Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті
03058, м. Київ, пр. Любомира Гузара, 1

ВІДГУК

офіційного опонента доктора технічних наук, професора Лахна В.А.
на дисертацію кандидата технічних наук, доцента Гончара Сергія Феодосійовича за темою «Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю
05.13.21 – «Системи захисту інформації»

Актуальність теми

Події останніх років в Україні та у світі показали нагальну необхідність забезпечення кібербезпеки інформаційних систем (ІС) об'єктів критичної інфраструктури, особливо енергетичного сектору. Одним з основних етапів побудови системи управління інформаційною безпекою (СУІБ), комплексної системи захисту інформації (КСЗІ) являється створення системи ризик-менеджменту. Власники ІС прагнуть звести до мінімуму ризики кібербезпеки. Економічна доцільність застосування і вибір тих чи інших заходів по опрацюванню ризику, включаючи як організаційні, так і технічні, визначається оціночним порівнянням вартості таких заходів з максимальною величиною збитків ІС у результаті дії декількох ризиків. Результати оцінювання сумарного ризику дають підстави для прийняття рішення щодо прийнятності їх рівня і необхідності чи економічної доцільності їх подальшої обробки. Оцінювання ризику кібербезпеки здійснюється з достатньою точністю, як правило, на підставі статистичних даних кіберінцидентів за певний проміжок часу. Разом з тим, по цілому ряду ризиків, особливо стосовно об'єктів критичної інфраструктури, такі дані відсутні, величина збитків занижена. Наявні підходи до визначення поняття ризиків та методи їх оцінювання недостатньо повно описують це поняття, не враховують суб'єктивний ризик, що ускладнює коректне його оцінювання. Невирішеним залишається питання, пов'язане із можливістю розрахунку суми ризиків, що дало би можливість здійснення кількісного оцінювання ризику у цілому, врахування при оцінюванні ризику людського чиннику, що являється надзвичайно актуальним для об'єктів критичної інфраструктури, у тому числі енергетичного сектору. Таким чином, на сучасному етапі розвитку науки та техніки існує об'єктивне протиріччя, яке полягає у наявності об'єктивно існуючих факторів ризику та обов'язковою наявністю суб'єктивного чиннику при оцінюванні такого ризику, прийнятті

51.11/01
від 19.03.2020

управлінського рішення і формування впливу на об'єкт управління, з іншого. З цих позицій, дисертаційна робота Гончара С.Ф. присвячена розв'язанню актуальної науково-практичної проблеми (яка має як теоретичне, так і практичне значення) пов'язаної з розробкою методології оцінювання ризиків кібербезпеки ІС об'єктів критичної інфраструктури.

Отже, зважаючи на зв'язок теми дисертацій Гончара С.Ф. з означеними вище питаннями, вважаємо її достатньо обґрунтованою та актуальною.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Викладені наукові положення, висновки та рекомендації є повністю обґрунтованими. Достовірність запропонованих дисертантом теоретичних положень, гіпотез і математичних моделей підтверджується відповідними експериментальними даними та результатами верифікації запропонованих моделей, методів та узагальненої методології. Отримані, під час експериментів, дані відповідають теоретичним висновкам роботи та повністю підтверджують їх. Коректно застосовані методи методологічні основи теорії ризиків, системного аналізу, методи експертних оцінок, елементи теорії комплексних чисел, теорії векторної алгебри.

Ідентичність змісту автореферату й основних положень дисертації

Проаналізувавши автореферат і дисертацію здобувача, можна зробити висновки, що в авторефераті з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертаційної роботи. Для основних положень дисертації та змісту автореферату характерна повна ідентичність.

У **вступі** автором представлена характеристика дисертації, обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету і задачі дослідження, визначено наукову новизну отриманих результатів та їх практичне значення, наведено інформацію про впровадження результатів, їх апробацію та публікації, структуру, об'єм та ключові слова.

У **першому розділі** проведено аналіз вітчизняної та зарубіжної наукової літератури за темою дисертаційної роботи. Досліджено національне нормативно-правове забезпечення кібербезпеки ІС об'єктів критичної інфраструктури та проаналізовано сучасні методи та методології оцінювання ризиків кібербезпеки, у тому числі об'єктів критичної інфраструктури. На основі проведеного аналізу, обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення мети, що поставлена в дисертаційній роботі.

