

## **РЕЦЕНЗІЯ**

Кандидата технічних наук, доцента,  
доцента кафедри захисту інформації

Національного університету «Львівська політехніка»

**Совина Ярослава Романовича**

на дисертацію

Курія Євгенія Олеговича

**«Методологія підвищення захищеності об'єктів критичної інфраструктури  
за рахунок перехресного впровадження стандартів аудиту з кібербезпеки»,**

подану на здобуття наукового ступеня доктора філософії за спеціальністю

125 «Кібербезпека»

(галузь знань 12 «Інформаційні технології»)

### **Актуальність теми дисертації.**

Захист критичної інфраструктури України завжди був пріоритетним завданням для забезпечення стійкості та обороноздатності держави. Особливої важливості цей захист набув у зв'язку з ростом інформаційних технологій та масовим переходом до режиму віддаленої роботи, а також через збройну агресію Росії проти України. Відповідно, забезпечення надійного захисту об'єктів критичної інфраструктури є надзвичайно важливим завданням, що потребує комплексного підходу та використання передових технологій.

Для ефективного захисту об'єктів критичної інфраструктури необхідно використовувати передові технології та методики кібербезпеки. Стандарти аудиту з кібербезпеки забезпечують систематичний підхід до ідентифікації потенційних загроз та впровадження заходів з їх запобігання. Вони допомагають упорядковувати процес забезпечення безпеки, встановлюючи загальноприйняті рамки та вимоги.

Кожен стандарт інформаційної безпеки має свою унікальну спеціалізацію та обсяг охоплення. Тому для підвищення захищеності об'єктів критичної інфраструктури ефективним є перехресне впровадження стандартів аудиту, коли

застосовуються вимоги з декількох стандартів одночасно для більш ефективного та всебічного захисту. Перевагами перехресного впровадження стандартів кібербезпеки на об'єктах критичної інфраструктури можуть бути підвищення загального рівня кібербезпеки, зниження ризику кібератак, підвищення стійкості до кіберінцидентів, та підвищення довіри з боку клієнтів та партнерів.

**Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри**

Тема дисертації відповідає науковому напрямку кафедри захисту інформації Національного університету «Львівська політехніка»: дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії, удосконалення інформаційної безпеки держави, контррозвідувальних методів протидії та техніки.

**Наукова новизна основних результатів дисертації** полягає у тому, що:

1. **Вперше** розроблено методологію проведення перехресного впровадження стандартів аудиту з кібербезпеки за рахунок впровадження розробленої таблиці зіставлення контролів безпеки провідних стандартів, що дозволяє організаціям і ОКІ уніфікувати взаємозв'язок між різними стандартами аудиту з кібербезпеки, визначити ступінь кореляції їхніх систем управління інформаційною безпекою вимогам визначених стандартів і оцінити відповідність контролів безпеки, необхідних для досягнення вимог додатковому стандарту безпеки, що у свою чергу підвищує комплексність та ефективність захисту ОКІ від кіберзагроз.

2. **Вперше** розроблено метод оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні контрольного списку, який містить детальний перелік перевірок для визначення статусу відповідності контролям безпеки, а також перелік доказів і документів, необхідних для досягнення відповідності. Даний метод має забезпечувати систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки, скорочувати час на впровадження стандарту і забезпечувати комплексний і всебічний захист ОКІ від кіберзагроз.

**3. Вперше розроблено** метод зіставлення контролів безпеки провідних стандартів на основі встановлення відповідності як між самими контролями безпеки, так і додатковими рекомендаціями для впровадження конкретних контролів і вимог. Даний метод має підвищувати ефективність захисту ОКІ за рахунок комплексного охоплення контролів безпеки.

**4. Вперше розроблено** методологію створення політик інформаційної безпеки ОКІ на основі інтеграції зведеної таблиці із зіставленням контролів безпеки провідних стандартів кібербезпеки. Дана методологія покликана підвищити ефективність захищеності ОКІ від загроз за рахунок автоматизації і пришвидшення процесу створення політик інформаційної безпеки з забезпеченням покриття усіх найважливіших доменів і контролів безпеки.

**Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна.**

Наукові положення, представлені в дисертації, відзначаються високим ступенем обґрунтованості. Вони базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується практичною реалізацією методології перехресного впровадження стандартів аудиту.

**Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.**

Наукові результати, отримані автором, можуть бути використані при розробці та побудові систем для автоматизації процесу аудиту та впровадження стандартів кібербезпеки в об'єктах критичної інфраструктури.

