ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ.Г.Є.ПУХОВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Гончар Сергій Феодосійович

УДК 004.056.5:005:004.3:004.4

ДИСЕРТАЦІЯ

МЕТОДОЛОГІЯ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.21 – «Системи захисту інформації»

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних проваджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.


_____ С.Ф. Гончар

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

Київ – 2020

АНОТАЦІЯ

Гончар С.Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

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 сумарних 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 сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням значення максимальних наслідків. Розроблено метод обчислення сумарного ризику 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 сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів. Розроблено алгоритмічне та програмне забезпечення обчислювальних систем для розрахунку сумарного ризику 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.

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.

Список публікацій здобувача:

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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ……. 15
ВСТУП 17
Розділ 1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 29
1.1. Нормативно-правове забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури ……..…… 29
1.2. Сучасні підходи до оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури ……..……... 39
1.3. Формулювання наукової проблеми і задач досліджень 69
1.4. Висновки до першого розділу 70
Список використаних джерел до першого розділу ……..…….. 71
Розділ 2. КІБЕРЗАГРОЗИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ОЦІНКА НЕБЕЗПЕКИ ЇХ РЕАЛІЗАЦІЇ ……...…..….. 85
2.1. Модель загроз інформаційних систем об'єктів критичної інфраструктури до кібератак ……..……..…….. 85
2.2. Структурна модель взаємодії елементів інформаційної системи об'єктів критичної інфраструктури ……. 106
2.3. Визначення ймовірності реалізації загроз кібербезпеки об'єктів критичної інфраструктури ……... 112
2.4. Оцінювання небезпеки кібератак в інформаційних системах об'єктів критичної інфраструктури …… 115
2.5. Метод визначення актуальності загрози кібербезпеки

об’єктів критичної інфраструктури ……...…… 124
2.6. Висновки до другого розділу 143
Список використаних джерел до другого розділу …….. 145
Розділ 3. МЕТОДИ РОЗРАХУНКУ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ……..... 150
3.1. Графічний метод розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури 150
3.2. Аналітичний метод розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури 164
3.3. Висновки до третього розділу ……..... 170
Список використаних джерел до третього розділу ……...…… 170
Розділ 4. МЕТОД РОЗРАХУНКУ КОМПЛЕКСНОГО РИЗИКУ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 173
4.1. Об’єктивна та суб’єктивна складові ризику кібербезпеки об’єктів критичної інфраструктури ……..……..…..…….. 173
4.2. Векторна модель ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури ……..…….. 177
4.3. Модель комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури ……..……. 189
4.4. Метод розрахунку комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури … 198
4.5. Висновки до четвертого розділу 205
Список використаних джерел до четвертого розділу ……..… 206
Розділ 5. СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ……..... 209
5.1. Етапи реалізації методології оцінювання ризику кібербезпеки інформаційних систем об’єктів

критичної інфраструктури ……..…….. 209
5.2. Структурна модель (рішення) обчислювальної системи розрахунку сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури ……..……. 236
5.3. Структурне модель (рішення) обчислювальної системи розрахунку комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури …. 242
5.4. Висновки до п’ятого розділу 248
Список використаних джерел до п’ятого розділу ……. 248
Розділ 6. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ СИСТЕМ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ……..... 252
6.1. Розробка алгоритмів та програмного застосунку обчислення сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури …… 252
6.2. Дослідження систем розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури …. 255
6.3. Висновки до шостого розділу 284
Список використаних джерел до шостого розділу ……. 285
ВИСНОВКИ..... 287
Додаток А. Документи, що підтверджують впровадження результатів дисертації 291
Додаток Б. Лістинги (коди) програмних засобів 306
Додаток В. Загрози загального характеру ……..... 309
Додаток Г. Загрози інформації, що можуть виникнути під час мережевої взаємодії 314
Додаток Д. Загрози інформації, що можуть виникнути під час роботи з

прикладним ПЗ 321
Додаток Е. Загрози інформації, що можуть виникати в мережевих ОС 324

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АЕС	- атомна електростанція
АС	- автоматизована система
АСУ	- автоматизована система управління
АСУ ОКІ	- автоматизована система управління об’єкту критичної інфраструктури
АСУ ТП	- автоматизовані системи управління технологічним процесом
ЕОМ	- електронно-обчислювальна машина
ЕС	- енергосистема
ЗІ	- захист інформації
ІБ	- інформаційна безпека
ІС ОКІ	- інформаційні системи об’єкту критичної інфраструктури
ІТ	- інформаційні технології
КІ	- критична інфраструктура
КСІІ	- ключова система інформаційної інфраструктури
ЛОМ	- локальна обчислювальна мережа
НБ	- національна безпека
НД ТЗІ	- нормативний документ з технічного захисту інформації
НСД	- несанкціонований доступ
НСО	- незалежна система оператора
ОЕС	- об’єднана енергосистема
ОКІ	- об’єкт критичної інфраструктури
ОР	- об’єкти ризику
ПЗ	- програмне забезпечення
СЗ	- система захисту
СЗБ	- суб’єкти забезпечення безпеки
СЗІ	- система захисту інформації
IEEE	- Institute of Electrical and Electronics Engineers
ICS	- Industrial Control Systems (системи управління промисловістю)

ISA - Industrial Automation and Control Systems Security

ISACA - Information Systems Audit and Control Association

ISO - International Organization for Standardization

ITSEC - Information Technology Security Evaluation Criteria

ITU-T - International Telecommunications Union

NERC - North American Electric Reliability Corporation

NIST - National Institute of Standards and Technology

SCADA - Supervisory Control And Data Acquisition (система диспетчерського управління і збору даних)

ВСТУП

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 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.); XX 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.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Нормативно-правове забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Основними нормативно-правовими документами на даний час, які стосуються питання забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури в Україні є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017р. [1], Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введене в дію Указом Президента України від 13 лютого 2017 року №32/2017 [2], Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [3], Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 [4], Доктрина інформаційної безпеки України від 25 лютого 2017р. №47/2017 [5] та деякі інші.

Так Закон України «Про основні засади забезпечення кібербезпеки України» [1] визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У даному Законі України, серед інших, дано визначення таких термінів, як «інцидент кібербезпеки», «кібератака», «кібербезпека», «кіберзагроза», «кіберзахист», «критична інформаційна інфраструктура», «об'єкти критичної інфраструктури», «об'єкт критичної інформаційної

інфраструктури». Даним Законом України визначено, що об’єкти критичної інфраструктури являються об’єктами кібербезпеки, а об’єкти критичної інформаційної інфраструктури являються об’єктами кіберзахисту. Зазначені об’єкти, які можуть бути віднесені до критичної інфраструктури, сформульовані принципи забезпечення кібербезпеки, приведений перелік заходів для функціонування національної системи кібербезпеки. Положеннями цього Закону України визначено заходи, спрямовані на забезпечення кібербезпеки та кіберзахисту, а також визначена відповідальність за порушення законодавства у сфері кібербезпеки.

Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введене в дію Указом Президента України від 13 лютого 2017 року №32/2017 [2], серед іншого, передбачається формування пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення вимог щодо кіберзахисту відповідних об'єктів. Крім того, передбачається протокол дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків.

Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [3], визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури. У відповідності до п.3 даних Вимог «кіберзахист об’єкта

критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю». Відповідно до п.7 зазначених Вимог «у випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об’єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури». У цьому ж пункті зазначається, що «створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки». А технічне завдання, в свою чергу, формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005. Тобто, ми можемо констатувати, що технічне завдання на створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Крім того, у даних Загальних вимогах наведено перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

та вимоги до формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки.

Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» [4], визначає механізм формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави. У відповідності до п.2 даного Порядку «об’єкти критичної інфраструктури» - це підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення. Відповідно до п.4 зазначеного Порядку, включені до переліку інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури є критичною інформаційною інфраструктурою держави, що захищається від кібератак у першу чергу (пріоритетно). У п. 8 даного Порядку зазначено, що заінтересовані органи формують пропозиції до переліку з урахуванням негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему. Такими негативними наслідками є [4]:

- виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1);
- негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2);
- негативний вплив на стан економічної безпеки держави (Н.3);
- негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4);
- негативний вплив на систему управління державою (Н.5);
- негативний вплив на суспільно-політичну ситуацію в державі (Н.6);

- негативний вплив на імідж держави (Н.7);
- порушення сталого функціонування фінансової системи держави (Н.8);
- порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9);
- порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н.10).

Крім того, у даному Порядку вказано, що до переліку не включаються інформаційно-телекомунікаційні системи, які не мають виходу каналами електрозв'язку за межі контрольованої зони [4].

Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 [5], спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС, ратифікованою Законом України від 16 вересня 2014 року № 1678-VII, і Стратегією сталого розвитку "Україна - 2020", схваленою Указом Президента України від 12 січня 2015 року № 5. Стратегією визначено цілі Стратегії національної безпеки України, актуальні загрози національній безпеці України, основні напрями державної політики національної безпеки України. У відповідності до п.3 Стратегії актуальними загрозами, серед інших є загрози інформаційній безпеці, загрози кібербезпеці і безпеці інформаційних ресурсів, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, загрози безпеці критичної інфраструктури. У відповідності до п. 4.12 Стратегії одним з основних напрямів державної політики національної безпеки України є Забезпечення кібербезпеки і безпеки інформаційних ресурсів. При цьому, пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою

своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Доктрина інформаційної безпеки України від 25 лютого 2017р. №47/2017 [6] визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Доктриною визначено її мета та принципи, національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, механізм реалізації Доктрини. У відповідності до п. 3. Стратегії встановлено, що національними інтересами України в інформаційній сфері, серед іншого, є розвиток та захист національної інформаційної інфраструктури, розвиток інформаційного суспільства, зокрема його технологічної інфраструктури, розвиток системи стратегічних комунікацій України, забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України, захищеність

державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом.

Проведений аналіз та дослідження нормативних документів дають можливість визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завданням із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту [7-21].

Оскільки, у відповідності до статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» [1] до об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров’я, то розглянемо для прикладу енергетичний сектор.

Сукупність атомних, теплових, гідравлічних і гідроакумулюючих електростанцій, теплоелектроцентралі, а також електростанції з відновлювальних джерел енергії (вітряні, сонячні та інші), магістральні електричні мережі Укренерго та розподільчі електромережі (обленерго), які об’єднані спільним режимом виробництва, передачі та розподілу електричної та теплової енергії утворюють Об’єднану енергетичну систему України (ОЕС України), рис. 1.1 [22].

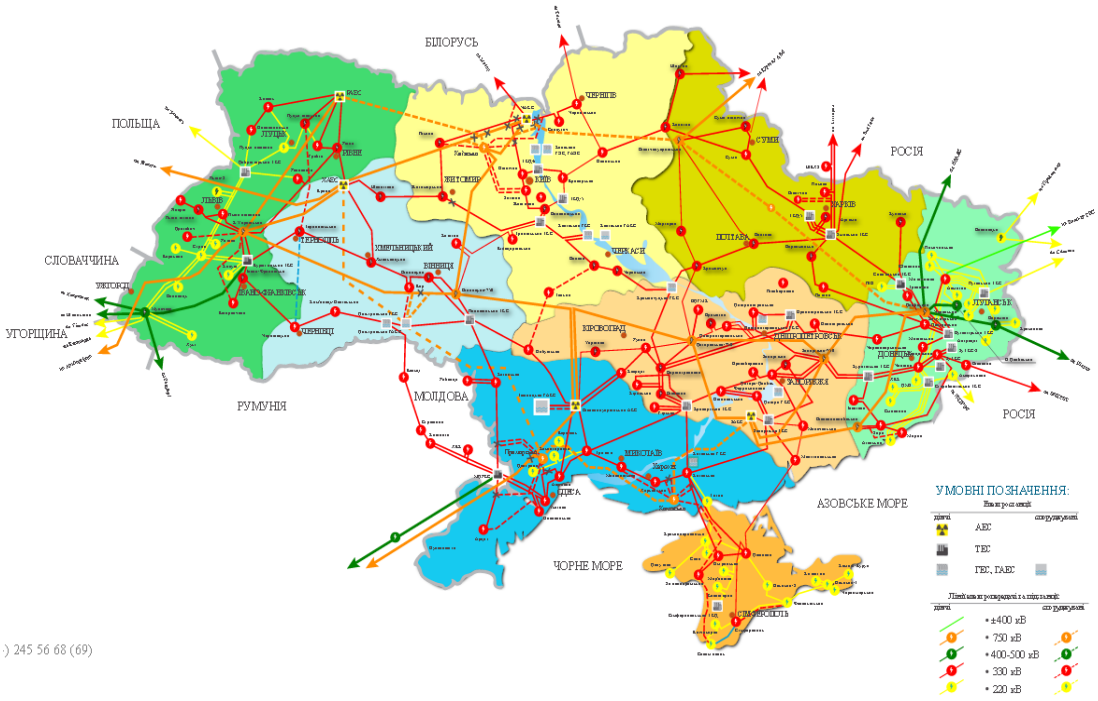


Рис. 1.1. Загальна структура електричної мережі ОЕС України

Структура ОЕС України побудована за регіональним принципом і об’єднує 8 енергетичних систем (ЕС) з функціями оперативно-диспетчерського управління (Дніпровська, Донбаська, Західна, Кримська, Південна, Південно-Західна, Північна та Центральна). До функцій енергосистем належить також передача електроенергії міждержавними електромережами та їх експлуатація [23]. Електроенергетична система складається з елементів, які можна розділити на три групи [23]:

- основні (силові) елементи - генеруючі агрегати електростанцій, води, що перетворюють енергію, або пара в електроенергію; трансформатори, автотрансформатори, випрямні установки, що перетворюють значення і вид струму і напруги; лінії електропередачі (ЛЕП), передавальні електроенергію на відстань; комутуюча апаратура (вимикачі, роз'єднувачі), призначені для зміни схеми ЕС і відключення пошкоджених елементів;

- вимірювальні елементи - трансформатори струму і напруги, призначені для підключення вимірювальних приладів, засобів управління і регулювання;
- засоби управління - релейний захист, регулятори, автоматика, телемеханіка, зв'язок, що забезпечують оперативне і автоматичне управління схемою і роботою ЕС.

Найбільш небезпечними для ЕС є аварійні режими, викликані короткими замиканнями і розривами ланцюга передачі електроенергії, зокрема, внаслідок неправдивих спрацьовувань захисту і автоматики, різноманітних кібератак, а також помилок експлуатаційного персоналу. Тривале існування аварійного режиму неприпустимо, оскільки при цьому не забезпечується нормальне електропостачання споживачів і існує небезпека подальшого розвитку аварії і поширення її на сусідні райони. Для запобігання виникненню аварії і припинення її розвитку застосовуються засоби автоматичного і оперативного управління, якими оснащуються диспетчерські центри, електростанції і підстанції. Також потрібна ефективна система кіберзахисту від кібератак технологічного характеру в реальному часі. Управління режимами ЕС здійснюється оперативним персоналом, а також автоматичними регуляторами і облаштуваннями протиаварійної автоматики (ПА). Налаштування автоматичних систем управління робиться відповідно до заздалегідь вибраних характеристик так, щоб забезпечити економічність роботи ЕС і відповідність вимогам якості що відпускається споживачам електроенергії. Вибір видів використовуваних автоматичних пристроїв, оцінка їх ефективності і впливу на надійність роботи ЕС робляться на основі спеціальних оптимізаційних розрахунків. Управління режимами ЕС має бути оптимальним, тобто що дає найкращий техніко-економічний ефект в умовах дії протилежних чинників. Наприклад, бажаючи збільшити передавану по ЛЕП потужність, можна викликати аварійне відключення цієї лінії через порушення стійкості її роботи [23].

Основна особливість функціонування об’єкту критичної

інфраструктури, у тому числі, енергетичної системи, полягає в єдності технологічного процесу і нерозривного зв'язку окремих її елементів, вимагає єдиного управління процесом роботи усієї системи. У зв'язку з цим з початку розвитку енергетичних систем стала розвиватися і техніка управління ними з єдиного центру – диспетчера [23].

Перелік активів для окремої ЕС, що можуть бути об’єктами кіберзагроз, приведено у табл. 1.1 [23]. Зазначений перелік не є вичерпним, він може змінюватися та доповнюватися.

Таблиця 1.1

Об’єкти кіберзагроз окремої ЕС

Загроза активу ЕС, *n*	Короткий опис активу
1	Баланси потужності підприємств енергетики України
2	Система управління (СУ) персоналом
3	СУ устаткуванням
4	Підрозділи СУ
5	Сукупність електричних схем
6	Сукупність диспетчерських щитів
7	Персонал СУ
8	Управління ОЕС країни
9	Устаткування повітряних ліній
10	Устаткування підстанцій
11	Управління вимикачами
12	Регулятори напруги з РПН
13	Перелік підстанцій
14	Типи устаткування
15	Персональні дані
16	Система посад персоналу
17	Розташування/адреса підрозділів
18	Моделі устаткування підстанцій
19	Моделі трансформаторів
20	Початкові дані (ПД) про гілки ДнЕС
21	ПД про гілки Північної ЕС
22	ПД про гілки Південної ЕС
23	ПД про гілки Південно-Західної ЕЕС
24	ПД про гілки Західної ЕЕС
25	ПД про вузли Центральної ЕЕС
26	ПД про вузли Дніпровської ЕС

Продовження таблиці 1.1

27	ПД про вузли Північної ЕЕС
28	ПД про вузли Південної ЕС
29	ПД про вузли ПЗЕС
30	ПД про вузли ЗЕС
31	ПД про вузли Центральної ЕС
32	Відеограми (SCADA)
33	Розташування ЕС
34	Підстанції
35	Система телесигналів
36	Система телевимірювань
37	Типи СУ
38	Параметри і характеристики повітряних ліній

Аналогічно можна привести перелік стосовно ЕС, що можуть бути об’єктами кіберзагроз, табл. 1.2.

Таблиця 1.2

Об’єкти кіберзагроз ЕС

Загроза ЕС, *e*	Короткий опис активу
1	Західна ЕС
2	Південно-Західна ЕС
3	Південна ЕС
4	Північна ЕС
5	Дніпровська ЕС
6	Центральна ЕС

Очевидно, що складові активів у таблиці 1.1 будуть компонентами активів у таблиці 1.2, і будуть разом складати ОЕС України.

Аналогічні моделі можливо розробити у випадку об’єктів критичної інфраструктури інших секторів.

1.2. Сучасні підходи до оцінювання ризиків кібербезпеки інформаційних систем 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.

Деякі автори зазначають [24], що кібер-ризики належать до порядку денного бізнесу кожної компанії, однак їх важко оцінити через відсутність достовірних даних та ретельного аналізу. Ці фахівці розглядають широкий спектр подій, пов'язаних з кібер-ризиком, та фактичні дані про витрати. Для цього вони визначають кіберзбитки з бази даних операційних ризиків та аналізують їх за допомогою методів статистики та актуарної науки. Вони використовують метод пік-порогового значення з теорії екстремальної цінності для виявлення "кібер-ризиків повсякденного життя" та "крайніх кібер-ризиків". Показано, що поведінка людини є основним джерелом кібер-ризику, а кібер-ризики сильно відрізняються порівняно з іншими категоріями ризику. Приведені моделі можуть бути використані для отримання послідовних оцінок ризику в залежності від країни, галузі, розміру та інших змінних [24].

Досліджено статтю [25], яка присвячена оцінці економічного впливу Інтернету речей (IoT) та пов'язаних з ним кібер-ризикових векторів і вершин - переосмислення вертикалей IoT. Автори адаптують до IoT як модель Cyber Value at Risk, добре налагоджену модель вимірювання максимально можливих втрат за даний період часу, так і модель MicroMort - широко використовувану модель прогнозування невизначеності через одиниці ризику смертності. Отриманий новий IoT MicroMort для обчислення ризику IoT тестується та підтверджується реальними даними з IoT-сканера BullGuard (понад 310 000 сканувань) та звіту Garner про пристрої, підключені до IoT. Розроблено два розрахунки, поточний стан кібер-ризику IoT та майбутні прогнози кібер-ризику IoT. Таким чином, зазначена наукова робота спрямовує зусилля на інтеграцію оцінок впливу на кібер-ризики та пропонує краще розуміння оцінки економічного впливу на кібер-ризик IoT [25].

У роботі [26] показано, що поширення технологій, вбудованих у підключені та автономні транспортні засоби (CAV), збільшує потенціал

кібератак. Системи зв'язку між транспортними засобами та інфраструктурою надають віддалений доступ для атак для зловмисних хакерів для використання вразливості системи. Підвищена сполучуваність у поєднанні з функціями автономного водіння створює значну загрозу величезним соціально-економічним вигодам, обіцяним CAV. Однак відсутність історичної інформації про кібератаки означає, що традиційні методи оцінки ризику роблять неефективними. У цій роботі пропонується проактивна модель класифікації кібер-ризиків CAV, яка долає цю проблему, включаючи відомі вразливості програмного забезпечення, що містяться в Національній базі даних про вразливість США, у етапи побудови моделі та тестування. Цей метод використовує модель Bayesian Network (BN), спираючись на змінні та причинно-наслідкові зв'язки, що випливають із загальної схеми оцінювання вразливості (CVSS), для представлення ймовірнісної структури та параметризації кібер-ризику CAV. Отримана модель BN підтверджується вибірковим тестом, що демонструє майже 100% точність прогнозу кількісного показника ризику та якісного рівня ризику. Потім модель застосовується до випадку використання GPS-систем CAV з криптографічною автентифікацією та без неї. У випадку використання демонструється, як модель може бути використана для прогнозування ефекту заходів щодо зменшення ризику [26].

У статті [27] зазначається, що кіберзлочинці без особливих перешкод ведуть свою торгівлю. Користувачі домашніх комп'ютерів особливо вразливі до нападу все більш досконалої та глобально розповсюдженої групи хакерів. Епоха смартфонів загострила ситуацію, запропонувавши хакерам ще більше нападників для експлуатації. Це може бути не зовсім збігом випадків, коли кіберзлочинність розмножується паралельно з урядами, що дотримуються порядку денного неолібералізму. Цей порядок денний має сильний потяг до індивідуалізації ризику, тобто, поради громадян, як дбати про себе, а потім залишати їх перед наслідками, якщо вони вирішать не дотримуватися порад. Насправді, громадяни "відповідальні". Оскільки реагування ефективне для

деяких ризиків, відповідальність на кібербезпеку сприяє глобальному успіху кібератак. Отже, має бути розроблений випадок для урядів, які беруть активнішу роль, ніж просто надання порад, як це відбувається у багатьох країнах. Автори надають конкретну пропозицією щодо режиму регулювання ризиків, який би більш ефективно зменшив кібер-ризик [27].

У науковій роботі [28] представлено кібер-ризик як критичний бізнес-ризик, що переливається на стратегічний ризик, кредитний ризик та регулятивний ризик на рівні організації, а також ринковий ризик та системний ризик на рівні портфеля. Потім автор аналізує унікальність кібер-ризику, необхідність вимірювання кібер-ризику та його поточні виклики, після чого проводиться огляд вартості кіберзлочинності, категорії втрат кібер-інцидентів та моделі для вимірювання очікуваних збитків від кібер-інцидентів, включаючи річну тривалість втрат, стандарт відхилення втрат та сприйнятий складений ризик. Потім він охоплює сучасні методи вимірювання кібер-ризиків, наприклад, загальну систему оцінювання вразливості (CVSS), CORAS, стохастичне моделювання, моделювання в Монте-Карло, кібер-значення з ризиком та факторний аналіз інформаційного ризику (FAIR). Квадрант кібер-ризику представлений у цій главі, застосовуючи вимірювання медичного ризику до кібер-контексту. Він класифікує фактори ризику на технологічні, нетехнологічні, притаманні (немодифікуючі) та контрольні (що змінюються) фактори. Наведено також приклади аналізу сценаріїв для оцінки контролю та кількісної оцінки втрат [28].

У роботі [29] пропонується система оцінювання кібер-ризиків, яка враховує найгірший випадок лікаря щодо можливості медичного обладнання вплинути на пацієнта. Підвищена підключеність медичних пристроїв прискорює лікування пацієнтів та забезпечує життєзабезпечення можливостей, але відсутність акценту на безпеці пристроїв призвело до кількох порушень кібербезпеки. Більшість медичних працівників не мають належних знань у галузі інформаційних технологій чи кібербезпеки, але вони

несуть відповідальність за оцінку того, які медичні пристрої забезпечують найкращий баланс ризику та ймовірності успіху. Система оцінювання також спирається на анкету безпеки, засновану на моделі STRIDE, яка допомагає створити оцінку ризику для медичного обладнання. Для демонстрації застосування та корисності системи оцінки ризику використовуються три тестові сценарії із застосуванням медичних пристроїв [29].

У статті [30] представлені аналітичні моделі оптимізації витрат на кібербезпеку фірми та кіберстрахування на основі ефективності витрат відповідно до зниження кіберзагроз, вразливості та впливу. На макрорівні стаття показує, як внесок приватного сектору у боротьбу з кіберзлочинністю може зменшити загальні кіберзбитки та створити економічну цінність. На мікрорівні ефективність фірми витрат на безпеку для подолання конкретних кіберзагроз може бути знижена, коли не будуть вжиті інші заходи, що залежать від безпеки. У статті виходить оптимальний поєднання вкладень в кібербезпеку в «знання та досвід», а не в «вжиття заходів щодо пом'якшення наслідків». У роботі пропонується налаштувати кіберстрахування для фірм із деталізованим покриттям, що залежить від загрози, та часткою надбавки, яка використовується для того, щоб допомогти клієнтам, які знають про ризики, та підштовхнути клієнтів у здійсненні заходів щодо зменшення ризику. Малі та середні підприємства можуть отримати найбільшу вигоду від такого інноваційного страхування в кібер-умовах [30].

У статті [31] розглядають можливість визначити вразливість електричних кіберфізичних систем (CPS) шляхом поширення несправностей під час кібератаки. Спочатку пропонується модель поширення несправностей, головним чином з урахуванням впливу перебоїв на деяких вузлах кібермережі на електричні фізичні системи. По-друге, два графіки, тобто графік розповсюдження та графік атаки, пропонуються для виявлення механізмів розповсюдження фізичних несправностей та аналізу інтенсивності атаки комбінацій різних вузлів зв'язку відповідно. По-третє, набір традиційних вразливих індексів на основі графіків розповсюдження та

атаки використовується для ідентифікації як критичних фізичних гілок, так і вузлів зв'язку в CPS. Нарешті, порівняльний аналіз із та без урахування CPS показує, що поширення несправностей серед більш складних та неправильних рішень, які приймає центр управління, викликає більшу вразливість електричної мережі через перерву інформації про передачу в кіберсистемі під дією кібератак [31].

У [32] зазначається, що традиційні рамки для оцінки ризиків не працюють добре для хмарних обчислень. Хоча останні роботи часто зосереджуються на ризиках, з якими стикаються фірми, які приймають або вибирають хмарні сервіси, мало досліджень про те, як хмарні провайдери можуть оцінювати власні послуги. У цій роботі автори використовують поглиблений огляд існуючої літератури, щоб висвітлити слабкі місця традиційних рамок оцінювання ризику для цього завдання. Використовуючи приклади, вони описують нову модель оцінки ризику (CSCCRA) та порівнюють її з трьома усталеними підходами. Для кожного підходу вони враховують його цілі, процес оцінки ризику, рішення, обсяг оцінки та спосіб концептуалізації ризику. Ця оцінка вказує на необхідність динамічних моделей, спеціально розроблених для оцінки хмарного ризику. Пропозиції авторів щодо майбутніх досліджень спрямовані на вдосконалення виявлення, оцінки та зменшення взаємозалежних хмарних ризиків, властивих визначеному ланцюгу поставок [32].

У дослідженні [33] досліджено поточний стан та майбутній напрямок використання інформаційних систем управління ланцюгами поставок для компаній з багатокомпонентним виробництвом. У статті представлений якісний метод дослідження для аналізу процесів ланцюга поставок та визначення шляхів його інформаційного забезпечення. На основі даних, зібраних від різних підприємств, можна зробити висновок, що для виявлення найбільш ефективних стратегій інформаційного забезпечення ланцюга поставок увага повинна зосереджуватися на виявленні та управлінні джерелами невизначеності, ризиків та кібербезпеки. Для успішної інтеграції

бізнес-процесів між постачальниками та замовниками виробники повинні вирішити складну проблему інформаційної безпеки. Таким чином у роботі запропонований новий підхід до виявлення та прогнозування ризику постачання в умовах невизначеності та запропоноване комплексне рішення щодо захисту даних в інформаційних системах управління ланцюгами поставок [33].

Велика кількість досліджень, наукових праць, у яких розглядається та аналізується сутність, зміст і типологія управлінських рішень в системі державного і муніципального управління [34-48].

У роботі [49] описано вплив злочинної діяльності, що ґрунтується на характері злочину, жертві та підставі (чи то короткострокової чи довгострокової / тривалості) впливу кіберзлочинності в Інтернеті. Останнім часом багато країн стикаються з численними кіберзагрозами, зокрема DoS (та DDoS), зловмисне програмне забезпечення, наклеп на веб-сайт, спам та фішинг-атаки на електронну пошту. У зв'язку з розвитком цих кіберзлочинів виявлення та оцінка ризику для безпеки має вирішальне значення для доступу до даних нових технологій, а також намагання зрозуміти, як технологіями можна зловживати. Тому існує потреба розробити спеціальну модель оцінки ризиків кібербезпеки для вирішення цих кіберзагроз. У цій роботі автори пропонують використовувати модель нечітких висновків (FIS) для отримання результату оцінки ризику на основі чотирьох факторів ризику, які є: вразливістю, загрозою, ймовірністю та впливом для визначення кола ризиків, які можуть загрожувати будь-якій організації та намагатися вирішити такі питання пропонованим організаціям. Автори провели різноманітні аналізи щодо цих факторів і, нарешті, результати оцінювання показують життєздатність запропонованого нами підходу [49].

