МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ГОНЧАР Сергій Феодосійович

УДК 004.056.5:005:004.3:004.4 (043.3)

МЕТОДОЛОГІЯ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2020

Дисертацією є рукопис.
Робота виконана в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ.

Науковий консультант: член-кореспондент НАН України,
доктор технічних наук, професор
Мохор Володимир Володимирович,
Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України, директор.

Офіційні опоненти: доктор технічних наук, професор
Лахно Валерій Анатолійович,
Національний університет біоресурсів і природокористування України, завідувач кафедри комп'ютерних систем і мереж;

доктор технічних наук, професор
Грищук Руслан Валентинович,
Житомирський військовий інститут
імені С. П. Корольова, начальник кафедри
захисту інформації та кібербезпеки;

доктор технічних наук, професор
Ковальчук Людмила Василівна,
Академія зовнішньої розвідки України,
професор СК № 22.

Захист відбудеться «03» квітня 2020 року о 15 годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, пр. Любомира Гузара, 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Любомира Гузара, 1.

Автореферат розісланий «03» березня 2020 р.

Учений секретар
спеціалізованої вченої ради С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Події останніх років в Україні і у світі показали нагальну необхідність забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, особливо енергетичного сектору. У відповідності до статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» об'єкти енергетичного сектору можуть бути віднесені до об'єктів критичної інфраструктури. У відповідності до Постанови Кабінету Міністрів України від 23.08.2016р. №563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» до переліку інформаційних систем об'єктів критичної інфраструктури держави енергетичного сектору включаються системи з урахуванням негативного впливу на стан енергетичної безпеки держави (регіону), до якого може призвести кібератака на такі системи.

У відповідності до зазначеного вище Закону України забезпечення кібербезпеки об'єкту критичної інфраструктури, у тому числі енергетичного сектору, досягається створенням системи управління інформаційною безпекою (СУІБ) у відповідності до міжнародного стандарту ISO/IEC 27001:2013 або створенням комплексної системи захисту інформації (КСЗІ) у відповідності до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Одним з основних етапів побудови СУІБ, КСЗІ являється створення системи ризик-менеджменту.

Власники інформаційних систем прагнуть звести до мінімуму ризики кібербезпеки. Економічна доцільність застосування і вибір тих чи інших заходів по обробці ризику, включаючи як організаційні, так і технічні, визначається оціночним порівнянням вартості таких заходів з максимальною величиною збитків інформаційних систем у результаті дії декількох ризиків. Під максимальною величиною збитків інформаційної системи будемо розуміти величину збитків при повному знищенні інформаційного активу. Результат оцінювання сумарного ризику дають підстави для прийняття рішення щодо прийнятності їх рівня і необхідності чи економічної доцільності їх подальшої обробки. Під сумарним ризиком будемо розуміти певну величину, що визначається збитками у результаті реалізації усіх складових ризиків, і ймовірністю реалізації цих ризиків. Така задача являється актуальною для визначення ризику кібербезпеки інформаційних системи об'єктів критичної інфраструктури для енергетичного сектору у цілому, з урахуванням критичних особливостей таких інформаційних систем у порівнянні з системами інформаційних технологій, а також з урахуванням ризику людського чиннику при прийнятті управлінського рішення.

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.

Існуючі 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 і техніки існує *об'єктивне протиріччя*, яке полягає у наявності об'єктивно існуючих факторів ризику з одного боку, та обов'язковою наявністю суб'єктивного чиннику при оцінюванні такого ризику, прийнятті управлінського рішення і формування впливу на об'єкт управління, з іншого.

З огляду на викладене вище, тема дослідження присвячена вирішенню важливої *науково-прикладної проблеми*, пов'язаної з розробкою методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, орієнтованої на створення відповідних методів визначення ризиків, *є актуальною*.

Дослідженню проблем, пов'язаних із процесом оцінювання ризику кібербезпеки інформаційних систем, що являється об'єктом дисертаційного дослідження присвячується значна частина публікацій вітчизняних і зарубіжних вчених, таких як: О. Замула, С. Казмірчук, О. Архіпов, Т. Прокопенко, Ю. Черданцева, О. Богданов, Thomas R. Peltier, Jinsoo Shin, Hanseong Son, Rahman Khalil ur, Gyunyoung Heo, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart та інші. Однак, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи і отримані результати безпосередньо пов'язані з "Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки", Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017р., Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», Постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», Стратегією національної безпеки України від 26 травня 2015 р. № 287/2015, Стратегією кібербезпеки України від 15 березня 2016 р. № 96/2016, Доктриною інформаційної безпеки України від 25 лютого 2017р. №47/2017 та низкою науково-дослідних робіт (НДР). Результати дисертаційної роботи відображені у звітах НДР Державного науково-дослідного інституту спеціального зв'язку та захисту інформації України за темою «Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури» (шифр «ІНФРАСТРУКТУРА», державний реєстраційний номер 0114U000038д), Національної академії СБ України за темою

«Організаційно-правові засади контррозвідувального захисту об’єктів критичної інфраструктури України» (державний реєстраційний номер 0117U000044т), Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за темами: «Дослідження розвитку систем технічної діагностики та розробка концептуальних основ створення багаторівневих систем моніторингу, діагностики та прогнозування технічного стану основного енергетичного обладнання АЕС України»; «Методичні та нормативно-правові основи забезпечення кібербезпеки функціонування енергетики України з урахуванням європейських вимог» (шифр «ОБ’ЄДНАННЯ», державний реєстраційний номер 0116U002970); «Розвиток наукових засад забезпечення інформаційної безпеки об’єктів критичної інфраструктури електроенергетичної галузі на основі методології системних досліджень» (шифр «БЕСКІДИ», державний реєстраційний номер 0117U005467); «Розробка методів оцінювання чутливості Об’єднаної енергосистеми України до кібернетичних впливів» (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320); «Розроблення методів забезпечення кібербезпеки функціонування Об’єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр «ІНТЕЛЕНЕРГО», державний реєстраційний номер 0119U101856).

Мета та задачі дослідження. Мета дисертаційного дослідження спрямована на вирішення важливої науково-прикладної проблеми, пов’язаної з розробкою методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури, орієнтованої на розроблення і використання відповідних методів розрахунку суми ризиків та обчислення комплексного ризику.

Для досягнення цієї мети в даній роботі необхідно було розв'язати такі основні задачі:

– проаналізувати сучасні методи оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об’єктів критичної інфраструктури;

– удосконалити структурну модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури;

– удосконалити метод визначення актуальності загрози кібербезпеки інформаційної системи об’єкту критичної інфраструктури;

– розробити методи розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури;

– розробити векторну модель ризиків та модель комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури;

– розробити метод обчислення комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури;

– розробити методологію оцінювання ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням розроблених методів;

– розробити структурні моделі (рішення) обчислювальних систем для розрахунку сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням розроблених методів;

– розробити алгоритмічне забезпечення та програмний застосунок обчислювальних систем для розрахунку сумарного ризику кібербезпеки

інформаційних систем об’єктів критичної інфраструктури з використанням запропонованих методів;

– здійснити експериментальне дослідження програмного застосунку системи оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури з метою перевірки адекватності реагування розроблених моделей та методів відносно тих чи інших ініціалізуючих величин.

Об’єктом дослідження є процеси оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Предметом дослідження є методи та моделі оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Методи дослідження. Проведені дослідження базуються на методологічній основі теорії ризиків, системному аналізі сучасних розробок для вирішення проблем оцінювання ризиків, методі експертних оцінок. Для розробки методу обчислення суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури використовувались елементи теорії комплексних чисел, теорії векторної алгебри. Для розробки методів обчислення суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури, з використанням значення наслідків повного знищення інформаційного активу, використовувались елементи теорії лінійної алгебри та аналітичної геометрії, теорії ймовірності і випадкових процесів. Як засоби розв’язування поставлених задач використовувалось математичне та комп’ютерне моделювання.

Наукова новизна одержаних результатів полягає в тому, що:

– *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;

– *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;

– *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;

– *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;

– *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;

– *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;

– *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.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані для оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури на основі розроблених методів розрахунку суми ризиків під час побудови та впровадження систем управління інформаційною безпекою, комплексних систем захисту інформації в автоматизованих системах різних класів при побудові моделі загроз, політики безпеки, плану захисту тощо.

Практична цінність роботи полягає у наступному:

– 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» (шифр "ІНФРАСТРУКТУРА", державний реєстраційний номер 0114U000038д);

– «Організаційно-правові засади контррозвідувального захисту об'єктів критичної інфраструктури України» (державний реєстраційний номер 0117U000044т);

– «Методичні та нормативно-правові основи забезпечення кібербезпеки функціонування енергетики України з урахуванням європейських вимог» (шифр «ОБ'ЄДНАННЯ», державний реєстраційний номер 0116U002970);

– «Розвиток наукових засад забезпечення інформаційної безпеки об'єктів критичної інфраструктури електроенергетичної галузі на основі методології системних досліджень» (шифр «БЕСКІДИ», державний реєстраційний номер 0117U005467);

– «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів» (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320);

– «Розроблення методів забезпечення кібербезпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр «ІНТЕЛЕНЕРГО», державний реєстраційний номер 0119U101856);

– «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 «Фарлеп-Інвест».

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [2] – дослідження аргументу комплексно-значної функції та обробка результатів досліджень; [4, 9, 22, 23] – проведення аналізу загроз безпеці інформації об'єктів критичної інфраструктури, здійснення дослідження ; [6, 7, 8, 25] – формулювання рекомендацій щодо забезпечення кібербезпеки об'єктів критичної інфраструктури; [11] – опис можливостей застосування теорії комплексних чисел при здійсненні операцій над ризиками; [12, 13, 15] – аналіз та дослідження небезпеки кібератак на об'єкти критичної інфраструктури та їх наслідки; [14] – розробка методу визначення актуальності загрози кібербезпеки інформаційної системи об'єкту критичної інфраструктури; [17, 18, 24] – формулювання рекомендацій щодо побудови системи управління інформаційною безпекою об'єктів критичної інфраструктури; [20] – розробка моделі комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури та методу його обчислення; [26] – розробка методів визначення суми ризиків; [27] – запропонована векторна модель ризиків. З робіт, опублікованих у співавторстві, для вирішення проблеми та задач, поставлених у дисертаційному досліджені, використовуються результати, отримані особисто здобувачем наукового ступеня.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідались і обговорювались на наукових конференціях, серед яких: міжнародна науково-практична конференція «Кібербезпека-2013» (Київ, 2013р.); І Міжнародна науково-практична конференція «Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК» (Київ, 2013р.); круглий стіл «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання» (Київ, 2014р.); ХХ Всеукраїнська науково-практична конференція «Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення» (Житомир, 2014р.); науково-технічна конференція «Інформаційна безпека України» (Київ, 2015р., 2016р.); XVII Міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2015р., 2018р.); Всеукраїнська наукова конференція «Математичне моделювання та математична фізика» (Кременчук, 2015р.); The international research and practical conference: «The development of technical sciences: problems and solutions» (Brno, The Czech Republic, 2018); VI Міжнародна наукова конференція «Моделювання-2018» (Київ, 2018р.); International Multidisciplinary Conference «Science and Technology of the Present Time: Priory Development Directions of Ukraine and Poland» (Wolomin, Republic of Poland, 2018); Всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019р.); XII Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 2019р.); V Міжнародна науково-практична конференція «Обчислювальний інтелект» (Ужгород, 2019р.); V Всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації» (Одеса, 2019р.).

Публікації. Основні положення дисертаційного дослідження опубліковано у 51 науковій праці, у тому числі: 1 монографія [1], 27 наукових статей у наукових журналах та збірниках наукових праць [2-28], з яких 2 наукові статі у виданнях, що входять до міжнародної бази даних Scopus [2, 26], 10 наукових статей у наукових виданнях, що входять до інших міжнародних наукометричних баз даних [10, 11, 13, 15, 20-23, 25, 27, 28], 14 наукових статей у вітчизняних фахових наукових журналах та збірниках наукових праць [3-9, 12, 14, 16-19, 24], 5 патентів України на корисну модель [29-33], а також 18 матеріалів та тез доповідей конференцій [34-51].