Результати дисертаційної роботи Курія Є.О. впроваджені у навчальний процес кафедри захисту інформації Національного університету «Львівська політехніка» при вивченні дисципліни «Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки» для студентів спеціальності 125 «Кібербезпека та захист інформації».

**Практичне значення одержаних результатів** полягає у можливості їх безпосереднього застосування для підвищення захищеності об'єктів критичної інфраструктури та забезпечення їхньої відповідності провідним стандартам аудиту з кібербезпеки.

1. Розроблено таблицю перехресної відповідності між контролями Додатку А двох останніх редакцій стандарту ISO 27001 (2013 і 2022 років). Використання розробленої таблиці відповідності скорочує час і ресурси необхідні для впровадження оновленої версії стандарту та приведення СУІБ до відповідності новим вимогам безпеки.

2. Розроблено універсальний шаблон для ідентифікації і управління ризиками інформаційної безпеки ОКІ. Даний шаблон забезпечує досягнення відповідності провідним стандартам аудиту з кібербезпеки, таким як ISO 27001, SOC 2, NIST чи PCI DSS без залучення спеціалістів з інформаційної безпеки.

3. Розроблено алгоритм зіставлення контролів безпеки провідних стандартів аудиту, який дозволяє організаціям і ОКІ забезпечити взаємозв'язок між різними стандартами кібербезпеки та оцінити відповідність їхніх СУІБ вимогам стандартів. Впровадження розробленої, у результаті використання даного алгоритму, таблиці зіставлення контролів дозволяє автоматизувати процес визначення унікальних контролів безпеки стандартів, зменшити час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки, і забезпечити ефективний захист ОКІ від кіберзагроз шляхом перехресного впровадження вимог декількох стандартів аудиту одночасно.

4. Розроблена таблиця відповідності контролів безпеки провідних стандартів аудиту, таких як ISO 27001, SOC 2, NIST та PCI DSS, демонструє, що у результаті зіставлення контролів безпеки, при впровадженні стандарту ISO 27001:2022 організація покриває в середньому від 66% до 94% контролів інших досліджених стандартів, що зменшує час і ресурси на впровадження унікальних контролів безпеки кожного стандарту.

5. Розроблено форму оцінювання для проведення оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, яка містить детальний перелік перевірок для визначення статусу відповідності контролям безпеки, а також

перелік доказів і документів, необхідних для досягнення відповідності. Розроблена форма оцінювання у вигляді контрольного списку забезпечує систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки і, завдяки розробленим практичним рекомендаціям по впровадженню стандарту ISO 27001, скорочує час на впровадження стандарту. Зокрема, використання даної форми, в комбінації з використанням методології перехресного впровадження стандартів аудиту з кібербезпеки, дає змогу впроваджувати стандарти аудиту ефективніше та до 50% швидше в порівнянні з традиційними методами.

Запропоновані в роботі підходи та методи дають змогу підвищити рівень захищеності об'єктів критичної інфраструктури від кіберзагроз за рахунок використання методології перехресного впровадження стандартів аудиту з кібербезпеки. Ця методологія підвищує рівень інформаційної безпеки та захищеності ОКІ, а також зменшує час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки одночасно.

Основні результати дисертаційної роботи впроваджено з метою покращення внутрішніх процесів, пов'язаних з інформаційною безпекою, і сприяння забезпеченню статусу відповідності міжнародним стандартам інформаційної безпеки у компаніях ТОВ «Бінарікс Україна», ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ» і ТОВ «ПІК РІСОРСИС».

#### **Повнота оприлюднення результатів дисертаційної роботи.**

Основні результати дослідження викладено у дев'яти наукових публікаціях, а саме: чотирьох статтях у наукових фахових виданнях України та п'яти тезах виступів на науково-практичних заходах. Три публікації проіндексовано в наукометричній базі Scopus.

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів. Основні положення та результати дисертації викладені в таких наукових працях здобувача:

#### ***Статті у наукових фахових виданнях України:***

1. A model of decoy system based on dynamic attributes for cybercrime investigation / S. Vasilishyn, V. Susukailo, I. Oprirskyu, Y. Kurii, I. Tyshyk // Східно-



Європейський журнал передових технологій = Eastern-European Journal of Enterprise Technologies. 2023. № 1/9 (121). P. 6–20.