Робота [50] є першою з серії робіт про заходи ризику та уніфікацію економічної бази, що охоплює міждисциплінарну сферу «кіберноміки». Це також перший навчальний документ, який офіційно запропонував одиниці вимірювання кібер-ризику. У цій роботі використовуються

мультидисциплінарні методології для застосування перевірених методів вимірювання ризику у фінансах та медицині для визначення нових одиниць ризику, що є центральними в кіберноміці. Використання встановлених одиниць ризику - MicroMort (MM) для вимірювання медичного ризику та Value-at-Risk (VaR) для вимірювання ринкового ризику - BitMort (BM) та hekla (названий на честь ісландського вулкана) визначаються як одиниці кібер-ризику. Методи та приклади обчислення ризику вводяться в цій роботі для вимірювання економічної ефективності факторів контролю, формулювання «готовності платити» (ціноутворення на ризик) для зниження кібернебезпеки, обмеження кібер-ризику та апетиту до кібер-ризику. Кіберноміка, побудована навколо БМ та Гекла, інтегрує управління кібер-ризиками та економіку для вивчення вимог банку даних з метою вдосконалення рішень щодо аналізу ризиків для: 1) оцінки цифрових активів; 2) вимірювання впливу ризику цифрових активів; 3) оптимізація капіталу для управління залишковим кіберризиком. Створення адекватних, цілісних та статистично надійних точок даних про сутність, портфоліо та глобальний рівень для розвитку банку даних з кіберноміки є важливим для стійкості нашого спільного цифрового майбутнього. У цій роботі пояснюється необхідність створення схем даних, таких як Міжнародна класифікація цифрових активів (IDAC) та Міжнародна класифікація кібер-інцидентів (ICCI) [50].

Автор у [51] зазначає, що якщо ви будете шукати в Google термін "викупна програма", ви побачите дві речі. Перший - це визначення WannaCry, нападу небезпечного програмного забезпечення, яке 12 травня 2017 року поширилось по всьому світу та торкнулося сотні цілей, включаючи комунальні послуги, великі корпорації та, головне, покалічило NHS у Великобританії1. Але можна також побачити серію новин, і, незалежно від того, в який день ви вводите "викупницьку програму" на панель пошуку, ви, ймовірно, побачите історії про напади за кілька днів тому, або, в деяких випадках, лише кілька годин тому. Всі підприємства ризикують піддатися

кібератакам, які занадто часто є успішними. Це пов’язано з нестачею бюджету чи бюджети витрачаються неправильно? Чи достатньо просто витратити більше грошей, щоб допомогти? Усі підприємства стикаються з бюджетним тиском - це означає, що вони повинні розуміти, як витратити свої бюджети розумно. І саме тут керовані постачальники послуг можуть відігравати вирішальну роль. Автор Тім Браун із SolarWinds пояснює, як забезпечити правильну комбінацію технологій та персоналу [51].

У відповідності з [52] власники критичної інфраструктури та оперативні критики завжди шукають способи мінімізувати кібер-ризик, зберігаючи при цьому витрати на кібербезпеку. Протягом сотень років страхова галузь кількісно оцінює ризик, щоб мінімізувати ризик та отримати максимальний прибуток. Для досягнення цих цілей страховики постійно збирають та аналізують статистичні дані для покращення їх прогнозів, стимулювання інвестицій клієнтів у самозахист та періодично вдосконалюють їх моделі для підвищення точності оцінок ризику. У цій статті представлено основу, яка включає принципи роботи страхової галузі для надання кількісних оцінок кібер-ризику. Автор використовує методи оптимізації, щоб запропонувати рівні інвестицій у кібербезпеку та страхування власників та операторів критичної інфраструктури. Цей аналіз може бути використаний для кількісного формулювання стратегій мінімізації кібер-ризику [52].

Дослідники у [53] зазначають, що кіберфізичні суспільства стають залежними від кібер-сфери у повсякденному житті. Оскільки кібервійни все більше стають частиною майбутніх конфліктів, потрібні нові та нові рішення для допомоги урядам у забезпеченні їх національної інфраструктури. Кібермиротворення - це одне таке рішення: виникає та багатодисциплінарна сфера досліджень, яка стосується технічних, політичних, урядових та суспільних областей думки. У цій статті автори спираються на попередні роботи, розвиваючи кібермиротворчу діяльність щодо спостереження, моніторингу та звітності. Вони застосовують практичний підхід: описуючи

сценарій, за якого два кіберфізичні товариства відчувають негативні наслідки кібер-війни та вимагають кібер-експертизи для відновлення послуг, від яких залежать громадяни. Автори досліджують, як може розпочатися операція з підтримання кіберзахисту, і обговорюють проблеми, з якими вона зіткнеться. У статті подано низку пропозицій, включаючи використання віртуального середовища для спільної роботи для отримання багатьох переваг [53].

Кількісне емпіричне онлайн-дослідження [54] вивчало безпечну поведінку в Інтернеті та порівняння студентів у Великобританії та США, вимірюючи сприйняття ризику та інші виміри ризику. По-перше, сприйнятий ризик був найвищим для крадіжок особистих даних, кейлогерів, кібер-знущань та соціальної інженерії. По-друге, відповідно до існуючої теорії, важливими прогнозами сприйнятого ризику були добровільність, безпосередність, катастрофічний потенціал, боязнь, тяжкість наслідків та контролю, а також досвід роботи в Інтернеті та частота використання Інтернету. Більше того, контроль був важливим провісником запобіжної поведінки. Методологічні наслідки підкреслюють необхідність неокупного аналізу, а практичні наслідки підкреслюють повідомлення про ризики для користувачів Інтернету [54].

Велика кількість досліджень, наукових праць, у яких викладено основи методології та організації процесу розробки і реалізації управлінських рішень [55-69].

Технології Smart Grid [70] розробляються для модернізації електромережі за допомогою мережевої метрології та елементів управління, які дозволяють підвищити ефективність та запропонувати нові методи управління системою. Незважаючи на те, що ці технології пропонують великі переваги, вони також впроваджують нові класи ризику, особливо, створюючи нові вектори атак, які можуть бути використані кібератакою. Для оцінки та подолання ризиків у таких кіберфізичних системах, набір інструментів дизайнера системи повинен включати концепції, засновані на кібербезпеці, надійності та конструкції стійкості до відмов, інтегрованих у загальну

методологію. У цій роботі обговорюється фрагментарний пейзаж досліджень ризику кібер-атаки на інтелектуальні системи вимірювання, а потім спираємось на концепції з інженерії систем та проектування відмов, щоб організувати та уніфікувати деталі [70].

Кібербезпека є важливим питанням у галузі ядерної інженерії [71], оскільки ядерні об'єкти використовують цифрове обладнання та цифрові системи, які можуть призвести до серйозних небезпек у разі аварії. Регулюючі агенції по всьому світу оголосили вказівки щодо кібербезпеки, пов'язані з ядерними питаннями, включаючи Посібник з регулювання норм NRC в США 5.71. Важливо оцінити ризик кібербезпеки відповідно до цих нормативних посібників. У цьому дослідженні автори пропонують модель оцінки ризику кібербезпеки для ядерних приладів та систем управління з використанням Байєсівської мережі та дерев подій. Оскільки складно виконати тести на проникнення в системи, модель оцінки може інформувати про дослідження кіберзагроз для систем кібербезпеки ядерних установок шляхом використання попередньої, зворотної інформації та розрахунків зворотного розповсюдження. Крім того, пропонується методологія застосування аналітичних результатів з Байєсівської моделі мережі до моделі дерева подій, яка є імовірнісним методом оцінки безпеки. Запропонований метод дозволяє зрозуміти ризики безпеки та кібербезпеки [71].

У дослідницькій роботі [72] автори розробили новий нечіткий логічний контролер інтервалу типу 2 (IT2FLC) для вдосконалення моделі оцінки ризиків для кібербезпеки. Запропонований IT2FIS реалізує цю модель для отримання загального ризику для такої системи кібербезпеки, яка поєднується з трьома підмоделями, як: а) загальна спроможність, яка контролюється можливостями, наміром, б) загальною вірогідністю, що залежить від вразливості, загалом здатності та нарешті в) ризик, який вимірюється загальною вірогідністю, впливом. Комбінуючи ці три підмоделі, ми сформулювали та оптимізували загальну оцінку ризику для кібербезпеки. Цей підхід матиме розширений контроль для прогнозування можливості

оцінки ризику кібербезпеки, незважаючи на невизначеність даних та інформації про кібербезпеку через різні ризики, спричинені наслідками злочинної діяльності залежно від видів правопорушення, жертви та походження наслідків кіберзлочинності. Нарешті, обґрунтованість запропонованої моделі обговорюється за допомогою статистичного аналізу, адаптивного нейро-нечіткого висновку (ANFIS) та множинної лінійної регресії (MLR) [72].

Автори статті [73] стверджують, що держави, які використовують кіберпроксі, стикаються зі схожими дилемами. По-перше, уряди ризикують прометейською дилемою, коли вони оснащують кіберпроксі інструментами, які можуть бути проти них. По-друге, уряди ризикують дилемою ненавмисного загострення кризи шляхом надання повноважень проксі-сервісам з більш розширеними або менш стриманими політичними програмами, які можуть перевищувати їхні мандати. У роботі досліджується, як держави можуть управляти ризиками, пов'язаними з цими дилемами, та умовами, за яких вони, ймовірно, можуть дати відсіч [73].

Автори у роботі [74] зазначають, що кібербезпека стосується захисту підключених до Інтернету систем, таких як апаратне забезпечення, програмне забезпечення, а також дані (інформація) від кібератак (супротивників). Регулювання кібербезпеки необхідне для захисту інформаційних технологій разом з комп'ютерними системами з метою примусити різні організації, а також компанії захищати свої системи та інформацію від кібератак. Можливі кілька кібератак, таких як віруси, фішинг, троянські коні, глисти, напади на заборону обслуговування (DoS), незаконний доступ (наприклад, крадіжка інтелектуальної власності або конфіденційної інформації), а також напади на систему контролю. У цій статті автори акцентують увагу на важливості різних стандартів в кіберзахисті та архітектурі кібербезпеки, обговорюють загрози безпеці, атаки та заходи в галузі кібербезпеки. Також обговорюють різні проблеми стандартизації в галузі кібербезпеки, національну стратегію кібербезпеки для

забезпечення кіберпростору, а також різні урядові політики щодо захисту кібербезпеки. Нарешті, надають деякі рекомендації, які мають вирішальне значення для кібербезпеки та кіберзахисту [74].

У травні минулого року уряд Великобританії повідомив [75], що дві третини великого бізнесу країни зазнали кібератаки протягом попередніх 12 місяців. Тому не дивно, що кібербезпека є на порядку денному для уряду - підкреслено нещодавніми інвестиціями в розмірі 1,9 млрд. фунтів стерлінгів у п'ятирічну стратегію кібербезпеки, яка була розпочата в лютому 2017 року з офіційним відкриттям Національного центру кібербезпеки. Нещодавно уряд Великобританії повідомив, що дві третини великого бізнесу країни зазнали кібератаки протягом попереднього року. Тож не дивно, що кібербезпека належить до порядку денного уряду. У статті зазначається, що кібербезпеку потрібно використовувати в усіх куточках кожної урядової організації. Від управління фінансами до найменших працівників, кожен повинен відігравати свою роль у забезпеченні безпечної та безпечної урядової інфраструктури. Джо Кім з Solar Winds розглядає деякі кроки, які можуть зробити державні ІТ-команди, щоб допомогти захистити свої організації від рішучих кібер-злочинців, які шукають вигідну оплату праці [75].

Велика кількість досліджень, наукових праць, у яких особливу увагу приділено прийомам розробки і вибору управлінських рішень в умовах невизначеності і ризику, аналізу факторів якості та ефективності управлінських рішень в органах влади і управління [76-90].

У статті [91] розглядається стан сучасних оцінок ризику кібербезпеки систем нагляду та контролю даних (SCADA). Автори вибрали та детально дослідили двадцять чотири методи оцінки ризику, розроблені для або застосовуються в контексті системи SCADA, описали суть методів, а потім проаналізували їх з точки зору мети; домен програми; розглянуті етапи управління ризиками; охоплені ключові концепції управління ризиками; вимірювання впливу; джерела імовірнісних даних; оцінка та підтримка інструментів. На основі проведеного аналізу запропоновано інтуїтивну схему

класифікації методів оцінки ризиків кібербезпеки для систем SCADA, а також окреслено п'ять наукових проблем, які стоять перед цією областю, і вказано на підходи, які можна використовувати [91].

У [92] зазначається, що промислова система управління (ICS) - це паралельний термін, що відноситься до групи технологій автоматизації процесів, таких як системи нагляду та збору даних (SCADA) та розподілені системи управління (DCS), на які, на жаль, зазнали зростаючої кількості атак в останні роки. Оскільки вони надають життєво важливі послуги критичній інфраструктурі, такі як комунікації, виробництво та енергетика серед інших, ворожі зловмисники, які здійснюють напади, становлять серйозну загрозу для щоденного управління національними державами. ICS мають унікальні вимоги до продуктивності та надійності і часто використовують операційні системи, додатки та процедури, які сучасні IT-фахівці можуть вважати нетрадиційними. Ці вимоги, як правило, відповідають пріоритету доступності та цілісності, з подальшим конфіденційністю та включають управління процесами, які, якщо виконуються неправильно, становлять істотний ризик для здоров'я та безпеки людського життя, шкоди навколишньому середовищу, а також серйозні фінансові такі питання, як втрати виробництва. Недоступність критичної інфраструктури (наприклад, електроенергія, транспорт) може мати економічний вплив далеко за межі систем, що зазнають прямого та фізичного пошкодження. Ці наслідки можуть негативно вплинути на місцеву, регіональну, національну чи, можливо, глобальну економіку [92].

Система аналізу та оцінки ризиків кібербезпеки (CSRAS) була розроблена як інструмент для аналізу вимог безпеки та технічного контролю безпеки на основі загальної процедури оцінки ризику кібербезпеки з урахуванням характеристик систем ІС [93].

Кібербезпека є актуальною проблемою безпеки в ядерній промисловості, особливо в галузі приладів та контролю [94]. Для систематичного вирішення проблеми кібербезпеки потрібна модель, яка

може бути використана для оцінки кібербезпеки. У цій роботі запропоновано модель ризику кібербезпеки, засновану на Байєсівській мережі, для комплексного оцінювання кібербезпеки ядерних об'єктів. Запропонована модель дає змогу оцінювати як процедурні, так і технічні аспекти кібербезпеки, які пов'язані з дотриманням норм керівництва та архітектури системи відповідно. Модель аналізу якості діяльності була розроблена для оцінки того, наскільки люди та / або організації відповідають нормативним рекомендаціям, пов'язаним з кібербезпекою. Модель аналізу архітектури була створена для оцінки вразливості та заходів пом'якшення наслідків щодо їх впливу на кібербезпеку. Дві моделі об'єднані в єдину модель, яку називають моделлю ризику кібербезпеки, щоб кібербезпеку можна було оцінити одночасно з процедурних та технічних точок зору. Модель застосовувалася для оцінки ризику кібербезпеки системи захисту реактора дослідницького реактора та для демонстрації його корисності та доцільності [94].

У критичних інфраструктурах, таких як атомна електростанція (AEC), кібератака може мати серйозні наслідки через ініціювання небезпечних подій або виведення важливих систем безпеки [95]. Завдяки застосуванню цифрових технологій до критичних для безпеки інфраструктури кібер-атаки стали однією з нових небезпечних загроз. Оскільки кібератака проводиться навмисно, слід розглянути численні можливі випадки розвитку системи кібербезпеки, такі як шляхи, методи та потенційні цільові системи атаки. Тому, перш ніж розробляти стратегію кібербезпеки, поінформовану про ризик, слід проаналізувати важливість кібератак та значних критичних цифрових активів (CDA). У роботі [95] запропоновано метод аналізу важливості кібератак на AEC, використовуючи метод ймовірнісної оцінки безпеки (PSA). Для розробки структури аналізу важливості для кібератак були визначені можливі кібератаки з режимами відмов, а також була розроблена модель PSA для кібератак. Для практичних досліджень кількісні оцінки сценаріїв кібератаки проводилися за пропонованим методом.

Використовуючи кількісну важливість кібератак та виявляючи значні CDA, які потрібно захищати від кібератак, можна розробити ефективну та надійну оборонну стратегію проти кібератак на АЕС [95].

Після аварії Фукусіма-Даїчі в 2011 році ризик, що виникає через багато енергоблоків, тобто ризик через декілька атомних електростанцій (АЕС) на ділянці, став важливим питанням у кількох країнах, таких як Корея, Канада та Китай [96]. Однак багатоядерний ризик тривалий час обговорювався в ядерній спільноті до того, як сталася ядерна аварія Фукусіма-Даїчі. Регулюючі органи у всьому світі та міжнародні організації запропонували вимоги або вказівки щодо зменшення ризику, що складається з різних одиниць. Побоювання, пов'язані з ризиком, пов'язаним з кількома одиницями, можна узагальнити в трьох наступних питаннях:

- наскільки аварія АЕС на ділянці впливає на безпеку інших АЕС на тому ж майданчику?
- який загальний ризик ділянки з багатьма АЕС?
- чи буде ризик одночасних аварій на декількох АЕС на ділянці, наприклад, аварії Дакуї Фукусіма?

Багатоодинична оцінка ризику (MURA) в комплексній структурі - це практичний підхід для отримання відповідей на вищезазначені питання. Незважаючи на те, що до ядерної аварії Фукусіма-Даїчі мало ядерних досліджень, які мають оцінити ризик багато одиниць, все ще існує кілька питань, які мають бути вирішені, щоб виконати повну оцінку ризику. Ця стаття [96] спрямована на те, щоб надати огляд проблем, пов'язаних із ризиком, що складаються з різних одиниць, та його оцінку. Автор обговорює декілька найважливіших питань у поточній оцінці ризику, щоб отримати корисну інформацію про багатоодиничний ризик із сучасними технологіями оцінювання безпеки (PSA). Також розглядаються якісні відповіді на вищезазначені питання [96].

Відповідні стратегії реагування на нові і постійні кібератаки повинні бути в змозі знизити ризики до прийнятного рівня, не жертвуючи місією для

безпеки [97]. Існуючі підходи або оцінюють вплив, не враховуючи негативних побічних ефектів місії, або будуються вручну на основі традиційних оцінок ризику, не залишаючи осторонь технічних труднощів. У цій роботі запропоновано динамічну систему реагування на ризик-менеджмент (DRMRS), що складається з активного та реактивного програмного забезпечення для управління, спрямоване на автоматичне оцінювання сценаріїв загроз, а також передбачення виникнення потенційних атак. Автори застосовують кількісний підхід, орієнтований на ризик, який забезпечує комплексний огляд загроз, враховуючи їх вірогідність успіху, спричинений вплив, вартість можливих реакцій та негативні побічні ефекти відповіді. Відповіді вибираються та пропонуються операторам на основі оцінок фінансових, операційних та загроз. DRMRS застосовується до реального дослідження випадку критичної інфраструктури з кількома сценаріями загрози [97].

Критичні інфраструктури, що мають важливе значення для нашого сучасного життя, такі як електромережі та водяні насоси, контролюються системами нагляду та збору даних (SCADA) [98]. За останні два десятиліття підключення критичної інфраструктури до Інтернету стало надзвичайно важливим завдяки продуктивності та комерційним потребам. Поєднання підключень до Інтернету до систем з малою мірою захисту, а також той факт, що безпека через незрозумілість вже не працює, перенесла тему безпеки SCADA на перший план в останні кілька років. Для вирішення цих викликів у роботі [98] пропонуються методи виявлення кібератаки на основі розпізнавання тимчасового шаблону. Методи розпізнавання тимчасових шаблонів не тільки шукають аномалії в даних, що передаються компонентами SCADA по мережі, але й шукають аномалії, які можуть виникнути шляхом неправильного використання законних команд, таким чином, що несанкціоновані та неправильні інтервали часу між ними можуть калічити систему. Зокрема, автори пропонують два алгоритми на основі прихованих моделей Маркова (HMM) та штучних нейронних мереж (ANN).

Оцінюють алгоритми за реальними та імітованими даними SCADA за допомогою п'яти різних методів вилучення функцій; в кожному методі алгоритми враховують різні аспекти необроблених даних. Результати показують, що методи розпізнавання тимчасових шаблонів, особливо ті, що базуються на вилученні часових особливостей, можуть виявляти кібератаки, в тому числі ті, що передбачають законні функції, які відомі в літературі як важко виявити [98].

Дослідники широко визнають загрозу для систем управління промисловістю (ICS) від кібератак [99]. Оператори ICS прагнуть вирішити ці загрози ефективно та з урахуванням витрат, які не піддають своїх операцій додатковим ризикам шляхом інвазивного тестування. Хоча існуючі стандарти та вказівки пропонують вичерпні поради щодо перегляду безпеки інфраструктури ICC, обмеження ресурсів та часу може призвести до неповних оцінок або небажано довгих графіків виконання контрзаходів. У статті [99] розглядається проблема проведення ефективних оцінок ризику кібербезпеки та здійснення пом'якшення наслідків у великих, встановлених операціях ICS, для яких повний огляд безпеки не може бути здійснений у обмежений термін. Внесок - процес протидії кіберзахисту захищеної системи промислового управління (ICS-CDTP). ICS-CDTP визначає пріоритетні райони, де вплив атак найбільший, і де початкові інвестиції швидко зменшують загальну експозицію організації. ICS-CDTP розроблений як попередник більш широкого цілісного огляду впродовж усієї операції, дотримуючись встановлених підходів до управління безпекою. ICS-CDTP - це нова комбінація діамантової моделі аналізу на вторгнення, життєвого циклу атаки та матриці CARVER, що дозволяє ефективно тиражувати вектори атаки та ймовірні цілі для дієздатного антагоніста. ICS-CDTP визначає та фокусує увагу на ключових процесах ICS та їх впливі на кіберзагрози з метою підтримки критичних операцій. У статті визначено ICS-CDTP та наводиться приклад його застосування за допомогою фіктивного очищення води та пояснюється його оцінка як частина масштабної серйозної

гри [99].

Інфраструктури морських портів покладаються на використання інформаційних систем для співпраці, тоді як важливою частиною співпраці є забезпечення кіберзахисту цих систем [100]. Аналіз графіків атак та оцінка ризику надають інформацію, яку можна використовувати для захисту активів мережі від кібератак. Крім того, графіки атак забезпечують функціональність, яку можна використовувати для виявлення вразливих ситуацій в мережі та їх використання потенційними зловмисниками. Існуючі методи генерування графіків атак неадекватні для задоволення певних вимог, необхідних в динамічному середовищі управління ризиками ланцюгів постачання, оскільки вони не враховують змінні, що допомагають досліджувати конкретні мережеві частини, що задовольняють певним критеріям, таким як точки входу та цілі, довжина поширення а також місцезнаходження та можливості потенційного зловмисника. У статті [100] автори представили метод виявлення шляху кібер-атаки, який використовується як складова системи управління морськими ризиками. Метод використовує обмеження та глибинний пошук, щоб ефективно генерувати графіки атак, які зацікавлені адміністратором [100].

Велика увага приділяється питанням інформаційної безпеки в галузі економіки, викликів оптимізації витрат на управління кібер-ризиками, викликів у кількісному оцінці витрат на безпеку, викликів у визначенні оптимального рівня інвестицій у безпеку та ризики та інвестиції в кібербезпеку [101]. У роботі представлені сучасні моделі оптимізації витрат на кібер-ризики, моделі витрат для прогнозування та моделі витрат на інвестиції, тобто визначають, скільки потрібно витратити на кібер-ризик, включаючи рентабельність інвестицій в безпеку (ROSI), чисту присутність вартості (NPV), та внутрішня норма прибутку (IRR). У роботі приводяться моделі прийняття рішень щодо оптимальних стратегій управління ризиками, тобто коли буде досягнута точка зменшення рентабельності інвестицій в кібер-ризики [101].

Велика кількість досліджень, наукових праць, у яких розглянуто напрями вдосконалення процесу розробки та прийняття управлінських рішень на основі застосування інформаційно-комунікативних технологій [102-116].

Порушення кібербезпеки негативно впливають на норму прибутку, ринкову капіталізацію та імідж фірми [117]. Глобальні організації вдаються до використання технологічних пристроїв для зменшення частоти порушень кібербезпеки. Щоб мінімізувати вплив фінансових втрат від порушень кібербезпеки, автори [117] радять використовувати продукти кіберстрахування. У цій статті пропонуються моделі, які можуть допомогти фірмам визначитися з корисністю продуктів кіберстрахування, пропонується мережу Байєсівської віри (CBBN) для оцінки кіберзахищеності та розрахунку очікуваних втрат. Беручи це за основу і використовуючи концепції теорії колективного моделювання ризиків, автори також розраховують кошти, які може стягувати страховик кібер-ризику для відшкодування кібер-збитків. Крім того, для надання допомоги страховикам з кібер-ризику та ефективного проектування продукції пропонується модель пільгового ціноутворення (UBPP) на основі корисних послуг. UBPP враховує профілі ризику та багатство потенційної страхової фірми перед тим, як запропонувати премію [117].

Було здійснено чимало зусиль та досліджень для підвищення безпеки критичної інфраструктури, зокрема [118]. Як одне із зусиль, було створено численні оперативні центри безпеки (SOC) для захисту від кібератак. На жаль, захистити від кібератак занадто важко, оскільки є занадто багато подій безпеки для аналізу та реагування на них. Зменшення подій у сфері безпеки є дуже важливим для підвищення ефективності реагування на інциденти. У роботі [118] автори вивчали кіберзагрози проти корейських електроенергетичних компаній, аналізуючи вихідні дані. В результаті цього аналізу було виявлено, що 95% усіх кібератак походили від іноземних країн. Якщо IT-система не пов’язана із закордонним бізнесом, слід подумати про

блокування непотрібних зовнішніх діапазонів IP. Автори запропонували модель посиленого контролю безпеки (ESC) з процесом блокування пріоритетності (BP) для критичних інфраструктур для покращення щоденних заходів щодо реагування на інциденти. Ця модель має процес блокування пріоритетності із шістьма факторами, які слід враховувати, вирішуючи, які IT-системи блокувати від зовнішніх діапазонів IP: зовнішнє відношення, реальний вхід, складність блокування, толерантність до зупинки, зовнішнє відношення та вплив зупинки. Враховуючи ці шість факторів, модель ESC може дати можливість встановити пріоритет ступеню блокування впливу (BID) IT-систем і допомогти прийняти рішення щодо блокування від непотрібних зовнішніх діапазонів IP. Ця модель ESC зменшить події в галузі безпеки та покращить умови концентрації на решті незаблокованих та важливих IT-систем [118].

Як уже зазначалося вище, на даний час кібербезпека є серйозною проблемою не тільки для систем автоматизації офісу, але і для систем промислового управління (ICS) [119]. Якщо ICS піддаються кібератаці, можуть статися серйозні аварії, такі як вибухи та витоки шкідливих речовин. Тому, кібербезпека є дуже важливим фактором обговорення безпеки та не повинна розглядатися окремо. Як правило, аналіз ризиків проводиться на етапі проектування та експлуатації установки, щоб уникнути ризику експлуатації систем промислового управління. Однак, оскільки традиційні методи аналізу зосереджені на «обладнанні» та «продуктах» заводу, важко розглянути систему верхнього шару. У статті автори пропонують оцінку ризику для безпеки, щоб можна було пов'язати фізичні процеси та системи промислового управління. Автори запропонували метод аналізу ризиків з використанням теоретичної моделі аварійних систем та процесів (STAMP) [119].

Зростає усвідомлення того, що ідентифікація ризику відіграє важливу роль у дослідженні фактичної та потенційної шкоди пацієнтам [120]. Хоча сучасні методи ідентифікації ризику в охороні здоров'я мають сильні сторони

та обмеження, відкритим питанням є те, чи були вони реалізовані оптимально та наскільки добре вони інтегровані для забезпечення повної картини ризику в складних системах охорони здоров’я. Щоб висвітлити це, у статті [120] розглядаються характеристики методів реактивної та проактивної ідентифікації ризиків, а також їх вплив на практику ідентифікації ризиків. Виявлені різні точки навчання з інших галузей, що мають важливе значення для безпеки, і обговорюється інтеграція декількох методів, щоб забезпечити більш всебічний вигляд у сфері управління ризиками. Як особливий приклад, у цій статті розглядається прогностичний метод, розроблений командою майбутньої авіаційної безпеки (FAST), щоб покращити ідентифікацію існуючих ризиків в авіаційній галузі, шляхом виявлення ризиків, які виникають через майбутні зміни. Метод FAST також демонструє інтеграцію методів ідентифікації ризиків, пропонуючи чотири взаємодоповнюючих підходи для використання в авіаційній галузі. Дослідження забезпечує концептуальні рамки, які можуть бути використані в охороні здоров'я для інтеграції декількох методів для прискорення покращення безпеки пацієнтів за допомогою комплексного охоплення системи [120].

У проблемах з оцінкою ризику безпеки часто залучаються численні експерти та декілька критеріїв, а дані оцінки часто даються у вигляді інтервальних чисел [121]. У роботі, в основному, пропонується новий метод побудови матриці ризиків для оцінки ризиків для безпеки в нафтовій і газовій промисловості. Для кращої оцінки ризиків у цій роботі пропонується визначення номера інтервалу з функцією розподілу та функцією корисності. Частота та наслідок ризику - лише два необхідні показники в матриці ризику, і їх значення потрібні у вигляді чітких значень. Таким чином, в цій роботі будується багатоекспертний та багатокритеріальний інформаційний синтез на основі моделі інтервальних номерів (MEMCIF-IN). По-перше, побудована багатоекспертна та багатокритеріальна модель синтезу для об'єднання окремих інтервальних чисел у колективне інтервальне число та інтеграції декількох критеріїв у комплексний індекс. У моделі синтезу ваги експертів з

оцінки розраховуються виходячи з об'єктивних ваг та суб'єктивних ваг одночасно, а інформація про окремі інтервальні числа зберігається без втрати інформації у кінцевому результаті. По-друге, пропонується оператор безперервної зваженої впорядкованої зваженої сукупності (C-WOWA). В операторі C-WOWA одночасно враховуються ваги позиції, які генеруються функцією корисності, і значення ваг, які генеруються функцією щільності ймовірності. Вагові позиції в операторі C-WOWA можуть виправити вплив на позиції експертів щодо ризику, а значення ваг можуть відображати важливість самих точок в інтервальному числі. Нарешті, матриця ризику будується, щоб показати, який ризик високий, а який низький. Крім того, реалізовано додаток, яке показує практичність та раціональність запропонованого способу [121].