Структура та обсяг роботи. Дисертаційна робота складається з анотації, списку скорочень, вступу, змісту, шістьох розділів, висновків, додатків, списку використаних джерел, та містить 266 сторінок основного тексту, 56 рисунків, 19 таблиць, 36 сторінок додатків. Список використаних джерел налічує 228 найменувань на 24 сторінках. Загальний обсяг дисертаційної роботи складає 326 сторінок.

ОСНОВНА ЧАСТИНА

У анотації та вступі представлена загальна 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 інформаційних систем об’єктів критичної інфраструктури та проаналізовано сучасні методи та методології оцінювання ризиків кібербезпеки, у тому числі об’єктів критичної інфраструктури.

Проведений аналіз показує, що у науковій літературі розглядаються і досить детально аналізуються методи оцінювання ризику, у тому числі для систем SCADA. Описується суть методів, розглядаються етапи управління ризиками, запропонована схема класифікації методів ризиків кібербезпеки для SCADA систем. Досліджено широкий спектр загроз, які призводять до ризику кібербезпеки, створено базу даних фактичних втрат у випадку реалізації цих загроз, здійснено аналіз втрат з використанням методів статистики та актуарної математики. Розроблені структури для розрахунку кількісних оцінок ризиків кібербезпеки. Розглядаються моделі оцінювання ризиків кібербезпеки з використанням апарату нечіткої логіки, нові метрики ризику, основані на адаптації існуючих методів розрахунку ризиків і невизначеностей, таксономічна класифікація вимог до оцінювання ризиків кібербезпеки, досліджуються модель оцінювання ризику кібербезпеки для пристроїв і систем управління ядерних установок з використанням Байєсовської мережі, дерева подій, ймовірнісного методу оцінювання ризику кібербезпеки.

Дослідження існуючих методів оцінювання ризиків (табл. 1) дало можливість встановити, що практично всі досліджені методи дозволяють здійснювати

оцінювання ризиків на технічному рівні, в процесі оцінювання пропонуються способи протидії ризикам, а також заходи по запобіганню та виявленню ризиків.

Результати аналізу показують, що існуючі методи не дають можливості вирішувати задачі, пов'язані із можливістю визначення суми ризиків, що дало би змогу здійснення кількісного оцінювання ризику проекту у цілому або вибраного напряму розвитку процесу, а також обчислення комплексного ризику.

Таблиця 1

Зведені дані методів оцінювання ризиків

Метод	*Критерії*						
	Можливість ідентифікації ризику	*Можливість визначення наслідків*	*Визначення ймовірності*	*Можливість визначення рівня*	*Можливість оцінювання ризику*	*Визначення суми ризиків*	*Визначення комплексного ризику*
Brainstorming	+	–	–	–	–	–	–
Structured or semi-structured interviews	+	–	–	–	–	–	–
Toxicity assessment	+	+	+	+	+	–	–
Delphi method	+	–	–	–	–	–	–
Checklist	+	–	–	–	–	–	–
PHA	+	–	–	–	–	–	–
HAZOP	+	+	+	+	+	–	–
HACCP	+	+	–	+	+	–	–
SWIFT	+	+	+	+	+	–	–
Scenario analysis	+	+	+	+	+	–	–
FMEA	+	+	+	+	+	–	–
Fault tree analysis	+	–	+	+	+	–	–
Event tree analysis	+	+	+	+	+	–	–
Cause and consequence analysis	+	+	+	+	+	–	–
Cause-and-effect analysis	+	+	–	–	–	–	–
LOPA	+	+	+	+	–	–	–
Decision tree	–	+	+	+	+	–	–
HRA	+	+	+	+	+	–	–
Bow tie analysis	–	+	+	+	+	–	–
Monte Carlo simulation	–	–	–	+	+	–	–
Consequence/probability matrix	+	+	+	+	+	–	–
Cost/benefit analysis	+	+	+	+	+	–	–
MCDA	+	–	+	–	+	–	–

Таким чином, у першому розділі, на основі проведеного аналізу, обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення мети, що поставлена в дисертаційній роботі.

У другому розділі удосконалено структурну модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури, а також удосконалено метод визначення актуальності загрози кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Розглянемо структурну модель взаємодії елементів таких систем (рис. 1), а також вплив кожної із складових систем (організаційна, технічна, персонал) на забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

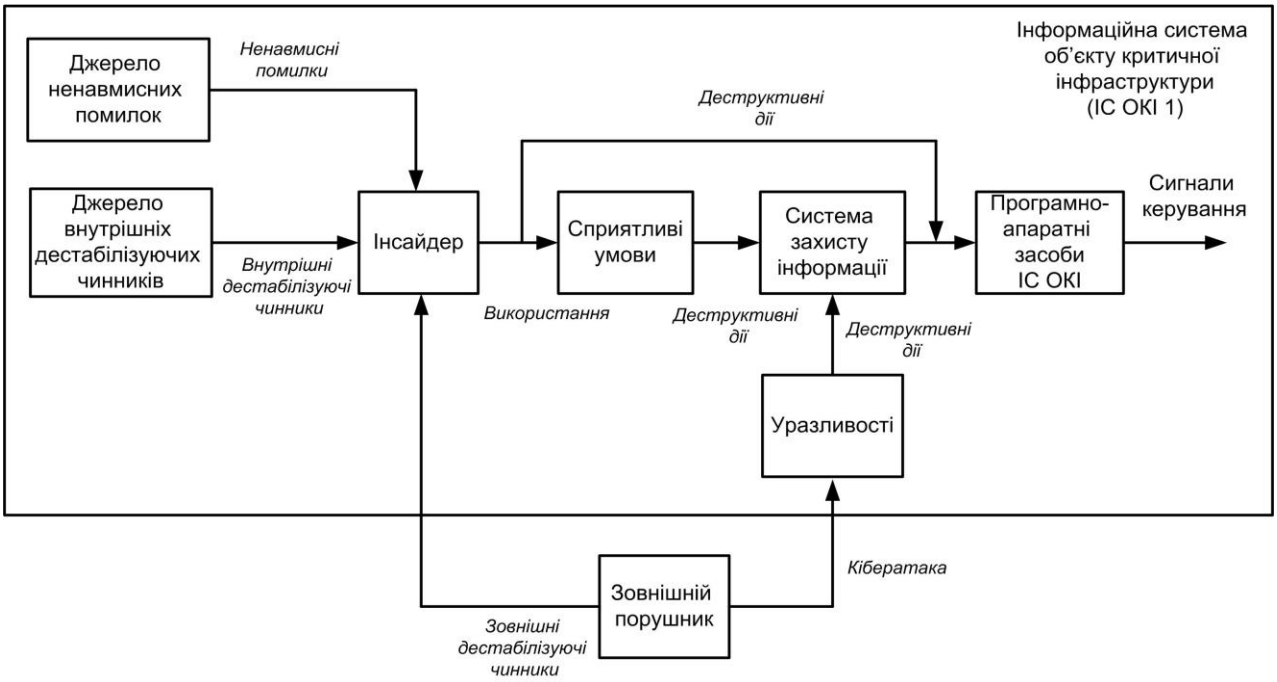


Рисунок 1 – Структурна модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури

Під зовнішніми дестабілізуючими чинниками маємо на увазі наступні загрози:

– загрози несанкціонованого доступу до інформації, несанкціонованих змін або викрадення інформації, відмова в обслуговуванні або профілактика авторизованого доступу, відмова від дії, яка мала місце, або вимога підтвердження дії, якої не було;

– загрози реалізації інформаційно-психологічного впливу на персонал інформаційної системи об'єкту критичної інфраструктури. Такі впливи можуть мати на меті дезорієнтацію, дезінформацію, дезорганізацію, придушення, руйнування тощо.

Під внутрішніми дестабілізуючими чинниками маємо на увазі людські потреби, через які може здійснюватися вплив на кіберзахист інформаційної системи об'єкту критичної інфраструктури, а саме:

- вітальні (природні): їжа, одежа, житло, відпочинок, комфорт, екологія тощо;

- самоактуалізація (пізнавальні): активність, навички, уміння, діяльність, ініціатива, дослідницький пошук тощо;
- інтелектуальні (наукові): освіта (знання), виховання, мислення, цінна інформація, самосвідомість, істина тощо;
- психічні (естетичні): прив'язаність, спорідненість, чиста совість, піднесеність тощо;
- соціальні (групові): спілкування, засоби спілкування, увага до себе, спільна діяльність тощо;
- самореалізація (індивідуальні): творчість, самовдосконалення, самоповага, повага зі сторони інших, визнання, досягнення успіху і високої оцінки, службове зростання тощо;
- духовні (етичні): щастя, свобода совісті, цілісність світогляду, доброта, честь тощо.

Із приведеної структурної моделі взаємодії, рис. 1, можна бачити, що джерела кіберзагроз для інформаційних систем об'єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини (інсайдер).

Для об'єктів критичної інфраструктури, наприклад, енергетичного сектору негативний вплив на стан енергетичної безпеки держави (регіону), до якого може призвести кібератака на таку систему буде визначатися наступним чином:

$$H = \sum_{n=1}^{N} H_n ,$$

де H_n – наслідки від реалізації n-ї загрози кібербезпеці інформаційної системи; n змінюється від 1 до N; N – кількість загроз.

Загроза кібербезпеці інформаційної системи, яка циркулює в інформаційній системі об'єкта критичної інфраструктури, буде вважатися актуальною, якщо для вказаної інформаційної системи об'єкта критичної інфраструктури з заданими структурно-функціональними характеристиками і особливостями функціонування існує ймовірність реалізації розглянутої загрози порушником з відповідним потенціалом і її реалізація призведе до неприйнятних збитків від порушення конфіденційності, цілісності або доступності інформації.

Небезпека загрози в інформаційних системах об'єктів критичної інфраструктури буде визначатися оцінюванням можливих наслідків від її реалізації з позиції впливу на функціонування цих систем, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної загрози.

Актуальність n-ї загрози кібербезпеці інформаційної системи у загальному вигляді можливо описати наступним чином:

$$A_n = f\left\{P\left(H_{nu}\middle|K_n\right); H_n\right\},$$

де $P(H_{nu} \mid K_n)$ – ймовірність реалізації *n*-ї загрози з використанням *u*-ї уразливості за умови наявності сприятливих для цього умов K_n;

H_n – наслідки від реалізації *n*-ї загрози кібербезпеці інформаційної системи об'єкта критичної інфраструктури.

Визначення ймовірності реалізації загрози кібербезпеці інформаційної системи визначаємо експертним методом (з урахуванням структурно-функціональних характеристик і особливостей функціонування інформаційної системи), шляхом введення градації даного показника щодо *n*-ої загрози, який залежить від наступних факторів:

K_n – наявність чи відсутність сприятливих умов для реалізації *n*-ої загрози;

S_n – наявність чи відсутність необхідної статистики щодо фактів реалізації *n*-ої загрози (виникнення інцидентів порушення кібербезпеки інформаційної системи);

q_n – наявність чи відсутність у потенційних порушників мотивації для реалізації *n*-ої загрози, внутрішніх та/або зовнішніх дестабілізуючих чинників, тобто модель порушника та модель загроз інформаційної системи об'єкта критичної інфраструктури;

ω_n – можлива частота реалізації *n*-ої загрози.

Можливість реалізації *n*-ої загрози кібербезпеці інформаційної системи можливо оцінити виходячи із рівня захищеності інформаційної системи і потенціалу порушника, необхідного для реалізації цієї загрози безпеці інформації в інформаційній системі об'єкта критичної інфраструктури із заданими структурно функціональними характеристиками і особливостями функціонування. Можливість реалізації *n*-ої загрози можливо описати наступним чином:

$$W(H_n) = f(X_n; Y_n),$$

де X_n – рівень захищеності інформаційної системи об'єкту критичної інфраструктури щодо реалізації *n*-ої загрози;

Y_n – потенціал порушника, необхідний для реалізації *n*-ої загрози, тобто модель загроз.