У **другому розділі** виконано аналіз факторів, що впливають на стан кібербезпеки ІС об'єкту критичної інфраструктури. Приведена модель імовірних деструктивних дій обслуговуючого персоналу автоматизованих систем управління технологічними процесами (АСУ ТП) при умові наявності зовнішніх та/або внутрішніх дестабілізуючих впливів. Приведено життєвий цикл аналізу ймовірності реалізації загроз інформаційної безпеки АСУ ТП. Удосконалено метод визначення актуальності загрози кібербезпеки ІС об'єкту критичної інфраструктури.

У **третьому розділі** запропоновані методи розрахунку суми ризиків кібербезпеки ІС об'єктів критичної інфраструктури. Визначення сумарного ризику дозволяє розраховувати загальні потенційні збитки, що виникли або можуть виникнути в процесі реалізації певного проекту. Прикладом може бути розрахунок сумарного ризику складної розподіленої ІС об'єкту критичної інфраструктури. На основі запропонованих методів можливо будувати системи підтримки прийняття рішень щодо зменшення ризику.

У **четвертому розділі** розроблено векторну модель, модель комплексного ризику кібербезпеки ІС об'єктів критичної інфраструктури та метод визначення комплексного ризику. Зазначені моделі дозволяють ввести метрику векторів ризиків та здійснювати векторні операції над ними. Розроблений метод обчислення комплексного ризику кібербезпеки ІС об'єктів критичної інфраструктури може використовуватися при обчисленні суми ризиків об'єктивної та суб'єктивної складових методології оцінювання ризиків кібербезпеки ІС об'єктів критичної інфраструктури.

У **п'ятому розділі** розроблено методологію оцінки ризику кібербезпеки ІС об'єктів критичної інфраструктури, яка, за рахунок використання методів розрахунку суми ризиків і методу обчислення комплексного ризику, дозволяє забезпечити підтримку процесу створення інструментальних засобів для оцінки ризиків кібербезпеки ІС об'єктів критичної інфраструктури. Також, запропоновано структурні рішення обчислювальних систем для розрахунку суми ризиків кібербезпеки ІС об'єктів критичної інфраструктури. За рахунок використання розроблених методів та методології, можливо розробити засоби для розрахунку суми ризиків та обчислення комплексного ризику з урахуванням об'єктивної та суб'єктивної складових.

Шостий розділ містить результати наукових досліджень, пов'язаних із розробкою алгоритмічного та програмного забезпечення обчислювальних систем для розрахунку суми ризиків та обчислення комплексного ризику кібербезпеки ІС об'єктів критичної інфраструктури з використанням розроблених методів. Отримані в розділі результати підтверджують ефективність розроблених методів та методології забезпечення кібербезпеки ІС

об'єктів критичної інфраструктури, орієнтованої на створення відповідних методів та засобів розрахунку сумарних ризиків. Проведені експериментальні дослідження з метою підтвердження теоретичних положень та практичних розробок дисертаційного дослідження, а також виконано впровадження та практичне застосування розробок, в результаті чого було підтверджено їх ефективність при здійсненні заходів щодо забезпечення кібербезпеки ІС об'єктів критичної інфраструктури.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та лістинги (коди) розроблених програмних засобів.

Наукова цінність результатів роботи

Наукова новизна отриманих результатів роботи полягає у наступному:

1. Удосконалено структурну модель взаємодії елементів інформаційних систем об'єктів критичної інфраструктури, яка, за рахунок використання параметрів оцінювання рівня впливу внутрішніх та зовнішніх дестабілізуючих чинників на суб'єкт деструктивних дій, дозволяє розробити модель порушника даної інформаційної системи з урахуванням кіберзагроз, об'єктами яких є адміністратор, користувачі, технічний персонал;

2. Удосконалено метод визначення актуальності загрози кібербезпеки інформаційної системи об'єкту критичної інфраструктури, який, за рахунок використання параметрів оцінювання потенційного рівня загрози, визначених з використанням удосконаленої структурної моделі взаємодії елементів інформаційної системи, а також параметрів, що характеризують потенційних порушників для реалізації загрози, дозволяє розробити модель загроз даної інформаційної системи з урахуванням кіберзагроз, об'єктами яких є адміністратор, користувачі, технічний персонал;