Функціонування систем з багатьма водоймами у реальному часі є життєво важливим питанням у галузі управління водоймищами [122]. Невизначеність, спричинена прогнозуванням притоку, означає, що аналіз ризику необхідний для такої операції в режимі реального часу. Однак різниці у тривалості прогнозних періодів для різних водойм у системі рідко враховуються при аналізі ризиків для багатьох водосховищ. У цій статті [122] представлений двоступеневий метод аналізу ризику затоплення багатобазових систем, який враховує різницю в тривалості прогнозного періоду проживання. Метою запропонованого методу є оцінка невизначеності прогнозування повеней шляхом поділу горизонту експлуатації на прогнозний час очікування та поза прогнозний період часу. Ризик у межах прогнозованого часу оцінюється шляхом підрахунку частоти відмов серед усіх сценаріїв за допомогою прогнозів на основі сценарію. Ризик, що перевищує прогнозний часовий період, визначається за допомогою маршрутизації заплави пластів з проектними гідрографами повені, які вибираються відповідно до різниці тривалості прогнозних періодів між будь-якими двома водоймами. Запропонований двоступеневий метод аналізу ризику перевіряється за допомогою методу стохастичного моделювання на

основі вибірки Монте-Карло. Модель операції боротьби з паводком у режимі реального часу встановлюється шляхом використання запропонованого двоступеневого методу аналізу ризиків як обмеження. Запропонований метод розширює наше розуміння управління ризиками для операцій з контролю затоплення в режимі реального часу в системах з багатьма водоймами [122].

Інтеграція обчислювальних і комунікаційних можливостей з електромережою призвела до численних уразливості в кіберфізичній системі (CPS) [123]. Ця загроза кібербезпеці може суттєво вплинути на фізичну інфраструктуру, економіку та суспільство. У традиційних IT-середовищах вже існує безліч випадків нападу, що демонструє, що несанкціоновані користувачі мають можливість доступу та маніпулювання конфіденційними даними із захищеного мережевого домену. Електромережі також сильно прийняли інформаційні технології (IT) для виконання завдань контролю, моніторингу та обслуговування в реальному часі. У статті [123] представлено сучасні найбільш релевантні дослідження кібербезпеки в енергосистемах. У ній розглядається дослідження, яке демонструє ризики кібербезпеки та розробляє рішення для підвищення безпеки електромережі. Для досягнення цієї мети висвітлено: опитування сучасних технологій інтелектуальної мережі, практики та стандарти енергетики, рішення, що стосуються питань кібербезпеки, огляд існуючих тестових панелей CPS для дослідження кібербезпеки та невирішені проблеми кібербезпеки. Дослідження кібербезпеки енергомережі було проведено в Державному університеті штату Вашингтон (WSU) з тестовою панеллю CPS-обладнання в циклі. Крім того, показано, як запропоновані системи можуть бути розгорнуті для захисту електромережі від кібер-зловмисників [123].

Цілісна оцінка ризиків кібербезпеки є складною багатокомпонентною та багаторівневою проблемою, що включає апаратні, програмні, екологічні та людські фактори [124]. У рамках постійних зусиль з розробки цілісної, прогнозної моделі оцінки ризиків кібербезпеки необхідна характеристика людських факторів, що включає поведінку людини, щоб зрозуміти, як дії

користувачів, захисників та зловмисників впливають на ризик кібербезпеки. Робоча група, що розробляли цю нову модель та метод оцінки кібербезпеки, вирішила розрізняти довіру та впевненість, використовуючи «довіру» лише для людських факторів, та «впевненість» для всіх нелюдських факторів (наприклад, апаратного та програмного забезпечення) для того, щоб зменшити плутанину між двома поняттями в цій моделі. Автори розробили початкову основу для того, як включити довіру як фактор / параметр у більш широку характеристику впливу людини (користувачів, захисників та зловмисників) на ризик кібербезпеки. Довіра до людських факторів складається з двох основних категорій: притаманні їм характеристики, те, що є частиною особистості, і ситуативні характеристики, те, що знаходиться поза людиною. Використання довіри як людського чинника в цілісній оцінці ризику кібербезпеки також залежатиме від розуміння того, як різні ментальні моделі та позиції ризику впливають на рівень довіри, що надається людині, і на упередження, що впливають на здатність надавати довіру [124].

Важливе значення має співвідношення характеристики людини з намірами поведінки в кібербезпеці [125]. Автори представляють всебічне дослідження, яке вивчає, як переваги прийняття ризику, стилі прийняття рішень, демографічні ознаки та особливості особистості впливають на поведінку безпеки на захист пристрою, пароль покоління, активна обізнаність та оновлення. Було проведено опитування 369 студентів, викладачів та співробітників у великому державному університеті та виявили, що індивідуальні відмінності становлять 5% -23% відхилення в намірах поведінки в кібербезпеці. Такі характеристики, як прийняття фінансових ризиків, раціональне прийняття рішень, екстраверсія та гендерна ознака, були визнані важливими унікальними прогнозами гарної поведінки в безпеці. Дослідження виявило як валідацію, так і протиріччя супутньої роботи на додаток до пошуку раніше не повідомлених кореляцій. Показано, як вплив індивідуальних відмінностей на наміри поведінки в безпеці може бути специфічним для навколишнього середовища. Таким чином, деякі

рішення щодо безпеки повинні також залежати від навколишнього середовища [125].

Ключовим елементом удосконалення є визнання важливості поведінки людини під час проектування, побудови та використання технології кібербезпеки [126]. У статті автори описують, чому включення розуміння поведінки людини в продукти та процеси кібербезпеки може призвести до більш ефективної технології. Наведено два приклади: перший демонструє, як використання науки про поведінку призводить до явних поліпшень, а другий ілюструє, як поведінкова наука пропонує потенціал для значного підвищення ефективності кібербезпеки. На основі зворотного зв'язку, зібраного практикуючими на попередніх інтерв'ю, увага акцентується на двох важливих поведінкових аспектах: когнітивне навантаження та упередженість. Далі визначаються перевірені та потенційні результати науки про поведінку, які мають значення для кібербезпеки, пов'язані не лише з когнітивним навантаженням та упередженістю, але й з евристикою та моделями науки про поведінку [126].

Перехід від послідовної комунікації «точка до точки» до мереж традиційних інформаційних технологій (IT) створив нові проблеми в забезпеченні кібербезпеки для систем контролю та збору даних (SCADA) в критичній інфраструктурі [127]. Поточні дослідження ландшафту атаки для критичної інфраструктури зосереджені на атаках, що базуються на IT, або на протоколах. Тим не менш, обмежений фокус на дослідженні на «більшій картині», поєднанні IT-атак та критичних інфраструктурних протокольних атак та мало уваги до кібератак, спрямованих на всю критичну інфраструктурну систему на базі SCADA. Через такі вузькі дослідження виникає повна відсутність уваги при осмисленні повномасштабних кібератак на критичні інфраструктурні системи на базі SCADA. Як результат, нові атаки, що поєднують різні вразливості в інженерних системах та IT-системах, ще не розкриті. У роботі [127] автори зіставили наявні відомі атаки, виявили та об'єднали існуючий діапазон ландшафтів атаки, розширили та «заповнили

прогалини» у ландшафті, тим самим представивши повну структуру кібератаки, яка сприймає напади на всю критичну інфраструктуру на базі SCADA. Ця структура визначає чотири типи атак, традиційні атаки на основі IT, атаки, характерні для протоколу, атаки на основі конфігурації та атаки управління процесом, що дозволяє нам описати практичні атаки. Перевага розпізнавання діапазону атак на цілі критичні системи полягає в тому, що це дозволяє захищатись від атак із значно більшою ефективністю та інтелектом [127].

Проведений аналіз методів оцінки ризиків інформаційної безпеки показав [128], що метод на основі побудови «Матриці СУІБ» дозволяє оцінити ступінь захисту вже існуючої СЗІ та ступінь виконання всіх вимог по забезпеченню інформаційної безпеки. Однак, даний метод не завжди застосуємо до інформаційної системі, яка створюється. Також для удосконалення даного методу необхідно додати декілька якісних шкал або можливість самостійно створювати шкали за обраним критерієм оцінювання. Метод оцінки ризиків інформаційної безпеки на основі теорії нечітких множин навіть при недостатньому обсязі вхідних даних дозволяє побудувати адекватну модель впливу загроз на ресурс, який підлягає захисту. При цьому можливо розглядати кілька розгалужень реалізації загрози або безлічі загроз на ресурс. Таким чином, можна оцінити найбільш ймовірні загрози на ІС і, на базі отриманої інформації, створити або модернізувати систему захисту інформації. Однак і цей метод має свої недоліки, оскільки не враховує час реалізації загрози, а бере до уваги тільки суб'єктивну ймовірність реалізації загрози або безлічі загроз. Реалізація загрози може зайняти час більший, ніж інформаційний ресурс буде мати цінність. Тому, для вдосконалення даного методу пропонується ввести коефіцієнт нормування за часом згідно з думкою експерта при складанні опитувальних листів і проведенні оцінювання ризиків ІБ [128].

Так, у [129] показано, що незважаючи на те, що просування в галузі інформаційних технологій підвищило ефективність транспортної

інфраструктури, це, у свою чергу, створило більш високий ризик, пов'язаний з кіберсистемами. Мета цього дослідження - інформувати транспортну політику та управління в США шляхом виявлення перешкод на надійному ринку кіберстрахування та підвищення кіберстійкості транспортної інфраструктури. Це здійснюється за допомогою змішаного підходу, що включає аналіз даних про кіберінциденти в США для транспортних систем та серію інтерв'ю з менеджерами транспортної інфраструктури та страховиками. Внески включають нові погляди на природу кібер-ризику для транспортної інфраструктури та рекомендації щодо науково-дослідних потреб для покращення управління кібер-ризиками та страхування. Результати показують, що щорічно збільшується кількість транспортних компаній, що постраждали від кіберінцидентів та пов'язаних з цим витрат. Найчастіші випадки пов'язані з порушенням даних, тоді як випадки порушення конфіденційності мають найвищий середній збиток за інцидент. Оцінка кібер-ризиків, заходи щодо пом'якшення наслідків та безпеки та страхування в різній мірі впроваджуються в транспортних інфраструктурних системах, але, як правило, недостатньо. Наразі менеджери інфраструктури не мають інструментів для жорсткої оцінки та управління кібер-ризиком. Обмежені дані та моделі також гальмують точне моделювання кібер-ризику для страхових цілей. Навіть після розробки вдосконалених інструментів та моделювання придбання страхування може стати важливою стратегією управління ризиками, щоб дати змогу системам транспортної інфраструктури відновитися після кібер-інцидентів [129].

В розглянутих джерелах 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. 1.3) 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.

Таблиця 1.3

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	+	–	–	–	–	–	–
Delphi method	+	–	–	–	–	–	–

Продовження табл. 1

Checklist	+	–	–	–	–	–	–
PHA	+	–	–	–	–	–	–
HAZOP	+	+	+	+	+	–	–
HACCP	+	+	–	+	+	–	–
Toxicity assessment	+	+	+	+	+	–	–
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	+	–	+	–	+	–	–

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.

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.

1.3. Формулювання наукової проблеми і задач досліджень

Виходячи з вищевикладеного, мету і задачі дисертаційної роботи можна сформулювати в наступному.

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.

1.4. Висновки до першого розділу

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. Проведений аналіз та дослідження нормативних документів дають можливість визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завданням із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи

створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту.

3. Дослідження існуючих методів оцінювання ризиків 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.

4. 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, що враховував би вплив людського чиннику.

Основні результати дисертаційної роботи, представлені в розділі 1, опубліковані в працях автора [7-21].

Список використаних джерел до першого розділу

1. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] // Закон України. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19.

2. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації [Електронний ресурс] // Указ Президента України від 13.02.2017 року № 32/2017. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/n0015525-16#n2.

3. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] // Постанова КМ України від 19.06.2019 р. № 518. – 2019. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8.

4. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави

[Електронний ресурс] // Постанова КМ України від 23.08.2016 р. № 563. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF.

5. Стратегія національної безпеки України [Електронний ресурс] // Указ Президента України від 26.05.2015 року № 287/2015. – 2015. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/287/2015#n14.

6. Доктрина інформаційної безпеки України [Електронний ресурс] // Указ Президента України від 25.02.2017 року № 47/2017. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/47/2017.

7. Гончар С.Ф. Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. - №1(25). С. 158-163.

8. Гончар С.Ф. Структура модели интеллектуальных электроэнергетических систем, учитывающая необходимость обеспечения их кибербезопасности / Юдін О.Ю., Леоненко Г.П., Гончар С.Ф. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. - №1(27). – С. 60-69.

9. Гончар С.Ф. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Вісник Національного університету «Львівська політехніка» «Комп’ютерні системи та мережі». – 2014. - №806. – С. 34-39.

10. Гончар С.Ф. Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури / Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №80. – С. 27-32.

11. Гончар С.Ф. Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №81. – С. 12-19.

12. Гончар С.Ф. Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об’єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф., Ониськова А.В. // Моделювання та інформаційні технології. – 2017. - №82. – С. 40-48.

13. Гончар С.Ф. Концепція створення автоматизованої системи управління кібербезпекою об’єктів критичної інфраструктури / Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №83. – С. 70-76.

14. Гончар С.Ф. Актуальность исследования и разработки систем защиты информации территориально-распределенных автоматизированных систем управления технологическими процессами : праці міжнародної науково-практичної конференції «Кібербезпека-2013», Ялта, – 2013. – С. 33-37.

15. Гончар С.Ф. Особенности обеспечения кибербезопасности индустриальных систем управления : тези доповідей міжнародної науково-практичної конференції «Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК», Київ, – 2013. – С. 36-37.

16. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв’язання», Київ, 2014. – С. 92-95.

17. Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Соціокультурний аспект забезпечення інформаційної безпеки об’єктів критичної інфраструктури : тези доповідей XX Всеукраїнської науково-практичної конференції «Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення», Житомир, 2014. – С. 195-196.

18. Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Забезпечення інформаційної безпеки об’єктів критичної інфраструктури України : наукові доповіді та тези учасників науково-технічної конференції «Інформаційна безпека України», Київ, 2015. – С. 95-96.

19. Гончар С.Ф., Леоненко Г.П., Левченко С.М. Критерії віднесення

об’єктів до критичної інфраструктури з урахуванням світового досвіду : наукові доповіді та тези учасників науково-технічної конференції «Інформаційна безпека України», Київ, 2016. – С. 40-41.

20. Гончар С.Ф., Леоненко Г.П., Ткаченко В.В. Пріоритетні напрями розвитку нормативно-правового забезпечення інформаційної безпеки критичної інфраструктури України. : наукові доповіді та тези учасників науково-технічної конференції «Інформаційна безпека України», Київ, 2016. – С. 41-42.

21. Гончар С.Ф., Комаров М.Ю., Леоненко Г.П. Система управління інформаційною безпекою. Аналіз нормативної бази : Матеріали XX Ювілейної Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», 2018р., Київ, 2018. – С. 250-251.

22. Робота ОЕС [Електронний ресурс] / Укренерго – Режим доступу до ресурсу: https://ua.energy/diyalnist/dyspetcherska-informatsiya/robota-oes-ukrayiny-za-tyzhden/.

23. Розробка методів оцінювання чутливості об’єднаної енергосистеми України до кібернетичних впливів. Звіт (проміжний) з НДР (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320), К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2018. – 113 с.

24. Martin Eling. What are the actual costs of cyber risk events? / Martin Eling, Jan Wirfs. // European Journal of Operational Research. – 2019. – №272. – С. 1109–1119.

25. Future developments in cyber risk assessment for the internet of things / Petar Radanliev, David Charles De Roure, Razvan Nicolescu та ін.]. // Computers in Industry. – 2018. – №102. – С. 14–22.

26. Connected and autonomous vehicles: A cyber-risk classification framework / Barry Sheehan, Finbarr Murphy, Martin Mullins, Cian Ryan. // Transportation Research Part A: Policy and Practice. – 2019. – №124. – С. 523–536.

27. Is the responsibilization of the cyber security risk reasonable and judicious? / Karen Renaud, Stephen Flowerday, Merrill Warkentin та ін.]. // Computers & Security. – 2018. – №78. – С. 198–211.

28. Keyun Ruan. Chapter 4 - Cyber Risk Measurement in the Hyperconnected World / Keyun Ruan. // Digital Asset Valuation and Cyber Risk Management. – 2019. – С. 75–86.

29. A cyber risk scoring system for medical devices / Ian Stine, Mason Rice, Stephen Dunlap, John Pecarina. // International Journal of Critical Infrastructure Protection. – 2017. – №19. – С. 32–46.

30. Shaun S. Wang. Integrated framework for information security investment and cyber insurance / Shaun S. Wang. // Pacific-Basin Finance Journal. – 2019. – №57. – С. 101–173.

31. Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks / Zang Tianlei, Gao Shibin, Liu Baoxu та ін.]. // Reliability Engineering & System Safety. – 2019. – №189. – С. 232–241.

32. Cyber risk assessment in cloud provider environments: Current models and future needs / Olusola Akinrolabu, Jason R.C. Nurse, Andrew Martin, Steve New. // Computers & Security. – 2019. – №87. – С. 101–106.

33. Andrii Boiko. Information systems for supply chain management: uncertainties, risks and cyber security / Andrii Boiko, Vira Shendryk, Olha Boiko. // Procedia Computer Science. – 2019. – №149. – С. 65–70.

34. Зуб А.Т. Принятие управленческих решений. Теория и практика: учебное пособие для студентов вузов / А. Т. Зуб. –М.: ФОРУМ: ИНФРА-М, 2010. –400 с.

35. Смирнов Э.А. Управленческие решения: учебник для студентов вузов / Э. А. Смирнов. –М.: РИОР, 2010. –362 с.

36. Фатхутдинов Р.А. Управленческие решения: учебник для студ. вузов / Р. А. Фатхутдинов. -6-е изд., перераб. и доп. –М.: ИНФРА-М, 2009. – 344 с.

37. Филинов Н.Б. Разработка и принятие управленческих решений: учебное пособие / Н. Б. Филинов; Высшая школа менеджмента, Гос. ун-т – Высшая школа экономики. –М.: ИНФРА-М, 2009. – 308 с.

38. Саак А.Э., Тюшняков В.Н. Разработка управленческого решения: Учебник для вузов / А.Э. Саак, В.Н. Тюшняков. –СПб.: Питер, 2007. –272 с.

39. Абчук В.А. Лекции по менеджменту: Решение. Предвидение. Риск / В. А. Абчук. –СПб.: Союз, 1999. –335с.

40. Балдин К.В. Управленческие решения: учебник для студ. вузов / К. В. Балдин, С. Н. Воробьев, В. Б. Уткин. - 4-е изд. –М.: Дашков и Ко, 2007. – 496 с.

41. Барышников Ю.Н. Разработка управленческого решения: учебно-методическое пособие / Ю. Н. Барышников ; Рос. акад. гос. службы при Президенте РФ. –М.: РАГС, 2009. –100 с.

42. Баттрик Р. Техника принятия эффективных управленческих решений / Р. Баттрик; пер. с англ. под ред. В. Н. Фунтова. - 2-е изд. - СПб.: Питер, 2006. –416 с.

43. Бирман Л.А. Управленческие решения: учебное пособие для вузов / Л. А. Бирман; Ин-т бизнеса и делового администрирования (ИБДА). –М.: Дело, 2004. –208 с.

44. Вертакова Ю.В. Управленческие решения: разработка и выбор: учебное пособие для студ. вузов / Ю. В. Вертакова, И. А. Козьева, Э. Н. Кузьбожев. –М.: КНОРУС, 2005. –352 с.

45. Гайдаенко Т.А. Маркетинговое управление. Полный курс MBA. Принципы управленческих решений и российская практика: учебник для студ. вузов / Т. А. Гайдаенко. - 3-е изд., перераб. и доп. –М.: Эксмо, 2008. – 512 с.

46. Глущенко В.В. Разработка управленческого решения: прогнозирование-планирование: теория проектирования экспериментов / В. В. Глущенко, И. И. Глущенко. –Железнодорожный: Крылья, 1997. –400с.

47. Голубков Е.П. Технология принятия управленческих решений / Е.

П. Голубков. –М.: Дело и Сервис, 2005. –544 с.

48. Екатеринославский Ю.Ю. Управленческие ситуации: анализ и решения / Ю. Ю. Екатеринославский. –М.: Экономика, 1988. –191с.

49. Improving risk assessment model of cyber security using fuzzy logic inference system / Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan та ін.]. // Computers & Security. – 2018. – №74. – С. 323–339.

50. Keyun Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk / Keyun Ruan. // Computers & Security. – 2017. – №65. – С. 77–89.

51. Tim Brown. Are miserly budgets putting businesses at risk of cyber-attack? / Tim Brown. // Computer Fraud & Security. – 2018. – №8. – С. 9–11.

52. A framework for incorporating insurance in critical infrastructure cyber risk strategies / Derek Young, Juan Lopez Jr., Mason Rice та ін.]. // International Journal of Critical Infrastructure Protection. – 2016. – №14. – С. 43–57.

53. Developing cyber peacekeeping: Observation, monitoring and reporting / Michael Robinson, Kevin Jones, Helge Janicke, Leandros Maglaras. // Government Information Quarterly. – 2019. – №36. – С. 276–293.

54. Risk perceptions of cyber-security and precautionary behaviour / Paul van Schaik, Debora Jeske, Joseph Onibokun та ін.]. // Computers in Human Behavior. – 2017. – №75. – С. 547–559.

55. Ерофеева В.А. Учет, информация, управление: прямые и обратные связи / В.А.Ерофеева. –М.: Финансы и статистика, 1992. –192с.

56. Иванов А.И., Малявина А.В. Разработка управленческих решений: Учебное пособие по спец. «Менеджмент». – М.: Изд-во Моск. акад. экон. и права: Калита, 2000. –111с.

57. Ивасенко А.Г. Разработка управленческих решений: учебное пособие для студентов вузов / А. Г. Ивасенко, Я. И. Никонова, Е. Н. Плотникова. - 2-е изд., перераб. и доп. –М.: КНОРУС, 2010. –168 с.

58. Истомин Е.П. Управленческие решения: учебник для студ. вузов / Е. П. Истомин, А. Г. Соколов; Балтийский ин-т управления. –СПб.:

Андреевский изд. дом, 2005. –248 с.

59. Карданская Н.Л. Основы принятия управленческих решений: учебное пособие / Н. Л. Карданская. –М.: Рус. Деловая Лит., 1998. –288с.

60. Карданская Н.Л. Принятие управленческого решения: учебник для вузов / Н. Л. Карданская. –М.: ЮНИТИ, 1999. –407с.

61. Карпов А.В. Психология принятия управленческих решений / А. В. Карпов; под ред. В. Д. Шадрикова. –М.: Юристъ, 1998. –440с.

62. Кодин В.Н. Как работать над управленческим решением: учебное пособие для студ. вузов / В. Н. Кодин, С. В. Литягина. –М.: КНОРУС, 2009. – 192 с.

63. Комаров Е.И. Общий менеджмент: учебное пособие / Е. И. Комаров; Акад. народ. хозяйства при Правительстве РФ. –М.: РИОР: ИНФРА-М, 2010. –269 с.

64. Ларичев О.И. Теория и методы принятия решений, а также Хроника событий в Волшебных Странах: учебник / О.И. Ларичев. –М.: Логос, 2000. – 296 с.

65. Литвак Б.Г. Разработка управленческого решения: учебник для студ. вузов / Б. Г. Литвак ; Академия нар. хозяйства при правительстве Рос. Федерации. - 5-е изд., испр. и доп. –М.: Дело, 2004. –416 с.

66. Литвак Б.Г. Практические занятия по управлению: Мастер-класс / Б.Г.Литвак. –М.: Экономика, 2002. –354с.

67. Литвак Б.Г. Управленческие решения: Учебник / Б.Г.Литвак. –М.: ЭКМОС, 1998. –248с.

68. Лифшиц А.С. Управленческие решения: учебное пособие для студ. вузов / А. С. Лифшиц. –М.: КНОРУС, 2009. –248 с.

69. Лукашевич В.В. Основы менеджмента: Учебное пособие для учащихся сред. проф. учеб. заведений / В.В.Лукашевич. –М.: ЮНИТИ-ДАНА, 2004. –285с.

70. Eric B. Rice. Mitigating the Risk of Cyber Attack on Smart Grid Systems / Eric B. Rice, Anas Al Majali. // Procedia Computer Science. – 2014. –

№28. – С. 575–582.

71. Jinsoo Shin. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET / Jinsoo Shin, Hanseong Son, Gyunyoung Heo. // Nuclear Engineering and Technology. – 2017. – №49. – С. 517–524.

72. Dipak Kumar Jana. Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security / Dipak Kumar Jana, Ramkrishna Ghosh. // Journal of Information Security and Applications. – 2018. – №40. – С. 173–182.

73. Erica D. Borghard. Can States Calculate the Risks of Using Cyber Proxies? / Erica D. Borghard, Shawn W. Lonergan. // Orbis. – 2016. – №60. – С. 395–416.

74. Jangirala Srinivas. Government regulations in cyber security: Framework, standards and recommendations / Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar. // Future Generation Computer Systems. – 2019. – №29. – С. 178–188.

75. Joe Kim. Cyber-security in government: reducing the risk / Joe Kim. // Computer Fraud & Security. – 2017. – №7. – С. 8–11.

76. Лукичева Л.И. Управленческие решения: учебник для студентов вузов / Л. И. Лукичева, Д. Н. Егорычев ; под ред. Ю. П. Анискина. - 5-е изд., стер. –М.: Омега-Л, 2010. –384 с.

77. Мадера А.Г. Моделирование и принятие решений в менеджменте: руководство для будущих топ-менеджеров / А. Г. Мадера. –М.: ЛКИ, 2010. – 688 с.

78. Менеджмент: учебник для студентов вузов / А. Н. Алексеев, Е. С. Бурыкин, О. И. Горелов и др.; под общ. ред. И. Н. Шапкина. –М.: Юрайт: ИД Юрайт, 2011. –690 с.

79. Организационная психология / Сост. Л.В.Винокуров, И.И.Скрипюк. –СПб.: Питер, 2001. –511с.

80. Орлов А.И. Принятие решений. Теория и методы разработки управленческих решений: учебное пособие для студ. вузов / А. И. Орлов. –

М.; Ростов н/Д: МарТ, 2005. –496 с.

81. Принятие решений [Электронный ресурс] / Разраб. корпорации «Диполь». - Электрон. дан. –М.: Равновесие-медиа, 2002. - 1 CD-ROM - (Бизнес-школа).

82. Пужаев А.В. Управленческие решения: учебное пособие для студ. / А. В. Пужаев. –М.: КНОРУС, 2010. –192 с.

83. Райн Б. Стратегический учет для руководителя / Б. Райн; Пер. с англ. под ред. В. А. Микрюкова. –М.: Аудит: ЮНИТИ, 1998. – 616с.

84. Рапопорт Б.М. Оптимизация управленческих решений / Б. М. Рапопорт. –М.: ТЕИС, 2001. –264с.

85. Ременников В.Б. Разработка управленческого решения: учебное пособие для вузов / В. Б. Ременников. –М.: ЮНИТИ-ДАНА, 2000. –140с.

86. Ременников В.Б. Управленческие решения: учебное пособие для вузов / В. Б. Ременников. - 2-е изд., перераб. и доп. –М.: ЮНИТИ-ДАНА, 2005. –144 с.

87. Розанова В.А. Психология управления: учебное пособие / В. А. Розанова. - 2-е изд., перераб. и доп. –М.: Бизнес-школа Интел-Синтез, 2000. – 384с.

88. Смит Джейн. 30 минут для выбора правильного решения / пер. с англ. П. Быстров. –М.: ЛОРИ, 2001. –80с.

89. Созинов В.А. Управленческие решения: учебное пособие для студ. вузов / В. А. Созинов. –Владивосток: Изд-во ВГУЭС, 2003. –200с.

90. Созинов В.А. Разработка управленческого решения: конспект лекций. Ч. 1. / В. А. Созинов. –Владивосток: Изд-во ВГУЭС, 1998. –75с.

91. A review of cyber security risk assessment methods for SCADA systems / Yulia Cherdantseva, Pete Burnap, Andrew Blyth та ін.]. // Computers & Security. – 2016. – №56. – С. 1–27.

92. Cyber security of critical infrastructures / Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke та ін.]. // ICT Express. – 2018. – №4. – С. 42–45.

93. Cheol-Kwon Lee. Introduction of a Cyber Security Risk Analysis and

Assessment System for Digital I&C Systems in Nuclear Power Plants / Cheol-Kwon Lee. // IFAC Proceedings Volumes. – 2013. – №46. – С. 2140–2144.

94. Development of a cyber security risk model using Bayesian networks / Jinsoo Shin, Hanseong Son, Rahman Khalil, Gyunyoung Heo. // Reliability Engineering & System Safety. – 2015. – №134. – С. 208–217.

95. Jong Woo Park. Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants / Jong Woo Park, Seung Jun Lee. // Nuclear Engineering and Technology. – 2019. – №51. – С. 138–145.

96. Joon-Eon Yang. Multi-unit risk assessment of nuclear power plants: Current status and issues / Joon-Eon Yang. // Nuclear Engineering and Technology. – 2018. – №50. – С. 1199–1209.

97. Dynamic risk management response system to handle cyber threats / G. Gonzalez-Granadillo, S. Dubus, A. Motzek та ін.]. // Future Generation Computer Systems. – 2018. – №83. – С. 535–552.

98. Meir Kalech. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques / Meir Kalech. // Computers & Security. – 2019. – №84. – С. 225–238.

99. The industrial control system cyber defence triage process / Allan Cook, Helge Janicke, Richard Smith, Leandros Maglaras. // Computers & Security. – 2017. – №70. – С. 467–481.

100. Cyber-attack path discovery in a dynamic supply chain maritime risk management system / Nikolaos Polatidis, Michalis Pavlidis, HaralambosMouratidis. // Computer Standards & Interfaces. – 2018. – №56. – С. 74–82.

101. Keyun Ruan. The Point of Diminishing Return on Cyber Risk Investment / Keyun Ruan. // Digital Asset Valuation and Cyber Risk Management. – 2019. – С. 99–115.

102. Созинов В.А. Разработка управленческого решения: конспект лекций. Ч. 2. / В. А. Созинов. –Владивосток: Изд-во ВГУЭС, 1998. –76с.

103. Травин В.В. Подготовка и реализация управленческих решений:

учебно-практическое пособие / В. В. Травин, М. И. Магура, М. Б. Курбатова. –М.: Дело, 2004. –80 с.

104. Тронин Ю.Н. Управленческие решения: учебное пособие для вузов / Ю. Н. Тронин, Ю. С. Масленченков. –М.: ЮНИТИ-ДАНА, 2004. –310 с.

105. Трояновский В.М. Разработка управленческого решения: учебное пособие / В. М. Трояновский. –М.: РДЛ, 2003. –208с.

106. Уваров В. В. Стратегический менеджмент и глобализация мировой экономики: Учебное пособие / В.В.Уваров, И.Н.Пятибратов. –М.: Изд-во Междунар. ун-та бизнеса и упр.: МЗ-Пресс, 2001. –281с.