Для оцінювання можливих наслідків H_n від реалізації *n*-ої загрози безпеці інформації визначаються можливий результат реалізації загрози кібербезпеці в інформаційній системі об'єкта критичної інфраструктури, вид збитку, до якого може призвести реалізація загрози кібербезпеці інформаційній системі, ступінь наслідків від реалізації загрози безпеці інформації для кожного виду збитку.

Можливі наслідки H_n від реалізації *n*-ої загрози кібербезпеці інформаційній системі визначаються наслідками від порушення конфіденційності, цілісності або доступності кожного виду інформації, що циркулює в інформаційній системі об'єкта критичної інфраструктури і визначається експертним методом.

Схематичне відображення методу визначення актуальності загрози кібербезпеки інформаційної системи об’єкту критичної інфраструктури, представлена у загальному вигляді на рис. 2.

За результатами проведеного оцінювання приймаються рішення щодо вжиття відповідних заходів, спрямованих на ефективне та своєчасне блокування (нейтралізацію) загроз безпеки інформації, в результаті реалізації яких можливі неприйнятні негативні наслідки.

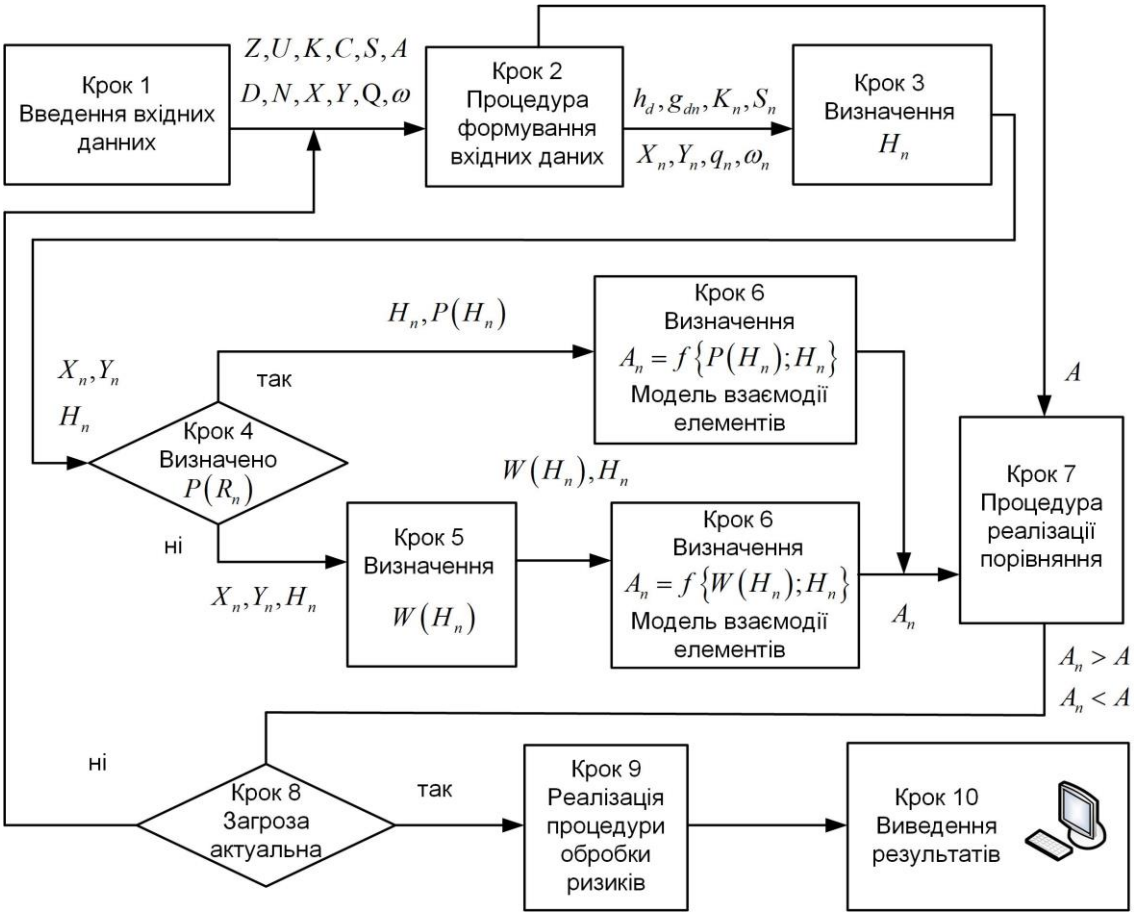


Рисунок 2 – Схематичне відображення методу визначення актуальності загрози

Збитки, завдані *n*-ою загрозою можуть визначатися в абсолютних одиницях: економічних втратах, часових втратах, об’ємі втраченої або пошкодженої інформації і т. п. Однак, з практичної точки зору це зробити досить складно, особливо на ранніх етапах проектування системи захисту інформації. Тому замість абсолютного збитку використовують відносний збиток, який по суті і буде являти собою ступінь небезпеки n-ї загрози для інформаційної системи – коефіцієнт небезпеки n-ї загрози B_n. Тобто, коефіцієнт небезпеки загрози буде являти собою відношення величини збитку, який виникає від деструктивних дій в результаті реалізації цієї загрози, до його максимального (неприйнятного) значення. Таким чином, коефіцієнт небезпеки загрози є відносною величиною і, тому, не залежить від виду збитку. Коефіцієнт небезпеки може бути визначений експертним шляхом.

Взаємозв'язок між загрозами і деструктивними діями, які виникають в результаті реалізації цих загроз можливо представити у вигляді матриці:

$$G = \left[g_{dn} \right], \tag{1}$$

де d змінюється від 1 до D; D – кількість можливих деструктивних дій; n змінюється від 1 до N; N – кількість загроз.

Елементи g_{dn} матриці (1) набувають значення 1, якщо n–та загроза призводить до реалізації d–ї деструктивної дії, і набувають значення 0 – в протилежному випадку.

Нехай B_d – коефіцієнт небезпеки виконання d–ї деструктивної дії, де d змінюється від 1 до D; D – кількість можливих деструктивних дій.

Тоді, враховуючи, що у випадку реалізації n-ї загрози може мати місце декілька деструктивних дій, коефіцієнт небезпеки n-ї загрози буде визначатися наступним чином:

$$B_n = \sum_{d=1}^{D} B_d \cdot g_{dn} ,$$

де B_d – коефіцієнт небезпеки виконання d–ї деструктивної дії, визначається за рівнем тяжкості наслідків даного виконання, як показник критичності об’єкту енергетичного сектору;

g_{dn} – коефіцієнт, який визначається, як елемент матриці (1).

У третьому розділі розроблено методи розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Розглянемо геометричний метод розрахунку суми ризиків. Ризик R, як зважене значення наслідків, може визначатися за формулою:

$$R\left(p,h \right) = p \cdot h . \tag{2}$$

де p – ймовірність випадкової події, що призводить до певних наслідків h.

Наслідки можуть бути як додатними так і від’ємними. Під додатними наслідками будемо розуміти збитки, під від’ємними – прибуток.

З урахуванням того, що ризик – це невизначена подія, яка у разі виникнення має негативний або позитивний вплив та призводить до втрат або прибутку в грошовому вираженні, то у випадку ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури під від’ємним наслідком будемо розуміти подію або умову, яка передбачає функціонування інформаційної системи об’єкта критичної інфраструктури у штатному режимі, не призводить до порушення пов’язаних з цим бізнес процесів, що дає змогу отримувати запланований підприємством прибуток.

На підставі виразу (2) залежність наслідків *h* в результаті настання деякої події від її ймовірності *p* можна представити у вигляді функції:

$$h = f\left(R, p\right). \tag{3}$$

Графік функції (3) приведений на рис. 3.

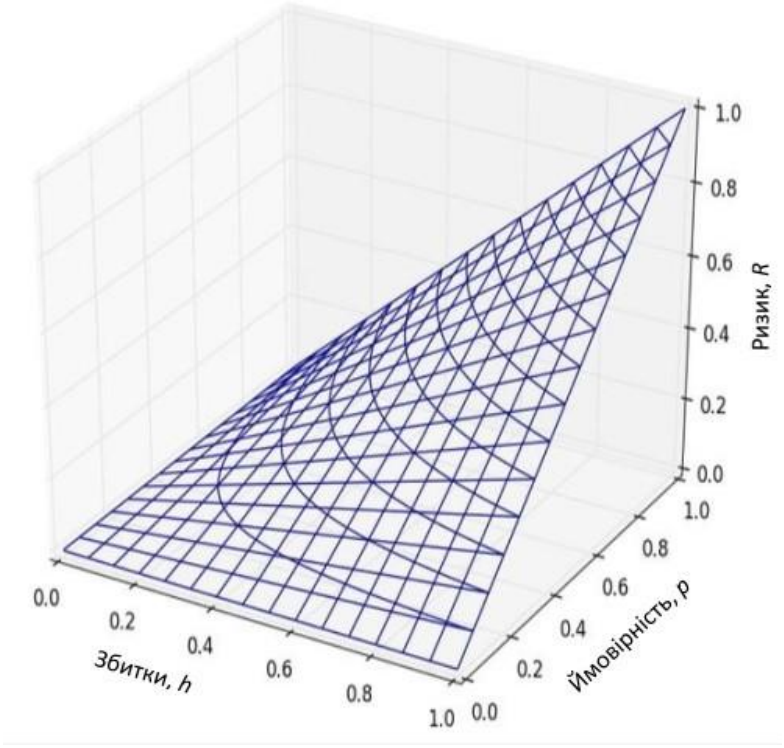


Рисунок 3 – Графік залежності наслідків від їх ймовірностей та величини ризику

Графік проекції функції ризику на площину *ph*, рис. 3, можна представити у вигляді виразу

$$h\left(p\right) = \frac{R_\alpha}{p},$$

де R_α – значення ризику, на рівні якого здійснюється переріз графіку функції (3);
$p \neq 0$.

Розглянемо графічний метод розрахунку суми ризиків.

Нехай існує *J* ризиків:

$$R_1 = p_1 \cdot h_1, \ \ldots, \ R_j = p_j \cdot h_j, \ \ldots, \ R_J = p_J \cdot h_J. \tag{4}$$

де кожний ризик R_j представлений графіком функції (3) і визначається ймовірністю p_j випадкової події, що може призвести до певних наслідків h_j (точки 1, 2, 3), рис.4.

Визначимо значення наслідків повного знищення інформаційного активу $h_{1m},...,h_{jm},...,h_{Jm}$ для кожного ризику відповідно.

Значення наслідків повного знищення інформаційного активу можуть бути визначені, як приклад, з використанням методу експертних оцінок.

Ймовірності подій, що призводять до наслідків повного знищення інформаційного активу в умовах дії кожного ризику визначається з графіку, як координати точок перетину (точки 4, 5, 6) графіків ризиків з лініями рівнів відповідних наслідків повного знищення інформаційного активу, тобто $p_{1m},...,p_{jm},...,p_{Jm}$, рис. 4.

