умовах міжнародної нестабільності, військового кон-

флікту значно посилила вразливість національної економіки до інформаційних загроз. Атаки на критичну інфраструктуру, фінансові системи та інформаційні ресурси можуть мати катастрофічні наслідки для економічної стабільності та національної безпеки.

Військові конфлікти XXI століття характеризуються не лише традиційними бойовими діями, але й активним використанням інформаційної зброї. Цілеспрямовані кібератаки, дезінформація та інформаційно-психологічні операції спрямовані на дестабілізацію економічних і соціальних систем противника. В таких умовах ідентифікація ключових тригерних точок інформаційної безпеки стає надзвичайно важливим завданням для забезпечення стійкості національної економіки.

Однією з головних загроз у сучасному інформаційному просторі є кібератаки на державні та приватні структури, що можуть призвести до втрати конфіденційної інформації, руйнування інформаційних систем або блокування ключових бізнес-процесів. В умовах міжнародної нестабільності та війни ця загроза стає особливо актуальною, оскільки економічна дестабілізація може використовуватись як інструмент ослаблення держави. Тригерні точки – це критичні вузли або процеси, ураження яких може спричинити масштабні негативні наслідки для всієї економічної системи. Ідентифікація цих точок дозволить створити ефективну систему моніторингу та управління ризиками цифровізації.

Аналіз останніх досліджень і публікацій. Питання ідентифікації тригерних точок впливу інформаційної безпеки на економічну в умовах міжнародної нестабільності набуває все більшої актуальності у сучасному науковому дискурсі. D. Sondermann, T. Gehrke, D. Baldassari [1] розглядають вплив цифрової трансформації на інформаційну безпеку, визначаючи основні тригерні точки, які можуть загрожувати економічній стабільності підприємств і держав. Дослідження A. Bonomi & T. Reiman [2] розкриває економічні наслідки інформаційної війни, підкреслюючи важливість виявлення та моніторингу тригерних точок для забезпечення стійкості національних економік. Дослідження енергоефективності цифрової економіки V. Onyshchenko, S. Onyshchenko, K. Verhal [3] підкреслює важливість забезпечення стійкості цифрової інфраструктури як одного з ключових факторів економічної стабільності на міжнародних ринках. Автори зазначають, що тригерні точки можуть бути пов'язані не лише з технологічними ризиками, а й з енергетичною безпекою. Багато науковців, зокрема О. Маслій, А. Черв'як та К.Д. Циганенко [4–7] зосереджуються на аналізі загроз, які виникають у цифровому середовищі та впливають на національну і міжнародну економічну безпеку. Автори відзначають, що ефективна ідентифікація тригерних точок дозволяє мінімізувати ризики, пов'язані з дестабілізацією ключових економічних секторів.

Доповнюють сучасний дискурс і міжнародні джерела, зокрема Digital Economy Report від UNCTAD [8], де підкреслюється взаємозв'язок цифрової трансформації та безпекових викликів на глобальному рівні. У звіті наголошується, що цифрові ризики можуть мати масштабні економічні наслідки, особливо в умовах міжнародної нестабільності. Звіти Cybersecurity and Infrastructure Security Agency [9] акцентують увагу на глобальних кіберзагрозах, що впливають на міжнародну економічну безпеку. Особливу увагу приділено ідентифікації критичних вразливостей цифрової інфраструктури, які можуть стати об'єктами атак. Аналітичні звіти Державної служби спеціального зв'язку та захисту інформації України [10] надають актуальну інформацію щодо загроз цифрового простору України, підкреслюючи важливість побудови безпекоорієнтованого середовища та ідентифікації критичних точок впливу на економічну безпеку держави.

Таким чином, останні дослідження підтверджують необхідність ідентифікації тригерних точок впливу інформаційної безпеки для забезпечення економічної стабільності в умовах міжнародної нестабільності.

Метою статті є дослідження ключових тригерних точок впливу інформаційної безпеки на економічну безпеку України в умовах міжнародної нестабільності. Дослідження спрямоване на виявлення найбільш уразливих сегментів цифрової інфраструктури, а також на аналіз потенційних наслідків для національної економіки у разі їх ураження.