107. Управление и контроль реализации социально-экономических целевых программ: [монография] / под ред. В. В. Кульбы, С. С. Ковалевского; Ин-т проблем управления им. В. А. Трапезникова РАН. –М.: ЛИБРОКОМ, 2009. –400 с.

108. Урубков А.Р. Курс MBA по оптимизации управленческих решений: практическое руководство по использованию моделей линейного программирования / А. Р. Урубков. –М.: Альпина Бизнес Букс, 2006. –176 с.

109. Учитель Ю.Г. Разработка управленческих решений: учебник для студ. вузов / Ю. Г. Учитель, А. И. Терновой, К. И. Терновой. - 2-е изд., перераб. и доп. –М.: ЮНИТИ-ДАНА, 2007. –383 с.

110. Хайниш С.В. Нестандартные ситуации: практикум для хозяйственных руководителей / С.В. Хайниш. –М.: Экономика, 1992. –206с.

111. Цветков А.Н. Методы решения творческих задач: учебно-практ. пособие / А. Н. Цветков, В. Е. Заремба. –М.: КНОРУС, 2009. –152 с.

112. Цыгичко В.Н. Руководителю - о принятии решений / В.Н.Цыгичко. - 2-е изд., испр. и доп. –М.: ИНФРА-М, 1996. –272с.

113. Чавкин А.М. Методы и модели рационального управления в рыночной экономике: разработка управленческих решений: учебное пособие / А. М. Чавкин. –М.: Финансы и статистика, 2001. –317с.

114. Чудновская С.Н. Управленческие решения: учебник для студ.

вузов / С. Н. Чудновская. –М.: Эксмо, 2007. –368 с.

115. Экономическая эффективность управленческих и хозяйственных решений: Справочник / Сост. Е.Г. Яковенко, В.Ф. Гапоненко, Ю.С. Карабасов. –М.: Знание, 1984. –200с.

116. Юкаева В.С. Управленческие решения: учебное пособие для студ. вузов / В. С. Юкаева. - 4-е изд. –М.: Дашков и Ко, 2009. –324 с.

117. Cyber-risk decision models: To insure IT or not? / Arunabha Mukhopadhyay, Samir Chatterjee, Debashis Saha та ін.]. // Decision Support Systems. – 2013. – №56. – С. 11–26.

118. Han Choong-Hee. The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system / Han Choong-Hee, Park Soon-Tai, Lee Sang-Joon. // International Journal of Critical Infrastructure Protection. – 2019. – №26. – С. 100–112.

119. An application of STAMP to safety and cyber security for ICS / Shun Kondo, Hiroto Sakashita, Souta Sato та ін.]. // Computer Aided Chemical Engineering. – 2018. – №44. – С. 2335–2340.

120. Integration of multiple methods in identifying patient safety risks / M.C. Emre Simsekler, Ayse P. Gurses, Brian E. Smith, Al Ozonoff. // Safety Science. – 2019. – №118. – С. 530–537.

121. A MEMCIF-IN method for safety risk assessment in oil and gas industry based on interval numbers and risk attitudes / Donghong Tian, Chunlan Zhao, Bing Wang, Meng Zhou. // Engineering Applications of Artificial Intelligence. – 2019. – №85. – С. 269–283.

122. Real-time reservoir flood control operation for cascade reservoirs using a two-stage flood risk analysis method / Xiaoqi Zhang, Pan Liu, Chong-Yu Xu та ін.]. // Journal of Hydrology. – 2019. – №577. – С. 123–154.

123. Chih-Che Sun. Cyber security of a power grid: State-of-the-art / Chih-Che Sun, Adam Hahn, Chen-Ching Liu. // International Journal of Electrical Power & Energy Systems. – 2018. – №99. – С. 45–56.

124. Trust as a Human Factor in Holistic Cyber Security Risk Assessment /

D. Henshel, M.G. Cains, B. Hoffman, T. Kelley. // Procedia Manufacturing. – 2015. – №3. – С. 1117–1124.

125. Correlating human traits and cyber security behavior intentions / Margaret Gratian, Sruthi Bandi, Michel Cukier та ін.]. // Computers & Security. – 2018. – №73. – С. 345–358.

126. Shari Lawrence Pfleeger. Leveraging behavioral science to mitigate cyber security risk / Shari Lawrence Pfleeger, Deanna D. Caputo. // Computers & Security. – 2012. – №31. – С. 597–611.

127. Nicholas R. Rodofile. Extending the cyber-attack landscape for SCADA-based critical infrastructure / Nicholas R. Rodofile, Kenneth Radke, Ernest Foo. // International Journal of Critical Infrastructure Protection. – 2019. – №25. – С. 14–35.

128. А.А. Замула. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации / А.А. Замула, А.В. Северинов, М.А. Корниенко. // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – №2. – С. 133–138.

129. Cyber risk and insurance for transportation infrastructure / Gina Tonn, Jay P. Kesan, Linfeng Zhang, Jeffrey Czajkowski. // Transport Policy. – 2019. – №79. – С. 103–114.

РОЗДІЛ 2
КІБЕРЗАГРОЗИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ОЦІНКА НЕБЕЗПЕКИ ЇХ РЕАЛІЗАЦІЇ

2.1. Модель загроз інформаційних систем об'єктів критичної інфраструктури до кібератак

На сьогоднішній день інформаційна безпека держави визначається, в тому числі, рівнем інформаційної безпеки існуючих складних людино-машинних систем управління об'єктами технічних, технологічних, організаційних і економічних комплексів країни – автоматизованих систем управління технологічними процесами (АСУ ТП) [6], [7].

І якщо, спочатку зазначені системи були у вигляді окремого комп'ютера із власними операційними системами і мережами, то розвиток та поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж дає можливість забезпечувати управління виробничою діяльністю в режимі реального часу, здійснювати дистанційний моніторинг систем управління технологічним процесом, підвищити безпеку підприємства і персоналу, зменшити витрати на експлуатацію.

Однак, ціною цих переваг являється підвищена уразливість до нового типу загроз інформаційної безпеки АСУ ТП – злому і порушення режимів функціонування ключових об'єктів, які відповідають за управління та забезпечення безпеки об'єктів критичної інфраструктури, до яких можна віднести: атомні і гідроелектростанції, нафто - і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня тощо. І від інформаційної безпеки систем управління подібними об'єктами залежить не тільки прибуток компаній, але й національна безпека.

Забезпечення інформаційної безпеки, яка включає в себе в якості основних складових духовно-світоглядну, архетипічну, соціально-моральну,

психічну, інтелектуальну і психофізіологічну безпеку, являє собою актуальну військово-політичну, наукову і соціально-економічну проблему [8]. На думку деяких фахівців [9], [10], наукове вирішення даної проблеми повинно базуватися на дослідженні відповідних інформаційних відносин активних компонентів вказаних систем, якими є обслуговуючий персонал, з відповідними активними компонентами конфронтуючих систем і між собою. Інформаційні відносини активних об’єктів в різних інформаційних середовищах (природних, штучних, гібридних) повинні включати відносини інформаційного відокремлення (ізоляції та захисту) і взаємодії (суперництво та співробітництво).

Крім того, деякі автори [11] висловлюють думку, що на даний час все більше зростає роль людського фактору на інформаційну безпеку АСУ ТП при недостатній кількості методів і засобів його оцінки та захисту. Засоби і методи, які наразі розробляються (наприклад, метод інженерної психології) дають змогу зменшити рівень помилкової інформації, але не досліджують проблему у цілому, в тому числі не проводять оцінку і захист, як від випадкових, так і від умисних деструктивних дій обслуговуючого персоналу.

При цьому, людський фактор являється одночасно і необхідним елементом людино-машинних систем управління і джерелом загроз інформаційній безпеці таких систем, рис. 2.1.

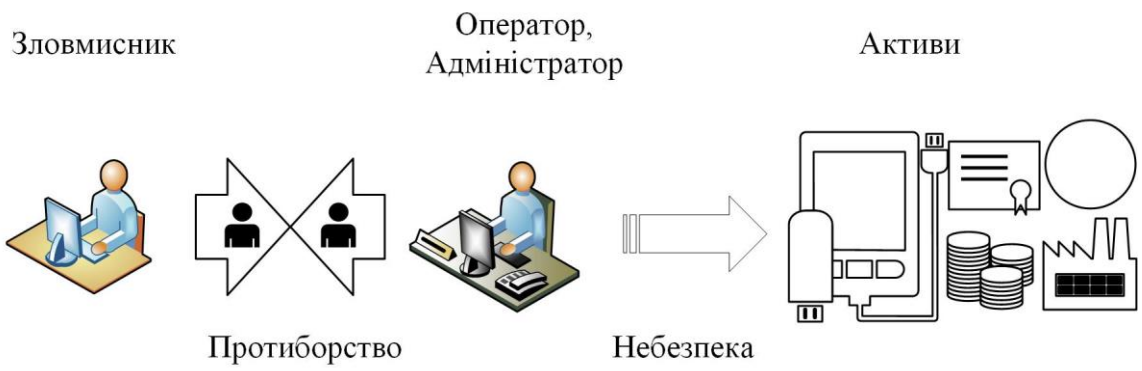


Рис. 2.1. Об’єктивне протиріччя

Таким чином, основними об’єктами інформаційно-психологічного впливу в АСУ ТП являється обслуговуючий персонал і особа, яка приймає рішення щодо управління процесами в тій чи іншій предметній області [11].

В складних людино-машинних системах управління персоналу доводиться приймати ті чи інші рішення. При цьому, на адекватність прийнятих рішень персоналом в таких системах можуть впливати такі фактори [10]: зовнішні та внутрішні дестабілізуючі впливи, нестійкість рішення при великій кількості альтернатив, тривалість часового інтервалу для прийняття рішення.

Враховуючи викладене, можна зазначити, що важливою задачею являється прийняття адекватних рішень обслуговуючим персоналом в різних інформаційних середовищах і відносинах. Для цього актуальним є отримання моделі імовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки.

Кількість альтернатив і тривалість часового інтервалу для прийняття рішення буде залежати від технологічних особливостей конкретної системи і вплив даних факторів може призвести до ненавмисних помилкових дій персоналу. В той же час, дія зовнішніх та/або внутрішніх дестабілізуючих впливів може призвести до навмисних деструктивних дій персоналу. Загальна схема дії таких чинників приведена на рис. 2.2. Розглянемо більш детально, що собою являє кожний з наведених чинників.

Під зовнішнім дестабілізуючим впливом $s=\overline{1,S}$ будемо розуміти множину загроз реалізації інформаційно-психологічного впливу на обслуговуючий персонал АСУ ТП. Такі впливи можуть мати на меті дезорієнтацію, дезінформацію, дезорганізацію, придушення, руйнування тощо. Виділяють п’ять відповідних груп засобів, які можуть бути застосовані для інформаційно-психологічного впливу на персонал людино-машинних систем управління [9]:

- засоби масової інформації, агітаційно-пропагандистські засоби;
- психотронні засоби;

- електронні засоби: радіоелектронні, оптикоелектронні, електронно-обчислювальні засоби і засоби комп'ютерних інформаційних технологій;

- лінгвістичні засоби;

- психотропні засоби.

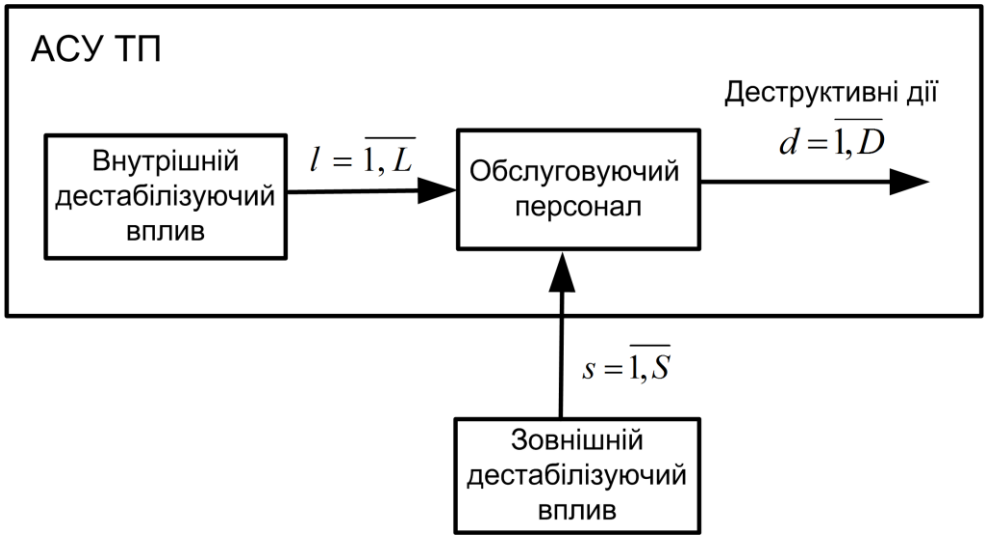


Рис. 2.2. Загальна схема дії чинників в АСУ ТП

Множина факторів внутрішнього дестабілізуючого впливу $l = \overline{1,L}$ являє собою множину людських потреб, через захищеність яких може розкриватися забезпечення інформаційної безпеки людино-машинних систем управління, а саме [9]:

- вітальні (природні): їжа, одяг, 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.

Таким чином, стан інформаційної безпеки персоналу АСУ ТП визначається двома основними чинниками: інформаційно-психологічною задоволеністю людських потреб персоналу і дестабілізуючими (навмисними або випадковими) інформаційно-психологічними та інформаційно-технічними впливами.

Множиною деструктивних дій $d = \overline{1, D}$ з боку обслуговуючого персоналу по відношенню до технічної компоненти будуть дії, спрямовані на порушення конфіденційності, цілісності, доступності та неспростовності інформації в АСУ ТП, тобто виникнення загрози інформаційної безпеки.

Загрози можуть бути реалізовані різними типами деструктивних дій. Взаємозв'язок між загрозами і можливими деструктивними діями приведений на рис. 2.3 [12].

Як бачимо з рис. 2.3, загрози інформації можна класифікувати за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто – порушення конфіденційності, цілісності доступності інформації і відповідальності.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;

- несанкціоновані зміни або викрадення інформації;

- відмова в обслуговуванні або профілактика авторизованого доступу;

- відмова у відповідальності.

Таким чином, конфіденційність буде забезпечуватись, якщо дотримуються встановлені правила доступу до системи, цілісність - якщо

дотримуються встановлені правила модифікації інформації або її видалення, доступність - якщо зберігається можливість доступу до системи або модифікації інформації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

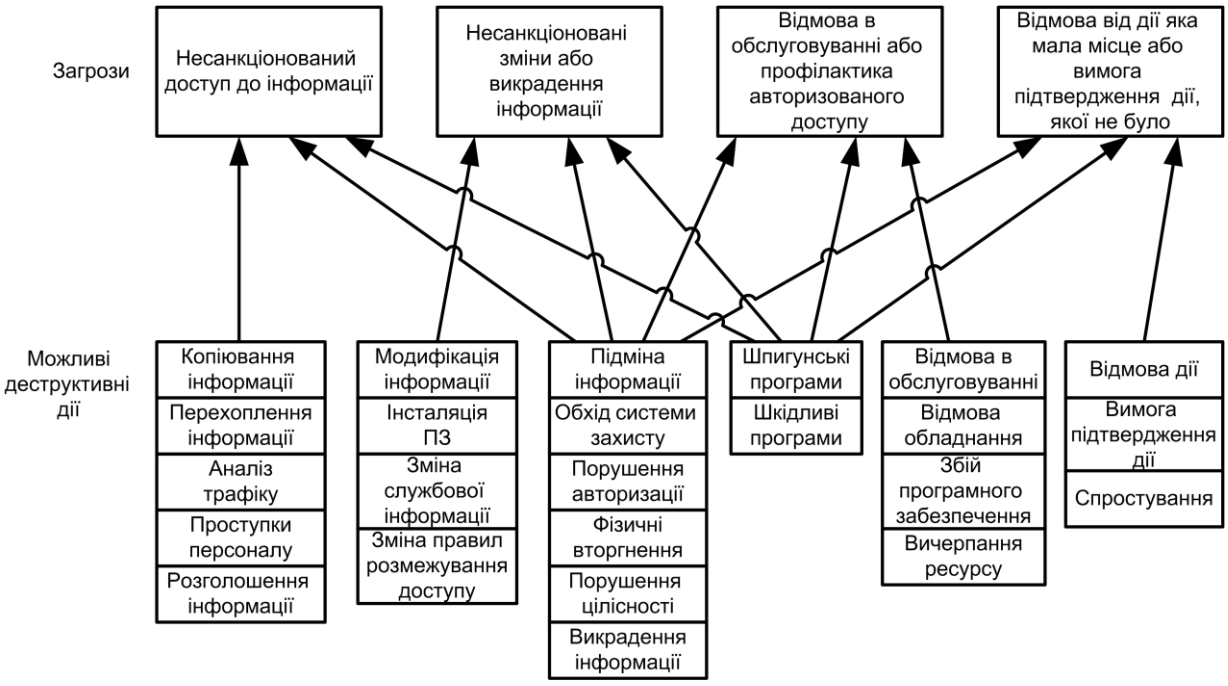


Рис. 2.3. Взаємозв’язок між загрозами і деструктивними діями

Загрози для автоматизованих систем управління технологічними процесами можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природних (стихійні лиха, кліматичні умови тощо). Однак, ми розглядаємо загрози, які можуть виходити від імовірних навмисних деструктивних дій обслуговуючого персоналу при умові наявності деструктивних впливів.

Очевидно, що обслуговуючий персонал складається з індивідів,

кожний з яких здатний здійснювати хороші або погані вчинки, бачити себе зі сторони спостерігача, усвідомлювати відповідні відчуття за здійсненні вчинки тощо.

Найпростішу модель, яка описує поведінку такого індивіда, його готовність до дій, можливо представити у вигляді імплікації [8]:

$$I = J \rightarrow Z = F\left(Z, J\right), \tag{2.1}$$

де Z - дія зовнішніх та/або внутрішніх дестабілізуючих впливів;

J – усвідомлення індивідом своїх дій по відношенню до дії дестабілізуючих впливів.

Нехай $P(I)$ - ймовірність здійснення індивідом деструктивних дій; $P(I|Z)$ - ймовірність здійснення індивідом деструктивних дій при умові дії зовнішніх та/або внутрішніх дестабілізуючих впливів; $P(Z)$ - ймовірність дії зовнішніх та/або внутрішніх дестабілізуючих впливів.

Очевидно, що кожний із зовнішніх дестабілізуючих впливів з множини $w = \overline{1,W}$ може діяти одночасно з кожним із внутрішніх дестабілізуючих впливів з множини $l = \overline{1,L}$. Тоді, враховуючи основні властивості ймовірності [13], ймовірність дії дестабілізуючих впливів буде визначатися з виразу:

$$P\left(Z\right) = \begin{Vmatrix} \left[P\left(w_1\right) + P\left(l_1\right) - P\left(w_1 l_1\right)\right] & \cdots & \left[P\left(w_1\right) + P\left(l_L\right) - P\left(w_1 l_L\right)\right] \\ \vdots & \ddots & \vdots \\ \left[P\left(w_w\right) + P\left(l_L\right) - P\left(w_w l_L\right)\right] & \cdots & \left[P\left(w_w\right) + P\left(l_L\right) - P\left(w_w l_L\right)\right] \end{Vmatrix}, \tag{2.2}$$

де $P\left(w\right)$ - ймовірність дії зовнішніх дестабілізуючих впливів;

$P\left(l\right)$ - ймовірність дії внутрішніх дестабілізуючих впливів;

$P(wl)$ - ймовірність одночасної дії зовнішніх та внутрішніх дестабілізуючих впливів.

Тоді, ймовірність здійснення індивідом деструктивних дій, спрямованих на порушення інформаційної безпеки, буде визначатися з виразу:

$$P(I) = \left\| P(I \mid Z_{wl}) \cdot P(Z_{wl}) \right\|, \qquad (2.3)$$

де $P(I|Z_{wl})$ - ймовірність здійснення індивідом деструктивних дій при умові дії w–го зовнішнього впливу та l–го внутрішнього впливу;

$P(Z_{wl})$ - ймовірність дії w–го зовнішнього впливу та l–го внутрішнього впливу і визначається з виразу (2.2).

Аналіз виразу (2.3) показує, що відсутність навмисних деструктивних дій з боку обслуговуючого персоналу, тобто забезпечення інформаційної безпеки АСУ ТП буде виконуватися при умові $P(I|Z_{wl}) = 0$ або $P(Z_{wl}) = 0$.

Загрози інформації класифікують за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто – порушення конфіденційності, цілісності доступності інформації і відповідальності.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;
- несанкціонована модифікація або викрадення інформації;
- відмова в обслуговуванні;
- відмова у відповідальності.

Загрози для об’єктів критичної інфраструктури можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни,

невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природні (стихійні лиха, кліматичні умови тощо). Приведемо більш детальний опис груп, що входять в категорію навмисних загроз [35]:

- Зловмисники. Найчастіше хакери зламують мережі для гостроти відчуттів в дусі змагань або для хвастощів серед колег. Раніше віддалений злом вимагав неабияких комп'ютерних знань та навичок, а тепер зловмисники можуть завантажити сценарії атаки і протоколи Інтернету. Таким чином, у той час як інструменти атаки стали більш складними, вони також стали більш легкими для використання.

- Оператори ботнету. Ботнет - комп'ютерна мережа, що складається з деякої кількості хостів, з запущеними ботами (автономним програмним забезпеченням). Найчастіше бот у складі ботнета є програмою, що потай встановлюється на пристрій жертви і дозволяє зловмиснику виконувати якісь дії з використанням ресурсів зараженого комп'ютера. Зазвичай ботнети використовуються для нелегальної або злочинної діяльності: розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні.

- Злочинні групи. Злочинні групи прагнуть атакувати системи для отримання грошової вигоди з допомогою спаму, фішингу, шпигунських програм для вчинення крадіжки та шахрайства в Інтернеті.

- Іноземні спецслужби. Іноземні спецслужби використовують кіберзасоби, як частину їх шпигунської діяльності, спрямованої на збір інформації або для проведення операцій в рамках інформаційних впливів на супротивника.

- Інсайдери. Незадоволені інсайдери є основним джерелом комп'ютерної злочинності. Інсайдерам не потрібно мати багато спеціальних знань про кібератаки, тому що можливості якими вони володіють, перебуваючи усередині системи, часто дозволяють їм отримати необмежений доступ до системи, а також здійснити її пошкодження або крадіжку даних. Також інсайдерські загрози становлять сторонні постачальники обладнання та

програм, а також співробітники, які ненавмисно впроваджують шкідливі програми в системі. Інсайдерами можуть бути працівники, підрядники, партнери по бізнесу.

- Фішери. Фішинг - вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логінів і паролів. Дана загроза реалізується шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів. У листі міститься пряме посилання на сайт, зовні відрізнити від справжнього, або на сайт з переадресацією. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленої сторінці свої логін і пароль.

- Сніфінг. Сніфінг - поширений вид атаки, коли всі пакети, отримані мережевою картою, пересилаються на обробку спеціальною програмою, званому сніфером. У результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного проникнення в систему під виглядом звичайного співробітника компанії.

- Спамери. Спам - розсилка реклами або інших видів повідомлень особам, які не висловлювали бажання їх отримувати.

- Автори шпигунських і шкідливих програм. Особи або організації, які зі злим умислом проводять атаки на користувачів шляхом написання і поширення шпигунського і шкідливого програмного забезпечення.

- Терористи. Терористи ставлять перед собою мету знищити, вивести з експлуатації критично важливі об'єкти інфраструктури, створити загрозу національній безпеці, викликати масові жертви, послабити економіку країни, завдати шкоди суспільній моралі. Терористи можуть атакувати одну мету, щоб відвернути увагу та ресурси від інших цілей.

- Промислові шпигуни. Метою шпигунства може стати компрометація інформації або її крадіжка з подальшим деструктивним використанням, до повної зупинки і банкрутства промислового об'єкта.

Загрози інформації класифікують за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки через уразливості. Уразливістю є недолік або слабке місце інформаційної системи, системи безпеки, процедур внутрішнього контролю, які можуть бути використані для порушення цілісності або доступності системи та її коректної роботи. Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів.

Класифікація уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами показана на рис. 2.4.

Розглянемо більш докладно уразливості автоматизованих систем управління [35].

1. Уразливості політик і процедур. До цієї категорії можна віднести:

- невідповідність або відсутність політики безпеки;

- невідповідність або відсутність процедур безпеки (повинні бути розроблені конкретні процедури безпеки і навчений відповідний персонал);

- відсутність підвищення кваліфікації персоналу у сфері безпеки;

- невідповідність архітектури безпеки;

- невідповідність або відсутність керівництва по впровадженню обладнання;

- відсутність відповідальності за документальне адміністрування політик і процедур безпеки;

- відсутність або недолік аудитів в області безпеки;

- відсутність конкретного плану аварійного відновлення системи у

випадку збою або аварії (план повинен бути готовий, апробований та доступний у разі виникнення апаратного або програмного збою, щоб уникнути простою і втрати виробництва);

- відсутність змін конфігурації управління (повинно здійснюватися управління модифікаціями апаратних засобів, програмованого обладнання, програмного забезпечення, щоб гарантовано захистити систему від невідповідних або неправомірних модифікацій до, під час, і після впровадження системи).

Рис. 2.4. Класифікація уразливостей інформаційної безпеки АСУ ТП

Аналіз показує, що уразливості політик і процедур в промислових автоматизованих системах управління виникають через відсутність або неповну, неадекватну документацію в галузі безпеки, у тому числі політик і керівництва (процедур), адміністрування аудиту, відновлення.

Розглянемо уразливості платформ. До даної категорії можна віднести:

1. Конфігурація:

- програмне забезпечення не оновлюється для виявлення вразливостей (через складність програмного забезпечення АСУ зміни повинні пройти комплексне тестування, що займає певний час і забезпечує уразливість до загроз);

- операційна система та програми безпеки впроваджуються і оновлюються без ретельних випробувань (повинні бути розроблені документовані процедури для тестування нових програм безпеки);

- параметри конфігурації використовуються за замовчуванням (це часто призводить до небезпечного відкриття портів інших служб і виконання небажаних програм);

- не зберігаються критичні конфігурації системи (для підтримки доступності системи і запобігання втрати даних повинні бути розроблені документовані процедури для відновлення параметрів конфігурації у разі випадкової або зловмисної зміни в конфігурації);

- зберігання незахищених конфіденційних даних (наприклад, паролі) на портативних пристроях (ці пристрої будуть втрачені або вкрадені і безпека системи може бути порушена);

- відсутність адекватної політики паролів (коли паролі повинні бути використані, наскільки стійкими вони повинні бути і як вони повинні зберігатися);

- відсутність пароля (паролі повинні бути реалізовані для запобігання несанкціонованого доступу - для входу в систему (якщо в системі є облікові записи користувачів), при включенні живлення (якщо в системі немає облікових записів користувачів), при виході та режиму заставки);

- розкриття паролів (прикладами можуть бути спільне використання паролів для різних облікових записів користувачів, повідомлення паролів стороннім, передача паролів в незашифрованому вигляді через незахищені підключення);

- підбір пароля (погано підібраний пароль може бути легко розгаданий зловмисником або комп'ютерною програмою для отримання несанкціонованого доступу);

- неадекватність контролю доступу (неправильно налаштований контроль доступу може дозволити оператору дії адміністратора або заборонити оператору коригувальні дії в аварійній ситуації).

2. Обладнання:

- невідповідне тестування змін системи безпеки;

- недостатній рівень фізичного захисту критично важливих систем;

- несанкціонований фізичний доступ сторонніх осіб до обладнання;

- незахищений віддалений доступ до компонентів АСУ;

- подвійні мережеві карти для з'єднання мереж (при підключенні до різних мереж можливий несанкціонований доступ з однієї мережі в іншу);

- відсутність документування активів (відсутність точного списку активів в системі може залишити несанкціоновані точки доступу);

- радіочастотний і електромагнітний імпульс (наслідки впливу можуть бути від тимчасового порушення управління до пошкодження плат);

- відсутність резервного електроживлення;

- втрата контролю навколишнього середовища системи (втрата контролю навколишнього середовища процесорів може привести до перегріву і пошкодження або роботі з помилками);

- відсутність резервування критично-важливих компонентів.

3. Програмне забезпечення:

- переповнення буфера (може викликати аварійне завершення або зависання програми, що веде до відмови обслуговування. Окремі види переповнення, наприклад переповнення в стековому кадрі, дозволяють

зловмиснику завантажити та виконати довільний машинний код від імені програми і з правами облікового запису, від якої вона виконується);

- не включені або ідентифікуються як відключені можливості безпеки, які були встановлені з програмним продуктом;

- відмова в обслуговуванні;

- неправильна обробка невизначених, погано визначених, або "неприпустимих" умов (деякі реалізації систем уразливі для пакетів, які спотворені або містять "неприпустимі" значення полів);

- використання незахищених галузевих протоколів передачі даних;

- передача повідомлень в незахищеному вигляді;

- запуск надлишкових сервісів, тобто тих служб, які не використовуються для вирішення поставлених завдань;

- використання пропрієтарного програмного забезпечення, яке було предметом обговорення на конференціях і в періодичних друкованих виданнях;

- недостатня перевірка справжності та контролю доступу для конфігурування та програмування;

- не встановлено програмне забезпечення виявлення/запобігання несанкціонованого проникнення;

- не підтримується протоколювання роботи всіх служб і сервісів;

- не реєструються інциденти.

4. Шкідливе програмне забезпечення:

- не встановлено захист від шкідливого програмного забезпечення;

- захист від шкідливого програмного забезпечення не актуальна, тобто не оновлюється або оновлюється рідко;

- захист від шкідливого програмного забезпечення впроваджена без проведення ретельних випробувань.

Як бачимо, уразливості платформ в АСУ ТП можуть виникати через недоліки, помилки, або неякісне обслуговування своїх платформ, у тому числі обладнання (апаратні засоби, операційні системи і додатки, відсутність

контролю фізичного доступу.

Розглянемо уразливості мережі. До даної категорії можна віднести:

1. Конфігурація мережі:

- невідповідність архітектури мережевої безпеки;

- відсутність контролю потоку даних;

- неякісно налаштовані параметри безпеки обладнання;

- відсутність резервування конфігурації мережевого пристрою;

- передача паролів в незахищеному вигляді;

- недостатньо часта зміна паролів доступу до мережевих пристроїв;

- неадекватність контролю доступу до мережевих пристроїв.

