

## **РЕЦЕНЗІЯ**

на дисертаційну роботу  
Полуциганової Вікторії Ігорівни  
на тему «Метод оцінки ризику на основі аналізу структури зв'язків  
загроз та вразливостей у кіберсистемах»,  
представлену на здобуття ступеня доктора філософії  
в галузі знань 12 Інформаційні технології  
за спеціальністю 125 Кібербезпека та захист інформації

### **Актуальність теми дисертації.**

Нині забезпечення збереженості властивостей інформації в організаціях, зокрема, й об'єктах критичної інфраструктури, досягається розроблянням і впроваджуванням та/або комплексних систем захисту інформації (НД ТЗІ 3.7-003-2005), та/або систем управління інформаційною безпекою (ДСТУ ISO/IEC 27001:2023), та/або систем безпеки інформації (НД ТЗІ 3.6-004-2021). Разом з тим, незалежно від обраного варіанту системи забезпечення збереженості властивостей інформації основою кожної з них є відповідні заходи та засоби. Вони обираються за результатами оцінювання ризиків інформаційної безпеки. Отримані оцінки зіставляються зі встановленим прийнятним рівнем і, як наслідок, приймається рішення про необхідність їх оброблення.

Водночас при оцінюванні ризиків інформаційної безпеки кіберсистем необхідно враховувати специфіку їх структури. Залишення поза увагою даного аспекту може призводити до зменшення точності отриманих результатів і, як наслідок, складнощів обирання заходів і засобів оброблення. Запобігання цьому можливе шляхом виявлення, аналізування і класифікування загроз залежно від уразливостей кіберсистеми. В даному випадку ризики оцінюються з урахуванням специфіки взаємозв'язку вразливостей та загроз з урахуванням структури їхньої сумісності. Такий підхід дозволить враховувати приховані зв'язки між уразливостями кіберсистем, а також ступінь впливу на кіберсистему кожної з них окремо та загалом.

Отже, тема дисертації Полуциганової Вікторії Ігорівни, виконання якої направлене на аналізування і синтезування моделей і методів оцінювання ризиків з урахуванням структурних властивостей сукупності зв'язків загроз та вразливостей кіберсистем, є актуальною та має науково-практичне значення.

**Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.**

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. Уперше побудовано модель зв'язків загроз та вразливостей у кіберсистемі у вигляді симпліціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків.

2. Уперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу.

3. Уперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак.

4. Розроблено процедуру побудови байєсівської оцінки ризику з урахуванням структури вразливостей системи та складеної функції втрат.

Обґрунтованість та достовірність наукових результатів у дисертації забезпечується ґрунтовним аналізуванням сучасних літературних джерел, коректною постановкою завдань, науковою обґрунтованістю теоретичних положень, використанням апробованого математичного апарату, узгодженістю теоретичних положень з результатами експериментальних досліджень, опублікованими науковими працями у фахових виданнях, апробуваннями отриманих результатів на всеукраїнських і міжнародних наукових конференціях.

Наукові дослідження виконані здобувачкою на кафедрі інформаційної безпеки ФТІ КПІ ім. Ігоря Сікорського в межах НДР «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» (держ. реєстрація № 0124U001957). Отримані при цьому результати впроваджено в освітньому процесі ФТІ КПІ ім. Ігоря Сікорського при підготовці здобувачів на другому (магістерському) та третьому (освітньо-науковому) рівнях вищої освіти за спеціальністю 125 Кібербезпека та захист інформації. Наукові напрацювання та пропозиції здобувачки використані протягом підготовки матеріалів для засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері». До того ж рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони, а також розроблення Загальних правил обміну інформацією про кіберінциденти.

Отже, в дисертаційній роботі поставлене наукове завдання з аналізування і синтезування моделей і методів оцінювання ризиків з урахуванням структурних властивостей сукупності зв'язків загроз та вразливостей кіберсистем виконано повністю, здобувачка оволоділа методологією наукової діяльності.