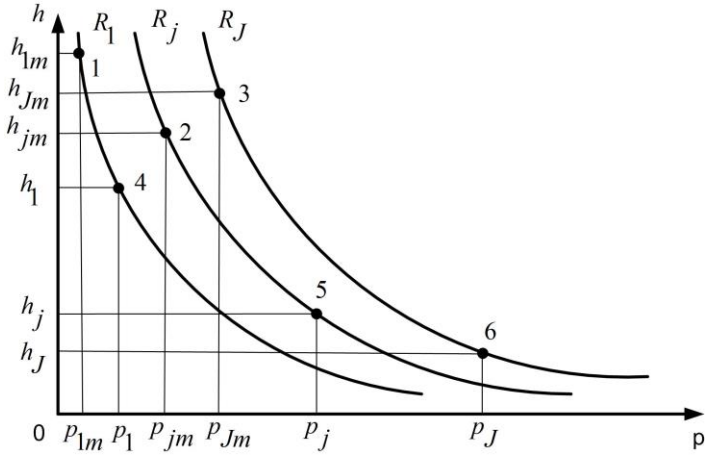


Рисунок 4 – Графік проекції функції ризику на площину *ph*

У випадку дії *J* ризиків (4) значення суми наслідків не буде перевищувати суми наслідків повного знищення інформаційного активу для кожного із *J* ризиків, без урахування синергетичного ефекту. Це означає, що значення суми наслідків повного знищення інформаційного активу буде дорівнювати сумі наслідків повного знищення інформаційного активу для кожного із *J* ризиків:

$$h_m = h_{1m} + ... + h_{Jm} = \sum_{j=1}^{J} h_{jm} . \qquad (5)$$

Наявність одного або декількох ризиків не виключає інших ризиків у той же період часу. З огляду на це, можемо констатувати, що події, які призводять до ризиків являються сумісними подіями. На підставі цього, ймовірність події, що призводить до дії *j* ризиків з наслідками повного знищення інформаційного активу для кожного ризику, визначається, як сума ймовірностей цих подій без ймовірності їх добутку:

$$p_m = \sum_{j=1}^{J} p_{jm} - \sum_{j<l}^{J} p_{jm} \cdot p_{lm} + \sum_{j<l<k}^{J} p_{jm} \cdot p_{lm} \cdot p_{km} + \ldots + (-1)^{J-1} \cdot \prod_{j=1}^{J} p_{jm} . \quad (6)$$

Сума *J* ризиків на підставі виразів (5) і (6) буде визначатися виразом:

$$R_S(h_m, p_m) = h_m \cdot p_m . \quad (7)$$

Використовуючи вираз (7), задаючи значення p від 0 до 1, будуємо графік функції, рис. 5:

$$h(p) = \frac{R_S}{p} , \quad (8)$$

де $p \neq 0$.

Ймовірність p_S дії суми *J* ризиків визначається на підставі виразу (6).

Величину наслідків h_S у випадку дії суми ризиків знаходимо, як ординату точки 2, рис. 5.

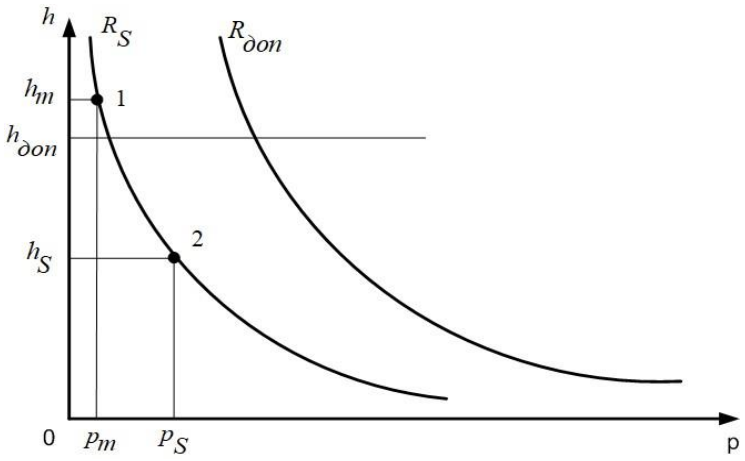


Рисунок 5 – Графік проекції функції суми ризиків на площину *ph*

Метою оцінювання ризику є сприяння прийняттю рішень. Оцінювання ризику включає порівняння результатів аналізу ризику до встановлених критеріїв ризику для визначення необхідності додаткових дій, варіантів обробки ризику.

Якщо у якості критерію для визначення варіантів обробки ризику вибрано рівень ризику $R_{доп}$, то порівнюються ризики R_S і $R_{доп}$. У випадку застосування у якості критерію величини наслідків $h_{доп}$ – використовуються значення наслідків h_S і $h_{доп}$.

Перевагою даного методу визначення суми ризиків є наочність і простота розрахунків.

Розглянемо аналітичний метод розрахунку суми ризиків. Ризик *R* визначається як ймовірність *p* випадкової події, що призводить до певних наслідків *h*, і може описуватися виразом (2).

Нехай існує *J* ризиків (4), де кожний ризик R_J визначається ймовірністю p_j настання випадкової події, що може призвести до певних наслідків h_j.

Визначимо значення наслідків повного знищення інформаційного активу для кожного ризику:

$$h_m = \{h_{1m}, ..., h_{Jm}\}.$$

Як було показано вище, події, які призводять до ризиків являються сумісними подіями.

Значення суми наслідків повного знищення інформаційного активу у випадку дії *J* ризиків буде визначатися з виразу (5).

Ймовірність p_{jm} кожної j–тої події, що призводить до відповідних наслідків повного знищення інформаційного активу h_{jm} в умовах дії ризиків R_j, визначається з виразу:

$$p_{jm}\left(R_j, h_{jm}\right) = \frac{R_j}{h_{jm}},$$

де $h_{jm} \neq 0$.

Ймовірність події, що призводить до дії ризиків з наслідками повного знищення інформаційного активу для кожного ризику, визначається з виразу (6). При цьому враховуємо, що події сумісні.

Сума дії *J* ризиків, на підставі виразів (5) і (6), буде визначатися виразом (7). Ймовірність p_S суми дії *J* ризиків визначається з виразу (8).

Таким чином, величина наслідків h_S у випадку дії суми ризику буде визначатися з виразу:

$$h_S\left(R_S, p_S\right) = \frac{R_S}{p_S}. \qquad (9)$$

де $p_S \neq 0$.

Якщо у якості критерію для визначення варіантів обробки ризику вибрано рівень ризику, то використовуються значення, отримані з виразу (7). У випадку застосування у якості критерію величини наслідків – використовуються значення, отримані з виразу (9).

Перевагою даного методу визначення суми ризиків є можливість автоматизації розрахунків.

Обмеженнями при використанні обох методів є умови:

$$R \neq 0, \quad h \neq 0, \quad p \neq 0.$$

У випадку, якщо ж $h = 0$ та/або $p = 0$, і, відповідно, $R = 0$, при використанні запропонованих методів такий ризик не враховується у розрахунках.

У четвертому розділі розроблено векторну модель, модель комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури та метод визначення комплексного ризику.

Прийняття рішень у сфері управління ризиками в значній мірі залежить від людського чиннику, який має суб'єктивний характер. Тому, коректне кількісне оцінювання повного ризику можливе шляхом визначення комплексного ризику. Під комплексним ризиком будемо розуміти ризик, який включає в себе складові об'єктивного та суб'єктивного ризиків.

Ризики характеризуються конкретним значенням. У той же час, ризики, як об'єктивні, так і суб'єктивні, характеризуються напрямком та значенням і їх можна подати у вигляді векторів, наприклад R_1 і R_2.

Для визначення результуючого комплексного ризику необхідно додати об'єктивний і суб'єктивний ризики. Але алгебраїчно додавати ці два ризики не можливо через те, що вони відмінні по своєму характеру.

При вирішенні такої задачі виникає необхідність отримувати числові характеристики векторів (довжини) та їх взаємного розміщення (кут між векторами).

Перевірка виконання аксіом лінійного (векторного) простору для представлення ризиків векторами, використовуючи метод розрахунку суми ризиків, а також аксіом евклідового простору для представлення векторів ризиків, у якості елементів двомірного простору R^2 дозволяють стверджувати, що довжина вектору ризику може визначатися, як корінь квадратний його скалярного квадрату:

$$\left|\overline{R_1}\right| = \sqrt{x_1^2 + y_1^2},$$

де x_1, y_1 – координати вектору ризику $\overline{R_1}$,

тобто, довжина вектору ризику дорівнює кореню квадратному із суми квадратів його проекцій на координатні осі, а косинус кута між векторами ризиків $\overline{R_1}$ і $\overline{R_2}$ у загальному випадку визначається:

$$\cos\{\varphi\} = \frac{\left(\overline{R}_1, \overline{R}_2\right)}{\left|\overline{R}_1\right| \cdot \left|\overline{R}_2\right|},$$

де $\left|\overline{R}_1\right|$ – абсолютне значення ризику R_1; $\left|\overline{R}_2\right|$ – абсолютне значення ризику R_2;

$\left|\overline{R_1}\right| \neq 0$, $\left|\overline{R_2}\right| \neq 0$.

Оскільки евклідовий простір являється лінійним, то на нього переносяться всі поняття, визначені для лінійного простору, наприклад, вводиться поняття базису і розмірності. Також для нього справедливі наслідки з аксіом евклідового простору.

З урахуванням викладеного, векторна модель ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури приведена на рис. 6.

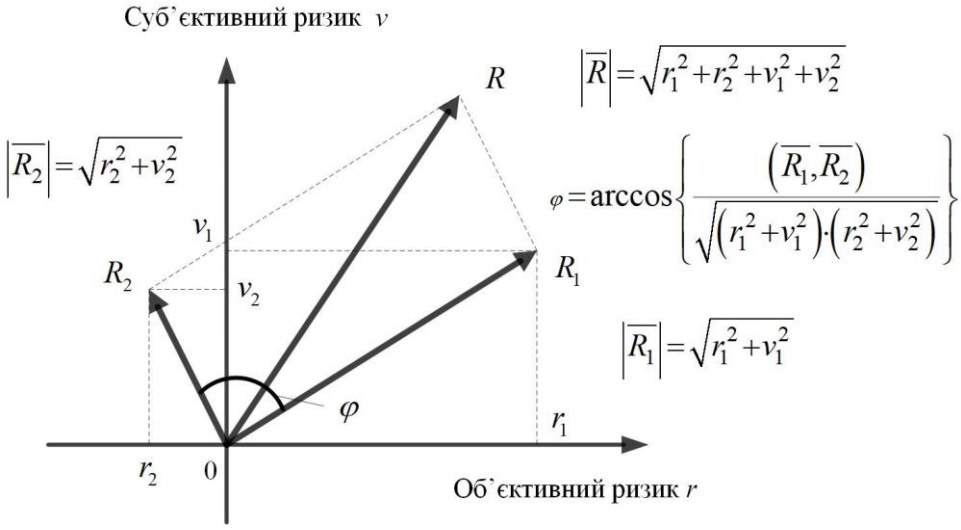


Рисунок 6 – Векторна модель ризику

Використовуючи векторну модель ризиків, розглянемо модель комплексного ризику, (рис. 7), та змістовну інтерпретацію комплексного ризику в залежності від φ, (рис.8).

У випадку $0<\varphi<\frac{\pi}{2}$ вектор повного ризику знаходиться в I четверті. При цьому, об'єктивний ризик $r>0$, суб'єктивний ризик $v>0$, аргумент комплексного ризику $\varphi=arctg\frac{|v|}{|r|}>0$, де $|r|\neq 0$. На практиці такий випадок має наступну інтерпретацію: існує об'єктивний ризик (ймовірність матеріальних збитків), величина якого визначається значенням *r*; існує суб'єктивний ризик) величиною *v*.

У випадку $\frac{\pi}{2}<\varphi<\pi$ вектор повного ризику знаходиться в II четверті. При цьому, об'єктивний ризик $r<0$, суб'єктивний ризик $v>0$, аргумент комплексного ризику $\varphi=arctg\frac{|v|}{-|r|}<0$, де $|r|\neq 0$. На практиці такий випадок має наступну інтерпретацію: існує реальна ймовірність отримання прибутку, величина якого визначається значенням $|r|$; існує суб'єктивний ризик (ймовірність моральних збитків) величиною *v*.

У випадку $\frac{\pi}{2}<\varphi<\frac{3\pi}{2}$ вектор повного ризику знаходиться в III четверті. При цьому, об'єктивний ризик $r<0$, суб'єктивний ризик $v<0$, аргумент комплексного ризику

$\varphi = arctg\dfrac{-|v|}{-|r|} > 0$, де $|r| \neq 0$. На практиці такий випадок має наступну інтерпретацію: існує реальна ймовірність отримання прибутку, величина якого визначається значенням $|r|$; існує суб'єктивна ймовірність отримання прибутку величиною v.