3.2. Мережеве обладнання:

- недостатній рівень фізичного захисту мережевого обладнання;

- несанкціонований доступ до портів мережевого обладнання;

- відсутність надлишковості для критично важливих сегментів мережі.

3. Периметр мережі:

- не визначений периметр безпеки;

- відсутня або неправильно налаштовано міжмережевий екран;

- мережі управління використовуються для трафіку інших типів;

- управління мережевими сервісами мережі АСУ реалізується в мережі ІТ (мережа АСУ стає залежною від мережі ІТ, у якої немає необхідного пріоритету надійності і доступності).

4. Моніторинг мережі:

- неадекватні журнали міжмережевого екрану (кількість контрольованих параметрів не достатньо для проведення аналізу інцидентів);

- відсутність регулярного моніторингу безпеки в мережі.

5. З'єднання:

- не ідентифікуються критичні шляхи контролю та управління;

- використання стандартних протоколів зв'язку;

- відсутня або недостатня аутентифікація користувачів, даних або пристроїв;

- відсутність перевірки цілісності з'єднань.

6. Бездротові мережі:

- невідповідність аутентифікації між бездротовими клієнтами і точками доступу;

- невідповідний захист даних між бездротовими клієнтами і точками доступу.

Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів.

З метою забезпечення інформаційної безпеки розглянемо деякі з існуючих методів своєчасного виявлення загроз автоматизованих систем (АС) [36]:

а) обмеження доступу;

б) контроль доступу до обладнання;

в) обмеження і контроль доступу до інформації;

г) надання привілеїв на доступ;

д) ідентифікація і установлення справжності об’єкта (суб’єкта);

е) захист інформації від витоку за рахунок побічного електромагнітного випромінювання і наведень.

Розглянемо кожний із приведених методів більш детально [36].

а) Обмеження доступу полягає у створенні деякої фізичної замкнутої перепони навколо об’єкта захисту із організацією контролює мого доступу осіб, пов’язаних з об’єктом захисту по своїх функціональних обов’язках.

Обмеження доступу до автоматизованої системи полягає у наступному:

- виділення спеціальної території для розміщення АС;
- обладнання по периметру виділеної зони спеціальних огороджень з охоронною сигналізацією;

- спорудження спеціальних приміщень або споруджень;
- виділення спеціальних приміщень в спорудженні;
- створення контрольно-пропускного режиму на території, в спорудженнях, в приміщеннях.

Задача засобів обмеження доступу – виключити випадковий і/або навмисний доступ сторонніх осіб на територію розміщення АС і безпосередньо до обладнання.

б) З метою контролю доступу до внутрішнього монтажу, ліній зв'язку і технологічних органів управління використовується обладнання контролю розкриття. Це значить, що внутрішній монтаж обладнання і технологічні органи, пульти управління закриті кришками, дверцятами або кожухами, на які встановлені датчики. Датчики спрацьовують при розкритті обладнання і видають електричні сигнали, які поступають на пристрій контролю.

в) Розмежування доступу до інформації в АС полягає в розділенні інформації, яка в ній циркулює на частини і організації доступу до неї посадових осіб у відповідності з їх функціональними обов'язками і повноваженнями.

Задача розмежування доступу до інформації – скорочення кількості посадових осіб, які не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед допущеного до неї персоналу.

При цьому, розділення інформації може здійснюватися по ступеню важливості, секретності, по функціональному призначенню, по документах тощо.

Зважаючи на те, що доступ здійснюється з різних технічних засобів, починати розмежування можна шляхом розмежування доступу до технічних засобів, розмістивши їх в окремих приміщеннях. Всі підготовчі функції технічного обслуговування обладнання, її ремонту, профілактики, перезавантаження програмного забезпечення тощо повинні бути технічно і організаційно відокремлені від основних задач системи.

г) Надання привілеїв на доступ до інформації полягає у тому, що із числа допущених до неї посадових осіб виділяється група, якій надається доступ тільки при одночасному пред'явленні повноважень усіх членів групи.

Задача методу – ускладнити навмисний перехват інформації порушником.

Даний метод ускладнює процедуру доступу до інформації, але перевагою є висока ефективність захисту.

д) Ідентифікація – це присвоєння будь якому об'єкту або суб'єкту унікального образа, імені або числа.

Встановлення справжності (аутентифікація) полягає в перевірці, чи являється об'єкт (суб'єкт), який перевіряється, насправді тим, за кого себе видає.

Кінцевою метою ідентифікації і встановлення справжності об'єкта в АС – допуск його до інформації з обмеженим доступом у випадку позитивного результату перевірки, або відмову в допуску у випадку негативного результату перевірки.

е) З метою захисту інформації з обмеженим доступом від витоку за рахунок побічного електромагнітного випромінювання і наведень проводяться виміри рівня небезпечних сигналів. Заміри виконуються в декількох точках на різних відстанях від джерела за допомогою спеціальної апаратури. Якщо рівень сигналу на границі встановленої зони перевищив допустимі значення, застосовують заходи захисту.

Заходи захисту можуть носити різноманітний характер в залежності від складності, вартості і часу їх реалізації, які визначаються при створенні конкретної АС.

Такими заходами можуть бути:

- удосконалення апаратури з метою зменшення рівня сигналів;
- встановлення спеціальних фільтрів;
- застосування генераторів шуму;
- використання спеціальних екранів;

- інші заходи.

В автоматизованих системах (АС) інформаційна безпека традиційно зосереджена на досягненні трьох цілей, конфіденційності, цілісності, доступності. Стратегія безпеки традиційної інформаційної технології направлена в першу чергу на конфіденційність з необхідними засобами управління доступом для досягнення заданої мети. При цьому цілісність займає другу сходинку по важливості задачі.

Стосовно інформаційних систем об'єктів критичної інфраструктури загальний пріоритет цих цілей часто відрізняється. Безпека в цих системах, перш за все, стосується підтримки доступності усіх компонентів системи. При цьому, цілісність являється часто другою по важливості задачею. Конфіденційність, як правило, для автоматизованих системах управління об'єктів критичної інфраструктури має найменше значення.

В переважній більшості випадках пріоритети повністю інвертовані. В той же час, в залежності від обставин у цілісності системи може бути самий високий пріоритет. Певні вимоги до функціонування, які висувають окремі компоненти або система в цілому, мають різні пріоритети для цілей (тобто, цілісність чи проблеми доступності можуть переважити конфіденційність, або навпаки).

Задачі забезпечення основних виробничих функцій автоматизованих системах управління об'єктів критичної інфраструктури іноді суперечать задачі забезпечення їх інформаційної безпеки і тому не можуть бути застосовані в АСУ ОКІ, а іноді навіть можуть бути небезпечними.

До основних особливостей ключових систем критичної інфраструктури, які суттєво впливають на зміст вимог по забезпеченню безпеки інформації, відносяться наступні [35]:

- основною інформацією, що захищається на об'єктах критичної інфраструктури держави є технологічна (забезпечує управління технологічними або чутливо важливими процесами) інформація програмно-технічна (програми системного і прикладного характеру, що забезпечують

функціонування об’єктів), командна (керуюча) і вимірювальна, яка не належить до інформації з обмеженим доступом (якщо в таких системах циркулює інформація з обмеженим доступом, то вона підлягає захисту згідно з чинними вимогами і нормами з технічного захисту інформації);

- переважна більшість ключових систем забезпечують керування безперервними технологічними процесами, що зумовлює значно більш жорсткі вимоги до часу і порядку виконання автоматизованих функцій, неможливість відключення на період проведення контрольних заходів в інтересах забезпечення безпеки інформації і оцінки їх реальної захищеності від негативних інформаційних впливів;

- різноманітність об’єктів, наявність в них різних, територіально і просторово розподілених елементів з поєднанням різноманітних інформаційних технологій;

- надзвичайна небезпека наслідків виведення з ладу і (або) порушення функціонування об’єктів критичної інфраструктури;

- широке застосування операційних систем реального часу, необхідність адаптації програмних та програмно-апаратних засобів захисту до цих операційних систем;

- компоненти системи об’єктів критичної інфраструктури працюють в режимі реального часу с жорстко заданими часовими параметрами и не потребують високої пропускної спроможності;

- для об’єктів критичної інфраструктури, наряду з інформаційною безпекою, пріоритетним є безпека обслуговуючого персоналу, збереження обладнання, запобігання виробничих втрат;

- на об’єктах критичної інфраструктури може бути дуже складний взаємозв’язок інформаційного захисту з фізичними процесами і наслідками в промисловому секторі. Тому, всі функції безпеки повинні бути протестовані на предмет відсутності загрози штатному функціонуванню систем;

- в системах об’єктів критичної інфраструктури дуже критичний час реакції системи на дію оператора. Доступ до системи жорстко

контролюється, але не повинен перешкоджати або втручатися в процес взаємодії оператора и системи;

- системи об’єктів критичної інфраструктури створюються для забезпечення промислових процесів і, зазвичай, не вистачає ресурсів для підтримки програм по забезпеченню безпеки.

2.2. Структурна модель взаємодії елементів інформаційної системи об’єктів критичної інфраструктури

Проведений аналіз існуючих систем захисту інформації [1, 2], дає змогу визначити основні складові частини системи кіберзахисту інформаційних систем об’єктів критичної інфраструктури:

- нормативно-правова;
- організаційна;
- технічна;
- підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Так, одними із актуальних питань є наявність нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури, приведення національної нормативно-правової бази з питань забезпечення кібербезпеки об’єктів критичної інфраструктури у відповідність з положеннями міжнародних документів; виконання узгодженості понятійного апарату, що використовується в існуючих національних законодавчих та нормативно-правових документах; доопрацювання (при необхідності - розробка) нормативних документів, вимог, методологій до оцінки загроз об’єктам, що є критичними для життєдіяльності держави, загальної методології оцінки ризиків для критично важливих об’єктів та критичної інфраструктури у цілому.

Крім того, слід зазначити, що керівники та/або власники об’єктів критичної інфраструктури повинні усвідомлювати можливість і ймовірність здійснення кібератак та наслідки, у випадку їх реалізації. Запровадження заходів з питань забезпечення кібербезпеки потребують залучення додаткових ресурсів, на що керівники цих об’єктів не завжди згодні, а механізм, який би вимагав від даних керівників запровадження необхідних заходів, відсутній. Тому, без запровадження згаданого механізму усі стандарти, інструкції тощо з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури будуть носити рекомендаційний характер, оскільки та інформація, яка циркулює, наприклад, в автоматизованих системах управління технологічними процесами, не відноситься ні до одного виду інформації, що підлягає захисту згідно із чинним законодавством.

Інформаційні системи об’єктів критичної інфраструктури зазвичай являються об’єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об’єкти захисту від кіберзагроз.

Кіберзагрози для інформаційних систем об’єктів критичної інфраструктури можуть виходити з різних джерел: навмисних, ненавмисних, природних. Основними з них є [3]: зловмисники, оператори ботнету, злочинні групи, іноземні спецслужби, інсайдери, фішери, сніфери, спамери, автори шпигунського і шкідливого програмного забезпечення, терористи, промислові шпигуни тощо.

На рис. 2.5 приведена структурна модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури. Розглянемо, яким чином впливає кожна із складових систем (організаційна, технічна, персонал) на забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

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

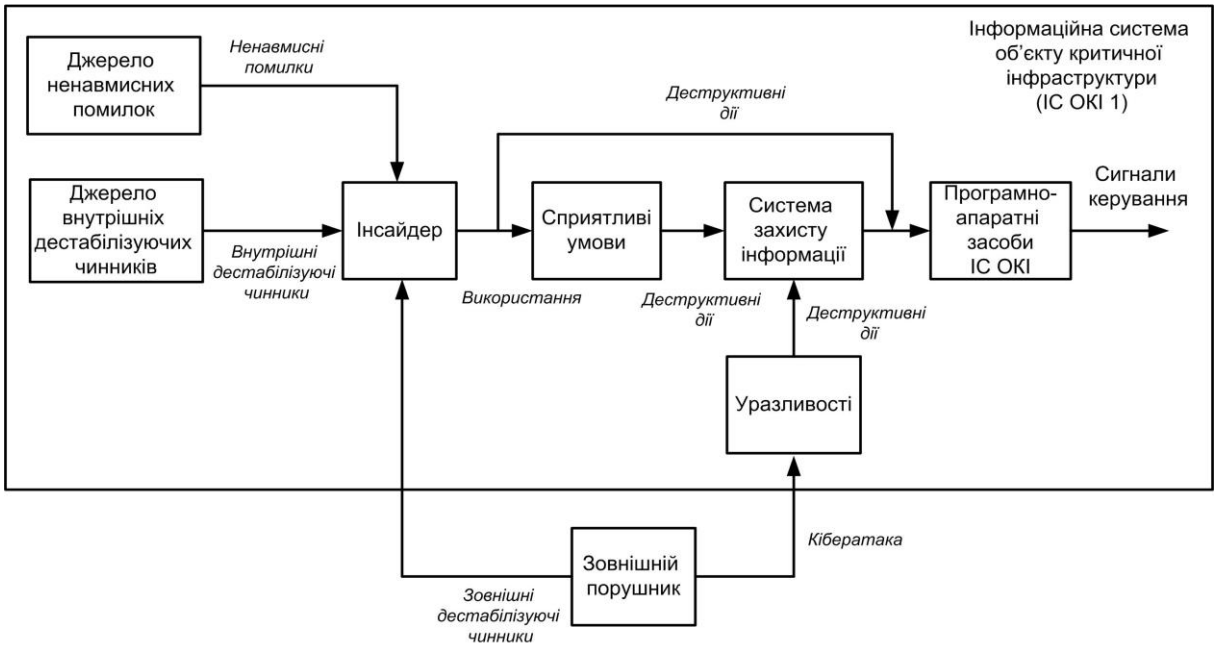


Рис. 2.5. Структурна модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури

При цьому, кібератакам зовнішнього порушника протистоїть система захисту інформації інформаційної системи об'єктів критичної інфраструктури, до функцій якої обов'язково повинні входити:

- захист периметра мережі;
- забезпечення безпеки міжмережевих взаємодій;
- моніторинг і аудит безпеки;
- виявлення і запобігання діям атак;
- резервне копіювання і відновлення даних;
- аналіз захищеності і керування політикою безпеки;
- контроль цілісності даних;

- захист від шкідливого програмного забезпечення;

- фільтрація контенту і запобігання витоку конфіденційної інформації;

- установка оновлень програмного забезпечення;

- адміністрування безпеки.

За результатами проведеного аналізу загроз та уразливостей [4], можливо зазначити, що захист таких систем повинен розглядатися по наступних напрямках:

- захист інформаційних і фізичних компонентів інформаційної системи об’єктів критичної інфраструктури;

- технічний захист інформації інформаційних систем об'єктів критичної інфраструктури;

- захист процесів, процедур і програм обробки інформації інформаційних систем об’єктів критичної інфраструктури;

- захист каналів зв'язку інформаційних систем об’єктів критичної інфраструктури;

- придушення побічних електромагнітних випромінювань;

- керування та контроль системою захисту.

Однак, основна відмінність інсайдера від зовнішнього порушника полягає у тому, що інсайдер має легітимний доступ до системи. В той час, як зовнішній порушник прикладає зусилля, щоб подолати систему захисту, прагнучи отримати доступ до інформації, інсайдер отримує цю інформацію абсолютно безперешкодно в межах своєї компетенції або незаконно розширюючи свої права і можливості. Тому, будь-який захист системи від зовнішнього порушника виявляється неефективним проти інсайдера. При цьому, зовнішній порушник може здійснювати кібератаки на програмно-апаратну складову інформаційної системи, використовуючи уразливості системи захисту інформації інформаційної системи об’єкту критичної інфраструктури, або чинити інформаційно-психологічний вплив на інсайдера (зовнішні дестабілізуючі чинники).

Окрім зовнішніх дестабілізуючих чинників до можливих деструктивних дії інсайдера можуть спонукати внутрішні дестабілізуючі чинники - людські потреби, через захищеність яких може розкриватися забезпечення кібербезпеки інформаційної системи об’єкта критичної інфраструктури, а також власні ненавмисні помилки.

Внутрішніми дестабілізуючими чинниками можуть бути [5]:

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

- потреби в безпеці: комфорт, постійність умов життя тощо;

- пізнавальні: активність, навички, уміння, діяльність, ініціатива, дослідницький пошук тощо;

- наукові: освіта (знання), виховання, мислення, цінна інформація, самосвідомість, істина тощо;

- соціальні: соціальні зв’язки, спілкування, увага до себе, спільна діяльність тощо;

- престижні: самоповага, повага зі сторони інших, визнання, досягнення успіху і високої оцінки, службове зростання тощо;

- духовні: щастя, свобода совісті, цілісність світогляду, доброта, честь тощо.

У залежності від того, які чинники спонукають інсайдера на деструктивні дії, останніх поділяють на типи. Ці типи розділяються у залежності від мети, мотивації і послідовності дій інсайдерів.

Необхідно відмітити, що якщо інсайдер отримує доступ до активів інформаційної системи об’єкта критичної інфраструктури незаконно розширюючи свої права та можливості, то для цього може бути необхідна наявність сприятливих умов. У випадку отримання інсайдером доступу до активів інформаційної системи об’єкта критичної інфраструктури у межах своєї компетенції необхідності у сприятливих умовах немає. Крім цього, при цьому обходиться система захисту інформації.

Тому, проведений аналіз показує, що з метою мінімізації ймовірності здійснення інсайдером деструктивних дій необхідно:

- вчасно виявляти та вживати певних заходів для зменшення впливу внутрішніх дестабілізуючих чинників;

- покращувати відбір співробітників на етапі прийняття на роботу та вживати відповідних заходів щодо підвищення їх фахового рівня для недопущення або мінімізації ненавмисних помилок.

Таким чином, із урахуванням викладеного можна зазначити, що на стан забезпечення кібербезпеки інформаційної системи об’єкта критичної інфраструктури впливають такі фактори:

- наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури;

- наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;

- наявність уразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;

- наявність чи відсутність сприятливих умов для реалізації кіберзагроз;

- привабливість активів, на які власне і спрямовуються кібератаки;

- наслідки від можливої реалізації кіберзагроз;

- рівень фахової підготовки співробітників, відповідальних за кібербезпеку на всіх рівнях: організація, підприємство, галузь, відомство тощо.

Також, одним із таких показників, на нашу думку може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.

Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, силові відомства, дипломатичні установи тощо.

Корисним для оцінки та аналізу стану кібербезпеки може бути поєднання кількості кібератак за певний інтервал часу з урахуванням їх

спрямованості. Це дасть змогу визначити вектор зацікавленості зловмисника та їх мету – кібердиверсія, кіберрозвідка, кібершпигунство тощо по відношенню до кожного напрямку.

Перелік показників, однозначно, може бути розширений з урахуванням досвіду та аналізу статистичних даних щодо приведених вище факторів.

2.3. Визначення ймовірності реалізації загроз кібербезпеки об’єктів критичної інфраструктури

Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів [14-17].

Причинами виникнення загроз інформації являються дестабілізуючі фактори – явища чи події, які можуть з'являтися на будь-якому етапі життєвого циклу системи. Наслідком виникнення дестабілізуючих факторів може бути ризик інформаційної безпеки – ймовірність того, що певна загроза використає уразливість системи, в результаті чого буде нанесено шкоду компонентам системи [18]. Отже, порушення інформаційної безпеки - це виникнення і реалізація загроз.

Разом з тим, слід відмітити, що загроза, яка не має відповідної уразливості, може не призводити до ризику. І навпаки, наявність уразливості не завдає шкоди сама по собі, так як необхідна наявність загрози, яка скористається нею.

Взаємозв’язок між загрозами, уразливостями і ризиком приведений на рис. 2.6 [19].

Уразливість, яка не має відповідної загрози, може не вимагати впровадження засобу контролю, але повинна усвідомлюватися і піддаватися постійному моніторингу.

Виходячи із зазначеного, можна зауважити, що ймовірність реалізації загрози буде залежати від наявності сприятливих умов для використання уразливостей, пов’язаних з цими загрозами.

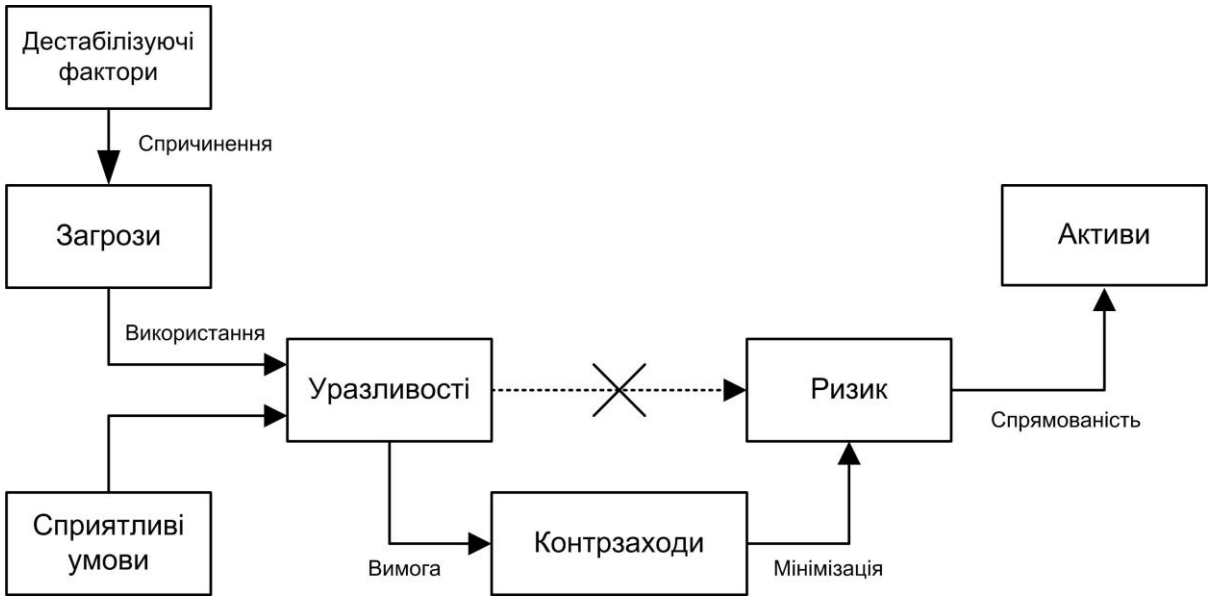


Рис. 2.6. Взаємозв’язок між загрозами, уразливостями і ризиком

Нехай R_{nu} – подія, яка відображає реалізацію n-ї загрози з використанням m-ї уразливості, де n змінюється від 1 до N; N - кількість загроз; u змінюється від 1 до U; U - кількість уразливостей; а K – подія, яка відображає наявність сприятливих умов для реалізації n-ї загрози з використанням u-ї уразливості. Крім того, будемо вважати, що події R_{nu} незалежні і складають повну групу несумісних подій.

Тоді, ймовірність реалізації n-ї загрози з використанням u-ї уразливості буде визначатися наступним чином:

$$P\left(R_{nu}\right)=\sum_{u=1}^{U}P\left(R_{nu}\left|K_{n}\right.\right)P\left(K_{n}\right), \tag{2.4}$$

де $P\left(R_{nu}\middle|K_n\right)$ - ймовірність реалізації *n*-ї загрози з використанням *u*-ї уразливості при умові наявності сприятливих умов K_n;

$P\left(K_n\right)$ - ймовірність наявності сприятливих умов для реалізації *n*-ї загрози.

Таким чином, ймовірність реалізації загроз з використанням уразливостей за умови наявності сприятливих умов можливо представити у вигляді матриці:

$$P\left(R\right)=\left[P\left(R_{nu}\right)\right]. \tag{2.5}$$

Елементи матриці у виразі (2.5) визначаються з виразу (2.4).

Очевидно, що захист інформації буде забезпечено у випадку, якщо:

$$\sum_{n=1}^{N}\sum_{u=1}^{U}P\left(R_{nu}\middle|K_n\right)=0. \tag{2.6}$$

В протилежному випадку буде ймовірність реалізації загрози і ймовірність нанесення шкоди компонентам системи.

Життєвий цикл процесу відображає послідовність стадій та фаз, що визначають динаміку реалізації і розвитку процесу.

Як випливає з виразу (2.5) та взаємозв’язку між загрозами, уразливостями і ризиком (рис. 2.6), для аналізу ймовірності реалізації загроз необхідні наступні вихідні дані:

- перелік джерел загроз;
- перелік загроз безпеки інформації;
- перелік уразливостей, через які можлива реалізація загроз;
- перелік сприятливих умов для реалізації загроз.

Життєвий цикл процесу аналізу ймовірності реалізації загроз представлений на рис. 2.7.

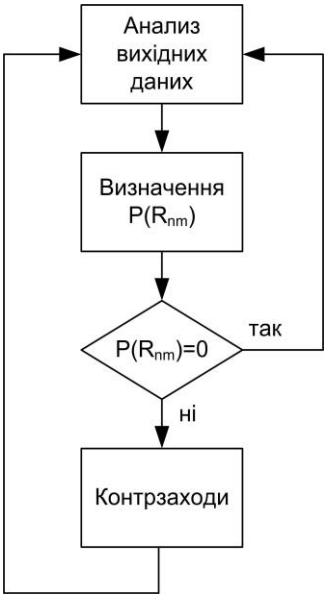
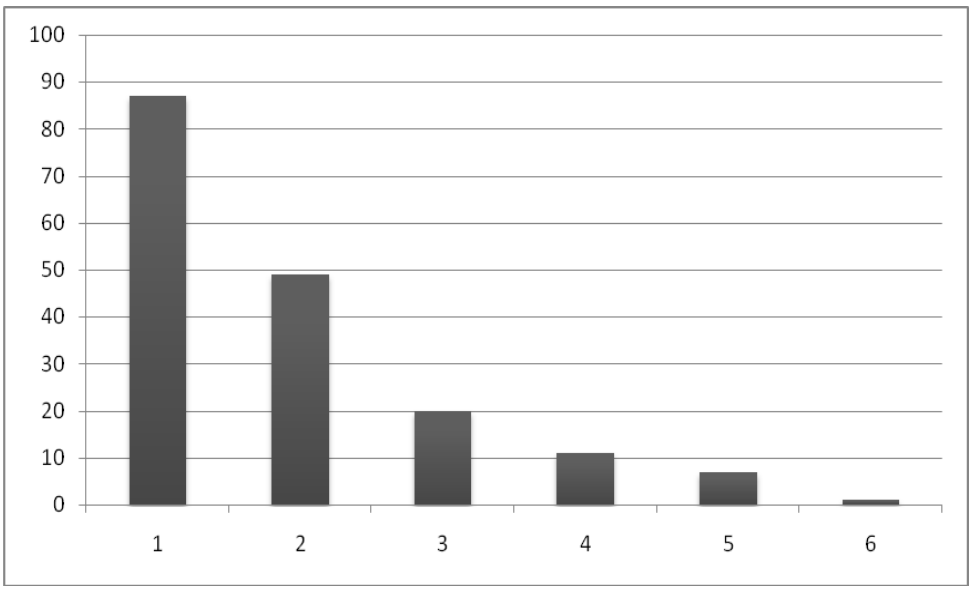


Рис. 2.7. Життєвий цикл процесу аналізу ймовірності реалізації загроз

2.4. Оцінювання небезпеки кібератак в інформаційних системах об'єктів критичної інфраструктури

Аналіз статистичних даних показує [20-23], що за останні 5 років найбільшу кількість уразливостей для атак виявлено в системах SCADA і людино-машинних інтерфейсах (ЛМІ), рис. 2.8.



1–SCADA; 2–ЛМІ; 3–ПЛК; 4–обладнання; 5–ПЗ; 6-інтерфейс/протокол

Рис. 2.8. Кількість уразливостей в компонентах АСУ ТП

Крім того, порушення інформаційної безпеки на об’єктах деяких критичних інфраструктур можуть мати значні фізичні впливи.

Основними категоріями впливу є:

- фізичний вплив – включає в себе безліч прямих наслідків аварій ІС ОКІ. Найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей. Інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;
- економічні впливи - наслідки другого порядку від фізичних впливів, що є похідними від аварій ІС ОКІ. Фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації. У великих масштабах, ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;
- соціальні впливи - наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

Враховуючи приведені вище категорії впливу порушення інформаційної безпеки ІС ОКІ можливо навести перелік наслідків цих впливів [23]:

- порушення національної безпеки;
- сприяння вчиненню акту тероризму;
- втрата або скорочення виробництва;
- каліцтва або загибель людей;
- пошкодження обладнання;
- викид (витікання, випаровування) або крадіжка небезпечних матеріалів;
- екологічні збитки;
- кримінальні або цивільно-правові зобов'язання;
- втрата приватної або конфіденційної інформації;
- втрата іміджу бренду або довіри клієнтів.

Слід зазначити, що елементи приведеного переліку не є незалежними. Очевидно, що один з наслідків може призвести до іншого.

Атаки спрямовані на те, щоб заподіяти шкоду активам. Актив - деяка сутність, цінна для особистості, організації або держави [22]. Тому програми безпеки спрямовані на захист активів від збитків.

Активи ІС ОКІ можуть бути класифіковані за видами наступним чином [25]: фізичні, логічні, людські.

Розглянемо більш детально кожний з видів активів.

Фізичні активи включають в себе будь-які фізичні компоненти або групи компонентів, які належать організації. В ІС ОКІ вони включають: системи управління, фізичні компоненти мережі передачі інформації або будь-які інші фізичні об'єкти, які певним чином залучені до процесів управління та аналізу виробничих процесів.

Логічні активи можуть включати в себе інтелектуальну власність, алгоритми, спеціальні знання, або інші інформаційні елементи, які містять в собі здатність функціонування організації або інноваційної діяльності. Крім того, ці види активів можуть містити суспільну репутацію, довіру покупця, або інші заходи, які, у разі їх пошкодження, безпосередньо впливають на виробничий процес. Логічні активи можуть бути представлені у формі особистої пам'яті, документів, інформації, що міститься на фізичному або електронному носіях інформації та включати в себе результати тестів, нормативних даних, або будь-яку іншу інформацію, яка розглядається як конфіденційна або приватна. Втрата логічних активів часто викликає значну шкоду організації і на тривалий час.

Активи ІС ОКІ є особливою формою логічних активів. Вони містять логіку автоматизації, яка приймає участь у виконанні виробничих процесів. Ці процеси надзвичайно залежать від повторного або безперервного виконання чітко визначених подій. І тому, нанесення шкоди цим активам, наприклад видалення або несанкціонована модифікація, може призвести до втрати цілісності або доступності безпосередньо до самого процесу.

