DOI: https://doi.org/10.36910/6775-2524-0560-2022-48-10
УДК [004.02/.032/.421] + 621.391 +004.031.42+007.2
Козубцова Леся Михайлівна[1] , к.т.н.
https://orcid.org/0000-0002-7866-8575
Козубцов Ігор Миколайович[1] , д.пед.н., к.т.н., с.н.с.
https://orcid.org/0000-0002-7309-4365
Здолбіцька Ніна Василівна[2] , к.т.н, доцент
https://orcid.org/0000-0002-1345-3581
Кошелюк Віктор Андрійович[2] **,** к.т.н.
https://orcid.org/0000-0002-4136-5087
[1] Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна
[2] Луцький національний технічний університет, м. Луцьк, Україна

ПОКАЗНИКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ І КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Козубцова Л.М., Козубцов І.М., Здолбіцька Н.В., Кошелюк В.А. Показники ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури. У науковій статті вирішено науково-технічну проблему з вибору показників ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури. Наукова новизна одержаного результату полягає в тому, що вперше запропоновано показники та критеріїв оцінювання ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури. Практичне значення роботи полягає в тому, що на основі одержаних показників та критеріїв у подальших роботах виникає можливість розробити методику оцінювання ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури.
Ключові слова: показники, критерії, оцінювання, ефективність, функціонування, система захисту інформації і кібербезпеки, об'єкти критичної інформаційної інфраструктури.

Kozubtsova L., Kozubtsov I., Zdolbitskaya N., Koshelyuk V. Performance indicators of the functioning of the information security system and cybersecurity of critical information infrastructure objects. The scientific article solves the scientific and technical problem of choosing performance indicators for the functioning of the information security system and cybersecurity of critical information infrastructure facilities. The scientific novelty of the obtained result lies in the fact that for the first time indicators and criteria for evaluating the effectiveness of the functioning of the information security system and cybersecurity of critical information infrastructure facilities are proposed. The practical significance of the work lies in the fact that based on the obtained indicators and criteria in further works, it becomes possible to develop a methodology for evaluating the effectiveness of the information security system and cybersecurity of critical information infrastructure objects.
Keywords: indicators, criteria, evaluation, efficiency, functioning, information security and cybersecurity system, critical information infrastructure objects.

Постановка завдання і зв'язок її з важливими науковими завданнями. Система захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури (СЗІКБ ОКІІ) – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки. Від значення рівня ефективності функціонування СЗІКБ ОКІІ залежить без перебільшення безпека держави. Відсутність єдиної методології оцінювання ефективності функціонування СЗІКБ ОКІІ призводить до нераціональних закупівель комплексів програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки. Ця науково-технічна проблема виникла в результаті суперечності:

появи потреби у СЗІКБ ОКІІ відносно нової системи, що раніше не існувало прототипу;

у відсутності методології оцінювання ефективності функціонування СЗІКБ ОКІІ.

Тому, сформулюємо наукове завдання дослідження: визначити можливі показники за якими об'єктивно оцінити ефективність функціонування СЗІКБ ОКІІ. Необхідність вирішенні даного наукового завдання є пріоритетним напрямком, що означений Законом України [1].

Аналіз останніх досліджень і публікацій. У публікації [2] автор застосовував показник ступінь досягнення мети функціонування системи захисту інформаційної для оцінки її ефективності.

В роботі [3] автором для оцінювання ефективності підрозділів захисту інформації застосовувалися показники економічної ефективності.

Методика [4] призначена оцінювати ефективність виконаних заходів націлених на

забезпечення кібербезпеки ОКІІ.

У методиці [5] для обчислення ефективність функціонування СЗІКБ, запропоновано систему часткових показників ($E_{ЧП}$):

кіберзахищеність;

укомплектованість засобами криптографічного захисту інформації (КЗІ), технічного захисту інформації (ТЗІ) та кіберзахисту (КЗ);

технічної готовності засобів КЗІ, ТЗІ та КЗ; коефіцієнтом укомплектованості справними засобами КЗІ, ТЗІ та КЗ;

укомплектованості штатних посад системними адміністраторами;

укомплектованості штатних посад обслуговуючим персоналом;

кіберзахищеність за результатами зовнішнього аудиту та penetration testing.

