Голові разової спеціалізованої
вченої ради
Національного університету
«Львівська політехніка»
д.т.н., професору
Дудикевичу Валерію Богдановичу

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора, Гнатюка Сергія Олександровича
в.о. проректора з наукової роботи Національного авіаційного університету
на дисертаційну роботу
Курія Євгенія Олеговича
«Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки»
подану до захисту на здобуття наукового ступеня доктора філософії за
спеціальністю 125 «Кібербезпека»
(галузь знань 12 «Інформаційні технології»)

1. Актуальність теми дисертаційної роботи

Дисертаційна робота описує особливості перехресного провадження стандартів аудиту з кібербезпеки на об'єктах критичної інфраструктури (ОКІ) і пропонує унікальний метод оцінки відповідності системи управління інформаційною безпекою (СУІБ) об'єкта критичної інфраструктури сучасним практикам інформаційної безпеки, і впровадження стандартів аудиту з кібербезпеки на основі цієї оцінки.

У роботі 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 провідних стандартів аудиту з кібербезпеки.

Також ця робота вирішує науково-практичну задачу з підвищення рівня інформаційної безпеки об’єктів критичної інфраструктури за рахунок використання методології перехресного впровадження стандартів аудиту з кібербезпеки.

У сучасному світі, де високотехнологічні системи стали невід'ємною частиною інфраструктури, питання кібербезпеки набувають дедалі більшої важливості. Масштабні та серйозні наслідки кібератак на об'єкти критичної інфраструктури підкреслюють необхідність надійного захисту. Порушення безпеки в таких секторах, як енергетика, транспорт та фінанси, можуть мати катастрофічні наслідки для економіки, соціальної стабільності та безпеки громадян. Забезпечення надійного захисту цих об'єктів є надзвичайно важливим завданням, яке вимагає комплексного підходу та впровадження передових технологій.

Для забезпечення ефективного захисту об'єктів критичної інфраструктури необхідно впроваджувати передові технології та методики кібербезпеки. Стандарти аудиту з кібербезпеки надають систематизований підхід до ідентифікації потенційних ризиків і впровадження заходів для їхнього запобігання. Вони допомагають організувати процес забезпечення безпеки, створюючи загальноприйняті рамки та вимоги, що дозволяють компаніям більш ефективно захищати свої системи та ресурси від кіберзагроз. Таким чином, впровадження стандартів аудиту є ключовим елементом у стратегії кібербезпеки, спрямованої на захист критично важливих інфраструктурних об'єктів.

Ефективне впровадження стандартів аудиту з кібербезпеки на об'єктах критичної інфраструктури вимагає системного підходу, ретельного планування та великої уваги до деталей. Важливо поєднувати технологічні та організаційні заходи для створення комплексної системи захисту, яка забезпечить надійність та стійкість інфраструктури в умовах постійної загрози кібератак.

2. Аналіз змісту дисертаційної роботи

Дисертація є завершеною дослідницькою роботою, що містить анотацію, вступ, 4 розділи, висновки, список використаних джерел та додатки.

У **вступі** автором обґрунтовано актуальність теми, сформульовано цілі та завдання дослідження, визначено наукову новизну та практичну цінність результатів дослідження, презентовано дані про апробацію та публікацію результатів дисертаційної роботи.

У **першому розділі** автор дослідив важливість захисту критичної інфраструктури України, особливо в контексті загроз кібербезпеці, зумовлених гібридною війною росії. Впровадження різноманітних стандартів аудиту з кібербезпеки, таких як ISO 27001, NIST SP 800-53, SOC 2, PCI DSS та інших, визначається автором як ефективний метод захисту. Ці стандарти надають організаціям структурований підхід до забезпечення цілісності, конфіденційності та доступності інформаційних активів організації. Проте впровадження цих стандартів часто ускладнюється відсутністю розуміння та ресурсів, а також складністю вибору та впровадження відповідного стандарту. Для подолання цих проблем необхідне правильне планування, розуміння контексту організації, ризик-орієнтований підхід та вивчення спільних рис і відмінностей різних стандартів аудиту з кібербезпеки.

У **другому розділі** автором проведено детальний аналіз стандарту ISO 27001, визначеного як один з ключових у галузі інформаційної безпеки. Аналіз дозволяє краще зрозуміти вимоги, структуру та принципи цього стандарту, включаючи нову редакцію 2022 року. Особлива увага приділена порівняльному аналізу з попередньою версією 2013 року, а також розробці перехресної відповідності між контролями для полегшення переходу між версіями та узгодження з іншими відомими стандартами кібербезпеки, такими як NIST SP 800-53, SOC 2 та PCI DSS.

У **третьому розділі** автор розробив універсальну методологію оцінки захищеності об'єкта критичної інфраструктури, засновану на використанні стандартів кібербезпеки. Шляхом аналізу існуючих методів впровадження стандартів було розроблено інноваційний метод оцінки відповідності СУІБ ОКІ вимогам стандарту ISO 27001 на основі контрольного списка. Крім того, розроблено методологію оцінки ризиків інформаційної безпеки, яка включає

визначення активів, ідентифікацію та оцінку ризиків та визначення стратегії обробки ризиків. Також розроблено методологію перехресного впровадження стандартів аудиту з кібербезпеки на основі зіставлення їхніх контролів безпеки та визначено перелік документації для досягнення відповідності стандарту. Результатом дослідження є комплексний підхід до забезпечення захищеності об'єкта критичної інфраструктури, що враховує сучасні підходи та вимоги у галузі кібербезпеки, сприяючи ефективному управлінню загрозами та ризиками і забезпечуючи високий рівень безпеки.