Людські містять людей, знання, а також теоретичні і практичні навички, якими вони володіють, і які пов'язані з їх виробничою діяльністю. Вони можуть включати в себе необхідні сертифікати або важливі навички, необхідні для дій під час надзвичайних ситуацій.

Оцінка збитків активам може бути виражена або кількісно або якісно [25].

Кількісна оцінка активу дає точну відповідь щодо фінансових витрат, які пов'язані з цим активом. Це може бути вартість заміни, вартість втраченого продажу або інші заходи грошово-кредитної політики.

Якісна оцінка активів, як правило, виражається більше на абстрактному рівні, як наприклад показники у відсотках або у відносних значеннях. Багато активів можуть бути проаналізовані тільки з точки зору якісних збитків.

Збитки в ІС ОКІ можуть бути класифіковані як прямі і непрямі. Прямі збитки є витратами, які пов'язані з заміною активів. Збитки можуть мати місце за причиною фізичного пошкодження активу, в результаті втрати цілісності або доступності, переривання точної послідовності або зміни характеру процесу. Логічні ж активи мають порівняно низькі прямі збитки по відношенню до їх корисності, оскільки носій, який використовується для зберігання активу, як правило, має низьку вартість. Незначні пошкодження людських активів з коротким часом відновлення можуть мати низькі прямі збитки для організації, навіть у випадку довгострокових наслідків для травмованої людини.

Непрямі збитки є збитками завданими внаслідок втрати активів. Вони можуть включати в себе збитки, пов'язані з процесом простою, переробки або інші виробничі витрати через втрату активів.

Для фізичних активів непрямі збитки, як правило, включають наслідки, які виникають через втрату компонентів. Непрямі збитки від пошкодження обладнання можуть призвести до ремонту, реінжинірингу або інших зусиль для відновлення контролю над промисловим процесом. Для логічних активів непрямі збитки часто є дуже великими. Вони включають в себе втрату довіри

громадськості, втрату ліцензії на діяльність, втрату конкурентних переваг від випуску інтелектуальної власності, як наприклад конфіденційний процес, нові технології тощо.

Шляхом здійснення упорядкування приведених вище даних за видами активів і способом вираження їх оцінки, можна співвіднести види збитків для кожного типу активів. Результуючі дані приведені у табл. 2.1.

Таблиця 2.1

Види збитків для кожного типу активів

Вид активу	Прямі збитки	Непрямі збитки	Оцінка збитків, кількісна/якісна
Фізичні	Можуть бути досить високими через заміну вартості активу	Наслідки в результаті втрати або пошкодження активу (в залежності від вартості активу)	Якісна або кількісна (спочатку якісна при високому рівні ризиків, а далі кількісна для більшої точності)
Логічні	Зазвичай досить низькі, часто порівняно дешеві і можуть бути досить легко відновлені	Досить часто великі	В основному якісна, але в деяких випадках може бути кількісною
Людські	Як правило, низькі і середні (в залежності від ступеня пошкодження)	Як правило низькі або великі (в залежності від ступеня травми)	Безпосередній якісний вплив на виробництво, а потім кількісний вплив для відновлення

Загрози можуть бути реалізовані різними типами атак. Тому контрзаходи, які впроваджуються для захисту інформації повинні

враховувати різні типи загроз і можливих атак. Взаємозв'язок між загрозами і можливими атаками приведений на рис. 2.3 [26].

Проведений аналіз показує, що для інформаційних систем об'єктів критичної інфраструктури максимальний рівень важливості мають ризики і потенціальні збитки, що можуть бути нанесені внаслідок відмови авторизованого доступу до ресурсів, несанкціоноване використання, модифікація, знищення ресурсів інформаційних систем об'єктів критичної інфраструктури. Вимога забезпечення конфіденційності інформації при цьому має мінімальний рівень важливості.

Ураховуючи викладене вище, та на підставі взаємозв'язку між загрозами і можливими кібератаками, рис. 2.3, приведемо ранжування можливих кіберзагроз інформаційній системі об'єкту критичної інфраструктури за коефіцієнтами важливості, табл. 2.2.

Таблиця 2.2

Коефіцієнти важливості загроз ІС ОКІ

Загрози (можливі деструктивні дії)	Коефіцієнт важливості, k_r		
	1	2	3
Копіювання інформації	+		
Перехоплення інформації	+		
Аналіз трафіку	+		
Розголошення інформації	+		
Проступки персоналу	+	+	+
Модифікація інформації			+
Інсталяція програмного забезпечення		+	
Зміна службової інформації			+
Зміна правил розмежування доступу		+	
Підміна інформації			+

Продовження таблиці 2.2

Обхід системи захисту		+	
Порушення авторизації		+	
Фізичні вторгнення			+
Порушення цілісності інформації			+
Викрадення інформації	+		
Шпигунські програми	+		
Шкідливі програми		+	+
Відмова в обслуговуванні			+
Відмова обладнання			+
Збій програмного забезпечення	+	+	+
Вичерпання ресурсу	+		
Відмова від дії	+		
Вимога підтвердження дії	+		
Спростування дії	+		

Коефіцієнт важливості 1 має найменший рівень, а коефіцієнт важливості 3 – найбільший рівень. Зазначені коефіцієнти враховуються у подальшому при визначенні наслідків від ймовірної реалізації зазначених загроз.

У залежності від об’єкту критичної інфраструктури перелік загроз у табл. 2.2 та коефіцієнти важливості загроз можуть змінюватися, з урахування особливостей кожного об’єкта та кожної інформаційної системи.

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

$$G = \left[g_{dn} \right], \tag{2.6}$$

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 (2.6) 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 (2.6).

Взаємозв’язок між загрозами та об’єктами критичної інфраструктури, можливо представити у вигляді матриці:

$$G = \left[g_{ne} \right], \qquad (2.7)$$

Елементи g_{ne} матриці (2.7) набувають значення 1, якщо n–та загроза має місце на e-му об’єкті критичної інфраструктури, і набувають значення 0 – в протилежному випадку.

Нехай H_n – наслідки від реалізації n–ї загрози, де n змінюється від 1 до N; N - кількість можливих загроз.

Тоді, наслідки від реалізації кіберзагроз об’єкту критичної інфраструктури (для енергетичного сектору – це одна із енергетичних систем, табл.1.2) буде визначатися наступним чином:

$$H_e = \sum_{n=1}^{N} H_{ne} \cdot k_{re} \cdot g_{ne} , \qquad (2.8)$$

де H_{ne} – наслідки від реалізації *n*–ї загрози на *e*-му об’єкті критичної інфраструктури. Визначається для кожної інформаційної системи кожного об’єкту критичної інфраструктури, з урахування специфіки функціонування;

k_{re} – коефіцієнт важливості загрози для даного об’єкта критичної інфраструктури, визначається з табл. 2.2;

g_{ne} – коефіцієнт, який визначається, як елемент матриці (2.7) для *n*–ї загрози *e*-го об’єкта критичної інфраструктури.

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

$$H = \sum_{e=1}^{E} H_e = \sum_{e=1}^{E} \sum_{n=1}^{N} H_{ne} \cdot k_{re} \cdot g_{ne} ,$$

де H_e - наслідки від реалізації загрози кібербезпеці інформаційної системи *e*-го об’єкту критичної інфраструктури; *e* змінюється від 1 до *E*; *E* - кількість об’єктів критичної інфраструктури (для енергетичного сектору кількість об’єктів у ОЕС України);

k_{re} – коефіцієнт важливості загрози для даного об’єкта критичної інфраструктури, визначається з табл. 2.2;

g_{ne} – коефіцієнт, який визначається, як елемент матриці (2.7) для *n*-ї загрози *e*-го об’єкта критичної інфраструктури.

На відміну від традиційних систем ІТ, в АСУ ТП існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями [22]. Тому, порушення інформаційної безпеки в АСУ ТП може призвести до наслідків у промисловому секторі.

Враховуючи зазначене, небезпека атаки в АСУ ТП буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем управління технологічними процесами, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної атаки.

Як випливає з виразів (2.8) і (2.9) для оцінки коефіцієнта небезпеки атак необхідні наступні вихідні дані:

- перелік загроз безпеки інформації;
- перелік можливих атак;
- взаємозв’язок між можливими атаками і загрозами;
- взаємозв’язок між можливими атаками і наслідками від їх реалізації.

2.5. Метод визначення актуальності загрози кібербезпеки об’єктів критичної інфраструктури

Кожна загроза безпеці інформації, якщо вона є актуальною для систем управління ОКІ, після ідентифікації підлягає нейтралізації і блокуванні, тобто, в системах управління ОКІ із заданими структурно функціональними характеристиками і особливостями функціонування існує ймовірність реалізації загрози порушником з відповідним потенціалом і реалізація цієї загрози призведе до неприпустимих негативних наслідків - збитку, втрат, шкоди.

При всій важливості питання щодо визначення актуальних загроз безпеці інформації на ОКІ, на сьогоднішній день в нашій державі зазначене питання залишається недостатньо вивченим та дослідженим і наполегливо потребує розвитку.

Кожна загроза характеризується ймовірністю її реалізації і нанесеними нею збитками [27-30]. Таким чином, показник актуальності загрози ОКІ буде пропорційний ймовірності реалізації даної загрози та коефіцієнту її небезпеки.

В класифікації загроз можливо виділити два найбільш важливих їх типу:

- намір завдати шкоди, який проявляється у вигляді анонсованого мотиву діяльності суб'єкта;
- можливість нанесення шкоди - існування достатніх для цього умов і факторів.

Особливість першого типу загроз полягає в невизначеності можливих наслідків, неясності питання про наявність у загрозливого суб'єкта сил і засобів, достатніх для здійснення наміру.

Можливість нанесення шкоди полягає в існуванні достатніх для цього умов і факторів. Особливість загроз даного типу полягає в тому, що оцінка потенціалу сукупності факторів, які можуть послужити перетворенню цих можливостей і умов для нанесення шкоди, може бути здійснена тільки суб'єктами загроз.

Метою визначення актуальності загроз безпеці інформації є встановлення того, чи існує можливість порушення конфіденційності, цілісності або доступності інформації, що міститься в ОКІ, і чи призведе порушення хоча б одного з вказаних властивостей безпеки інформації до неприйнятних збитків.

У процесі визначення загроз безпеці інформації на всіх стадіях (етапах) життєвого циклу інформаційних систем необхідно регулярно проводити ідентифікацію джерел загроз, оцінювати їх можливості і визначати на цій

основі загрози безпеці інформації. Дані про порушників і їх можливості з реалізації загроз безпеці інформації, отримані при ідентифікації джерел загроз, включаються до моделі загроз безпеці інформації.

З метою проведення дослідження та аналізу взаємодії джерел загроз, власне самих загроз, сприятливих умов реалізації цих загроз, уразливостей, активів, як об’єктів впливу зловмисників, а також системи захисту інформації, яка запобігає даному впливу, розглянемо узагальнену модель процесу захисту інформації, рис. 2.9.

Таким чином, для ідентифікації загроз безпеці інформації в ОКІ необхідно визначити:

- джерела загроз: можливості (тип, вид, потенціал) порушників;
- вразливості, які можуть використовуватися при реалізації загроз безпеці інформації;
- сприятливі умови для реалізації загроз безпеці інформації;
- активи: об'єкти впливу ОКІ, на які спрямована загроза безпеці інформації;
- коефіцієнт небезпеки загроз: результат і наслідки від реалізації загроз безпеці інформації.

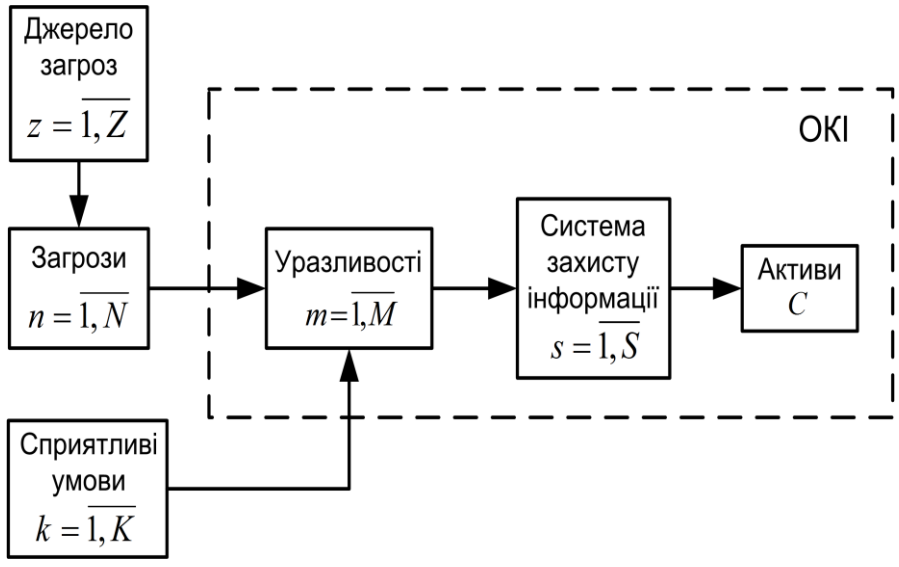


Рис. 2.9. Узагальнена модель процесу захисту інформації ОКІ

Структурна модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури показує, рис. 2.5, що кожну загрозу кібербезпеці інформаційної системи, яка циркулює в інформаційній системі об’єкту критичної інфраструктури, можливо описати наступним чином:

$$n = f\left(Z_n, U_n, K_n, H_n, C\right), \tag{2.10}$$

де Z_n - джерела *n*-ї загрози кібербезпеці інформаційної системи;

- U_n - уразливості, через які можливі реалізації *n*-ї загрози кібербезпеці інформаційної системи;
- K_n - сприятливі умови для реалізації *n*-ї загрози кібербезпеці інформаційної системи об’єкта критичної інфраструктури енергетичного сектору;
- H_n - наслідки від реалізації *n*-ї загрози кібербезпеці інформаційної системи об’єкта критичної інфраструктури;
- C - активи ОКІ, яким можуть бути нанесені збитки у випадку реалізації *n*-ї загрози кібербезпеці інформаційної системи.

Загроза безпеці інформації, яка циркулює на ОКІ, буде вважатися актуальною, якщо для вказаного ОКІ 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.

Це викликано тим, що в автоматизованих системах ОКІ існує досить тісний взаємозв’язок автоматизованих систем з фізичними процесами і виконавчими пристроями [30]. Тому, порушення безпеки інформації в даних системах може призвести до наслідків у промисловому секторі.

Враховуючи зазначене, небезпека загрози в автоматизованих системах ОКІ із множини загроз буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем ОКІ, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної загрози [31].

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

$$A_n = f\left\{P\left(H_{nu}\middle|K_n\right);H_n\right\}, \qquad (2.11)$$

де $P\left(H_{nu}\middle|K_n\right)$ - 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'єктів критичної інфраструктури (наприклад, для енергетичного сектору - ОЕС).

Ймовірність реалізації загрози можливо визначити на основі аналізу статистичних даних про частоту реалізації загроз безпеці інформації (виникненні інцидентів безпеки) в автоматизованих системах ОКІ і/або однотипних систем.

За відсутності таких статистичних даних актуальність загрози визначається на основі оцінки можливості реалізації загрози безпеці інформації, яка, в свою чергу, визначається на основі оцінки рівня захищеності автоматизованої системи ОКІ та потенціалу порушника, необхідного для реалізації даної загрози.

Коефіцієнт небезпеки загрози можливо визначити на основі оцінки ступеня наслідків від порушення конфіденційності, цілісності або доступності інформації в автоматизованих системах ОКІ.

Актуальність загроз безпеці інформації визначається щодо загроз, для яких експертним методом обумовлено наступне:

- можливості (потенціал) порушника достатні для реалізації загрози безпеці інформації;

- в автоматизованій системі ОКІ є потенційні уразливості, які можуть бути використані при реалізації певної загрози безпеці інформації;

- структурно-функціональні характеристики та особливості функціонування автоматизованої системи ОКІ не виключають можливості застосування способів, необхідних для реалізації певної загрози, тобто існує сценарій реалізації загрози;

- реалізація загрози безпеці інформації призведе до порушення конфіденційності, цілісності або доступності інформації, в результаті якого можливе виникнення неприйнятних негативних наслідків, заподіяння значної шкоди.

Джерелами інформації щодо вихідних даних про загрози безпеці інформації та їх характеристики можуть бути базові та типові моделі загроз безпеці інформації, визначені нормативними документами для різних класів і типів автоматизованих систем [32-33].

Визначимо оцінку ймовірності (можливості) реалізації загрози безпеці інформації. Під ймовірністю реалізації загрози безпеці інформації будемо розуміти показник, визначений експертним шляхом, що характеризує значення ймовірності реалізації певної (n-ої) загрози безпеці інформації в автоматизованій системі ОКІ із заданими структурно-функціональними характеристиками і особливостями функціонування. Для цього необхідно ввести градації даного показника щодо n-ої загрози, який можливо описати наступним чином:

$$P(R_n) = f(K_n; S_n; q_n; \omega_n), \qquad (2.12)$$

де 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 енергетичного сектору;

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

У випадку відсутності необхідних даних для оцінки ймовірності реалізації загрози безпеці інформації або наявності сумнівів в об'єктивності експертних оцінок при визначенні градацій ймовірності реалізації загроз безпеці інформації, актуальність *n*-ої загрози безпеці інформації визначається на основі оцінки можливості її реалізації.

Можливість реалізації *n*-ої загрози безпеці інформації можливо оцінити виходячи із рівня захищеності автоматизованої системи і потенціалу порушника, необхідного для реалізації цієї загрози безпеці інформації в автоматизованій системі ОКІ із заданими структурно функціональними характеристиками і особливостями функціонування. Отже, можливість реалізації *n*-ої загрози можливо описати наступним чином:

$$W(H_n) = f(X_n; Y_n), \tag{2.13}$$

де X_n - рівень захищеності автоматизованої системи ОКІ щодо реалізації *n*-ої загрози;

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

Очевидно, що при введенні автоматизованої системи ОКІ в експлуатацію повинен забезпечуватися високий рівень захищеності від

порушника із заданим потенціалом.

Однак, в ході експлуатації автоматизованих систем ОКІ можлива поява нових уразливостей систем, підвищення потенціалу порушника, зміна структурно-функціональних характеристик, важливості оброблюваної інформації, особливостей функціонування зазначених систем та інших умов, що призводять до виникнення нових загроз безпеці інформації, які можуть суттєво знизити рівень проектної захищеності даних систем. У цьому випадку для підтримки рівня захищеності автоматизованих систем ОКІ в ході експлуатації повинен проводитися регулярний аналіз зміни загроз безпеці інформації, а актуальні загрози безпеці інформації повинні підлягати періодичній переоцінці.

Таким чином, рівень захищеності автоматизованої системи ОКІ можливо визначити на основі аналізу наступної інформації:

- чи з'явилися додаткові загрози безпеці інформації в ході експлуатації;

- чи можуть бути вжиті заходи захисту інформації щодо додаткових загроз безпеці інформації, що з’явились в ході експлуатації;

- з якою оперативністю можна нейтралізувати додаткові загрози безпеці інформації, які з’явилися в ході експлуатації.

Потенціал порушника для реалізації певної загрози безпеці інформації можливо визначити на основі даних, наведених у базових і типових моделях загроз безпеці інформації, які визначаються нормативними документами для інформаційних систем різних класів і типів.

Визначимо оцінку ступеня можливого збитку від реалізації загрози безпеці інформації. Для оцінки ступеня можливого збитку H_n від реалізації n-ої загрози безпеці інформації визначаються можливий результат реалізації загрози безпеці інформації в автоматизованій системі ОКІ, вид збитку, до якого може призвести реалізація загрози безпеці інформації, ступінь наслідків від реалізації загрози безпеці інформації для кожного виду збитку.

В результаті реалізації загрози безпеці інформації можливі прямий або непрямий впливи на конфіденційність, цілісність, доступність інформації, що

циркулює в автоматизованій системі управління ОКІ [34].

Прямий вплив на конфіденційність, цілісність, доступність інформації можливий в результаті реалізації прямої загрози безпеці інформації. У цьому випадку об'єктами впливу загрози є безпосередньо інформація та/або інші об'єкти захисту, які забезпечують отримання, обробку, зберігання, передачу, знищення інформації в автоматизованих системах ОКІ, в результаті доступу до яких або впливу на які можливий вплив на конфіденційність, цілісність або доступність інформації.

Непрямий вплив на конфіденційність, цілісність, доступність інформації розглядається в результаті реалізації непрямих загроз безпеці інформації. Реалізація непрямих загроз безпеці інформації не приводить безпосередньо до впливу на конфіденційність, цілісність, доступність інформації, але створює умови для реалізації одної або декількох прямих загроз безпеці інформації, що дозволяють реалізувати такий вплив. У цьому випадку в якості результату реалізації непрямої загрози необхідно розглядати результати реалізації всіх прямих загроз безпеці інформації, які можливо реалізувати в разі реалізації даної непрямої загрози.

При визначенні ступеня можливого збитку необхідно виходити з того, що в залежності від цілей і завдань, що вирішуються автоматизованою системою ОКІ, видів оброблюваної інформації, вплив на конфіденційність, цілісність або доступність кожного виду інформації, що міститься в системі, може призвести до різних видів збитку. При цьому для різних власників інформації будуть характерні різні види збитку.

Як зазначається в [30], основними категоріями впливу в автоматизованих системах управління ОКІ є:

- фізичний вплив – включає в себе безліч прямих наслідків аварій автоматизованих систем управління технологічними процесами. Найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей. Інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;

- економічні впливи - наслідки другого порядку від фізичних впливів, що є похідними від аварій автоматизованих систем управління технологічними процесами. Фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації. У великих масштабах, ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;

- соціальні впливи - наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

Враховуючи приведені вище категорії впливу в автоматизованих системах управління ОКІ можливо навести перелік наслідків цих впливів [30]:

- порушення національної безпеки;
- сприяння вчиненню акту тероризму;
- втрата або скорочення виробництва;
- травми або смерть людей;
- пошкодження обладнання;
- викид (витікання, випаровування) або крадіжка небезпечних матеріалів;
- екологічні збитки;
- кримінальні або цивільно-правові зобов'язання;
- втрата приватної або конфіденційної інформації;
- втрата іміджу бренду або довіри клієнтів.

Зазначені наслідки можуть доповнюватися іншими видами залежно від цілей і завдань, що вирішуються автоматизованою системою ОКІ, а також виду інформації, яка в ній обробляється.

Ступінь можливих наслідків H_n від реалізації n-ої загрози безпеці інформації визначається ступенем негативних наслідків від порушення конфіденційності, цілісності або доступності кожного виду інформації, що циркулює в автоматизованій системі ОКІ.

Таким чином, ступінь негативних наслідків від порушення

конфіденційності, цілісності або доступності інформації визначається для кожного виду збитку, залежить від цілей і завдань, які виконуються автоматизованою системою ОКІ, і може мати різні значення для різних власників інформації і операторів, і визначається експертним методом.

Для оцінки ступеня можливого збитку від реалізації загрози безпеки інформації визначаються можливий результат реалізації загрози безпеки інформації в інформаційній системі об’єкту критичної інфраструктури, вид збитку, до якого може призвести реалізація загрози безпеки інформації, ступінь наслідків від реалізації загрози безпеки інформації для кожного виду збитку.

В якості результату реалізації загрози безпеки інформації розглядається безпосереднє чи опосередкований вплив на конфіденційність, цілісність, доступність інформації, що міститься в інформаційній системі об’єкту критичної інфраструктури.

Результат реалізації загрози безпеки інформації визначається впливом загрози на кожну властивість безпеки інформації (конфіденційність, цілісність, доступність) окремо відповідно до табл. 2.3 [37].

Таблиця 2.3

Результати реалізації загроз

Властивість безпеки інформації	Результат реалізації загрози безпеки інформації	
	Не має впливу	Має вплив
Конфіденційність $X^{К}_{к1}$	У результаті реалізації загрози безпеки інформації відсутня можливість неправомірного доступу, копіювання, надання або поширення інформації	У результаті реалізації загрози безпеки інформації є можливість неправомірного доступу, копіювання, надання або поширення інформації

Продовження таблиці 2.3

Цілісність $X^{Ц}_{к1}$	У результаті реалізації загрози безпеки інформації відсутня можливість знищення або модифікація інформації	У результаті реалізації загрози безпеки інформації є можливість знищення або модифікація інформації
Доступність $X^{Д}_{к1}$	У результаті реалізації загрози безпеки інформації відсутня можливість блокування інформації	У результаті реалізації загрози безпеки інформації є можливість блокування інформації

При визначенні ступеня можливого збитку необхідно виходити з того, що в залежності від цілей і завдань, що вирішуються ІС ОКІ, видів оброблюваної інформації, вплив на конфіденційність, цілісність або доступність кожного виду інформації, що міститься в ІС, може призвести до різних видів збитку. При цьому для різних власників інформації будуть характерні різні види збитку.

Основні види збитку і можливі негативні наслідки, до яких може призвести порушення конфіденційності, цілісності, доступності інформації, наведені в табл. 2.4 [37].

Таблиця 2.4

Основні види збитку і можливі негативні наслідки

Вид збитку	Можливі негативні наслідки від порушення конфіденційності, цілісності, доступності інформації
Економічний	Зниження, як мінімум, одного

(фінансовий)	економічного показника. Втрата (крадіжка) фінансових коштів. Недоотримання очікуваної (прогнозованої) прибутку. Необхідність додаткових (незапланованих) витрат на виплати штрафів (неустойок) або компенсацій. Необхідність додаткових (незапланованих) витрат на закупівлю товарів, робіт або послуг (у тому числі закупівля програмного забезпечення, технічних засобів, вийшли з ладу, заміна, налагодження, ремонт зазначених коштів). Необхідність додаткових (незапланованих) витрат на відновлення діяльності. Втрата клієнтів, постачальників. Втрата конкурентної переваги. Неможливість укладення договорів, угод. Інші прямі або непрямі фінансові втрати
Соціальний	Створення передумов для нанесення шкоди здоров'ю громадян. Можливість порушення функціонування об'єктів забезпечення життєдіяльності

	громадян. Організація пікетів, страйків, мітингів та інших акцій. Звільнення. Збільшення кількості скарг в органи державної влади чи органи місцевого самоврядування. Поява негативних публікацій у загальнодоступних джерелах. Неможливість (переривання) надання соціальних послуг (сервісів). Інші наслідки, що призводять до наростання соціальної напруженості в суспільстві
Політичний	Створення передумов до загострення відносин у міжнародних відносинах. Зрив двосторонніх (багатосторонніх) контактів з закордонними партнерами. Нездатність виконання міжнародних (двосторонніх) договірних зобов'язань. Неможливість укладення міжнародних (двосторонніх) договорів, угод. Створення передумов до внутрішньополітичної кризи. Порушення виборного процесу. Інші наслідки у

	внутрішньополітичній та зовнішньополітичних сферах діяльності
Репутаційний	Порушення законодавчих та підзаконних актів. Порушення ділової репутації. Зниження престижу. Дискредитація працівників. Втрата довіри. Нездатність виконання договірних зобов'язань. Інші наслідки, що призводять до порушення репутації
Збиток в області оборони, безпеки та правопорядку	Створення передумов до наступу негативних наслідків для оборони, безпеки та правопорядку. Порушення громадського правопорядку. Несприятливий вплив на забезпечення громадського правопорядку. Можливість втрати або зниження рівня контролю за громадським правопорядком. Відсутність можливості оперативного оповіщення населення про надзвичайну ситуацію. Інші наслідки, що приводять до збитку в області оборони, безпеки та

	правопорядку
Збиток суб'єкту персональних даних	Створення загрози особистої безпеки. Фінансові чи інші матеріальні втрати фізичного особи. Вторгнення в приватне життя. Створення загрози здоров'ю. Моральна шкода. Втрата репутації. Інші наслідки, що призводять до порушення прав суб'єкта персональних даних
Технологічний	Неможливість вирішення завдань (реалізації функцій) або зниження ефективності вирішення завдань (реалізації функцій). Необхідність зміни (перестроювання) внутрішніх процедур для досягнення цілей, вирішення завдань (реалізації функцій). Ухвалення неправильних рішень. Простій інформаційної системи або сегмента інформаційної системи Інші наслідки, що призводять до порушення технології обробки інформації

Зазначені види збитку можуть доповнюватися іншими видами залежно від цілей і завдань, що вирішуються ІС ОКІ, а також виду інформації, яка в

ній оброблюється.

Ступінь можливого збитку від реалізації загрози безпеки інформації визначається ступенем негативних наслідків від порушення конфіденційності, цілісності або доступності кожного виду інформації, що є в ІС ОКІ.

Ступінь негативних наслідків від порушення конфіденційності, цілісності або доступності інформації визначається для кожного виду збитку, залежить від цілей і завдань, розв'язуваних ІС ОКІ, і може мати різні значення для різних власників інформації і операторів. В якості єдиної шкали вимірювання ступеня негативних наслідків приймаються значення “незначні”, “помірні” і “істотні” негативні наслідки. Кожним власником визначається у зазначеній єдиній шкалі вимірювань ступінь негативних наслідків від порушення конфіденційності, цілісності або доступності інформації стосовно всіх цілей і завдань, які вирішує ІС ОКІ.

Ступінь можливого збитку визначається експертним методом згідно з табл. 2.5 [37].

Таблиця 2.5

Ступінь можливого збитку

Ступінь збитку	Характеристика ступеня збитку
Висока	В результаті порушення однієї з властивостей безпеки інформації (конфіденційності, цілісності, доступності) можливі суттєві негативні наслідки. ІС ОКІ і (або) власник інформації не можуть виконувати покладені на них функції
Середня	В результаті порушення однієї з властивостей безпеки інформації (конфіденційності, цілісності, доступності) можливі помірні негативні наслідки. ІС ОКІ і (або) власник інформації не можуть виконувати хоча б одну з покладених на них функцій

Продовження таблиці 2.5

Низька	В результаті порушення однієї з властивостей безпеки інформації (конфіденційності, цілісності, доступності) можливі незначні негативні наслідки. ІС ОКІ і (або) власник інформації можуть виконувати покладені на них функції з недостатньою ефективністю або виконання функцій можливе тільки з залученням додаткових сил і засобів

Кожному значенню ступеня збитку, табл. 2.5., присвоюється відповідний коефіцієнт, який визначається експертним шляхом, і використовується у виразі (2.8).