Мета статті. Охарактеризувати математичні показники та відповідні критерії оцінювання ефективності функціонування СЗІКБ ОКІІ.

Матеріали й методи. Для вирішення поставлених завдань використовувалася сукупність методів теоретичного дослідження: історичного аналізу та узагальнення наукової літератури щодо проблеми дослідження; структурно-генетичного аналізу та синтезу при уточненні об'єкта та предмета дослідження; метод сходження від абстрактного до конкретного; метод аналітично-порівняльного аналізу при аналітично-порівняльному оцінюванні новизни результатів дослідження; синтез та узагальнення – для обґрунтування методологічних та методичних засад дослідження; узагальнення – формулювання висновків та рекомендацій щодо продовження подальших досліджень.

Виклад основного матеріалу. Під «ефективністю СЗІКБ ОКІІ» (E) будемо розглядати ступінь досягнення цією системою максимально можливих результатів функціонування за узагальненим показником. Під показником ефективності СЗІКБ ОКІІ» ($E_{П}$) будемо розуміти значення, що характеризує ступінь досягнення виконання системою поставлених перед нею цільової функції (CF).

Відповідно до сучасних тенденцій у сфері кібербезпеки перспективна СЗІКБ ОКІІ та аналізу [6–16] система має забезпечувати виконання наступну цільову функцію CF (1):

$$CF\ [ID;\ PR;\ DE;\ RS;\ RC], \quad (1)$$

де ID – функція «Ідентифікація ризиків кібербезпеки»;

PR – функція «Кіберзахист»;

DE – функція «Виявлення кіберінцидентів»;

RS – функція «Реагування на кіберінциденти»;

RC – функція «Відновлення стану кібербезпеки».

Перелічені функції є заходами кіберзахисту, що рекомендовані у Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури [17].

На практиці до показника ефективності висуваються наступні вимоги:

мати певний фізичний зміст;

бути придатним для кількісного аналізу;

мати просту і зручну форму;

відображати одну із значущих сторін функціонування системи;

забезпечувати необхідну чутливість.

На підставі визначених рекомендацій [17] та світового досвіду та рекомендацій National Institute of Standards and Technology (NIST) [6 – 16] нами запропоновано наступна сукупність часткових показників ($E_{ЧП}$), які формують загальні показники ($E_{П}$) ефективності СЗІКБ ОКІІ.

Визначимо наступні показники, результат подано в табл. 1.

Таблиця 1. Система зв'язку показників E ефективності СЗІКБ ОКІІ

Показники $E_{П}$	часткові показники $E_{ЧП}$
Функція «Ідентифікація ризиків кібербезпеки (ID)»	Ступінь реалізації управління активами (ID.AM)
	Ступінь реалізації середовища надання життєво важливих послуг та функцій (ID.BE)
	Ступінь реалізації управління безпекою (ID.GV)

	Ступінь реалізації оцінювання ризиків (ID.RA)
	Ступінь реалізації стратегії управління ризиками (ID.RM)
	Ступінь реалізації управління ризиками системи постачання (ID.SC)
Функція «Кіберзахист (PR)»	Ступінь реалізації управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)
	Ступінь обізнаності та навченості (PR.AT)
	Ступінь реалізації безпеки даних (PR.DS)
	Ступінь реалізації процесів та процедур кіберзахисту (PR.IP)
	Ступінь реалізації технічного обслуговування (PR.MA)
	Ступінь впровадженості технології кіберзахисту (PR.PT)
Функція «Виявлення кіберінцидентів (DE)»	DE.AE Аномалії та кіберінциденти
	Ступінь реалізації безперервного моніторингу кібербезпеки (DE.CM)
	Ступінь реалізації процесів виявлення кіберінцидентів (DE.DP)
Функція «Реагування на кіберінциденти (RS)»	Ступінь реалізації системи планування реагування (RS.RP)
	Ступінь реалізації комунікації (RS.CO)
	Ступінь реалізації системи аналізу (RS.AN)
	Ступінь забезпечення мінімізації наслідків (RS.MI)
	Ступінь удосконалення (RS.IM)
Функція «Відновлення стану кібербезпеки (RC)»	Ступінь реалізації планування відновлення (RC.RP)
	Ступінь реалізації удосконалення (RC.IM)
	Ступінь реалізації комунікації (RC.CO)

Критерії оцінки ефективності функціонування СЗІКБ ОКІІ. Для оцінки індикаторів часткових показників $I_{ЧП}$ рекомендуємо наступні критерії табл. 2.