У **четвертому розділі** автором представлено метод і форму оцінювання для аналізу організації на відповідність стандарту ISO 27001 та впровадження стандартів аудиту з кібербезпеки. Також у розділі проведено оцінку ступеня перехресного покриття стандартів кібербезпеки та оцінено ефективність застосування розробленої методології для впровадження стандартів аудиту.

Ефективність та переваги запропонованої у дослідженні методології порівняно з аналогами демонструють її значний потенціал у підвищенні рівня кібербезпеки в організаціях та об'єктах критичної інфраструктури, що стає важливим кроком у їхньому захисті від сучасних кіберзагроз.

У **висновках** дисертаційної роботи викладено основні результати дослідження і рекомендації, які випливають з проведених досліджень.

3. Наукова новизна одержаних результатів

Найсуттєвіші результати дослідження, що містять наукову новизну, полягають у тому, що:

– 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;

– вперше розроблено метод оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні контрольного списка, 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;

– 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;

– 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.

4. 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 «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисципліни «Нормативно-правове забезпечення та

міжнародні стандарти кібербезпеки» для студентів першого рівня вищої освіти напрямку підготовки 125 «Кібербезпека та захист інформації».

5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна

Наведені в дисертації результати базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих припущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується практичною реалізацією методології перехресного впровадження стандартів аудиту з кібербезпеки.

6. Практичне значення одержаних результатів полягає у тому, що:

– 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;

– 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;

– 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;

– 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;

– 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 списка 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.

7. Повнота оприлюднення результатів дисертаційної роботи

Основні результати дисертаційної роботи Курія Євгенія Олеговича 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 проіндексовапо в наукометричній базі Scopus.

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів.

8. Оцінка структури дисертації, її мови та стилю викладення

Дисертація за структурою, мовою та стилем викладення оформлена відповідно до вимог МОН України, що висуваються до подібного роду наукових робіт. Дисертація написана грамотною українською мовою з використанням

сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним. Зміст наукових праць доповнює основні положення дисертації.

У дисертаційній роботі відсутні порушення академічної доброчесності. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Ознайомлення з текстом анотації дає змогу констатувати, що її зміст повною мірою відображає основні положення і висновки дисертації та не містить зайвої інформації.

9. Зауваження та дискусійні положення щодо змісту роботи

У цілому, позитивно оцінюючи дисертаційне дослідження, необхідно зробити певні зауваження та вказати на окремі положення роботи, що викликають дискусію:

1. У підрозділі 1.4 було проаналізовано декілька популярних стандартів аудиту з кібербезпеки, але не було достатньо обґрунтовано, чому саме ці стандарти були обрані та які критерії використовувались для їх вибору. Бажано б було включити до аналізу додаткові найпоширеніші галузеві стандарти, щоб підвищити універсальність та застосовність розробленої методології;

2. У підрозділі 2.1 автор досліджує та порівнює контрольні заходи стандарту ISO 27001 версій 2013 та 2022 років. Проте, автор не надає конкретних рекомендацій для здійснення переходу на оновлену версію стандарту. Хоча в таблиці зіставлення наведено відповідність між контролями обох версій, а також проведено детальний аналіз змін, все ж відсутня чітка методологія та рекомендації для ефективного переходу СУІБ об'єкта критичної інфраструктури на нову версію стандарту ISO 27001;

3. У підрозділі 3.3, при представленні методології оцінки ризиків інформаційної безпеки об'єктів критичної інфраструктури, бракує більш конкретних практичних кроків щодо впровадження і використання цієї методології. Хоча розроблений шаблон для оцінки ризиків частково покриває практичний аспект, автору варто було б навести приклади застосування цієї методології і надати практичні рекомендації щодо її впровадження. Також

доцільно було б провести порівняння розробленої методології з існуючими методологіями для оцінки ризиків інформаційної безпеки та вказати її основні переваги;

4. У розділі 4.3 при аналізі показника ефективності методології на основі часу впровадження стандартів аудиту в організаціях, в основному наведено результати оцінки для таких стандартів як ISO 27001 та SOC 2. Проте бажано б було представити результати порівняльної оцінки для інших розглянутих в роботі стандартів, таких як NIST 800-53 та PCI DSS. Також, у цьому розділі, при аналізі показника ефективності методології, представлено результати впровадження стандартів в основному для приватних компаній. В даній секції бракує висвітлення результатів впровадження саме в об'єктах критичної інфраструктури та опису основних відмінностей і особливостей такого впровадження.

5. Дисертант визначив науково-практичне завдання як підвищення рівня захищеності об'єктів критичної інфраструктури від кіберзагроз, проте з тексту роботи і висновків не зрозуміло на скільки саме підвищено рівень захищеності.

6. Відсутні порівняння отриманих результатів з аналогами, що ускладнює оцінювання реального внеску здобувача в галузі кібербезпеки.

7. У дисертаційній роботі присутня низка лексичних та стилістичних помилок.

Водночас, висловлені зауваження та пропозиції мають дискусійний характер, не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової і практичної цінності.

Загальні висновки щодо дисертаційної роботи

Дисертаційна робота Курія Євгенія Олеговича «Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки» є завершеним, самостійним та цілісним науковим дослідженням, що містить наукову новизну та практичну цінність отриманих результатів, які дозволяють підвищити рівень захищеності об'єктів критичної інфраструктури шляхом перехресного впровадження провідних стандартів аудиту з кібербезпеки. Зміст дисертаційної роботи

«Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки» відповідає обраній темі та забезпечує досягнення поставленої мети, відповідає вимогам порядку присудження ступеня доктора філософії, а її автор, Курій Євгеній Олегович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний опонент

в.о. проректора з наукової роботи
Національного авіаційного університету
доктор технічних наук, професор Сергій ГНАТЮК