При обробці в ІС ОКІ двох і більше видів інформації ступінь можливого збитку визначається окремо для кожного виду інформації, що обробляється в ІС ОКІ, стосовно до кожного виду збитку. Підсумковий ступінь можливого збитку встановлюється за найвищим значенням ступеня можливого збитку, визначеним для конфіденційності, цілісності, доступності інформації кожного виду інформації стосовно до кожного виду збитку [37]:

$$X_K = max_i\ (X^i_K);\ i = К, Ц, Д.$$

З урахуванням викладеного, схематичне відображення методу визначення актуальності загрози кібербезпеки інформаційної системи об’єкту критичної інфраструктури, представлена у загальному вигляді на рис.2.10.

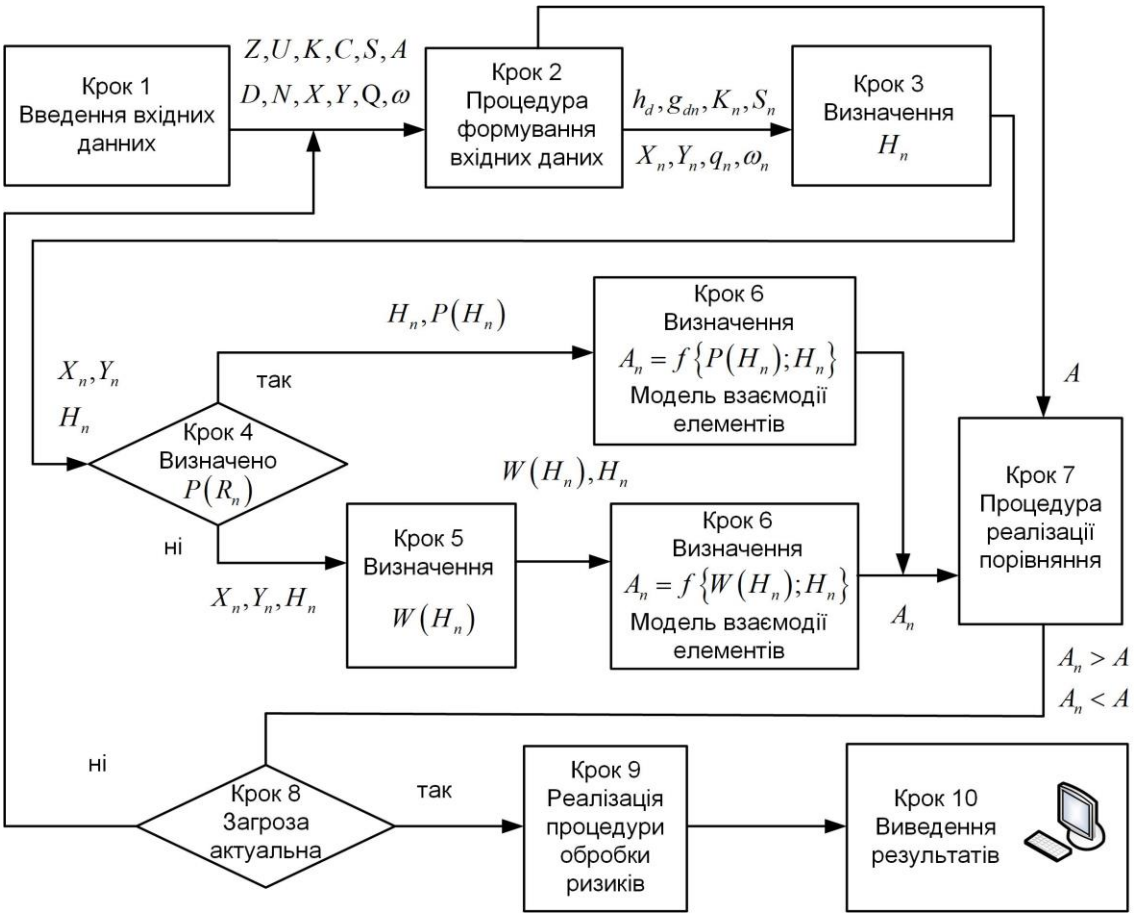


Рис. 2.10. Схематичне відображення методу визначення актуальності загрози

У випадку виявлення загрози безпеці інформації визначаємо її актуальність.

Визначення актуальності загрози ґрунтується на аналізі вхідних даних, а саме:

- наявності чи відсутності сприятливих умов для реалізації даної загрози;
- наявності чи відсутності необхідної статистики щодо фактів реалізації даної загрози;
- наявності чи відсутності у потенційних порушників мотивації для реалізації даної загрози;
- можлива частота реалізації даної загрози;
- рівень захищеності автоматизованої системи ОКІ щодо реалізації даної загрози;
- потенціал порушника, необхідний для реалізації даної загрози.

Разом з тим, визначається ступінь можливих наслідків у випадку реалізації виявленої загрози.

У подальшому, в залежності від наявних вихідних даних, здійснюється або оцінка ймовірності реалізації виявленої загрози, або оцінка можливості її реалізації.

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

2.6. Висновки до другого розділу

1. Виконано аналіз факторів, що впливають на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури. Результати проведеного аналізу можливо використати при розробці пропозицій та заходів щодо кіберзахисту інформаційних систем об’єктів критичної інфраструктури.

2. Приведена модель імовірних деструктивних дій обслуговуючого персоналу АСУ ТП при умові наявності зовнішніх та/або внутрішніх дестабілізуючих впливів.

3. Проведено аналіз джерел загроз та уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами, досліджено взаємозв’язки між загрозами, уразливостями і ризиком для автоматизованих систем управління технологічними процесами.

4. Приведено життєвий цикл аналізу ймовірності реалізації загроз інформаційної безпеки автоматизованих систем управління технологічними процесами та сформульовано вихідні дані, які необхідні для цього аналізу.

5. Враховуючи викладене можна сформулювати наступні висновки:

- за результатами дослідження, загрози класифіковані за наступними категоріями:

- несанкціонований доступ до інформації;

- несанкціоновані зміни або викрадення інформації;

- відмова в обслуговуванні або профілактика авторизованого доступу;

- відмова у визнанні участі, авторства або відмова від одержання.

- активи ІС ОКІ класифіковані за видами як фізичні, логічні та людські, а збитки представлені як прямі і непрямі.

- в ході аналізу взаємозв'язку між загрозами і можливими атаками визначено підходи до оцінки коефіцієнта небезпеки атак в ІС ОКІ. Вихідними даними необхідними для оцінки коефіцієнта є:

- перелік загроз безпеки інформації;

- перелік можливих атак;

- взаємозв'язок між можливими атаками і загрозами;

- взаємозв'язок між можливими атаками і наслідками від їх реалізації.

6. 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.

7. 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.

Основні результати дисертаційної роботи, представлені в розділі 2,

опубліковані в працях автора [3, 7, 14, 20,21, 30, 34].

Список використаних джерел до другого розділу

1. Кабінет міністрів України. (2016, Серп. 23). Постанова № 563, Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF. Дата звернення: Серп. 02, 2016.

2. В.В. Домарев, Безопасность информационных технологий. Методология создания систем защиты. Киев, Украина: ООО "ТИД "ДС", 2002.

3. С.Ф. Гончар, Г.П. Леоненко, та О.Ю. 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. International Electrotechnical Commission. 2009. IEC 62443-1-1, Industrial communication network – Network and system security. Part 1-1: Terminology, concepts and models. [Online]. Available: https://webstore.iec.ch/publication/7029. Accessed on: Aug. 02, 2016.

5. Д.А. Ловцов, и Н.А. Сергеев, Управление безопасностью эргасистем. Москва, Россия: РАУ-Университет, 2001.

6. Мохор В.В. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В.В.Мохор, А.М. Богданов, А.С. Килевой – К.: ООО «ТриК», 2013. – 129 с.

7. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання». – К.: НАДУ, 2014. – С. 92-95.

8. Лефевр В.А. Алгебра совести / Лефевр В.А.; [пер. с англ. В. Лефевр и Е. Юдиной]. - М.: Когито-Центр, 2003. – 426 с.

9. Ловцов Д.А., Сергеев Н.А. Управление безопасностью эргасистем / Под ред. Д.А. Ловцова, - 2-е изд. испр. и доп. – М.: РАУ-Университет, 2001. – 224 с.

10. Силов В.Б. Принятие стратегических решений в нечеткой обстановке. – М.: ИНПРО – РЕС, 1995. – 228с.

11. Емелин В.И. Методы и модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими системами: дис. … доктора техн. наук : 05.13.19 / Емелин Вадим Иванович. – СПб., 2012. – 238 с.

12. Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.

13. Теория вероятностей и математическая статистика. Базовый курс с примерами и задачами / [Кибзун А. И., Горяинова Е. Р., Наумов А. В,, Сиротин А.Н.]. – М.: ФИЗМАТЛИТ, 2002. – 224 с.

14. Гончар С.Ф. Особенности обеспечения кибербезопасности индустриальных систем управления : тези доповідей міжнародної науково-практичної конференції «Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК», Київ, – 2013. – С. 36-37.

15. Мохор В.В. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В.В.Мохор, А.М. Богданов, А.С. Килевой – К.: ООО «ТриК», 2013. – 129 с.

16. Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.

17. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.

18. Information technology – Security techniques – Information security risk management: BS ISO/IEC 27005:2008.

19. Industrial communication networks – Network and system security: IEC 62443.– Part 3.

20. Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. Випуск 1 (25).

21. Особенности обеспечения кибербезопасности индустриальных систем управления / Гончар С.Ф. // Тези доповідей міжнародної науково-практичної конференції “Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК”, Київ, – 2013. – С. 36-37.

22. Мохор В.В. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В.В.Мохор, А.М. Богданов, А.С. Килевой – К.: ООО «ТриК», 2013. – 129 с.

23. Грицай Г., Тиморин А., Гольцев Ю., Ильин Р. Безопасность промышленных систем в цифрах. – М.: Positive Technologies, 2012.

24. Теоретико-методологічний аспект забезпечення інформаційної безпеки об’єктів критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Вісник Національного університету “Львівська політехніка”: “Комп’ютерні системи та мережі”. №806. – 2014. – 34 с.

25. Industrial communication networks – Network and system security: IEC 62443-1-1. – Part 1-1: Terminology, concepts and models.

26. Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.

27. IBM 2015 Cyber Security Intelligence Index [Електронний ресурс] // IBM corporation. – 2015. – Режим доступу до ресурсу: http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/sew03073usen.pdf.

28. Cyber security challenges: how do retailers protect the bottom line? [Електронний ресурс] // – 2014. – Режим доступу до ресурсу:

https://securityintelligence.com/cyber-security-challenges-how-do-retailers-protect-the-bottom-line.

29. IBM X-Force Research 2016 Cyber Security Intelligence Index report [Електронний ресурс] // IBM corporation. – 2016. – Режим доступу до ресурсу: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=SEJ03320 USEN &attachment=SEJ03320USEN.PDF.

30. С. Гончар. Визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами, Захист інформації. 2015. – Том 17, № 3. 225-230 с.

31. О.Юдін. Аналіз підходів до визначення галузей критичної інфраструктури. Матеріали XVIII міжнародної науково-практичної конференції “Безпека інформації у інформаційно-телекомунікаційних системах”. Вип.18. - 91 с. м. Київ, 25-26 травня 2016р. / НДЦ «Тезіс» НТУУ «КПІ» / Редкол.: Л.О. Євдоченко (голова) та ін.. – К.: Держспецзв’язку, 2016. – 62с.

32. В.Домарев Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС", 2002. – 688 с.

33. НД ТЗІ 2.1-002-09. Загальні положення про захист інформації в комп’ютерних системах від несанкціонованого доступу : офіц. текст : [затверджений наказом ДСТСЗІ СБ України 28 квітня 1999 року № 22].

34. 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) (2015). 47-52 с.

35. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.

36. Сычев Ю.Н. Основы информационной безопасности : Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007. – 300 с.

37. Дослідження та аналіз проблем захисту інформації на об’єктах критичної інфраструктури. Звіт з НДР (шифр «ІНФРАСТРУКТУРА», державний реєстраційний номер 0114U000038д), К.: ДержНДІ Спецзв’язку, 2015. – 517 с.

РОЗДІЛ 3
МЕТОДИ РОЗРАХУНКУ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Графічний метод розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Дослідженню проблем, пов'язаних із оцінкою ризику кіберзагроз присвячені публікації вітчизняних і зарубіжних вчених [1-6].

Так у [7] розглядаються і детально аналізуються двадцять чотири методи оцінки ризику для систем SCADA. Описується суть методів, розглядаються етапи управління ризиками, запропонована схема класифікації методів ризиків кібербезпеки для SCADA систем.

У роботі [8] 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.

Структура, яка включає в себе принципи роботи страхової галузі для надання кількісних оцінок ризиків кібербезпеки представлена в [9]. Запропонована структура використовує методи оптимізації, щоб запропонувати рівні інвестицій в заходи з кібербезпеки і страхування для стейкхолдерів об'єктів критичної інфраструктури і може бути використана для розробки стратегій по мінімізації ризиків кібербезпеки.

Удосконалення моделі оцінки ризиків кібербезпеки з використанням апарату нечіткої логіки запропоновано в [10]. Модель враховує чотири фактори ризику: уразливість, загроза, ймовірність та вплив.

Нові метрики ризику, шляхом адаптації існуючих методів для розрахунку ризиків і невизначеностей представлені в [11]. Також у роботі пропонується таксономічна класифікація вимог до оцінки кібер-ризиків.

Розглянуті метрики ризику дозволяють вимірювати ризик «Internet of Things», а модель ризику дозволяє встановити прийнятний рівень ризику «Internet of Things».

В роботі [12] пропонується модель оцінки ризику кібербезпеки для пристроїв и систем управління ядерних установок з використанням Байєсовської мережі і дерева подій. Зазначається, що забезпечення кібербезпеки являється важливою проблемою в області ядерної техніки, так як ядерні установки використовують цифрове обладнання і цифрові системи, що можуть призвести до серйозних небезпек у випадку аварії. Показано, що органи, які здійснюють регулювання по усьому світу оголосили про керівні документи кібербезпеки, пов'язані з ядерними установками, включаючи «NRC Regulatory Guide 5.71» (США) і важливо оцінити ризик кібербезпеки у відповідності з цими нормативними документами. В роботі пропонується ймовірнісний метод оцінки ризику кібербезпеки.

Проте, незважаючи на велику кількість досліджень, спрямованих на розробку методів оцінки ризику кібербезпеки, невирішеним залишаються задачі, пов'язані із можливістю визначення сумарного ризику кібербезпеки, максимальних збитків в результаті дії сумарного ризику, ймовірність виникнення максимальних збитків в результаті дії сумарного ризику.

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 в результаті дії сумарного ризику.

Таким чином, оцінювання ризику являється важливою, актуальною науково-практичною задачею і основою для прийняття рішень по обробці ризику.

Метою дослідження є розробка методів оцінювання сумарного ризику кібербезпеки об'єктів критичної інфраструктури.

Існує досить багато понять «ризик». Одне з них визначає ризик *R*, як ймовірність або можливість *p* настання випадкової події, що призводить до певних наслідків *h*, і може визначатися за формулою:

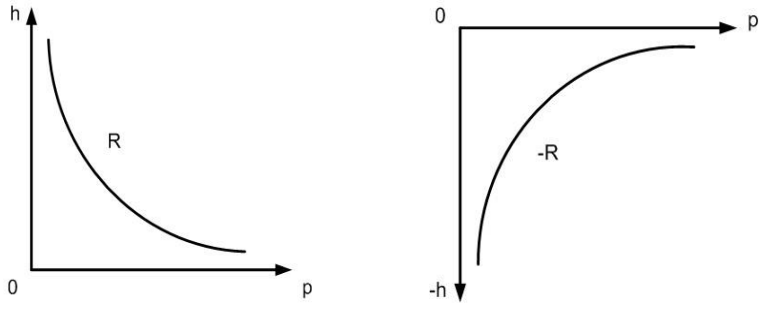
$$R(p,h) = p \cdot h, \tag{3.1}$$

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 або умова, 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.

Графік функції (3.2) для кожного значення $R = const$ буде представляти собою криву, рис. 3.1. На рис. 3.1(а) представлено додатній ризик R, тобто ймовірність *p* настання випадкової події, що призводить до певних втрат. На рис. 3.1(б) представлено від'ємний ризик $-R$, тобто ймовірність *p* настання випадкової події, що призводить до прибутку.



а) б)

Рис. 3.1. Графічне представлення ризику

На підставі виразу (3.1) залежність наслідків h в результаті настання деякої події від її ймовірності p можна представити у вигляді функції:

$$h = f\left(R, p\right). \tag{3.2}$$

Графік проекції функції ризику на площину ph, рис. 3.2, 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 (3.2);

$p \neq 0$.

Нехай існує множина із J ризиків:

$$\begin{gathered} R_1 = p_1 \cdot h_1, \\ \ldots, \\ R_j = p_j \cdot h_j, \\ \ldots, \\ R_J = p_J \cdot h_J. \end{gathered} \tag{3.3}$$

де кожний ризик R_i представлений графіком функції (3.2) і визначається ймовірністю або можливістю p_i настання випадкової події, що може призвести до певних наслідків h_i (точки 1, 2, 3), рис. 3.3. Припустимо, що наслідками у даному випадку будуть збитки.

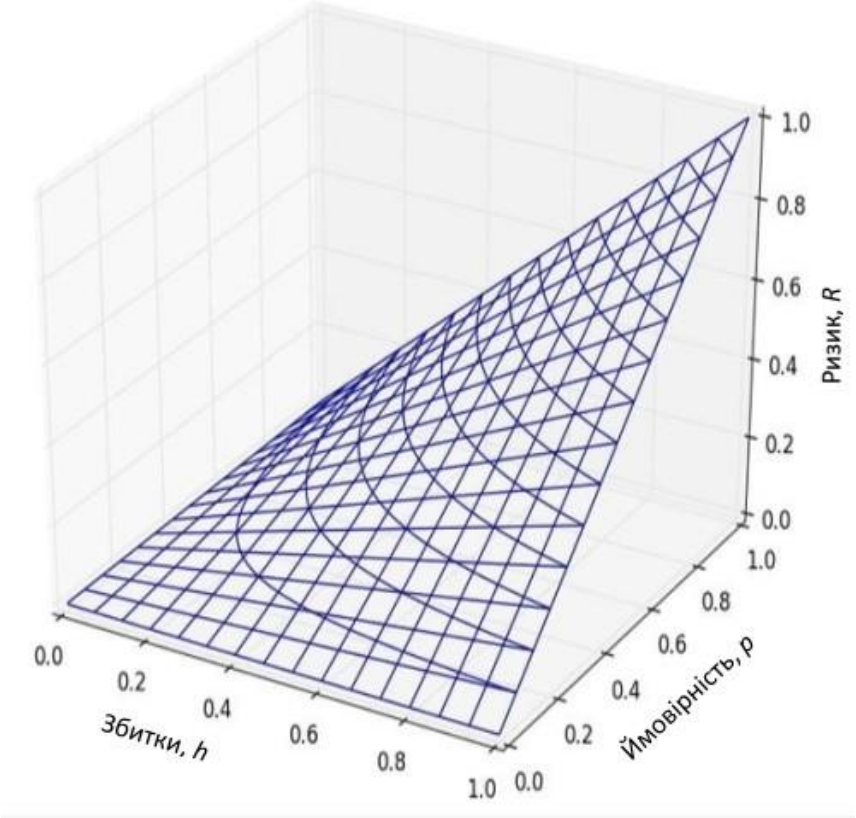


Рис. 3.2. Графік залежності наслідків від їх ймовірностей та величини ризику

Ймовірність буде змінюватися в межах від 0 до 1, а збитки від 0 до максимального значення збитків для певного виду загрози. При цьому буде обмеження: ні ймовірність ні збитки не будуть рівні нулю. Тобто, ні один із ризиків, сума яких визначається, не повинен дорівнювати нулю. Такі ризики просто не враховують у розрахунках.

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, як максимальні збитки, що можуть бути завдані активам компанії (матеріальні, нематеріальні, людські). Якщо мова йде про нематеріальні активи, то їх завжди можливо перерахувати в грошовий еквівалент. Для цього необхідно залучати кваліфікованих фахівців експертів.

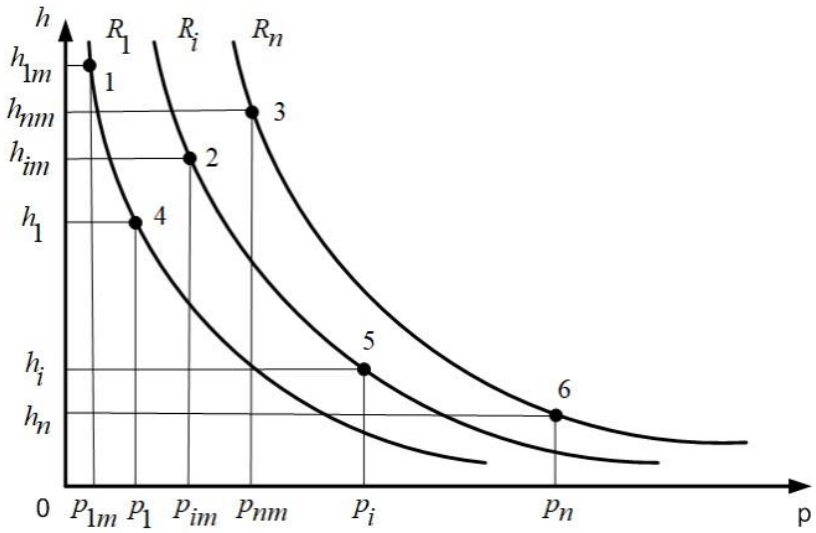


Рис. 3.3. Графік проекції функції ризику на площину *ph*

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. 3.3.

У випадку дії *J* ризиків із множини (3.3) значення суми наслідків не буде перевищувати суми наслідків повного знищення інформаційного активу для кожного із *J* ризиків, без урахування синергетичного ефекту. Вплив даного ефекту не досліджувався у даній роботі і може складати обмеження використання зазначеного методу.

Це означає, що значення суми наслідків повного знищення інформаційного активу буде дорівнювати сумі наслідків повного знищення інформаційного активу для кожного із *J* ризиків:

$$h_m = h_{1m} + ... + h_{Jm} = \sum_{j=1}^{J} h_{jm} . \qquad (3.4)$$

Дія одного або декількох ризиків не виключає дії 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 виникнення 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:

$$p_m = \sum_{j=1}^{J} p_{jm} - \sum_{j<l}^{J} p_{jm} \cdot p_{lm} + \sum_{j<l<k}^{J} p_{jm} \cdot p_{lm} \cdot p_{km} + ... + (-1)^{J-1} \cdot \prod_{j=1}^{J} p_{jm} . \qquad (3.6)$$

Сума *J* ризиків на підставі виразів (3.4) і (3.6) буде визначатися виразом:

$$R_S(h_m, p_m) = h_m \cdot p_m . \qquad (3.7)$$

Використовуючи вираз (3.7), задаючи значення p від 0 до 1, будуємо графік функції, рис. 3.4:

$$h(p) = \frac{R_S}{p} , \qquad (3.8)$$

де $p \neq 0$.

Ймовірність p_S сумарної дії *J* ризиків визначається на підставі виразу (3.6), заміною p_{im} на p_i. Отримаємо вираз:

$$p_S = \sum_{j=1}^{J} p_j - \sum_{j<l}^{J} p_j \cdot p_l + \sum_{j<l<k}^{J} p_j \cdot p_l \cdot p_k + ... + (-1)^{J-1} \cdot \prod_{j=1}^{J} p_j . \qquad (3.9)$$

Величину наслідків h_S у випадку дії сумарного результуючого ризику знаходимо, як ординату точки 2, рис. 3.4.

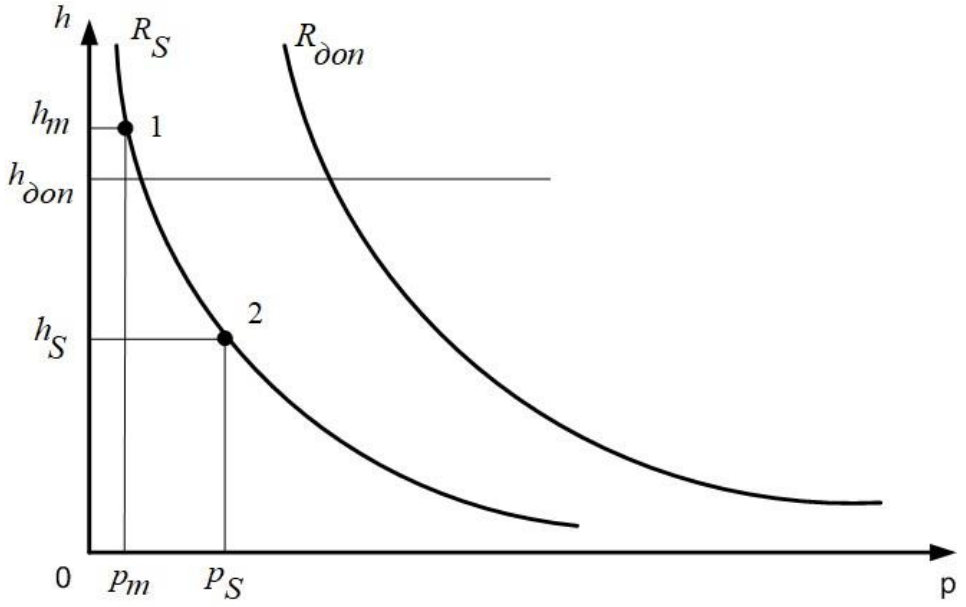


Рис. 3.4. Графік проекції функції суми ризиків на площину *ph*

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.

Визначення суми ризиків даним методом дозволяє розраховувати загальні потенційні збитки, що виникли або можуть виникнути в процесі реалізації певного проекту. Прикладом може бути розрахунок сумарного ризику для бізнесу. Складовими ризиками можуть бути різні види ризику, які виникають в бізнес-процесі, які не дорівнюють нулю та мають ненульову ймовірність заподіяння збитків протягом даного періоду часу.

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 $h_{доп}$. Критерії допустимого ризику або допустимих збитків визначаються власником інформаційної системи, для якої здійснюється розрахунок ризику.

Перевагою даного методу визначення сумарного ризику є наочність і простота розрахунків.

Недоліками даного методу є зазначені вище обмеження: складові ризики не повинні бути рівними нулю і при застосуванні даного методу не враховується дія синергетичного ефекту (у даній дисертаційній роботі не досліджувалася).

Розглянемо застосування графічного методу розрахунку суми ризиків.

На рис. 3.5 такі криві ризиків представлені для випадків *R=1*; *R=5*; *R=10*. В різних точках однієї гіперболи значення ризику буде одне і те саме, але значення ймовірності і збитку будуть різними.

Розглянемо точки А, В и С. Очевидно, що в цих точках ризик буде однаковий і рівний *R=10*. Однак, відрізки ОА, ОВ і ОС мають різну довжину і різний кут нахилу до горизонтальної осі – напрямок. Таким чином, з урахуванням викладеного, ризик може бути представлений величиною та напрямком, тобто вектором.

З урахуванням того, що ризики можуть бути додатними та від'ємними, то у разі наявності таких ризиків одночасно, виникає необхідність здійснювати дослідження та оцінку результуючого ризику.

Нехай *A* – випадкова подія з ймовірністю настання p_1, призводить до певного збитку h_1, і спричиняє ризик $R_1 = p_1 \cdot h_1$, а *B* – випадкова подія з ймовірністю настання p_2, призводить до певного збитку h_2, і спричиняє ризик $R_2 = p_2 \cdot h_2$. Якщо ці дві події настають одночасно, то виникає необхідність оцінки результуючого ризику, для прийняття рішення щодо його подальшої обробки. Якими ж будуть результуючий ризик, результуюча ймовірність та результуючий можливий збиток?

Нехай ризик $R_1=2$, а ризик $R_2=4$. Тоді, використовуючи вираз (3.2)

будуємо гіперболи 1 і 2, що відображають ризики R_1 і R_2 відповідно, рис. 3.6.