Таблиця 2. Критерії оцінювання індикаторів часткових показників $I_{ЧП}$

Критерій $I_{ЧП}$	Рівень
$I_{ЧП}= 0$	не реалізовано функцію
$I_{ЧП} = 1$	реалізовано функцію

Для оцінки часткових показників $E_{ЧП}$ рекомендуємо наступні критерії табл. 3.

Таблиця 3. Критерії оцінювання часткових показників $E_{ЧП}$

Критерій $E_{ЧП}$	Рівень
$0 \le E_{ЧП} \le 0,25$	незадовільний (НЗ)
$0,25< E_{ЧП} \le 0,5$	низький (Н)
$0,5< E_{ЧП} \le 0,75$	середній (С)
$0,75< E_{ЧП} \le 0,9$	високий (В)
$0,9< E_{ЧП} \le 1$	найвищий (НВ)

Для оцінки показників $E_{П}$ рекомендуємо наступні критерії табл. 4.

Таблиця 4. Критерії оцінювання показників $E_{П}$

Критерій $E_{П}$	Рівень
$0 \le E_{П} \le 0,25$	незадовільний (НЗ)
$0,25< E_{П} \le 0,5$	низький (Н)
$0,5< E_{П} \le 0,75$	середній (С)
$0,75< E_{П} \le 0,9$	високий (В)
$0,9< E_{П} \le 1$	найвищий (НВ)

Критерії оцінювання ефективності функціонування СЗІКБ ОКІІ за узагальненим показником подані в (табл. 5).

Таблиця 5. Критерії оцінки ефективності функціонування СЗІКБ ОКІІ за узагальненим показником

Критерій E	Рівень
$0 \le E \le 0,25$	Частковий
$0,25< E \le 0,5$	Ризик-орієнтований

$0,5< E \leq 0,75$	Повторюваний
$0,75< E \leq 1$	Адаптивний

Рекомендації [17] визначають чотири ієрархічних рівні впровадження заходів кіберзахисту на ОКІІ (рис. 1). Рівні впровадження заходів кіберзахисту характеризують ступінь практичного впровадження на ОКІІ заходів із кіберзахисту, здатність ОКІІ досягти запланованих результатів кіберзахисту та надають інструментарій оцінювання ступеня впровадження процесів управління кібербезпекою.