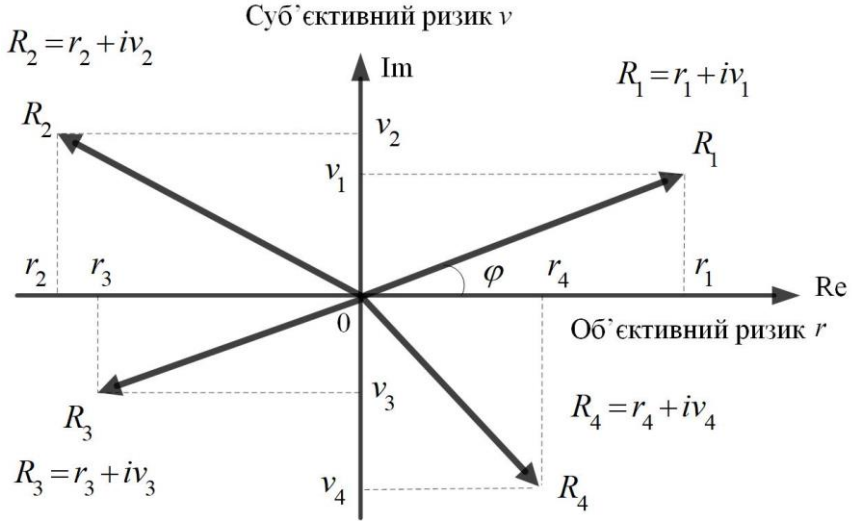


Рисунок 7 – Модель комплексного ризику

У випадку $\dfrac{3\pi}{2} < \varphi < 2\pi$ вектор повного ризику знаходиться в IV четверті. При цьому, об'єктивний ризик $r > 0$, суб'єктивний ризик $v < 0$, аргумент комплексного ризику $\varphi = arctg\dfrac{-|v|}{|r|} < 0$, де $|r| \neq 0$. На практиці такий випадок має наступну інтерпретацію: існує реальний ризик (ймовірність збитків), величина якого визначається значенням r; існує суб'єктивна ймовірність отримання прибутку величиною v.

Якщо $v = -r$, то сприйняття ризику протилежне до реального ризику. При цьому $\varphi = 3\pi/4$ і $\varphi = 7\pi/4$. В цьому випадку суб'єкт не просто недооцінює реальний ризик, який відображає ймовірність втрати своїх активів, а навпаки, помилково припускає певну ймовірність отримання прибутку.

Що стосується практичної інтерпретації, то тут можна розглядати два варіанти:

– суб'єкт не поінформований про реальний стан справ і не усвідомлює реального ризику;

– суб'єкт піддається інформаційному впливу з метою психологічної дестабілізації та/або спонукання до прийняття неадекватного управлінського рішення.

При $\varphi = 0$ і $\varphi = \pi$ уявний ризик досягає нульового значення або максимальної невизначеності при певному значенні реального ризику. Тобто, незалежно від реального ризику, суб'єкт або не отримує ніякої інформації про реальний ризик, або

ця інформація суб'єктом не сприймається зовсім. Даний випадок демонструє приховування інформації про реальний ризик або її ігнорування суб'єктом.

Таким чином, при $v = r$ суб'єкт адекватно сприймає реальний ризик, при $v < r$ суб'єкт недооцінює реальний ризик, а при $v > r$ – переоцінює його.

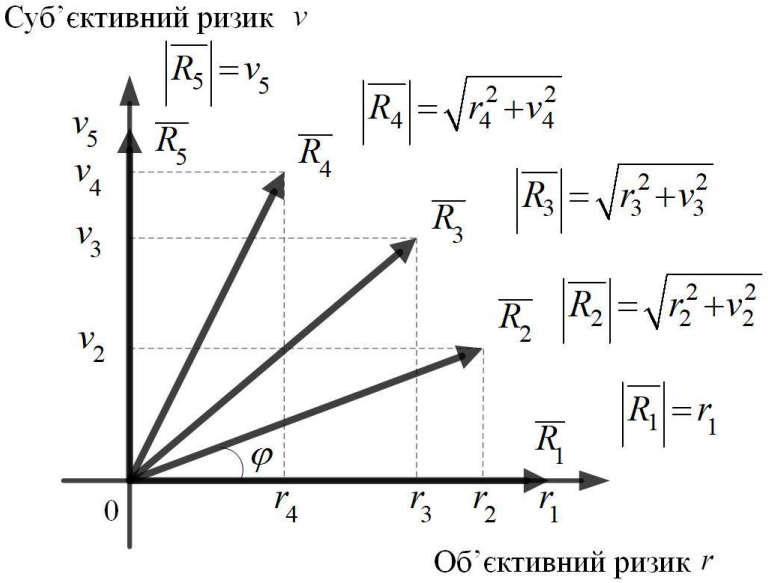


Рисунок 8 – Інтерпретація комплексного ризику

Аналіз векторної моделі ризику, рис. 6, та моделі комплексного ризику, рис. 7, дозволяє здійснити інтерпретацію комплексного ризику, у залежності від кута нахилу вектору ризику до осі абсцис, рис. 8. У випадку відсутності суб'єктивної складової комплексного ризику, тобто $v_1 = 0$, величина комплексного ризику дорівнює величині об'єктивного ризику, тобто $|\overline{R_1}| = r_1$. Якщо існує об'єктивний ризик, наприклад r_2 і суб'єктивний ризик v_2, то наявність суб'єктивного ризику буде збільшувати величину комплексного ризику $|\overline{R_2}|$. Із збільшенням величини суб'єктивного ризику, збільшується абсолютне значення комплексного ризику, на рис. 8 $|\overline{R_3}|$ та $|\overline{R_4}|$. У випадку відсутності об'єктивної складової комплексного ризику, тобто $r_5 = 0$, величина комплексного ризику дорівнює величині суб'єктивного ризику, тобто $|\overline{R_5}| = v_5$.

Розглянемо метод розрахунку комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням теорії векторної алгебри. Використовуючи векторну модель ризиків та модель комплексного ризику комплексний ризик можна представити у вигляді комплексного числа:

$$R = r + i\,v, \tag{25}$$

де $r = p_{об} \cdot h_{об}$ – об’єктивний ризик;

$v = p_{суб} \cdot h_{суб}$ – суб’єктивний ризик;

$i = \sqrt{-1}$.

У виразі (25) об’єктивний ризик r визначається, як добуток об’єктивної ймовірності $p_{об}$ події, що призводить до ризику, і величини реальних наслідків від настання такої події $h_{об}$. Суб’єктивний ризик v у виразі (25) визначається, як добуток суб’єктивної ймовірності $p_{суб}$ події, що призводить до ризику, і величини суб’єктивних наслідків від настання такої події $h_{суб}$. Під суб'єктивною ймовірністю події розуміємо припущення щодо її настання, що базується на особистому досвіді. Під об'єктивною ймовірністю події розуміємо припущення щодо її настання, що базується на частоті, з якою подібний результат був отриманий в аналогічних умовах. Технічно суб'єктивну і об’єктивну ймовірності можна визначити за допомогою спеціально організованих експертних процедур.

При цьому, модуль комплексного ризику $|R|$ визначає дійсну його характеристику: $|R_S| = \sqrt{r^2 + v^2}$, а аргумент комплексного ризику: $\varphi_S = arctg\frac{v}{r}$, де $r \neq 0$, являється показником превалювання однієї складової ризику над іншою.

Враховуючи, що:

$$r = |R| \cdot \cos\varphi_S \,;\; v = |R| \cdot \sin\varphi_S \,, \tag{26}$$

комплексний ризик можна представити в тригонометричній і в показниковій формах відповідно:

$$R = |R| \cdot \left(\cos\varphi_S + i \cdot \sin\varphi_S\right);\; R = |R| \cdot e^{i\cdot\varphi_S}.$$

Вираз (26) можна записати у вигляді:

$$\cos\varphi_S = \frac{r}{|R|}, \tag{27}$$

де $|R| \neq 0$.

У виразі (27) $\cos\varphi_S$ показує, яку частину повного ризику складає об’єктивний ризик.

Схематичне відображення методу обчислення комплексного ризику зображено на рис. 9.

У п’ятому розділі запропонована методологія оцінювання суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури та розроблені структурні рішення обчислювальних систем.

Узагальнена методологія, розроблена в даному розділі, базується на методі експертних оцінок і розроблених у даній дисертаційній роботі методах та включає

наступні основні етапи:

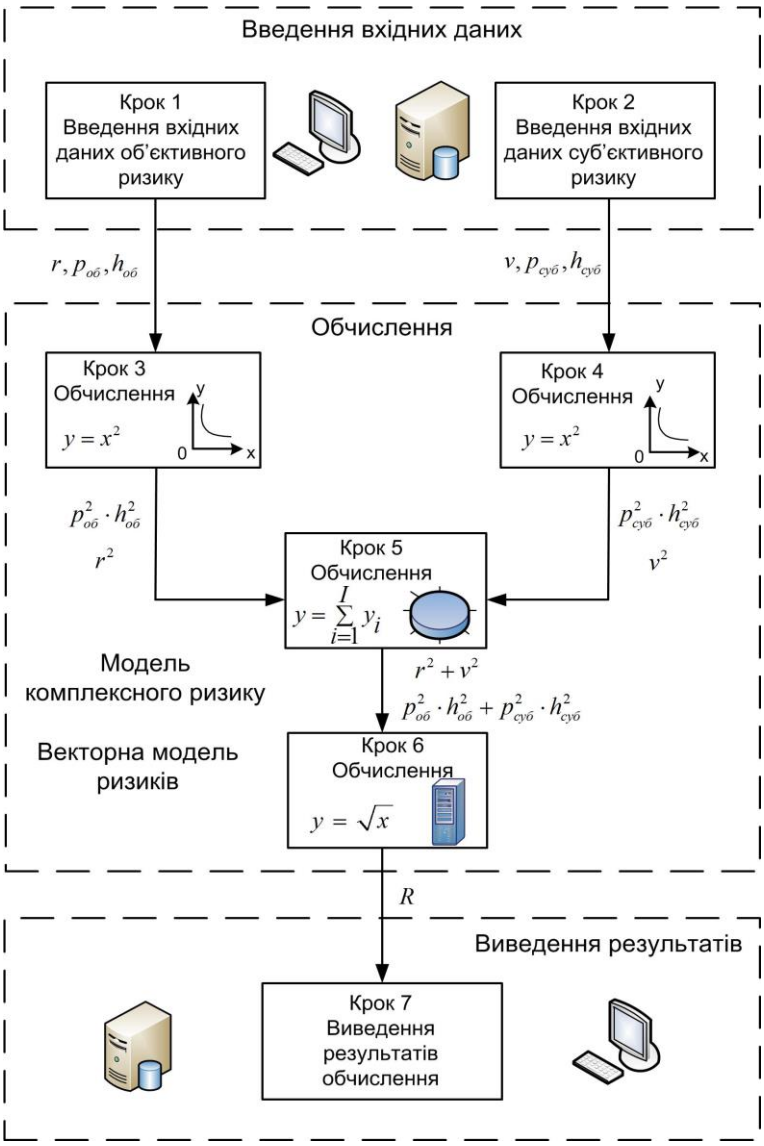


Рисунок 9 – Схематичне відображення методу обчислення комплексного ризику

– Етап 1. Підготовка та введення вхідних даних.

Визначаються параметри, які являються базовими, для обчислення суми ризиків, використовуючи запропоновані у дисертаційній роботі методи. Визначення базових параметрів може бути здійснено існуючим методом експертних оцінок.

Введення вхідних даних здійснюється в модуль пам'яті і далі в модулі обчислення. В модулі пам'яті формується база даних вхідних даних та результатів обчислень.

– Етап 2. Обчислення суми ризиків об'єктивної складової.

Обчислення суми ризиків об'єктивної складової здійснюється методом визначення наслідків повного знищення інформаційного активу:

$$R_{S_{об}} = h_{m_{об}} \cdot p_{m_{об}} \cdot$$

– Етап 3. Обчислення суми ризиків суб’єктивної складової.