Виклад основного матеріалу. Інформаційна безпека визначається як стан захищеності інформаційних ресурсів від несанкціонованого доступу, використання, розголошення, зміни або знищення [5]. В умовах війни інформаційна безпека виходить за межі технічних аспектів і охоплює стратегічні, економічні та соціальні компоненти [11]. Вона тісно пов'язана з економічною безпекою, оскільки порушення інформаційних систем можуть призвести до дестабілізації економіки, зокрема до втрати контролю над фінансовими потоками, логістичними ланцюгами або критичними інфраструктурними об'єктами.

У сучасній економіці, яка значною мірою залежить від цифрових технологій, порушення інформаційної безпеки може мати катастрофічні наслідки. Наприклад, атака на фінансову систему може призвести до паніки на ринку, втрати довіри до банківської системи та значного відтоку капіталу. Аналогічно, атаки на логістичні системи можуть зупинити постачання критично важливих товарів, що вплине на загальну економічну стабільність держави.

Тригерні точки – це критичні елементи або процеси, які, у разі їх порушення або знищення, можуть спричинити ланцюгову реакцію, що призведе до масштабних негативних наслідків для економічної системи [1]. У контексті інформаційної безпеки тригерні точки можуть включати [2]:

Критична інфраструктура – енергетичні системи, транспортні мережі, фінансові установи, які є вразливими до кібератак.

Інформаційні ресурси державного управління – системи, що забезпечують функціонування органів влади, зокрема бази даних громадян, реєстри нерухомості тощо.

Фінансові системи – банківська інфраструктура, платіжні системи, біржі, що є мішенню для кібератак з метою дестабілізації економічної системи.

Комунікаційні мережі – інтернет-зв'язок, мобільний зв'язок, які забезпечують функціонування бізнесу та державних структур.

Підприємства критичного значення – виробничі потужності, що забезпечують стратегічно важливі галузі (оборонна, харчова, фармацевтична промисловість).

Ідентифікація тригерних точок дозволяє зосередити зусилля на захисті найбільш вразливих і важливих сегментів, що знижує ризик масштабних економічних втрат.

Оцінка ризиків є ключовим етапом у забезпеченні інформаційної безпеки [4]. У контексті військового конфлікту необхідно враховувати як традиційні кіберзагрози, так і специфічні виклики, пов'язані з інформаційною війною. Основні етапи оцінки ризиків інформаційної безпеки включають елементи, зображені на рис. 1.

Інформаційна війна є невід'ємною складовою сучасних військових конфліктів. Основна мета – посіяти паніку, дестабілізувати економіку та знизити моральний дух населення. Основні методи інформаційної війни включають елементи, зображені на рис. 2.

Ідентифікація тригерних точок у контексті інформаційної війни дозволяє створити ефективні стратегії протидії та забезпечити стабільність економічної системи навіть в умовах інтенсивного інформаційного тиску.

У контексті повномасштабного вторгнення рф в Україну інформаційна безпека стає ключовим фактором підтримки економічної стійкості держави. Останні кейси в Україні демонструють, як збої в цифровій інфраструктурі можуть призводити до економічних втрат і навіть соціально-політичної дестабілізації. Деякі приклади інцидентів та їх вплив на економічну безпеку зображено у табл. 1.

Наступним етапом є оцінка ризиків за обраним нами методом Failure Mode and Effect Analysis (FMEA) – це систематичний підхід до оцінки ризиків, що застосовується для виявлення, аналізу та попередження можливих дефектів або загроз у процесах та системах [9]. Цей метод дозволяє визначити, які фактори (тригерні точки) можуть спричинити найбільші загрози для інформаційної безпеки, а також оцінити їх потенційний вплив на економічну безпеку в умовах війни.