3. Вперше розроблено методи обчислення сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, які, за рахунок використання параметрів оцінювання актуальності загрози, визначених з використанням удосконаленої структурної моделі взаємодії елементів інформаційних систем та удосконаленого методу визначення актуальності загрози, а також параметрів, що характеризують, для кожного ризику, наслідки повного знищення інформаційного активу; ймовірностей подій, що призводять до таких ризиків; дозволяють розраховувати суму визначеної множини ризиків, загальні наслідки та ймовірність їх реалізації;

4. Вперше розроблено векторну модель та модель комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, яка, за рахунок використання величини скалярного добутку векторів ризиків, визначених з використанням методу обчислення сумарного ризику, а також

величин об'єктивних та суб'єктивних складових ризиків, дозволяє ввести довжину векторів ризиків, кут між ними та здійснювати векторні операції над ними;

5. Вперше розроблено метод обчислення комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, який, за рахунок використання значень довжин векторів ризику та кутів між ними, визначених з використанням векторної моделі та моделі комплексного ризику, дозволяє здійснювати оцінювання зазначених ризиків з урахуванням величини впливу людського чиннику;

6. Вперше розроблено методологію оцінювання ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, яка, за рахунок використання удосконаленої структурної моделі взаємодії елементів, удосконаленого методу визначення актуальності загрози, методу обчислення сумарного ризику, векторної моделі та моделі комплексного ризику, методу обчислення комплексного ризику, дозволяє забезпечити підтримку створення обчислювальних систем для автоматизації процесу оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури;

7. Вперше запропоновано структурні моделі (рішення) обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, які, за рахунок використання удосконаленої структурної моделі взаємодії елементів, удосконаленого методу визначення актуальності загрози, методу обчислення сумарного ризику, векторної моделі та моделі комплексного ризику, методу обчислення комплексного ризику, методології оцінювання ризику, дозволяють автоматизувати процес розрахунку сумарного ризику та обчислення комплексного ризику з урахуванням величин об'єктивної та суб'єктивної складових.

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

Основні наукові положення дисертації опубліковано у 51 науковій праці, у тому числі: 1 монографія, 27 наукових статей у наукових журналах та збірниках наукових праць, з яких 2 наукові статі у виданнях, що входять до міжнародної бази даних Scopus, 10 наукових статей у наукових виданнях, що входять до інших міжнародних наукометричних баз даних, 14 наукових статей у вітчизняних фахових наукових журналах та збірниках наукових праць, 5 патентів України на корисну модель, а також 18 матеріалів та тез доповідей конференцій.

Значення результатів для практики

Отримані в дисертаційній роботі результати можуть бути використані для оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури на основі розроблених методів та моделей.

Зокрема, практична цінність одержаних результатів полягає у такому:

розроблено алгоритмічне забезпечення на основі запропонованого структурного рішення обчислювальної системи «Калькулятор ризиків» для реалізації відповідного програмного засобу розрахунку суми ризиків, що дозволяє здійснювати автоматизований розрахунок наслідків від дії сумісних подій, з урахуванням показників, таких як ймовірність подій, що призводять до наслідків, та величина цих наслідків;

– розроблено алгоритмічне забезпечення на основі запропонованого структурного рішення обчислювальної системи «Калькулятор комплексного ризику» для реалізації відповідного програмного засобу розрахунку суми ризиків, що дозволяє здійснювати автоматизований розрахунок повного ризику, з урахуванням об'єктивної та суб'єктивної його складових, з використанням теорії векторної алгебри та комплексних чисел;

– на основі запропонованого алгоритму розроблено програмний застосунок, що використовує запропоновані методи та здійснює оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Результати теоретичних та практичних досліджень знайшли застосування у таких науково-дослідних роботах:

– «Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури»;

– «Організаційно-правові засади контррозвідувального захисту об'єктів критичної інфраструктури України»;

– «Методичні та нормативно-правові основи забезпечення кібербезпеки функціонування енергетики України з урахуванням європейських вимог»;

– «Розвиток наукових засад забезпечення інформаційної безпеки об'єктів критичної інфраструктури електроенергетичної галузі на основі методології системних досліджень»;

– «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів»;

– «Розроблення методів забезпечення кібербезпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж»;

– «Дослідження розвитку систем технічної діагностики та розробка концептуальних основ створення багаторівневих систем моніторингу,

діагностики та прогнозування технічного стану основного енергетичного обладнання АЕС України».

