ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
д.т.н., проф. Іван ДЕМИДОВ
"30" квітня 2024 р.

Висновок
про наукову новизну, теоретичне та практичне значення результатів дисертації «Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки»
здобувача наукового ступеня доктора філософії за спеціальністю *125 Кібербезпека* (галузь знань *12 Інформаційні технології)*
Курія Євгенія Олеговича
наукового семінару кафедри захисту інформації

1. Актуальність теми дисертації

Захист об'єктів критичної інфраструктури (ОКІ) 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 та актуальним завданням, що потребує комплексного підходу та використання передових технологій.

Для ефективного захисту ОКІ 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 межі та вимоги.

Кожен стандарт інформаційної безпеки має свою унікальну спеціалізацію та обсяг охоплення. Тому для підвищення захищеності об'єктів критичної інфраструктури доцільним є перехресне впровадження стандартів аудиту, коли застосовуються вимоги з декількох стандартів одночасно для більш ефективного та всебічного захисту. Перевагами перехресного впровадження стандартів аудиту з кібербезпеки на об'єктах критичної інфраструктури є підвищення загального рівня кібербезпеки, зниження ризику кібератак, підвищення стійкості до кіберінцидентів, та підвищення довіри з боку клієнтів та партнерів.

2. 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.

3. Особистий внесок здобувача в отриманні наукових результатів

Дисертація є самостійною науковою працею, в якій автор особисто розробив і впровадив нові наукові ідеї та методи, спрямовані на підвищення рівня захищеності об'єктів критичної інфраструктури від кіберзагроз за рахунок використання методології перехресного впровадження стандартів аудиту з кібербезпеки. Ідеї, положення чи гіпотези інших авторів, які присутні в дисертації, мають відповідні посилання і використані лише для підкріплення ідей та результатів здобувача.

4. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванні прийнятих допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується практичною реалізацією методології перехресного впровадження стандартів аудиту.

5. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру

Наукова новизна основних результатів дисертації полягає в розробленні методології перехресного впровадження провідних стандартів аудиту з кібербезпеки:

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

2. *Вперше розроблено* метод оцінки системи управління інформаційною безпекою 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. Розроблений метод забезпечує систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки, скорочує час на впровадження стандарта та забезпечує 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. Розроблений метод підвищує 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. Ця методологія підвищує ефективність захищеності ОКІ від загроз за рахунок автоматизації і пришвидшення процесу створення політик інформаційної безпеки з забезпеченням покриття усіх найважливіших доменів і контролів безпеки.

6. Перелік наукових праць, які відображають основні результати дисертації

Основні результати дослідження викладено у дев'яти наукових публікаціях, а саме: у шести статтях у наукових фахових виданнях України і трьох тезах виступів на науково-практичних заходах.

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. Kurii, Y. Opirskyy, 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. *Особистий внесок аспіранта: проведено аналіз та представлено порівняльну характеристику стандартів аудиту з кібербезпеки ISO 27001 та NIST SP 800-53.*
2. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1 (9 (121)), 6–20.doi: https://doi.org/10.15587/1729-4061.2023.273363. *Особистий внесок аспіранта: проведено аналіз недавніх кібератак на критичну інфраструктуру.*
3. Kurii, Y. ., & Opirskyy, 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. *Особистий внесок аспіранта: проведено огляд нової редакції стандарту ISO 27001:2022 та ключових змін у структурі та описі контролів безпеки, а також розроблено рекомендації для досягнення відповідності вимогам оновленої версії стандарту.*
4. 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. *Особистий внесок аспіранта: розроблено метод оцінки системи управління інформаційною безпекою об'єкта критичної інфраструктури на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні детального контрольного списка.*
5. Vakhula O., Kurii Y., Opirskyy 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. *Особистий внесок аспіранта: проведено огляд і аналіз нових вимог стандарту ISO 27001:2022 і, зокрема, контролю A.8.9 - Управління налаштуваннями.*
6. 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. *Особистий внесок аспіранта: проведено дослідження та аналіз останньої версії стандарту PCI DSS v.4.0., зокрема, її основних змін та вдосконалень у порівнянні з попередньою версією PCI DSS v.3.2.1.*