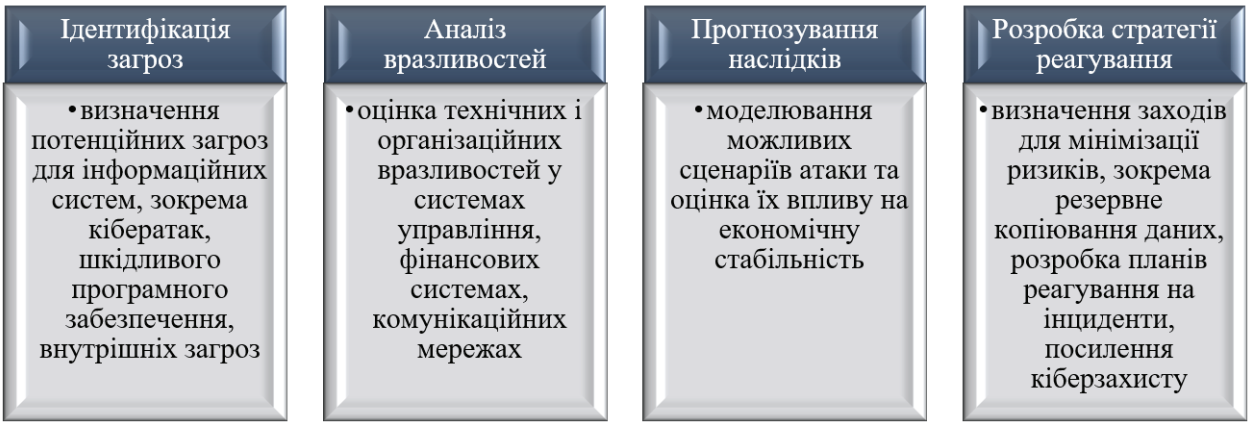

Рис. 1. Основні етапи оцінки ризиків інформаційної безпеки

Джерело: [6]

Рис. 2. Основні методи інформаційної війни

Джерело: [3; 7]

Таблиця 1

Приклади інцидентів та їх вплив на економічну безпеку

№	Інцидент	Дата	Наслідки	Виявлені тригерні точки
1	DDoS-атака на банківську систему	Лютий 2022 року	Порушення онлайн-транзакцій, паніка серед населення	Недостатній захист мережі, відсутність резервних каналів
2	Втручання в енергетичну інфраструктуру	Березень 2022 року	Часткові відключення електроенергії, збої у промисловості	Недостатній захист SCADA-систем, відсутність планів реагування
3	Атака на державні інформаційні портали	Квітень 2023 року	Втрата доступу до урядових сервісів, витік інформації	Слабкі паролі, відсутність багатофакторної автентифікації

Джерело: складено авторами за даними [10]

Основні етапи FMEA для ідентифікації тригерних точок впливу інформаційної безпеки на економічну в умовах війни:

1. Ідентифікація компонентів системи. Визначення ключових цифрових інфраструктур, що підлягають аналізу. У нашому випадку аналізу підлягають банківські системи, енергетичні мережі, державні інформаційні ресурси.

2. Визначення можливих режимів відмов. Виявлення потенційних сценаріїв загроз або вразливостей для кожного компонента. У нашому випадку аналізу підлягають DDoS-атака на банківські мережі, злом SCADA-систем енергетичної інфраструктури та неавторизований доступ до державних порталів.

3. Оцінка кожного ризику за трьома параметрами:

P (Probability) – оцінка ймовірності того, що загроза реалізується. Шкала: від 1 (дуже низька ймовірність) до 10 (дуже висока ймовірність).

S (Severity) – визначення потенційного впливу загрози на систему. Шкала: від 1 (незначний вплив) до 10 (катастрофічний вплив).

D (Detection) – оцінка здатності системи виявити загрозу до її реалізації. Шкала: від 1 (висока здатність до виявлення) до 10 (дуже низька здатність до виявлення).

Розрахунок пріоритету ризику (Risk Priority Number, RPN) обчислюється за формулою 1 [8]:

$$RPN = P \times S \times D \quad (1)$$

Чим вище значення RPN, тим критичнішою є загроза, і тим більше уваги потрібно приділити її усуненню. Результати обрахунку наведемо у табл. 2.

Інтерпретація результатів оцінки ризиків інформаційної безпеки за методом FMEA. Високі значення RPN (понад 200) вказують на критичні тригерні точки, які потребують негайного реагування. Середні значення RPN (100–200) свідчать про необхідність посилення захисних заходів. Низькі значення RPN (менше 100) можуть бути прийнятними, але їх варто моніторити.