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Національної академії Служби безпеки України, Державного науково-дослідного інституту спеціального зв'язку та захисту інформації, Державного підприємства «Державний науково-технічний центр з ядерної та радіаційної безпеки», Державного підприємства «Український державний центр радіочастот», Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, ПрАТ «ФарлепІнвест».

Зауваження до дисертації та автореферату

1. На наш погляд, використання векторної алгебри та комплексних величин, не дозволяє говорити про новизну при оцінюванні ризиків.

2. Є деяка плутанина в поняттях. Так на сторінці 14 автореферату у формулі (2) ризик (R) визначається як **зважене значення наслідків** і може визначатися формулою: $R(p,h)=p\cdot h$, де $p-$ ймовірність випадкової події, що призводить до певних наслідків h. А на с. 18 автореферату та в тексті дисертації ризик (R) визначається, як ймовірність випадкової події, яка призводить до певних наслідків і може описуватися виразом (2) автореферату або виразом (3.1) дисертації. Але навіть рис. 3 в авторефераті або рис. 3.2 в тексті дисертації ілюструє, що ризик і ймовірність - це різні змінні.

3. На сторінці 152 дисертації все та ж формула $R(p,h)=p\cdot h$, дає можливість перетворити її в формулу: $h=f(R,p)$, що можливо при p не в рівному нулю. І тоді h дорівнює $\int\left(\frac{1}{p}\right)\cdot\left(\frac{\partial R}{\partial h}\right)dp$. Такий запис, мабуть, не дає «з легкістю» стверджувати, що $h(p)=\frac{R_\alpha}{p}$. Напевно, треба зробити деякі припущення. Хотілося б відзначити, що автор не навів посилання на джерело, де він взяв таке визначення ризиків.

4. Що стосується новизни, з точки зору розрахунку сумарних ризиків, то на мою думку, в теорії ймовірностей немає проблем розглядати суми випадкових величин. Отже, пункт новизни, внаслідок того, що робота дає можливість розглядати сумарний ризик, не є очевидним.

5. Не вказано, у середовищі яких програмних засобів здійснювалися математичні розрахунки, побудова графіків, зокрема у главі 3, рис. 3.2, 3.5, 3.6-3.8. Хоча, для розрахунку сумарних ризиків і комплексних ризиків досить «MathCad».

6. У шостому розділі здобувач наводить результати експериментального дослідження для підтвердження достовірності отриманих теоретичних положень та практичних результатів. Усі одержані результати описані й проаналізовані. Але, на наш погляд, не в повній мірі дотримано процедурне питання при проведенні експерименту. Мають бути визначені його мета, завдання, план проведення експерименту, спосіб оброблення результатів тощо. Не визначено, яким чином обирались параметри експериментів на підприємствах.

7. Робота не позбавлена незначних нестач оформлення, у дисертації є друкарські та редакторські помилки. Наприклад, с. 122, 127, 153, 209 та ін.

Висновки

Не зважаючи на зазначені недоліки, дисертаційна робота Гончара Сергія Феодосійовича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку теорії й практики кібербезпеки та захисту інформації. Усі одержані наукові результати можуть застосовуватися у різних галузях критичної інфраструктури держави для формування та забезпечення системи кібербезпеки.

Отже, вважаю, що дисертаційна робота «Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури» повністю відповідає чинним вимогам МОН України, зокрема «Порядку присудження наукових ступенів», затвердженого Постановою КМУ від 24.07.2013 р. № 567 (із змінами, внесеними згідно з Постановами КМУ № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р. № 567 від 27.07.2016 р.), а її автор Гончар Сергій Феодосійович заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент
Завідувач кафедри комп'ютерних систем і мереж
Національного університету біоресурсів
і природокористування України,
доктор технічних наук, професор В. Лахно

Підпис професора Лахна В.А засвідчую

ПІДПИС ЗАСВІДЧУЮ
Начальник відділу кадрів
М.В. Михайліченко
10. 03 2020 р.