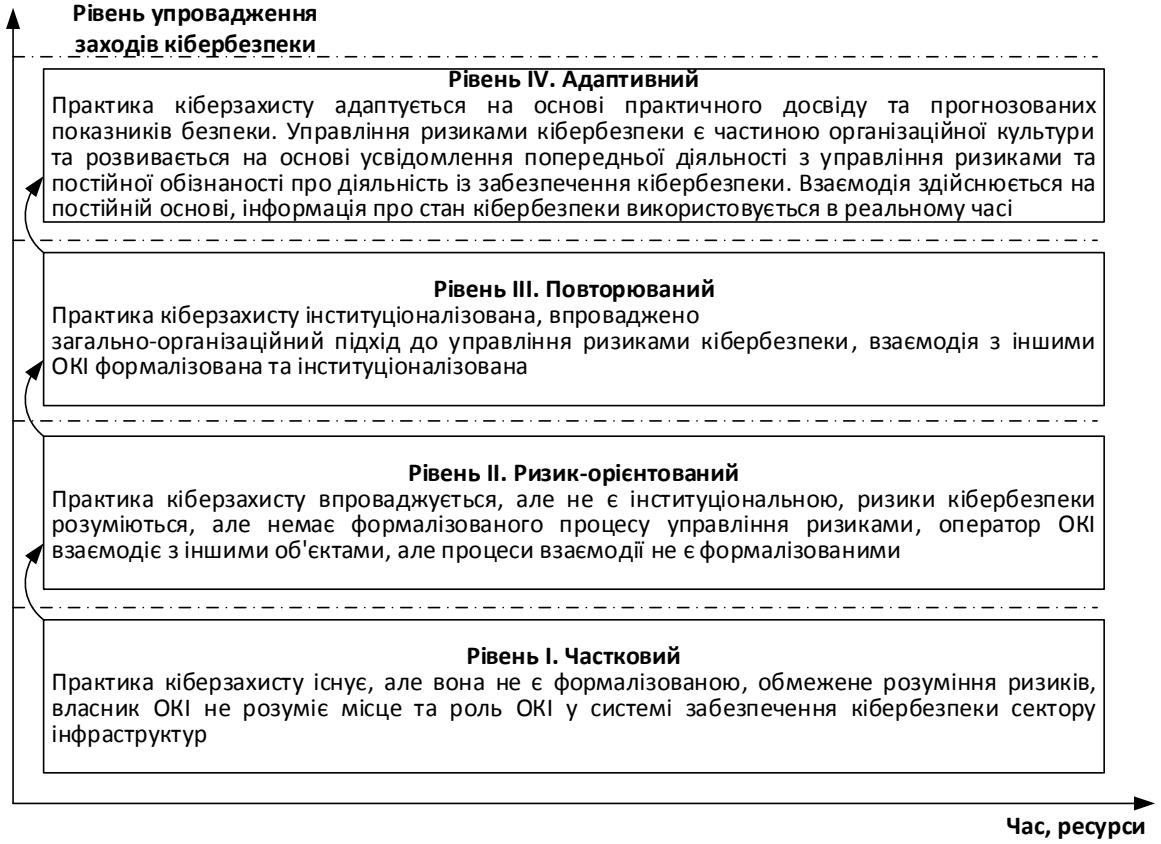

Рис. 1. Рівні впровадження заходів кіберзахисту на ОКІІ

Висновки. На сучасному етапі розвитку науки вирішено науково-технічну проблему з невизначеності за якими показниками проводити процедуру оцінювання вибору ефективність функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури. На разі вбачається при оцінці ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури два ключових показника за функціональною спроможністю та технічною надійністю.

Наукова новизна. Вперше запропоновано часткові показники ефективності функціонування СЗІКБ ОКІІ та у відповідності до їх значень критерії їх оцінювання.

Практичне значення. На основі одержаних показників та критеріїв можна розробити методику оцінювання ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури.

Перспективи подальших досліджень. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, становлять підґрунтя для подальшого обґрунтування методики обчислювання числового значення ефективності функціонування СЗІКБ ОКІІ.

Список бібліографічного опису

1. Закон України "Про основні засади забезпечення кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/2163-19.
2. Маслова Н.А. Методы оценки эффективности систем защиты информационны систем. *Искусственный интеллект*. 2008. № 4.С. 253 – 264.
3. Андреев К. Метод оценки экономической эффективности подразделения по защите информации. *Информационная безопасность*. 2010. №5. URL: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-

ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii.
4. Козубцова Л.М., Хлапонин Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. №2 (41). С. 17-22.
5. Козубцова Л.М., Рудоміно-Дусятська І.А., Сновида В.Є. Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки. Науковий журнал «*Комп'ютерно-інтегровані технології: освіта, наука, виробництво*». 2021. Випуск №45. С. 19-25. URL: http://cit-journal.com.ua/index.php/cit/article/view/315/405.
6. Department of Energy (2021) Cybersecurity Capability Maturity Model. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
7. Center for Internet Security (2021) CIS Controls V8. URL: https://www.cisecurity.org/controls.
8. Information Systems Audit and Control Association (ISACA) (2021) Control Objectives for Information and Related Technologies. URL: https://www.isaca.org/resources/cobit.
9. International Energy Agency (2021) Enhancing Cyber Resilience in Electricity Systems. URL: https://webstore.iea.org/
download/direct/4359.
10. International Society of Automation (2013) ISA 62443-3-3:2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels (ISA, North Carolina, USA). URL: https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu.
11. International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO, Geneva, Switzerland). URL: https://www.iso.org/standard/54534.html.
12. National Institute of Standards and Technology and North American Electric Reliability Corporation (2020) Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards. URL: https://doi.org/10.18434/mds2-2348.
13. North American Electric Reliability Corporation (2021) NERC CIP Enforceable Standards. URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
14. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). URL: https://doi.org/10.6028/NIST.CSWP.04162018.
15. National Institute of Standards and Technology (2021) National Online Informative References Program. URL: https://csrc.nist.gov/projects/olir.
16. Joint Task Force Transformation Initiative (2015) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. URL: https://doi.org/10.6028/NIST.SP.800-53r4.
17. Додаток 1. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв'язку від 6 жовтня 2021 р. № 601 (у редакції наказу Адміністрації
Держспецзв'язку від 12 жовтня 2021 року № 616). https://cip.gov.ua/services/cm/api/attachment/download?id=42961.

References

1. The law of Ukraine "On basic principles of ensuring cybersecurity of Ukraine". URL: https://zakon.rada.gov.ua/laws/
show/2163-19. (in Ukraininan).
2. Maslova N.A. Methods of evaluating the effectiveness of information systems protection systems. Artificial Intelligence. 2008. No. 4.pp. 253-264. (in Russian).
3. Andreev K. Method of assessing the economic efficiency of the information protection unit. Information security. 2010. No.5. URL: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii. (in Russian).
4.Kozubtsova L.M., Khlaponin Yu.I., Kozubtsov I.M. Methodology for evaluating the effectiveness of measures to ensure cybersecurity of critical information infrastructure objects of organizations. Modern information technologies in the field of security and defense. 2021. No.2 (41). pp. 17-22. (in Ukraininan).
5. Kozubtsova L.M., Rudomino-Dushyatskaya I.A., Lunoda V.E. Calculus of performance indicators of the system of information security and cybersecurity // scientific journal "Computer-Integrated Technologies: Education, Science, production". 2021. issue No.45. pp. 19-25. URL: http://cit-journal.com.ua/index.php/cit/article/view/315/405. (in Ukraininan).
6. Department of Energy (2021) Cybersecurity Capability Maturity Model. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
7. Center for Internet Security (2021) CIS Controls V8. URL: https://www.cisecurity.org/controls.
8. Information Systems Audit and Control Association (ISACA) (2021) Control Objectives for Information and Related Technologies. URL: https://www.isaca.org/resources/cobit
9. International Energy Agency (2021) Enhancing Cyber Resilience in Electricity Systems. URL: https://webstore.iea.org/
download/direct/4359.
10. International Society of Automation (2013) ISA 62443-3-3:2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels (ISA, North Carolina, USA). URL: https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu

11. International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO, Geneva, Switzerland). URL: https://www.iso.org/standard/54534.html
12. National Institute of Standards and Technology and North American Electric Reliability Corporation (2020) Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards. URL: https://doi.org/10.18434/mds2-2348.
13. North American Electric Reliability Corporation (2021) NERC CIP Enforceable Standards. URL: https://www.nerc.com/pa/
Stand/Pages/CIPStandards.aspx.
14. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). URL: https://doi.org/10.6028/
NIST.CSWP.04162018.
15. National Institute of Standards and Technology (2021) National Online Informative References Program. URL: https://csrc.nist.gov/projects/olir.
16. Joint Task Force Transformation Initiative (2015) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. URL: https://doi.org/10.6028/NIST.SP.800-53r4.
17. Appendix 1. methodological recommendations for improving the level of cyber protection of critical information infrastructure, approved by Order No. 601 of the State Service for Special Communications administration of October 6, 2021 (as amended by the Order of the administration Gosspetsvyaz No. 616 dated October 12, 2021). https://cip.gov.ua/services/cm/api/
attachment/download?id=42961. (in Ukraininan).