Обчислення суми ризиків суб’єктивної складової здійснюється методом визначення наслідків повного знищення інформаційного активу:

$$R_{S_{суб}} = h_{m_{суб}} \cdot p_{m_{суб}} .$$

– Етап 4. Визначення суми ризиків об’єктивної і суб’єктивної складових.

Визначення суми ризиків об’єктивної і суб’єктивної складових здійснюється з використанням методу обчислення комплексного ризику:

$$R_S = \sqrt{\left(R_{S_{об}}\right)^2 + \left(R_{S_{суб}}\right)^2} .$$

– Етап 5. Візуалізація результатів обчислень.

Результати обчислень виводяться на пристрій відображення інформації і в модуль пам’яті.

Структурно-аналітичне відображення розробленої методології представлено на рис. 10.

На основі запропонованої методології можна побудувати системи, як програмні так і апаратно-програмні, з використанням розроблених методів, спрямованих на оцінювання суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

На підставі даної методології вперше розроблено комплекс структурних моделей (рішень) обчислювальних систем оцінювання ризику кібербезпеки інформаційних систем, що реалізують запропоновані у даній дисертаційній роботі методи, рис. 11, рис. 12.

Структурна модель (рішення) обчислювальної системи «Калькулятор ризиків», рис.11(а), яка, за рахунок використання модулів введення, обчислення і аналізу даних, блоків розрахунку, визначення та формування даних, що реалізують запропоновані методи розрахунку суми ризиків, дозволяє здійснювати автоматизований розрахунок наслідків від дії сумісних подій, з урахуванням показників, таких як ймовірність подій, що призводять до наслідків, та величина цих наслідків.

До складу обчислювальної системи, рис. 11(а), входять: модуль введення початкових даних 1, блок пам’яті 2, модуль обчислення і аналізу даних 3, модуль виведення та візуалізації інформації 11, модуль обчислення і аналізу даних 3 містить блоки формування масиву ризиків подій 4, блок розрахунку значення збитків повного знищення інформаційного активу у результаті суми ризиків 5, блок формування масиву ймовірностей подій, що призводять до повного знищення інформаційного активу в умовах дії кожного ризику 6, блок визначення ймовірності суми ризиків сумісних випадкових подій 7, блок визначення ймовірності події, що призводить до суми ризиків з наслідками повного знищення інформаційного активу

для кожної події 8, блок розрахунку суми ризиків в умовах дії ризиків 9, блок розрахунку збитків при дії суми ризиків 10.

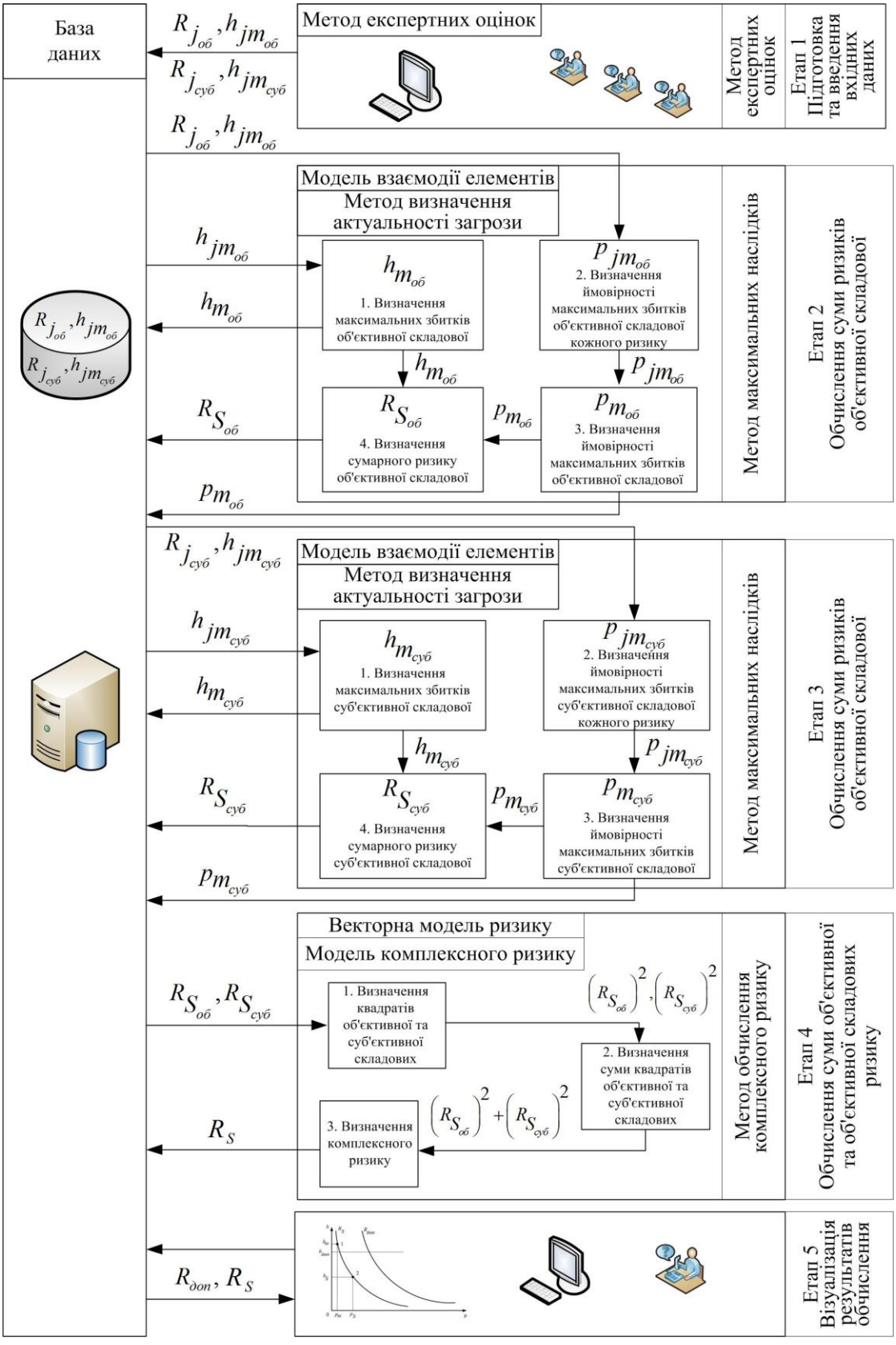
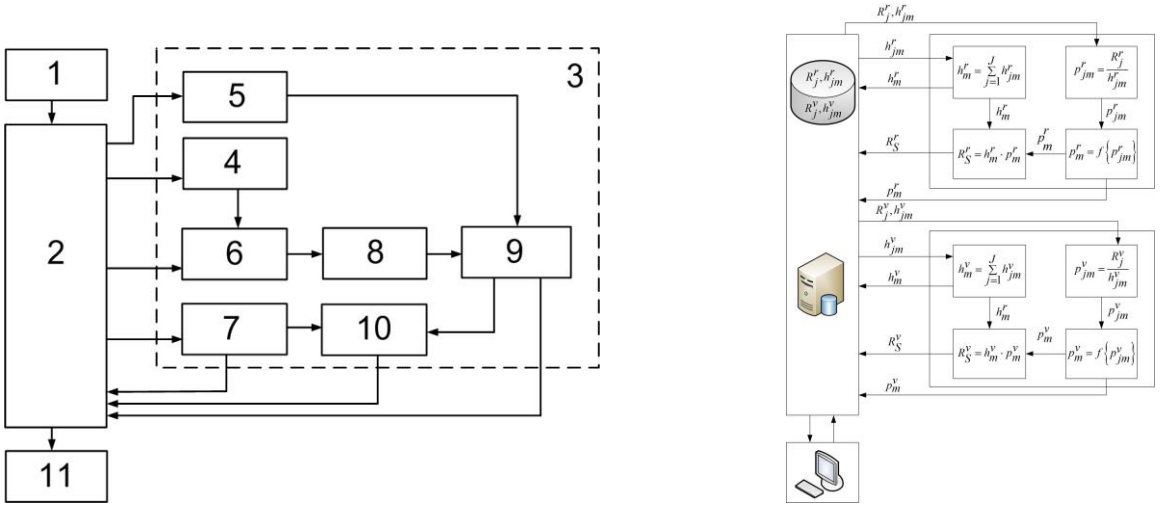


Рисунок 10 – Структурно-аналітичне відображення розробленої методології оцінювання ризиків

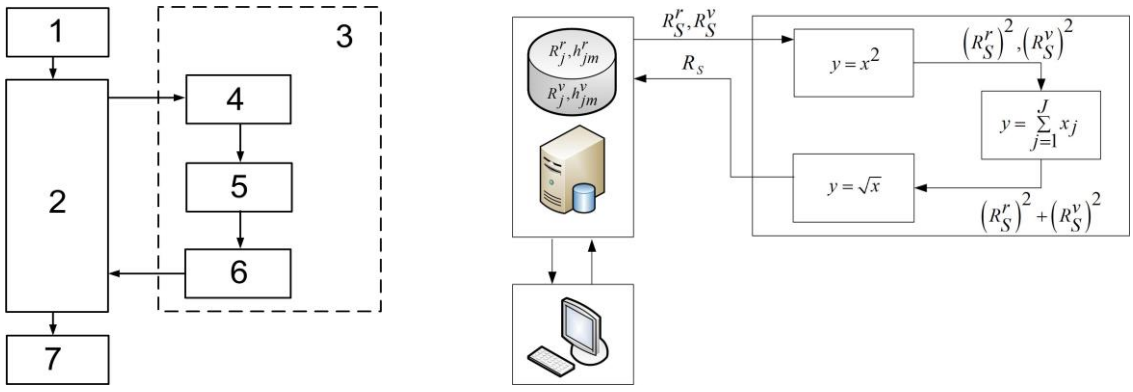


а) б)

Рисунок 11 – Структурна модель (рішення) (а) та структурно-аналітичне відображення (б) обчислювальної системи «Калькулятор ризиків»

Структурна модель (рішення) обчислювальної системи «Калькулятор комплексного ризику», рис. 12(а), яка, за рахунок використання модулів введення, обчислення і аналізу даних, блоків розрахунку, визначення та формування даних, що реалізують запропонований метод розрахунку суми ризиків, дозволяє здійснювати автоматизований розрахунок повного ризику, з урахуванням об'єктивної та суб'єктивної його складових, з використанням теорії векторної алгебри та комплексних чисел.

До складу обчислювальної системи, рис. 12(а), входять: модуль введення початкових даних 1, блок пам'яті 2, модуль обчислення і аналізу даних 3, модуль виведення та візуалізації інформації 7, модуль обчислення і аналізу даних 3 містить блок розрахунку квадрату вхідних даних 4, блок суматора вхідних даних 5, блок розрахунку квадратного кореня 6.



а) б)

Рисунок 12 – Структурна модель (рішення) (а) та структурно-аналітичне відображення (б) обчислювальної системи «Калькулятор комплексного ризику»

Запропоновані обчислювальні системи можуть бути використані як частина системи підтримки прийняття рішень.

У шостому розділі приведені експериментальні дослідження програмного застосунку систем оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури на основі комп'ютерної реалізації розроблених методів.

На базі запропонованої методології та структурних рішень обчислювальних систем розроблено програмний застосунок запропонованих методів. Експериментальні дослідження розробленого програмного застосунку здійснювалися з метою перевірки адекватності реагування розроблених моделей та методів відносно тих чи інших ініціалізуючих величин.

Використовуючи запропоноване програмне рішення при побудові комплексної системи захисту інформації атомних електростанцій, виконано обчислення ризиків від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, табл. 2. Ймовірність реалізації загроз задається в межах від 0 до 1, а величина збитків визначається у відносних одиницях за 10-ти бальною шкалою в межах від 0 до 10, де 10 відповідає повному знищенню інформаційного активу. Зазначені параметри визначаються методом експертних оцінок.