### **Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.**

За своїм змістом дисертаційна робота здобувачки Полуциганової Вікторії Ігорівни повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації та напрямам досліджень відповідно до освітньо-наукової програми «Кібербезпека».

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувачки в наукові напрями «Математичні методи моделювання і проєктування систем захисту інформації» та «Системний аналіз безпеки складних систем».



Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Полущиганової Вікторії Ігорівни є результатом самостійних досліджень здобувачки та не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

### **Мова та стиль викладення результатів.**

Дисертаційна робота виконана в науковому стилі державною мовою з використанням загальноприйнятої термінології. Завдяки цьому забезпечується аргументованість і логічність викладення отриманих результатів відповідно до поставленої мети та сформульованих взаємопов'язаних часткових завдань її досягнення.

Дисертація складається з вступу, чотирьох розділів, списку використаних джерел, висновків і двох додатків. Загальний обсяг дисертації 207 сторінок.

У *вступі* обґрунтовано актуальність обраної теми дисертації; визначено мету, завдання і методи дослідження; сформульовано наукову новизну та практичне значення отриманих результатів; виокремлено особистий внесок здобувачки насамперед у наукових працях зі співавторами; наведено інформацію щодо апробування, опублікування результатів дисертації, а також її структури та обсягу.

У *першому розділі* досліджено актуальність проблеми оцінювання ризиків і загальні підходи до її подолання. Насамперед проаналізовано поточний стан його методології, сфер застосування. Виокремлено завдання пріоритезування, типізування ризиків. Показано, що вирішення кожного з них пов'язане з прийняттям рішень. Зокрема досліджено загальні підходи до оцінювання ризиків – Вальда, Байеса, ланцюги Маркова. Крім них проаналізовано гармонізований в Україні міжнародний стандарт ISO 31000. Як підґрунтя дисертаційних досліджень наведено термінологію у галузі інформаційної безпеки. До того ж приділено увагу формалізуванню дослідження уразливостей, загроз та інцидентів, а також складності кіберсистем.

У *другому розділі* знайдено структурні характеристики кіберсистем. Встановлено обумовленість виконання даного завдання залежно від наявності/відсутності даних про систему. Це пов'язано з відображенням структурною характеристикою складності зв'язків і ступеня сумісності елементів системи вразливостей. Для описання її структури розроблено алгоритми переходу від матриці інцидентності до симпліціального комплексу, побудови структурного дерева, локальних карт, пошуку нащадків за ланцюгами симплексів. Їх застосовність дозволяє ідентифікувати приховані зв'язки як потенційні вразливості кіберсистем. Отримані результати розв'язання завдань Q-аналізу продемонстровано на прикладах залежності загроз та вразливостей у хмарному середовищі та мережевих структурах.

У *третьому розділі* розроблено узагальнений метод оцінювання ризиків на основі врахування складних зв'язків між елементами та вразливостей

протягом життєвого циклу кіберсистеми. Залежно від сумісності реалізації структурних компонентів загроз розглянуто варіанти задання функції середнього ризику. При цьому враховано ймовірнісні характеристики сумісного реалізування вразливостей. Як наслідок, ризик для симплеціального комплексу загалом визначається з поправками на надмірність унаслідок склеювання між симплексами. З урахуванням його структури запропоновано формулу байєсового оцінювання ризику, поліноміальність якої обумовлена сумісністю загроз і профілем атак.

У четвертому розділі розробленим методом оцінено ризик безпеки інформаційної системи об'єкта критичної інфраструктури. Викладено основні етапи виявлення та аналізування сумісності вразливостей між собою та систему загроз загалом. Створено симплеціальний комплекс, структурне дерево та досліджено взаємозв'язок між уразливостями обраної інформаційної системи об'єкта критичної інфраструктури. Доведено існування уразливостей, через які можливе реалізування загроз зі значним непрямим впливом на конфіденційність, цілісність і доступність інформації. Здійснено структурне класифікування наявних загроз безпеці інформаційної системи об'єкта критичної інфраструктури на основі Q-аналізу. Побудовано формулу байєсового оцінювання ризику з урахуванням впливу дослідженої складної структури кіберсистеми. Показано зменшення загального ризику її безпеки до 23,3% залежно від розподілення загроз і профілю атак.