Наукові публікації у збірниках матеріалів та тез конференцій:

7. Yevhenii KURII, Ivan OPIRSKYY, 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. *Особистий внесок аспіранта: проведено аналіз оновленої редакції стандарту ISO 27001:2022 та розроблено рекомендації для досягнення відповідності вимогам оновленої версії.*
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. *Особистий внесок аспіранта: проведено порівняльну характеристику провідних стандартів аудиту з кібербезпеки..*
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. *Особистий внесок аспіранта: проведено аналіз переваг і недоліків застосування методології перехресного впровадження стандартів аудиту з кібербезпеки для підвищення захищеності об'єктів критичної інфраструктури.*

7. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо

Основні результати дисертаційного дослідження апробовано на міжнародних наукових та науково-практичних конференціях, семінарах:

- IX Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (25-26 травня 2023 року, Львів, Україна);
- Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» (15-16 лютого 2024 року, м. Тернопіль, Україна, м. Ополе, Польща);
- V Міжнародна науково-практична інтернет-конференція «Стратегії розвитку сучасної освіти і науки» (27 лютого 2024 року, Ждяр-над-Сазавою, Чеська Республіка);
- Наукові семінари кафедри захисту інформації (2022-2024 рр.).

8. 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 першого рівня вищої освіти спеціальності 125 *Кібербезпека та захист інформації.*

9. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані

Методологія та методи, представлені в науковій роботі, сприяють підвищенню рівня захищеності об'єктів критичної інфраструктури від кіберзагроз. Розроблена методологія перехресного впровадження стандартів аудиту з кібербезпеки підвищує рівень інформаційної безпеки та захищеності ОКІ, а також зменшує час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки одночасно.

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».

10. Оцінка структури дисертації, її мови та стилю викладення

Дисертаційна робота викладена на 287 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, в яких міститься 21 рисунок та 10 таблиць, списку використаних джерел зі 125 найменувань, а також 6 додатків. За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

У ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.

11. З врахуванням зазначеного, **на науковому семінарі кафедри захисту інформації ухвалили:**

11.1. Дисертація Курія Євгенія Олеговича на тему «Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки» є завершеною науковою працею, у якій розв'язано конкретне науково-практичне завдання – підвищення рівня захищеності об'єктів критичної інфраструктури від кіберзагроз за рахунок використання методології перехресного впровадження стандартів аудиту з кібербезпеки, що має важливе значення для галузі знань 12 *Інформаційні технології.*

11.2. Основні наукові положення, методичні розробки, висновки та практичні рекомендації, викладені у дисертаційній роботі, логічні, послідовні, аргументовані, достовірні, достатньо обґрунтовані. Дисертація характеризується єдністю змісту.

11.3. У 9 наукових публікаціях відображені основні результати дисертації (з них 3 статті у наукових фахових виданнях України, 3 статті у наукових періодичних виданнях, що індексуються у наукометричній базі Scopus, та 3 матеріалів конференцій).

11.4. Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44, зі змінами).

11.5. Дисертація є результатом самостійних досліджень, не містить елементів фальсифікації, компіляції, плагіату та запозичень, що констатує відсутність порушення академічної доброчесності. Використання текстів інших авторів мають належні посилання на відповідні джерела.

11.6. З урахуванням наукової зрілості та професійних якостей Курія Євгенія Олеговича, дисертаційна робота «Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки» рекомендується для подання до розгляду та захисту у разовій спеціалізованій вченій раді.

За затвердження висновку проголосували:

"за"	***55***	***(п'ятдесят п'ять)***
"проти"	***–***	***(немає)***
"утримались"	***–***	***(немає)***

Головуючий на засіданні фахового семінару, д.т.н., професор, завідувач кафедри захисту інформації — Іван ОПІРСЬКИЙ

Рецензенти:

к.т.н., доцент, доцент кафедри захисту інформації — Ярослав СОВИН

к.т.н., доцент, доцент кафедри захисту інформації — Олег ГАРАСИМЧУК

Відповідальний в ІКТА за атестацію PhD, д.т.н., професор, професор кафедри захисту інформації — Любомир ПАРХУЦЬ

"23" квітня 2024 р.