З метою наочної візуалізації оцінки ризиків інформаційної безпеки нами побудована

Таблиця 2

Оцінка ризиків інформаційної безпеки методом FMEA

Компонент	Можлива загроза	Причина загрози	P	S	D	RPN	Рекомендовані заходи
Банківська система	DDoS-атака	Недостатній захист мережі	8	9	4	288	Посилення мережевої безпеки, впровадження CDN
SCADA-система енергетики	Неавторизований доступ	Слабка автентифікація	7	10	3	210	Впровадження багатофакторної автентифікації
Державний портал	Витік даних	Фішингові атаки	6	8	5	240	Підвищення обізнаності персоналу, антивірусні програми

Джерело: розраховано й складено авторами

діаграма Парето (рис.3), яка візуалізує найбільш критичні загрози за значенням RPN.

Блакитні стовпці відображають самі значення RPN для кожної загрози, а червона лінія демонструє кумулятивний відсоток (20% ідентифікованих загроз, зокрема, збої в системах управління логістикою та зломи фінансових платформ формують близько 80% потенційних втрат для економіки), що допомагає зосередити увагу на найважливіших інформаційних ризиках, що у свою чергу дозволяє ефективно розподіляти ресурси національної економіки для боротьби з найбільш критичними загрозами. Запропонований аналіз та ідентифікація тригерних точок на основі реальних прикладів дозволяють сформувати ефективні стратегії забезпечення інформаційної та економічної безпеки. Метод Failure Mode and Effect Analysis є ефективним інструментом для ідентифікації тригерних точок в інформаційній безпеці. Детальний аналіз дозволяє не лише виявити основні загрози, але й розробити рекомендації для їх мінімізації, що є критичним у забезпеченні економічної безпеки України в умовах війни.

Висновки і пропозиції. У результаті проведеного дослідження ідентифікації тригерних точок впливу інформаційної безпеки на економічну безпеку в умовах міжнародної нестабільності було сформульовано низку важливих висновків, які підкреслюють актуальність та необхідність комплексного підходу до забезпечення інформаційної стійкості держави. На основі методології FMEA було ідентифіковано найбільш критичні тригерні точки, які мають найбільший вплив на економічну безпеку. До них належать атаки на критичну інфраструктуру, кібератаки на фінансові системи та компрометація даних державних і комерційних установ. Візуалізація за допомогою діаграми Парето показала, що 20% ідентифікованих загроз (зокрема, збої в системах управління логістикою та зломи фінансових платформ) формують близько 80% потенцій-

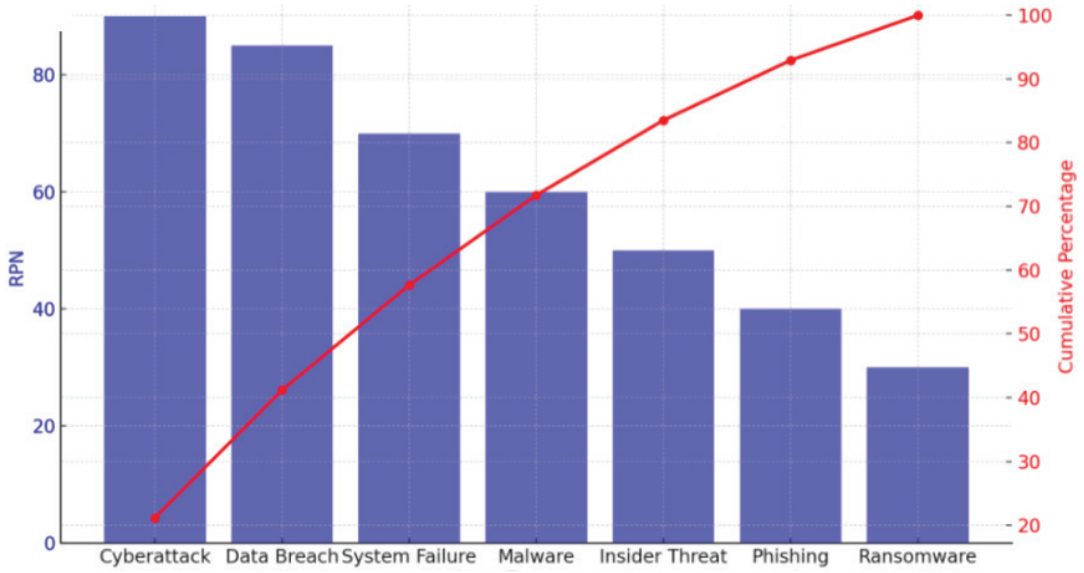

Рис. 3. Діаграма Парето із найбільш критичними загрозами за RPN

Джерело: побудовано авторами

них втрат для економіки. Це дозволяє спрямувати основні ресурси на нейтралізацію саме цих загроз.