Таблиця 2

Значення ризиків від загроз прикладного програмного забезпечення

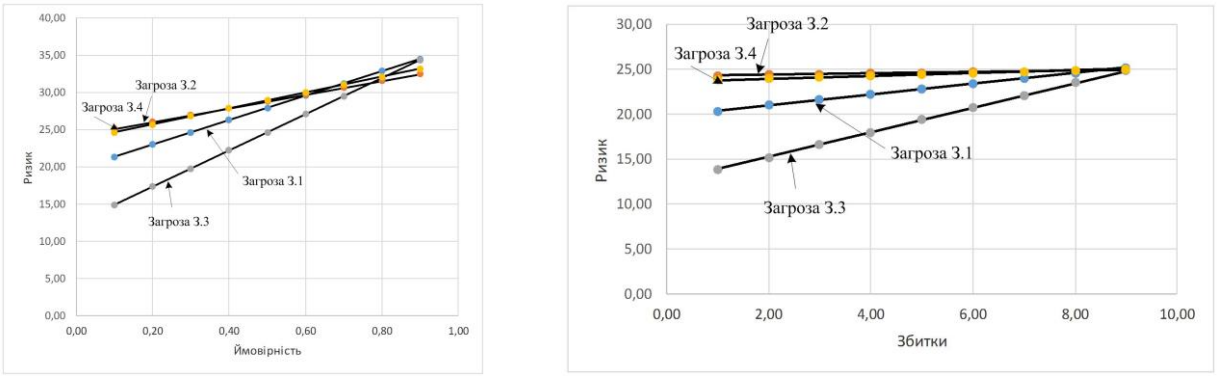
Іденти-фікатор загрози	Назва загрози	Ймовірність реалізації загрози	Величина збитків	Значення ризику
1	2	3	5	7
З.1	Помилка, збій та відмова прикладного ПЗ	0,3	8,09	2,43
З.2	Виконання недокументованих функцій	0,05	5,83	0,29
З.3	Розповсюдження вірусів	0,5	8,86	4,43
З.4	Несумісність версій ПЗ	0,1	6,5	0,65
	Результати обчислення	0,7	35,23	24,67

В графі «результати обчислення», табл. 2, приведено розраховані значення ризиків від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням інформаційних та керуючих систем атомних електростанцій. Також приведено розраховані значення наслідків при реалізації даних загроз і ймовірність цих наслідків.

За результатами експерименту, рис. 12 (а, б), видно, що система оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури «Калькулятор ризиків» адекватно реагує на зміну ініціалізуючих параметрів.

З використанням методології та методів, розроблених у даній дисертаційній роботі, проводилися роботи по створенню КСЗІ в інформаційній системі державного підприємства «Державний науково-технічний центр ядерної та радіаційної безпеки», здійсненні державних експертиз КСЗІ в автоматизованій інформаційній системі «Централізована база даних перенесених номерів» державного підприємства

«Український державний центр радіочастот» та захищеного вузла Інтернет доступу «Фарлеп-Інвест».



а) б)

Рисунок 12 – Залежності ризику від ймовірності (а) та збитків (б)

Отримані результати підтверджують функціонування системи оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури «Калькулятор ризиків» та її успішне практичне застосування.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну проблему, пов’язану з розробкою методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури, орієнтованої на створення відповідних методів та засобів розрахунку суми ризиків, на основі отриманих результатів, що полягають у розроблених теоретичних методах, моделях та засобах забезпечення кібербезпеки інформаційних систем, у тому числі об’єктів критичної інфраструктури.

При вирішенні цієї задачі отримані такі основні результати:

1. Проаналізовано сучасні методи оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об’єктів критичної інфраструктури, а також програмні продукти управлінням такими ризиками. Встановлено, що дослідженню проблем, пов’язаних із процесом оцінювання ризику кібербезпеки інформаційних систем, що являється об’єктом дисертаційного дослідження присвячується значна частина публікацій вітчизняних і зарубіжних вчених. Однак, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

2. Удосконалено структурну модель взаємодії елементів інформаційних систем об’єктів критичної інфраструктури, яка використовується при обчисленні суми ризиків об’єктивної та суб’єктивної складових на другому на третьому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Зазначена модель дозволяє розробити модель порушника даної інформаційної системи з урахуванням кіберзагроз, об’єктами яких є адміністратор, користувачі, технічний персонал.

3. Удосконалено метод визначення актуальності загрози кібербезпеки інформаційної системи об’єкту критичної інфраструктури, який використовується при обчисленні суми ризиків об’єктивної та суб’єктивної складових на другому на третьому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Зазначений метод дозволяє розробити модель загроз даної інформаційної системи з урахуванням кіберзагроз, об’єктами яких є адміністратор, користувачі, технічний персонал.

4. Розроблено методи для обчислення сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури, які використовуються при обчисленні суми ризиків об’єктивної та суб’єктивної складових на другому на третьому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Зазначені методи дозволяють розраховувати суму визначеної множини ризиків, загальні наслідки та ймовірність їх реалізації.

5. Розроблено векторну модель та модель комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури, які використовуються в методі обчислення комплексного ризику на четвертому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Зазначені моделі дозволяють здійснювати векторні операції над векторами ризиків.

6. Розроблено метод обчислення комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури, який використовується при обчисленні суми ризиків об’єктивної та суб’єктивної складових на четвертому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Зазначений метод дозволяє здійснювати оцінювання зазначених ризиків з урахуванням величини впливу людського чиннику.

7. Розроблено методологію оцінювання ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури, яка використовується при побудові апаратно-програмного комплексу оцінки та аналізу ризику. Зазначена методологія дозволяє забезпечити підтримку створення обчислювальних систем для автоматизації процесу оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

8. Запропоновано структурні моделі обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури, які використовуються при побудові апаратно-програмних комплексів розрахунку сумарного ризику та комплексного ризику. Зазначені моделі дозволяють автоматизувати процес розрахунку сумарного ризику та обчислення комплексного ризику з урахуванням величин об’єктивної та суб’єктивної складових.

9. Розроблено алгоритмічне забезпечення та програмний застосунок обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням розроблених методів. Зазначений програмний застосунок використано при побудові комплексних систем захисту інформації інформаційних систем об’єктів критичної інфраструктури.

10. Експериментальні дослідження програмного застосунку обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури, а також впровадження та успішне практичне використання зазначених розробок підтвердили достовірність теоретичних гіпотез та практичних розробок і висновків дисертаційної роботи.

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв’язку та захисту інформації України (відгук від 20.03.2019р. № 05/02-295), Національної академії Служби безпеки України (акт від 18.09.2019р.), Державного науково-дослідного інституту спеціального зв’язку та захисту інформації (акти від 08.10.2015р. та від 26.11.2015р.), Державного підприємства «Державний науково-технічний центр з ядерної та радіаційної безпеки» (акт від 06.06.2019р.), Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (акт від 11.07.2019р.), ПрАТ «Фарлеп-Інвест» (відгук від 09.07.2018р. №65/04-10), Державного підприємства «Український державний центр радіочастот» (відгук від 10.10.2019р. № 80/14.2-55/847/13063), а також використовуються у навчальному процесі Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України при підготовці фахівців у сфері вищої освіти за третім (освітньо-науковим) рівнем зі спеціальності 122 – «комп’ютерні науки» (акт від 11.07.2019р.).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. С. Гончар, Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. *Монографія. Київ: «Альфа реклама»*, 2019, 176 с.
2. V. Kichak, V. Rudyk and S. Gonchar, «Compensation of non-stationary temporal errors of the measurement channel», *Telecommunications and radio engineering*, vol. 69, no. 10, pp. 869-880, 2010.
3. С. Гончар, Г. Леоненко, О. Юдін, «Анализ угроз и уязвимостей индустриальных автоматизированных систем управления», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №2 (26), С. 9-14, 2013.
4. С. Гончар, «Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом», *Захист інформації*, Т. 16, № 1, С. 40-46, 2014.
5. С. Гончар, Г. Леоненко, О. Юдін, «Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури», *Спеціальні телекомунікаційні системи та захист інформації*, №1 (25), С. 158-163, 2014.
6. О. Юдін, Г. Леоненко, С. Гончар, «Структура модели интеллектуальных электроэнергетических систем, учитывающая необходимость обеспечения их кибербезопасности», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №1 (27), С. 60-69, 2014.
7. С. Гончар, Г. Леоненко, О. Юдін, «Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури», *Вісник*

Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі», №806, С. 34-39, 2014.

8. С. Гончар, «Визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами», *Захист інформації*, том 17, №3, С. 225-230, 2015.
9. С. Гончар, Г. Леоненко, О. Юдін, «Загальна модель загроз безпеці інформації АСУ ТП», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №1 (29), С. 78-82, 2015.
10. С. Гончар, «Модель імовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки», *Наукоємні технології*, № 3 (27), С. 250-253, 2015.
11. V. Mokhor, V. Bezshtanko, H. Kravtsov, I. Kotsiuba, O. Kruk, O. Makarevych, Y. Maksymenko, V. Tsurkan, «Analytical geometry approach for information security risk analyses», *Information Technology and Security*, Vol. 3, Iss.1 (4), pp. 60-67, 2015.
12. С. Гончар, Г. Леоненко, О. Юдін, «Підходи до оцінки небезпеки атак в інформаційних системах об'єктів критичної інфраструктури», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №2 (30), С. 47-52, 2015.
13. С. Гончар, Г. Леоненко, «Наслідки можливих кібератак на об'єкти критичної інфраструктури», *Information Technology and Security*, Vol. 4, Iss.1 (6), С. 108-113, 2016.
14. С. Гончар, О. Юдін, Г. Леоненко, «Алгоритм визначення актуальних загроз безпеці інформації на об'єктах критичної інфраструктури», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №2 (32), С. 40-48, 2016.
15. С. Гончар, Г. Леоненко, «Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури», *Information Technology and Security*, Vol. 4, Iss.2 (7), С. 262-268, 2016.
16. С. Гончар, «Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури», *Моделювання та інформаційні технології*, №80, С. 27-32, 2017.
17. М. Комаров, С. Гончар, «Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури», *Моделювання та інформаційні технології*, №81, С. 12-19, 2017.
18. М. Комаров, С. Гончар, А. Ониськова, «Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури», *Моделювання та інформаційні технології*, №82, С. 40-48, 2018.
19. С. Гончар, «Концепція створення автоматизованої системи управління кібербезпекою об'єктів критичної інфраструктури», *Моделювання та інформаційні технології*, №83, С. 70-76, 2018.
20. В. Мохор, С. Гончар, «Идея построения алгебры рисков на основе теории комплексных чисел», *Електронне моделювання*, Т.40, №4, С. 107-111, 2018.
21. С. Гончар, «Аналіз впливу на екологію стану кібербезпеки об'єктів критичної інфраструктури», *Екологічні науки*, № 2 (21), С. 65-68, 2018.