2. Kurii, Y. ., & Opirskyu, I. (2023). ISO 27001: АНАЛІЗ ЗМІН ТА ОСОБЛИВОСТІ ВІДПОВІДНОСТІ НОВІЙ ВЕРСІЇ СТАНДАРТУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 46–55. <https://doi.org/10.28925/2663-4023.2023.19.4655>;

3. Євгеній Курій, Віталій Сусукайло, Іван Опірський (2023). РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВІДПОВІДНОСТІ СТАНДАРТУ ISO 27001. Ukrainian Information Security Research Journal. 25(3):132-139. DOI: <https://doi.org/10.18372/2410-7840.25.17938>;

4. Курій Є. О., Опірський І. Р. (2024) Безпека платіжних операцій: огляд і характеристика ключових змін у новій редакції стандарту PCI DSS // Кібербезпека: освіта, наука, техніка. – Т. 3, № 23. – С. 145–155. DOI: <https://doi.org/10.28925/2663-4023.2024.23.145155>

*Статті у наукових періодичних виданнях інших держав, що включені до міжнародної наукометричної бази даних (Scopus):*

5. Kurii, Y. Opirskyu, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32;

6. Vakhula O., Kurii Y., Opirskyu I., Susukailo V. (2024) Security-as-code concept for fulfilling ISO/IEC 27001:2022 requirements // Paper presented at the CEUR Workshop Proceedings, vol. 3654, . 59–72.

*Наукові публікації у збірниках матеріалів та тез конференцій:*

7. Yevhenii KURIIL, Ivan OPIRSKYU, Leonid BORTNIK ISO/IEC 27001:2022 – ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD // Materials of IXth International Scientific and Technical Conference INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY, May 25–26, 2023. - Lviv, Ukraine, pp 15-17, ISBN 978-966-941-829-6;

8. Курій Є. О., Опірський І. Р. ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОСНОВНИХ ФРЕЙМВОРКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ // Інформаційне

суспільство: технологічні, економічні та технічні аспекти становлення (випуск 85): матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 15-16 лютого 2024 р.). – 2024. – С. 34–36.

9. Курій Є. О., Опірський І. Р. АНАЛІЗ ПЕРЕВАГ І НЕДОЛІКІВ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ // Materials of the V International Research and Practical Internet Conference «Development Strategies for Modern Education and Science», – 2024. – 2024. – С. 16–17.

#### **Зауваження по дисертації.**

1. У розділі 1.4 бракує більш детального обґрунтування щодо переліку стандартів, вибраних для створення таблиці зіставлення. Доцільно було б додати пояснення, чому саме ці стандарти були обрані, а також висвітлити їх важливість та актуальність у контексті аналізу.

2. У розділі 2.1, при порівнянні контролів двох версій міжнародного стандарту ISO 27001, доцільно було б навести деякі практичні рекомендації для переходу на оновлену версію стандарту 2022 року. Додатково до наведеної таблиці зіставлення контролів обох версій, ці рекомендації надали б більшої наочності щодо успішного переходу між версіями стандарту.

3. Деякі з показників ефективності системи, представлених у розділі 4.3, є дещо суб'єктивними при обчисленні і не містять відповідних доказів чи обґрунтування. Наприклад, показник ефективності методології, заснований на часі впровадження стандартів аудиту в організаціях, є досить приблизним і в певній мірі суб'єктивним, оскільки процес впровадження стандартів в організаціях варіюється залежно від типу і розміру організації, наявних ресурсів тощо.

4. У роботі помічено незначні розбіжності у форматуванні абзаців та списків.

Слід відзначити, що визначені зауваження не носять принципового характеру і не знижують наукової новизни і практичної значущості результатів дисертаційного дослідження та не впливають на загалом позитивну оцінку дисертаційної роботи.

### **Висновок.**

Не зважаючи на виявлені недоліки, дисертаційна робота Курія Євгенія Олеговича на тему «Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки» є завершеною науковою працею, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»), яка за своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає паспорту спеціальності 125 «Кібербезпека» та чинним вимогам, які встановлені у «Порядку присудження ступеня доктора філософії», який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №44, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

### **Офіційний рецензент**

Кандидат технічних наук, доцент,  
Доцент кафедри захисту інформації  
Національного університету  
«Львівська політехніка»

Ярослав СОВИН

Підпис к.т.н, доцента Совина Я.Р. засвідчую

Вчений секретар

Національного університету

«Львівська політехніка»

к.т.н., доцент



Роман БРИЛИНСЬКИЙ