Запропонована методологія, що включає оцінку ризиків за FMEA та діаграму Парето, є ефективним інструментом для визначення пріоритетних загроз і розробки стратегії реагування. Цей підхід дозволяє глибше розуміти механізми виникнення ризиків та адаптувати заходи інформаційної безпеки до динамічно змінюваних умов.

Для забезпечення міжнародної стабільності необхідно впроваджувати інтегровані системи інформаційної безпеки, що включають комплексний моніторинг, аналіз ризиків у реальному часі та адаптивне управління загрозами. Особлива увага повинна приділятися захисту логістичних та фінансових процесів від потенційних кібератак. Ідентифікація та аналіз тригерних точок інформаційної безпеки є ключовим етапом у забезпеченні економічної безпеки держави в умовах війни. Ефективне використання сучасних цифрових технологій створює умови для мінімізації загроз і підвищення стійкості національної економіки.

Література:

1. Sondermann D., Gehrke T., Baldassari D. Economic Security and Digital Transformation in the European Union. *Intereconomics*. 2022. № 57(4). P. 203–211.
2. Bonomi A., Reiman T. Information Warfare and Its Economic Implications. *Economic Security Journal*. 2022. № 8(1). P. 102–118.
3. Onyshchenko V., Onyshchenko S., Verhal K., Buriak A. The Energy Efficiency of the Digital Economy. *Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering,* Springer, Cham. 2023. Vol 299. P. 761–767. DOI: https://doi.org/10.1007/978-3-031-17385-1_64
4. Onyshchenko S. V., Masliy O. A., Buriak A. A. Threats and risks of ecological and economic security of Ukraine in the conditions of war. *XVII International Scientific Conference «Monitoring of Geological Processes and Ecological Condition of the Environment»*, November 7–10, 2023. Kyiv. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/13700/1/2023_11_Mon23-072.pdf
5. Buriak A., Masliy O. Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. *Економіка і регіон*. 2024. №1 (92). С. 281–287. DOI: https://doi.org/10.26906/EiR.2024.1(92).3341
6. Буряк А.А., Маслій О.А. Трансформація загроз економічній безпеці та безпеці інформаційного середовища України в умовах повномасштабної війни. *Держава та регіони. Серія: Економіка та підприємництво*. 2023. № 3 (129). С. 28–32. DOI: https://doi.org/10.32782/1814-1161/2023-3-5
7. Черв'як А.В., Буряк А.А., Циганенко К.Д. Особливості формування безпекоорієнтованого інформаційного середовища національної економіки. *Науковий вісник Херсонського державного університету. Серія «Економічні науки»*. 2024. № 52. С. 19–25. DOI: https://doi.org/10.32999/ksu2307-8030/2024-52-3
8. Digital Economy Report 2022. UNCTAD. URL: https://unctad.org/publication/digital-economy-report-pacific-edition-2022
9. Cybersecurity and Infrastructure Security Agency Reports, 2023. URL: https://www.cisa.gov/about/2023YIR
10. Державна служба спеціального зв'язку та захисту інформації України. Аналітичні звіти за 2023 рік. URL: https://cip.gov.ua/ua
11. Buriak A.A. Methodological approaches to assessing the impact of threats on the environmental security of society in the international security system. *International security studios: managerial, technical, legal, environmental, informative and psychological aspects.* International collective monograph. Volume II. NMBU, Research and Education. 2024. С. 482–510. DOI: https://doi.org/10.5281/zenodo.10838779

References:

1. Sondermann D., Gehrke T., Baldassari D. (2022). Economic Security and Digital Transformation in the European Union. *Intereconomics*, vol. 57(4), pp. 203–211.
2. Bonomi A., Reiman T. (2022). Information Warfare and Its Economic Implications. *Economic Security Journal*, vol. 8(1), pp. 102–118.
3. Onyshchenko V., Onyshchenko S., Verhal K., Buriak A. (2023). The Energy Efficiency of the Digital Economy. *Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering,* Springer, Cham, vol 299, pp. 761–767. DOI: https://doi.org/10.1007/978-3-031-17385-1_64
4. Onyshchenko S. V., Masliy O. A., Buriak A. A. (November 7–10, 2023). Threats and risks of ecological and economic security of Ukraine in the conditions of war. XVII International Scientific Conference *"Monitoring of Geological Processes and Ecological Condition of the Environment"*. Kyiv. Available at: https://reposit.nupp.edu.ua/bitstream/PoltNTU/13700/1/2023_11_Mon23-072.pdf (accessed November 22, 2024).
5. Buriak A., Masliy O. (2024). Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. *Economics and Region*, vol. 1(92), pp. 281–287. DOI: https://doi.org/10.26906/EiR.2024.1(92).3341
6. Masliy O., Buriak A. (2023). Transformation of threats for the economic security and security of the information environment of Ukraine in the conditions of a full-scale war. *State and regions. Series: Economy and entrepreneurship*, vol. 3 (129), pp. 28–32. DOI: https://doi.org/10.32782/1814-1161/2023-3-5
7. Cherviak A., Buriak A., Tsyhanenko K. (2024). Features of formation security-oriented information environment of the national economy. *Scientific Bulletin of Kherson State University. Series "Economic Sciences"*, vol. 52, pp. 19–25. DOI: https://doi.org/10.32999/ksu2307-8030/2024-52-3
8. Digital Economy Report 2022. UNCTAD. Available at: https://unctad.org/publication/digital-economy-report-pacific-edition-2022 (accessed November 22, 2024).
9. Cybersecurity and Infrastructure Security Agency Reports, 2023. Available at: https://www.cisa.gov/about/2023YIR (accessed November 22, 2024).
10. State Service of Special Communications and Information Protection of Ukraine. Analytical reports for 2023. Available at: https://cip.gov.ua/ua (accessed November 22, 2024).
11. Buriak A. A. (2024). Methodological approaches to assessing the impact of threats on the environmental security of society in the international security system. *International security studios: managerial, technical, legal, environmental, informative and psychological aspects.* International collective monograph. Vol. II. NMBU, Research and Education, pp. 482–510. DOI: https://doi.org/10.5281/zenodo.10838779

Summary. The study focuses on identifying critical trigger points where information security breaches significantly impact economic security amid international instability. In wartime, information security extends beyond technical concerns, encompassing strategic, economic, and social components, directly influencing economic stability. Disruptions in information systems can destabilize economies by affecting financial flows, supply chains, or critical infrastructure. In a modern digital economy, breaches can have catastrophic consequences. For example, an attack on financial systems can cause market panic and capital flight, while disruptions in logistics networks may halt essential goods supply, affecting national economic stability. Trigger points refer to critical elements whose disruption can initiate a chain reaction with widespread economic repercussions. Key trigger points include critical infrastructure (energy, finance), government information resources, financial systems. Identifying these points allows prioritizing protective efforts, reducing potential economic losses. Risk assessment, crucial for information security, must consider traditional cyber threats and warfare-specific challenges. A structured risk evaluation, using the Failure Mode and Effect Analysis (FMEA) method, identifies vulnerabilities and quantifies their potential impact based on probability, severity, and detection. High Risk Priority Number (RPN) values highlight the most critical threats, guiding resource allocation for mitigation. In the context of Russia's full-scale invasion of Ukraine, information security is pivotal for economic resilience. Recent incidents demonstrate how digital infrastructure failures can lead to economic and socio-political destabilization. Effective strategies involve real-time risk monitoring, adaptive threat management, and focused protection of financial and logistical systems. This approach, supported by tools like Pareto analysis and FMEA, enhances national economic stability by addressing the most impactful threats.

Keywords: information security, threats of digital space, economic security, international instability, security-oriented information environment.