22. М. Комаров, С. Гончар, «Аналіз і дослідження загроз для захищеного вузла інтернет доступу», *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, Т.29 (68), №4, Ч.1, С. 165-168, 2018.
23. М. Комаров, А. Ониськова, С. Гончар, «Аналіз та дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу», *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, Т.29 (68), №5, Ч.1, С. 138-142, 2018.
24. М. Комаров, С. Гончар, «Аналіз механізмів безпеки системи управління базами даних Oracle Database 12C enterprise Edition», *Моделювання та інформаційні технології,* №85, С. 107-116, 2018.
25. С. Гончар, Р. Герасимов, В. Ткаченко, «Дослідження проблеми кіберживучості Об'єднаної енергосистеми України», *Електронне моделювання*, Т.41, №1, С. 43-53, 2019.
26. В. Мохор, С. Гончар, О. Дибач, «Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури», *Ядерна та радіаційна безпека*, №2 (82), С. 57-61, 2019.
27. В. Мохор, С. Гончар, «Дослідження правомірності подання ризиків векторами у евклідовому просторі», *Електронне моделювання*, Т.41, №4, С. 73-84, 2019.
28. С. Гончар, «Методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури», *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, Т.30 (69), №4, Ч.1, С. 40-43, 2019.
29. Комаров М.Ю., Мохор В.В., Гончар С.Ф. Спосіб виявлення кібернетичних атак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури. *Патент на корисну модель №132581*. Патент опубліковано 25.02.2019, бюл. №4.
30. Мохор В.В., Гончар С.Ф., Бакалинський О.О. Апаратно-програмний комплекс розрахунку сумарного ризику. *Патент на корисну модель №135456*. Патент опубліковано 25.06.2019, бюл. № 12.
31. Мохор В.В., Гончар С.Ф., Бакалинський О.О. Апаратно-програмний комплекс розрахунку комплексного ризику. *Патент на корисну модель №136792*. Патент опубліковано 27.08.2019, бюл. № 16.
32. Мохор В.В., Бакалинський О.О., Гончар С.Ф. Апаратно-програмний комплекс візуалізації ризиків. *Патент на корисну модель №136949*. Патент опубліковано 10.09.2019, бюл. № 17.
33. Мохор В.В., Гончар С.Ф., Бакалинський О.О. Апаратно-програмний комплекс оцінки та аналізу ризику. *Патент на корисну модель №136947*. Патент опубліковано 10.09.2019, бюл. № 17.
34. С. Гончар, «Актуальность исследования и разработки систем защиты информации территориально-распределенных автоматизированных систем управления технологическими процессами», *Кібербезпека-2013: міжнар. наук.-практ. конф.*, Ялта, 2013, С. 33-37.
35. С. Гончар, «Особенности обеспечения кибербезопасности индустриальных систем управления», *Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК: міжнар. наук.-практ. конф.*, Київ, 2013, С. 36-37.
36. С. Гончар, «Шляхи удосконалення державної політики забезпечення

інформаційної безпеки критичної інфраструктури України», *Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання: круглий стіл*, Київ, 2014, С. 92-95.
37. С. Гончар, Г. Леоненко, О. Юдін, «Соціокультурний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури», *Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення: XX Всеук. наук.-практ. конф.*, Житомир, 2014, С. 195-196.
38. С. Гончар, Г. Леоненко, О. Юдін, «Забезпечення інформаційної безпеки об'єктів критичної інфраструктури України», *Інформаційна безпека України: наук.-техн. конф.*, Київ, 2015, С. 95-96.
39. С. Гончар, «Аналіз імовірних деструктивних дій персоналу АСУ ТП в аспекті інформаційної безпеки», *Безпека інформації у інформаційно-телекомунікаційних системах: XVII міжнар. наук.-практ. конф.*, Київ, 2015, С. 104-105.
40. С. Гончар, Г. Леоненко, О. Юдін, «Ймовірність реалізації загроз інформаційній безпеці АС критичної інфраструктури через можливі деструктивні дії персоналу», *Математичне моделювання та математична фізика: Всеук. наук. конф.*, Кременчук, 2015, С. 29-30.
41. С. Гончар, Г. Леоненко, С. Левченко, «Критерії віднесення об'єктів до критичної інфраструктури з урахуванням світового досвіду», *Інформаційна безпека України: наук.-техн. конф.*, Київ, 2016, С. 40-41.
42. С. Гончар, Г. Леоненко, В. Ткаченко, «Пріоритетні напрями розвитку нормативно-правового забезпечення інформаційної безпеки критичної інфраструктури України», *Інформаційна безпека України: наук.-техн. конф.*, Київ, 2016, С. 41-42.
43. С. Гончар, «Імовірнісний аналіз кіберзагроз інформаційних об'єктів енергетики», *The development of technical sciences: problems and solutions: The international research and practical conference*, Brno, The Czech Republic, 2018, С. 6-7.
44. М. Комаров, Г. Леоненко, С. Гончар, «Система управління інформаційною безпекою. Аналіз нормативної бази», *Безпека інформації в інформаційно-телекомунікаційних системах: XX Ювілейна Міжнар. наук.-практ. конф.*, 2018, Київ, 2018, С. 250-251.
45. S. Honchar, M. Komarov, A. Onyskova, «Model of Threats for a Secured Internet Access Node», *Моделювання-2018: Міжнар. наук.-практ. конф.*, Київ, 2018, С. 123-126.
46. С. Гончар, «Роль людського фактору у забезпеченні кібербезпеки об'єктів критичної інфраструктури», *Science and Technology of the Present Time: Priory Development Directions of Ukraine and Poland: International Multidisciplinary Conference*, Wolomin, Republic of Poland, 2018, pp. 89-90.
47. С. Гончар, М. Комаров, «Методика оцінки кіберстійкості об'єктів критичної інфраструктури», *Безпека соціально-економічних процесів в кіберпросторі: Всеук. наук.-практ. конф.*, 2019, Київ, 2019, С. 49-50.

48. С. Гончар, «Підхід до аналізу ризику на основі теорії комплексних чисел», *Комп'ютерні системи та мережні технології: XII Міжнар. наук.-практ. конф.*, Київ, 2019, С. 35-36.
49. С. Гончар, В. Ткаченко, В. Бурлаков, «Підходи до визначення захищеності комп'ютерних систем», *Обчислювальний інтелект: V Міжнар. наук.-практ. конф.*, Ужгород, 2019, С. 295-296.
50. С. Гончар, М. Комаров, «Спосіб виявлення кібератак на інформаційно-телекомунікаційні системи», *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: Всеук. наук.-практ. Інтернет-конф.*, Черкаси, 2019, С. 64-66.
51. С. Гончар, «Методологія оцінки суми ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури», *Перспективні напрями захисту інформації: V Всеук. наук.-практ. конф.*, Одеса, 2019, С. 26-28.

АНОТАЦІЯ

Гончар С.Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2020.

Дисертаційна робота присвячена вирішенню важливої науково-практичної проблеми, пов'язаної з підвищенням рівня захисту інформаційних систем критичної інфраструктури за рахунок розробки методології забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, орієнтованої на створення відповідних методів та засобів розрахунку суми ризиків. У роботі проаналізовано сучасні методи, методики, методології оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об'єктів критичної інфраструктури, а також програмні продукти управлінням такими ризиками. Обґрунтовано поняття комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, здійснено його змістовну інтерпретацію та розглянуто основні властивості. Розроблено методи обчислення суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням значення наслідків повного знищення інформаційного активу. Розроблено метод обчислення суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням теорії векторної алгебри та комплексних чисел. Розроблено методологію оцінювання ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів. Розроблено структурні рішення обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів. Розроблено алгоритмічне та програмне забезпечення обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів. Проведено експериментальні дослідження з

метою підтвердження теоретичних положень та практичних розробок дисертаційного дослідження.

Ключові слова: захист інформації, кібербезпека, оцінювання ризиків, комплексний ризик, об'єктивний ризик, суб'єктивний ризик, інформаційна система, управління ризиком.

АННОТАЦИЯ

Гончар С.Ф. Методология оценивания рисков кибербезопасности информационных систем объектов критической инфраструктуры. – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.21 – «Системы защиты информации». – Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, Киев, 2020.

Диссертация посвящена решению важной научно-практической проблемы, связанной с повышением уровня защиты информационных систем критической инфраструктуры за счет разработки методологии обеспечения кибербезопасности информационных систем объектов критической инфраструктуры, ориентированной на создание соответствующих методов и средств расчета суммы рисков. В работе проанализированы современные методы, методики, методологии оценивания рисков кибербезопасности информационных систем, в том числе объектов критической инфраструктуры, а также программные продукты управлением такими рисками. Обосновано понятие комплексного риска, осуществлена его содержательная интерпретация и рассмотрены основные свойства, что отличается от существующих понятий рисков учетом субъективной составляющей риска, и позволяет комплексно оценивать риски кибербезопасности информационных систем объектов критической инфраструктуры. Разработаны методы вычисления суммы рисков кибербезопасности информационных систем объектов критической инфраструктуры с использованием значений последствий полного уничтожения информационного актива, которые, в отличие от существующих, позволяют осуществлять расчет большего количества рисков и решения задач более широкого класса. Осуществлено исследование фактора субъективного риска в процессе оценивания рисков кибербезопасности информационных систем объектов критической инфраструктуры, в результате которых установлено справедливость аксиом евклидова пространства для представления в нем векторов рисков. Разработан метод вычисления суммы рисков кибербезопасности информационных систем объектов критической инфраструктуры с использованием теории векторной алгебры, который, в отличие от существующих, учитывает объективную и субъективную составляющие риска, позволяет повысить адекватность моделей указанных рисков. Разработана методология оценивания риска кибербезопасности информационных систем объектов критической инфраструктуры, которая, в отличие от существующих, за счет использования методов вычисления суммы рисков с использованием значений последствий полного уничтожения информационного актива, метода вычисления суммы рисков с использованием теории векторной алгебры, позволяет обеспечить поддержку процесса создания инструментальных

средств для оценивания рисков кибербезопасности информационных систем объектов критической инфраструктуры. На основе предложенной методологии можно построить системы, как программные, так и аппаратно-программные, с использованием разработанных методов, направленных на оценивание суммы рисков кибербезопасности информационных систем объектов критической инфраструктуры. Разработаны структурные решения вычислительных систем для расчета суммы рисков кибербезопасности информационных систем объектов критической инфраструктуры, которые, в отличие от существующих, за счет использования разработанных методов и методологии, позволяют осуществлять расчет большего количества рисков и решения задач широкого класса. Разработано алгоритмическое и программное обеспечение вычислительных систем для расчета суммы рисков кибербезопасности информационных систем объектов критической инфраструктуры с использованием разработанных методов. Проведены экспериментальные исследования с целью подтверждения теоретических положений и практических разработок диссертационного исследования. Полученные в диссертационной работе результаты могут быть использованы для оценивания рисков кибербезопасности информационных систем объектов критической инфраструктуры на основе разработанных методов расчета суммы рисков при построении и внедрении систем управления информационной безопасностью, комплексных систем защиты информации в автоматизированных системах разных классов при построении моделей угроз, политики безопасности, плана защиты информации и тому подобное. Результаты диссертационной работы внедрены в деятельность Администрации Государственной службы специальной связи и защиты информации Украины, Государственного научно-исследовательского института специальной связи и защиты информации, Института проблем моделирования в энергетике им. Е. Пухова НАН Украины, Государственного предприятия «Государственный научно-технический центр по ядерной и радиационной безопасности».

Ключевые слова: защита информации, кибербезопасность, оценивание рисков, комплексный риск, объективный риск, субъективный риск, информационная система, управление риском.

ABSTRACT

Honchar S. Methodology for assessment cybersecurity risk of information systems of critical infrastructure objects. – Manuscript.

Thesis for a Doctor of Technical Sciences degree in specialty 05.13.21 – «Information security systems». – Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, Kyiv, 2020.

The dissertation is devoted to solving an important scientific and practical problem related to increasing the level of protection of critical infrastructure information systems by developing a methodology to ensure the cybersecurity of critical infrastructure information systems, focused on creating appropriate methods and means of calculating total risks. The paper analyzes current methods, methodologies, methodologies for

assessing the cybersecurity risks of information systems, including critical infrastructure facilities, as well as software for managing such risks. The concept of complex risk of cybersecurity of information systems of critical infrastructure objects is substantiated, its meaningful interpretation has been carried out and the basic properties have been considered. Methods have been developed for calculating the total cybersecurity risk of information systems of critical infrastructure objects using the maximum effect value. A method has been developed for calculating the total cybersecurity risk of information systems of critical infrastructure facilities using vector algebra theory and complex numbers. A methodology has been developed for assessing the cybersecurity risk of information systems of critical infrastructure facilities using the developed methods. Structural solutions for computing systems were developed to calculate the total cybersecurity risk of information systems of critical infrastructure objects using the developed methods. Developed algorithmic and software computing systems to calculate the total cybersecurity risk of information systems of critical infrastructure objects using the developed methods. Experimental studies were carried out to confirm the theoretical positions and practical developments of the dissertation research.

Keywords: information protection, cybersecurity, risk assessment, complex risk, objective risk, subjective risk, information system, risk management.