У висновках узагальнено отримані наукові та практичні результати аналізування і синтезування моделей і методів оцінювання ризиків з урахуванням структурних властивостей сукупності зв'язків загроз та вразливостей кіберсистем.

У додатках викладено список публікацій і апробацій за темою дисертації; документи, якими підтверджується упровадження результатів її виконання.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

### **Оприлюднення результатів дисертаційної роботи.**

Результати дисертаційної роботи оприлюднено у 12 наукових публікаціях здобувачки, серед них: 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 8 – у матеріалах всеукраїнських і міжнародних наукових фахових конференцій.

Наукові публікації здобувачки характеризуються високим науковим рівнем і відповідністю принципам академічної доброчесності. Виокремлений її особистий внесок в оприлюднених публікаціях, зокрема, й зі співавторами є вагомим. Цим підтверджується самостійність отримання здобувачкою основних положень і результатів, що виносяться на захист.

Отже, наукові результати викладені в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувачки.



### **Недоліки та зауваження до дисертаційної роботи.**

1. У дисертаційній роботі приділено увагу дослідженню ефективного та безпечного функціонування складних кібернетичних систем. З огляду на це, доцільно було б відповідно уточнити формулювання об'єкту дослідження, наприклад: або кібернетична система, або процес функціонування кібернетичних систем.

2. У пункті 1.2.4 аналізування основних стандартів в галузі ризиків зведено здобувачкою тільки до ISO 31000. Попри його узагальнену направленість і з урахуванням тематики дисертаційної роботи доцільно було б розглянути, наприклад, і гармонізовані в Україні ІЕС 31010:2019, ISO/IEC 27005:2022. До того ж при тлумаченні поняття ризику рекомендовано враховувати настанови ДСТУ ISO Guide 73.

3. У пункті 2.1 викладено та схематично представлено на рис. 2.3 процедуру обрахунку нащадків для відслідковування найбільш взаємопов'язаних підсистем. Необхідно уточнити, по-перше, діапазони значень змінних, наприклад,  $i = \overline{0, m-1}$  (див. с. 106); по-друге, схематичне представлення циклів знаходження симпліціального ланцюга на рис. 2.3 (див. с. 107).

4. Наявність окремих помилок оформлення і викладення тексту дисертації, наприклад: «Аналіз оцінки ризиків...» (див. с. 26, 27, 152), доцільно було б або аналіз ризиків (Q-аналіз ризиків, див. с. 152), або оцінка ризиків. Тоді як в обох випадках для позначення процесів рекомендовано вживати аналізування, оцінювання; «Відповідно до ISO 31000:20095...» (див. с. 56, 57), доцільно було б «...ISO 31000:2009...»; необхідність уточнення оформлення окремих використаних джерел [10, 20, 36, 82, 101, 109].

Вважаю, що висловлені недоліки та зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значущість результатів та не впливають на позитивну оцінку дисертаційної роботи.

### **Висновок про дисертаційну роботу.**

Вважаю, що дисертаційна робота здобувачки ступеня доктора філософії Полущиганової Вікторії Ігорівни на тему «Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для галузі знань 12 Інформаційні технології.

Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6–9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувачка Полуциганова Вікторія Ігорівна заслуговує на присудження ступеня доктора філософії у галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

**Рецензент:**

доцент Спеціальної кафедри № 5  
ІСЗЗІ КПІ ім. Ігоря Сікорського  
кандидат технічних наук, доцент



Василь ЦУРКАН

Підпис кандидата технічних наук, доцента Цуркана Василя Васильовича засвідчую.

Заступник начальника  
ІСЗЗІ КПІ ім. Ігоря Сікорського  
(з навчальної роботи)  
кандидат технічних наук, доцент



Ігор ГИРЕНКО