Ризик R_1 буде описуватися графіком функції:

$$h_1(p) = \frac{R_1}{p_1}, \tag{3.10}$$

а ризик R_2 буде описуватися графіком функції:

$$h_2(p) = \frac{R_2}{p_2}. \tag{3.11}$$

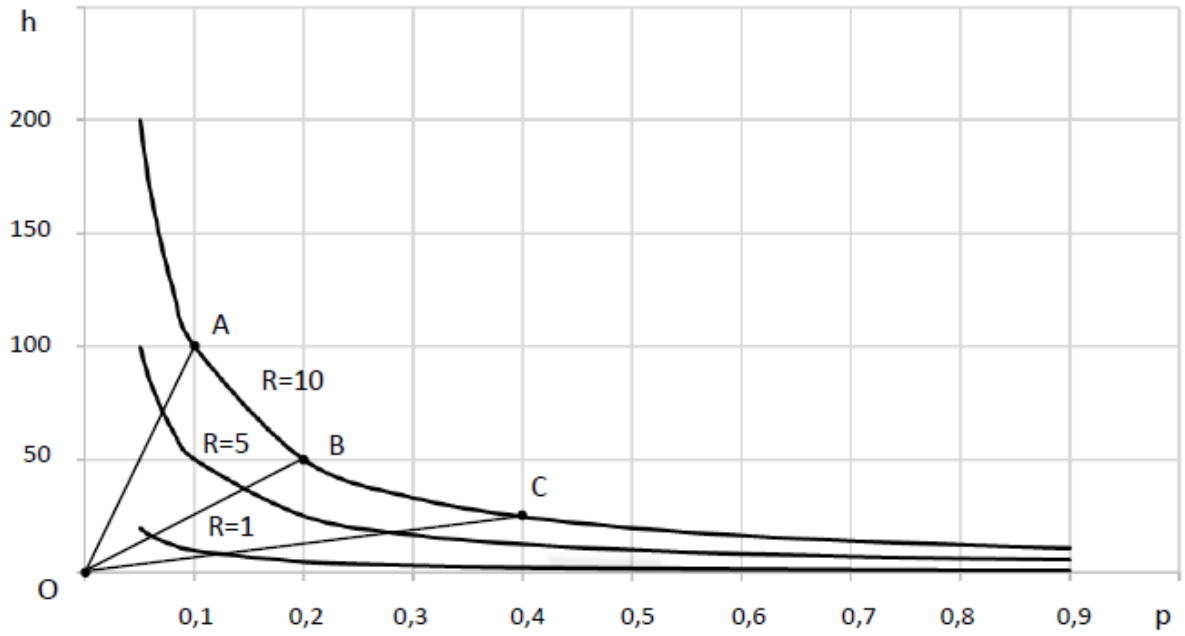


Рис. 3.5. Графічне представлення ризику

Використовуючи метод додавання графіків функцій, додаванням координат, будуємо графік результуючої функції:

$$h(p) = h_1(p) + h_2(p) = \frac{R_1 + R_2}{p(A + B)}. \tag{3.12}$$

З урахуванням того, що події А і В, які спричиняють ризики R_1 і R_2, можуть виникати одночасно і незалежно одна від одної, то дані події будуть сумісні і незалежні. Тоді вираз (3.12) можна записати у вигляді:

$$h(p) = \frac{R_1 + R_2}{p_1 + p_2 - (p_1 \cdot p_2)}. \qquad (3.13)$$

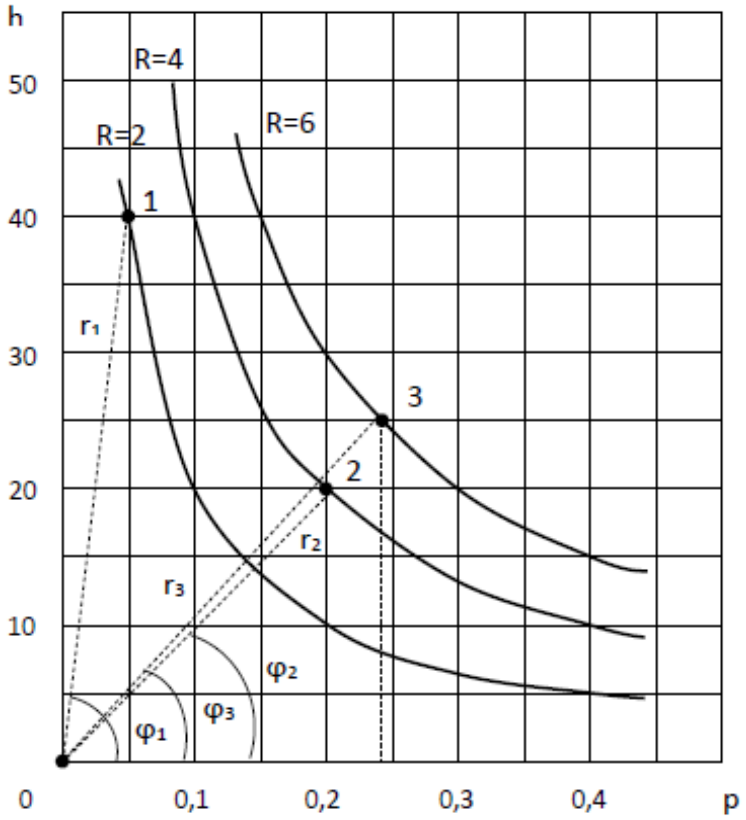


Рис. 3.6. Додавання ризиків

Вираз (3.13) дає можливість визначити значення збитку, який може мати місце в умовах дії двох ризиків.

Розглянемо приклад додавання двох ризиків, рис. 3.6. Нехай *A* – випадкова подія з ймовірністю настання $p_1=0,05$, призводить до певного збитку $h_1=40$, і спричиняє ризик (рис. 3.6, точка 1):

$$R_1 = p_1 \cdot h_1 = 0,05 \cdot 40 = 2, \qquad (3.14)$$

а B – випадкова подія з ймовірністю настання $p_2=0,2$, призводить до певного збитку $h_2=20$, і спричиняє ризик (рис. 3.6, точка 2):

$$R_2 = p_2 \cdot h_2 = 0,2 \cdot 20 = 4\,. \qquad (3.15)$$

Визначимо результуючий ризик $R=R_1+R_2$, як ймовірність p настання результуючої випадкової події, що призводить до певного результуючого збитку h. Ймовірність результуючої події буде визначатися, як ймовірність суми двох випадкових, несумісних і незалежних подій:

$$p = p_1 + p_2 - (p_1 \cdot p_2) = 0,05 + 0,2 - (0,05 \cdot 0,2) = 0,24\,. \qquad (3.16)$$

Використовуючи вираз (6) визначаємо результуючі збитки, що можуть виникнути в умовах існування результуючого ризику (рис. 3.6, точка 3):

$$h = \frac{R_1 + R_2}{p_1 + p_2 - (p_1 \cdot p_2)} = \frac{2+4}{0,05+0,2-(0,05 \cdot 0,2)} = \frac{6}{0,24} = 25\,. \qquad (3.17)$$

Використовувати запропонований метод додавання двох ризиків можна також у випадках, коли обидва ризики від'ємні. При цьому, графіки, зображені на рис. 3.6, будуть симетричні відносно горизонтальної осі, рис.3.7.

Нехай ризик $R_1=-2$, а ризик $R_2=-4$. Тоді, використовуючи вираз (3.2) будуємо гіперболи 1 і 2, що відображають ризики R_1 і R_2 відповідно, рис. 3.7.

Ризик R_1 буде описуватися графіком функції (3.10), а ризик R_2 буде описуватися графіком функції (3.11).

Використовуючи метод додавання графіків функцій, додаванням координат, будуємо графік результуючої функції $R_1=-6$.

Вираз (3.13) дає можливість визначити значення від'ємного збитку,

який може мати місце в умовах дії двох від'ємних ризиків.

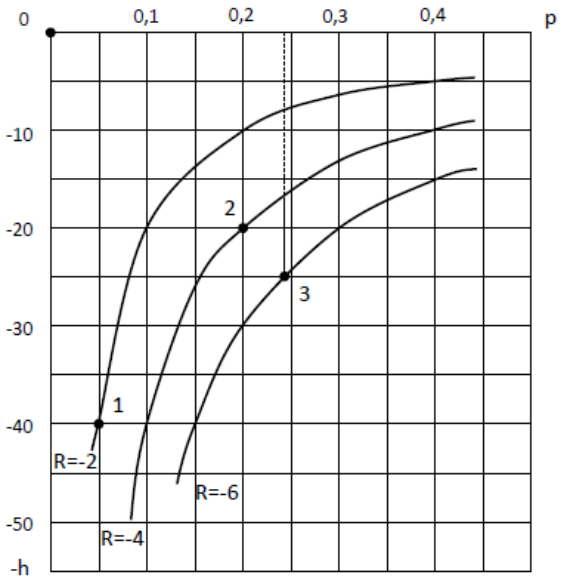


Рис. 3.7. Додавання від'ємних ризиків

Розглянемо приклад додавання двох від'ємних ризиків, рис. 3.7. Нехай *A* – випадкова подія з ймовірністю настання $p_1=0,05$, призводить до певного збитку $h_1=-40$, і спричиняє ризик (рис. 3.7, точка 1):

$$R_1 = p_1 \cdot h_1 = 0,05 \cdot (-40) = -2, \tag{3.18}$$

а *B* – випадкова подія з ймовірністю настання $p_2=0,2$, призводить до певного збитку $h_2=-20$, і спричиняє ризик (рис. 3.7, точка 2):

$$R_2 = p_2 \cdot h_2 = 0,2 \cdot (-20) = -4. \tag{3.19}$$

Визначимо результуючий від'ємний ризик $R=R_1+R_2$, як ймовірність *p* настання результуючої випадкової події, що призводить до певного результуючого від'ємного збитку *h*. Ймовірність результуючої події буде визначатися з виразу (3.16), як ймовірність суми двох випадкових, несумісних і незалежних подій.

На підставі виразу (3.13) визначаємо результуючі від'ємні збитки, що

можуть виникнути в умовах існування результуючого від'ємного ризику (рис. 3.7, точка 3):

$$h = \frac{R_1 + R_2}{p_1 + p_2 - (p_1 \cdot p_2)} = \frac{-2-4}{0,05+0,2-(0,05 \cdot 0,2)} = \frac{-6}{0,24} = -25. \qquad (3.20)$$

Використовуючи запропонований метод, розглянемо приклади операцій додавання та віднімання ризиків, рис. 3.8:

$R_3+R_2= R_1=2+4=6;$ $R_3-R_5=R_1=2-(-4)=6;$ $R_4+R_5=R_6=-2-4=-6;$

$R_4-R_2=R_6=-2-4=-6;$ $R_1-R_3= R_2=6-2=4;$ $R_1+R_4=R_2=6+(-2)=4;$

$R_3-R_1= R_5=2-6=-4;$ $R_3+R_6=R_5=2+(-6)=-4;$ $R_4+R_1=R_2=-2+6=4;$

$R_4-R_6=R_2=-2-(-6)=4;$ $R_6-R_5=R_4=-6-(-4)=-2;$ $R_6+R_2=R_4=-6+4=-2.$

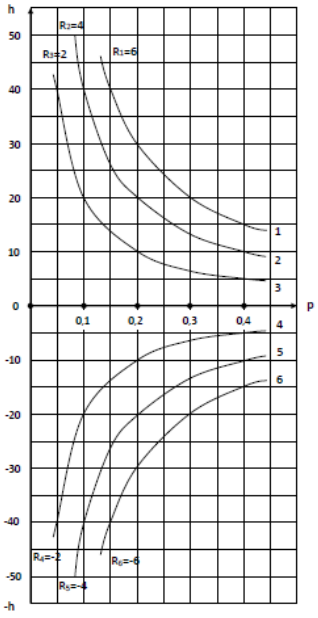


Рис. 3.8. Операції з ризиками

Величину можливих збитків (прибутків) у наведених вище прикладах можливо розрахувати з допомогою виразу (3.13). Аналогічно можна оцінювати ризики в умовах дії декількох ризиків.

3.2. Аналітичний метод розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Як зазначалося вище, ризик *R* визначається як ймовірність *p* випадкової події, що призводить до певних наслідків *h*, і може описуватися виразом (3.1).

Нехай існує множина із *J* ризиків:

$$R = \left\{ R_1 = p_1 \cdot h_1, ..., R_i = p_i \cdot h_i, ..., R_J = p_J \cdot h_J \right\}, \tag{3.21}$$

де кожний ризик R_i визначається ймовірністю p_i випадкової події, що може призвести до певних наслідків h_i.

Визначимо значення наслідків повного знищення інформаційного активу для кожного ризику. Отримуємо множину максимальних наслідків:

$$h_m = \left\{ h_{1m}, ..., h_{Jm} \right\}. \tag{3.22}$$

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 (3.4).

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::

$$p_{jm}\left(R_j, h_{jm}\right) = \frac{R_j}{h_{jm}}, \tag{3.23}$$

де $h_{jm} \neq 0$.

Ймовірність події, що призводить до дії ризиків з наслідками повного знищення інформаційного активу для кожного ризику, визначається з виразу (3.6). При цьому враховуємо, що події сумісні.

Сума дії J ризиків, на підставі виразів (3.4) і (3.6), буде визначатися виразом (3.7). Ймовірність p_S суми дії J ризиків визначається з виразу (3.9).

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

$$h_S\left(R_S, p_S\right) = \frac{R_S}{p_S}, \tag{3.24}$$

де $p_S \neq 0$.

Якщо у якості критерію для визначення варіантів обробки ризику вибрано рівень ризику, то використовуються значення, отримані з виразу (3.7). У випадку застосування у якості критерію величини наслідків – використовуються значення, отримані з виразу (3.24).

Перевагою даного методу визначення суми ризиків є можливість автоматизації розрахунків.

Обмеженнями при використанні графічного та аналітичного 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.

Як відомо, рівень ризику може бути прийнятним, виправданим, неприпустимим. У залежності від рівня ризику можуть застосовуватися

відомі методи його обробки, а саме: прийняття, зменшення, передача, ухилення.

Зазначені відомі методи обробки ризиків передбачають наступні дії:

- прийняття – резервування інформації (створення резервних копій), планування дій на випадок виходу елементів інформаційної системи з штатного режиму функціонування;

- зменшення – зменшення ймовірності кібератак на інформаційну систему, зменшення тяжкості наслідків від даних кібератак у випадку їх реалізації;

- передача – кіберстрахування, послуги по кіберзахисту іншими юридичними чи фізичними особами;

- ухилення – внесення коректив у бізнес-план та план дій по кіберзахисту.

Перелік дій по обробці ризиків кібербезпеки інформаційних систем може бути доповнений з урахуванням особливостей кожної системи.

Схематичне відображення аналітичного методу розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури приведена на рис. 3.9.

Нехай існує два ризики, які визначаються наступним чином:

$$R_1 = p_1 \cdot h_1; \quad R_2 = p_2 \cdot h_2. \tag{3.25}$$

Визначимо значення наслідків повного знищення інформаційного активу h_{1m} і h_{2m} для кожного із ризиків R_1 і R_2 відповідно.

Сумарне значення наслідку повного знищення інформаційного активу буде дорівнювати сумі наслідків повного знищення інформаційного активу для кожного із ризиків:

$$h_m = h_{1m} + h_{2m}. \tag{3.26}$$

Ймовірності подій, що призводять до наслідків повного знищення інформаційного активу в умовах дій ризиків R_1 і R_2, визначаються відповідно:

$$p_{1m} = \frac{R_1}{h_{1m}}; \qquad p_{2m} = \frac{R_2}{h_{2m}}. \tag{3.27}$$

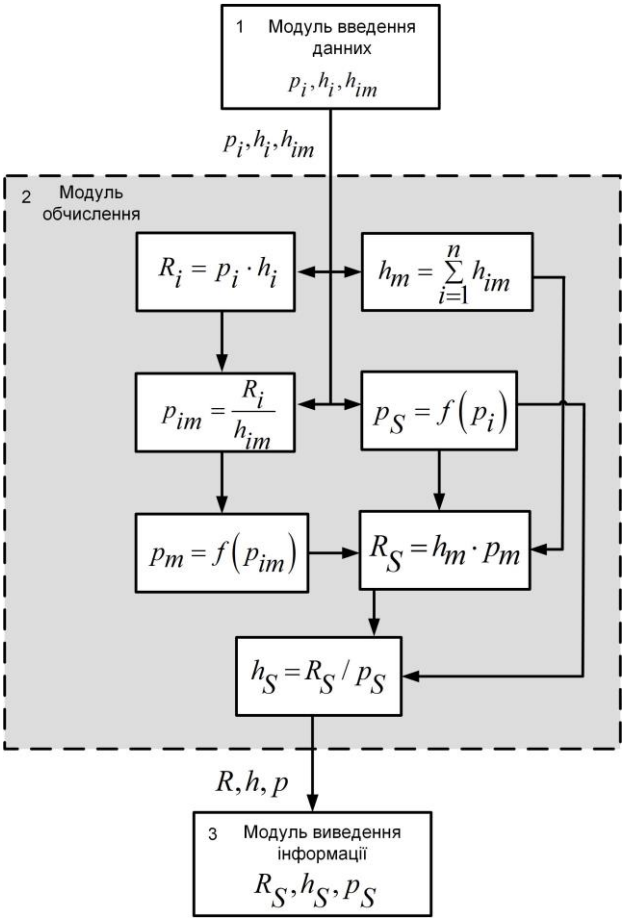


Рис. 3.9. Схематичне відображення методу розрахунку суми ризиків

Ймовірність події, що призводить до дії ризиків R_1 і R_2 з наслідками повного знищення інформаційного активу h_{1m} і h_{2m} в умовах дії кожного

ризику відповідно, визначається, як сума ймовірностей цих подій без ймовірності їх добутку:

$$p_m = p_{1m} + p_{2m} - p_{1m} \cdot p_{2m}. \tag{3.28}$$

Сумарний ризик дії ризиків R_1 і R_2, на підставі виразів (3.26) і (3.27) буде визначатися виразом:

$$R = h_m \cdot p_m. \tag{3.29}$$

З урахуванням виразу (3.27) вираз (3.28) можна представити у вигляді:

$$p_m = \frac{R_1}{h_{1m}} + \frac{R_2}{h_{2m}} - \frac{R_1 \cdot R_2}{h_{1m} \cdot h_{2m}} = \frac{R_1 \cdot h_{2m} + R_2 \cdot h_{1m} - R_1 \cdot R_2}{h_{1m} \cdot h_{2m}}. \tag{3.30}$$

Підставивши вирази (3.26) і (3.30) у вираз (3.29), отримаємо вираз для визначення сумарного ризику:

$$R = \left(h_{1m} + h_{2m}\right) \cdot \left(\frac{R_1 \cdot h_{2m} + R_2 \cdot h_{1m} - R_1 \cdot R_2}{h_{1m} \cdot h_{2m}} \right), \tag{3.31}$$

або після перетворень:

$$R = R_1 + R_2 + R_1 \cdot \frac{h_{2m}}{h_{1m}} + R_2 \cdot \frac{h_{1m}}{h_{2m}} - R_1 \cdot R_2 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right). \tag{3.32}$$

На підставі (3.32), з урахуванням (3.25) і (3.28) отримаємо вираз для визначення наслідків, у випадку дії сумарного результуючого ризику R:

$$h = \frac{R_1 + R_2 + R_1 \cdot \frac{h_{2m}}{h_{1m}} + R_2 \cdot \frac{h_{1m}}{h_{2m}} - R_1 \cdot R_2 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right)}{p_1 + p_2 - p_1 \cdot p_2}. \quad (3.33)$$

Нехай наслідки повного знищення інформаційного активу h_{1m} і h_{2m} ризиків R_1 і R_2 будуть однаковими, тобто $h_{1m} = h_{1m} = h_m$. Тоді вираз (3.32) можна представити у вигляді:

$$R = 2 \cdot \left(R_1 + R_2 - \frac{R_1 \cdot R_2}{h_m} \right). \quad (3.34)$$

У випадку рівності ризиків, тобто $R_1 = R_2 = R_0$, вираз (3.32) можна представити у вигляді:

$$R = R_0 \cdot \left(2 + \frac{h_{2m}}{h_{1m}} + \frac{h_{1m}}{h_{2m}} - R_0 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right) \right), \quad (3.35)$$

де $h_{1m} \neq 0$ і $h_{2m} \neq 0$.

У випадку рівності збитків повного знищення інформаційного активу, тобто $h_{1m} = h_{1m} = h_m$, і рівності ризиків, тобто $R_1 = R_2 = R_0$, вираз (3.32) можна представити у вигляді:

$$R = 2 \cdot R_0 \cdot \left(2 - \frac{R_0}{h_m} \right), \quad (3.36)$$

де $h_m \neq 0$.

3.3. Висновки до третього розділу

1. Запропоновані методи дають можливість визначати сумарний ризик кібербезпеки інформаційних систем об’єктів критичної інфраструктури, сумарні збитки в результаті дії множини кіберзагроз, сумарну величину збитків в результаті дії однієї кіберзагрози за певний період часу, ймовірність виникнення максимальних втрат в результаті дії множини кіберзагроз.

2. Визначення сумарного ризику даними методами дозволяє розраховувати загальні потенційні збитки, що виникли або можуть виникнути в процесі реалізації певного проекту. Прикладом може бути розрахунок сумарного ризику складної розподіленої інформаційної системи об’єкту критичної інфраструктури. Складовими ризиками можуть бути різні види ризику, які виникають в процесі функціонування інформаційної системи, які не дорівнюють нулю та мають ненульову ймовірність заподіяння збитків протягом даного періоду часу.

3. На основі запропонованих методів можливо будувати системи підтримки прийняття рішень щодо застосування заходів по зменшенню ризику.

Основні результати дисертаційної роботи, представлені в розділі 3, опубліковані в працях автора [6, 14].

Список використаних джерел до третього розділу

1. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. 2016. Vol. 253. Issue 1. P.1-13.

2. Jain P., Pasman H. J., Waldram S., Pistikopoulos E. N., Mannan M. S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. Journal of Loss Prevention in the Process Industries. 2018. Vol. 53. P. 61–73.

3. Mokhor V., Bakalynskyi O., Bohdanov O., Tsurkan V. Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry. Information technology and security. 2017. Vol. 5. Issue 1. P.71-82.

4. Bochkovskyi A., Gogunskii V. Development of the method for the optimal management of occupational risks. Eastern-European Journal of Enterprise Technologies. 2018. Vol. 1, № 3 (97). P.6-13.

5. Prokopenko T., Grigor O. Development of the comprehensive method to manage risks in projects related to information technologies. Eastern-European Journal of Enterprise Technologies. 2018. № 2(3) (92). P.37-43.

6. Мохор В.В., Гончар С.Ф. Идея построения алгебры рисков на основе теории комплексных чисел. Электронное моделирование. 2018, 40, № 4, с.107–111.

7. Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. Vol. 56. 2016. P.1-27.

8. Martin Eling, Jan Wirfs._What are the actual costs of cyber risk events? European Journal of Operational Research. 2019. Vol. 272, Issue 3. P.1109-1119.

9. Derek Young, Juan Lopez Jr., Mason Rice, Benjamin Ramsey, Robert McTasney. A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection. Vol. 14. 2016. P.43-57.

10. MansourAlali, AhmadAlmogren, Mohammad MehediHassan, Iehab A.L.Rassan, Md Zakirul AlamBhuiyan. Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security. Vol. 74. 2018. P.323-339.

11. Petar Radanlieva, David Charles De Rourea, Razvan Nicolescub, Michael Huthb, Rafael Mantilla Montalvoc, Stacy Cannadyc, Peter Burnap. Future developments in cyber risk assessment for the internet of things. Computers in Industry. Vol. 102. 2018. P.14-22.

12. Jinsoo Shin, Hanseong Son, Gyunyoung Heo. Cyber Security Risk

Evaluation of a Nuclear I&C Using BN and ET. Nuclear Engineering and Technology. Vol. 49. Issue 3. 2017. P.517-524.

13. Диев В.С. Риск: оценка и принятие решений // Философия науки. 2010, № 4 (47), с. 15–32.

14. Гончар С.Ф. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури / Мохор В.В., Дибач О.М. // Ядерна та радіаційна безпека. – 2019. – №2(82). – С.57-61.

РОЗДІЛ 4
МЕТОД РОЗРАХУНКУ КОМПЛЕКСНОГО РИЗИКУ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

4.1. Об'єктивна та суб'єктивна складові ризику кібербезпеки об'єктів критичної інфраструктури

Прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У відповідності до цього закону кіберзахист – це є сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення кібератак та захист від них, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Забезпечення кібербезпеки досягається створенням системи управління інформаційною безпекою (СУІБ) та (або) створенням комплексної системи захисту інформації (КСЗІ).

Одним з основних етапів створення СУІБ, КСЗІ є процес оцінки ризиків кібербезпеки. Стейкхолдери інформаційних систем прагнуть звести до мінімуму ризики кібербезпеки, а також мінімізувати витрати на заходи по мінімізації цих ризиків. Результати оцінки ризику дають підстави для прийняття рішення щодо прийнятності його рівня і необхідності чи економічної доцільності його подальшої обробки. Для досягнення цієї мети необхідно здійснювати дослідження, спрямовані на перспективи побудови

моделей реагування на ризики кібербезпеки.

Дослідженню проблем, пов’язаних із оцінкою ризику, присвячено публікації вітчизняних та зарубіжних вчених [1—7].

Брюс Шнайер зазначає [8], що прийняття рішень у сфері управління ризиками в значній мірі залежить від відчуття ризику, тобто сприйняття ризику. Як універсальні характеристики можливих результатів будь-яких втрат використовуються гроші, оскільки вони є мірою вартості товарів і послуг, відіграють роль загального еквівалента, оцінюють вартість всіх інших товарів і обмінюються на будь-який з них. Але виявляється, що підхід, при якому «ціна ризику» обчислюється в грошах, не є досконалим. Це зазначено у новій теорії про вимірювання ризику Д. Бернуллі [9]. Його основна теза полягає у тому, що ризик кожний сприймає по-своєму, і тому оцінювати його однаково не можна. При цьому оцінка корисності благ залежить від людини, яка перебуває в ризикованій ситуації.

Отже, знання вартості (збитків) і ймовірності не завжди є достатнім для визначення цінності результату, оскільки корисність в кожному окремому випадку може залежати від суб'єкта, який робить оцінку. Кожен суб'єкт має свою систему цінностей і реагує на ризик відповідно до цієї системи.

Філософсько-методологічне значення теорії Д. Бернуллі полягає в тому, що він першим показав, що оцінка ризику залежить від суб'єкта. При цьому гроші, незважаючи на всю їх універсальність, не можуть бути єдиним засобом «вимірювання» людських переваг. Він висунув тезу про те, що цінність будь чого повинна мати за основу не ціну, а швидше, корисність. Поняття корисності асоціюється з користю, бажаністю або задоволенням.

Таким чином, будуючи моделі раціонального вибору в умовах ризику, намагаються зробити їх універсальними, незалежними від суб'єкта прийняття рішень, тобто об’єктивними. Відсутність суб'єкта в моделях прийняття рішень зумовлюють суперечності, про що найяскравіше свідчить теорія Бернуллі. Кожен суб'єкт має свою систему цілей, цінностей і оцінок, і його поведінка в умовах ризику визначається саме цією системою,

а не однаковими для всіх логіко-методологічними стандартами. У результаті суб'єкт обирає ту систему, яка найповніше відповідає його цілям, оцінкам і цінностям. Це можна назвати суб’єктивним ризиком. Водночас, загальні методологічні підходи до вироблення рішень в умовах ризику потрібні, оскільки людина в такій ситуації хоче мати раціональну основу для прийняття розсудливих рішень [9]. Ідеї Д. Бернуллі отримали подальший розвиток у теорії корисності Дж. Фон Неймана і О. Моргенштерна [10].

Значну роль при оцінці ризику відіграє те, які потреби індивіда можна задовольнити у випадку сприятливого результату і яку загрозу для нього може становити несприятливий результат. Доцільність врахування суб’єктивного ризику підтверджується дослідженнями, описаними у роботі [11], де запропоновано класифікацію, яка показує, що негативні наслідки можуть бути розподілені в залежності від їх значення для людини, яка приймає рішення.

Таким чином, прийняття рішень у сфері управління ризиками в значній мірі залежить від людського чиннику, який має суб’єктивний характер, а також від відчуття ризику. А найтиповішим фактором, за яким відчуття безпеки може відрізнятися від реальної безпеки, є сприйняття ризику, його усвідомлення. 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. Проте існуючі методи оцінки ризиків не враховують їх суб’єктивну складову, що ускладнює коректну оцінку ризиків. Невирішеними залишаються задачі, пов’язані із можливістю здійснення операцій над ризиками. При вирішенні таких задач виникає необхідність отримувати числові характеристики векторів та їх взаємного розміщення, тобто введення метрики у векторному просторі.

Метою проведених досліджень було підтвердити правомірність подання ризиків у векторному евклідовому просторі, що відкриває перспективи побудови моделей поводження з ризиками на основі

застосування апарату теорії лінійної алгебри, аналітичної геометрії, функцій комплексної змінної, що є актуальною науково-практичною проблемою і має теоретичне та практичне значення.

Розглянемо подання ризику векторами об’єктивної та суб’єктивної складових. У [12] зазначено, що ризик – це об'єктивно-суб'єктивна категорія, яка відображає особливості сприйняття суб'єктами економічних відносин ймовірності настання певної ситуації, що може виникнути в будь-який час і в будь-якій діяльності в процесі здійснення дій або прийняття рішень та може спричинити непередбачені негативні наслідки (втрату прибутку, недоотримання доходів) або позитивні наслідки (прибуток), або призвести до нульового результату. Враховуючи викладене, можна зазначити, що об’єктивний ризик відображає реальні втрати або прибутки, які є наслідком ймовірної реалізації певної події. Величина об’єктивного ризику не залежить від сприйняття чи не сприйняття даного ризику особою, яка приймає рішення. Суб’єктивний ризик спонукає особу, яка приймає рішення, на ті чи інші дії, не враховуючи об’єктивного ризику.

В залежності від можливого результату ризики поділяють на додатні та від’ємні [13]. Додатній ризик означає можливість отримання збитку, тобто це ризик, який може спричинити погіршення ситуації (змінити в гіршу сторону продукт, збільшити терміни виконання робіт, підвищити вартість робіт, знизити якість тощо). До таких ризиків належать природні, екологічні, політичні, транспортні, частина комерційних ризиків (майнові, виробничі, торгові). Від’ємний ризик відображає можливість покращити продукт, скоротити терміни виконання робіт, зменшити їх вартість, підвищити якість тощо, тобто – ймовірність отримання прибутку. Отже, ризики можуть набувати конкретних додатних і від’ємних значень.

Водночас, у роботі [14] зазначено, що ризик відображає ймовірність розбіжності прогнозованого значення збитків з деяким заздалегідь прорахованим значенням. Якщо значення збитків не досягає прорахованого показника, то ризик негативний, якщо перевищує його – то ризик

позитивний. Таким чином, ризик набуває знак. Зрештою, ризик набуває напрямок. Вектор задано, якщо задані його довжина і напрям. Ризики, як об'єктивні, так і суб'єктивні, мають напрямок та значення, і їх можна подати у вигляді векторів.

Для визначення результуючого повного ризику необхідно додати об'єктивний і суб'єктивний ризики. Але алгебраїчно додавати ці два ризики не можливо через те, що вони різні за характером і лінійно незалежні. Ідея побудови алгебри ризиків запропонована у роботі [15]. При вирішенні такої задачі виникає необхідність отримувати числові характеристики векторів (довжини) та їх взаємного розміщення (кут між векторами), тобто введення метрики у просторі. Це здійснюється веденням у векторному просторі додаткової операції, яка називається скалярним добутком. Такий векторний простір називають евклідовим простором.

4.2. Векторна модель ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Евклідовим простором розмірності n називають n-мірний лінійний простір над полем дійсних чисел, у якому кожній парі векторів x та y поставлено у відповідність дійсне число, яке позначається через (x, y) і називається скалярним добутком цих векторів, при цьому, виконуються аксіоми:

$$(x, y) = (y, x); \tag{4.1}$$

$$(x + y, z) = (x, z) + (y, z); \tag{4.2}$$

$$(ax, y) = a(x, y), \tag{4.3}$$

де a – будь-яке дійсне число;

$$(x, x) > 0, \tag{4.4}$$

для будь-якого вектору, якщо $x \neq 0$; $(x,x) = 0$, якщо $x = 0$.

Для можливості введення таких понять, як довжина вектору, кут між векторами, проекція вектору на вісь, ортогональність векторів у відношенні до ризиків, необхідно дослідити справедливість аксіом евклідового простору для об'єктивного та суб'єктивного ризиків.

Дослідження здійснюється виходячи із твердження, що скалярний добуток двох векторів ненульових ризиків $\overline{R_1}$ та $\overline{R_2}$ у евклідовому 2-мірному просторі буде добуток довжин векторів цих ризиків та косинуса кута між ними $\cos\{\varphi\} = \cos\{\overline{R_1}, \overline{R_2}\}$, а також використовуючи координатне представлення векторів, рис. 4.1.

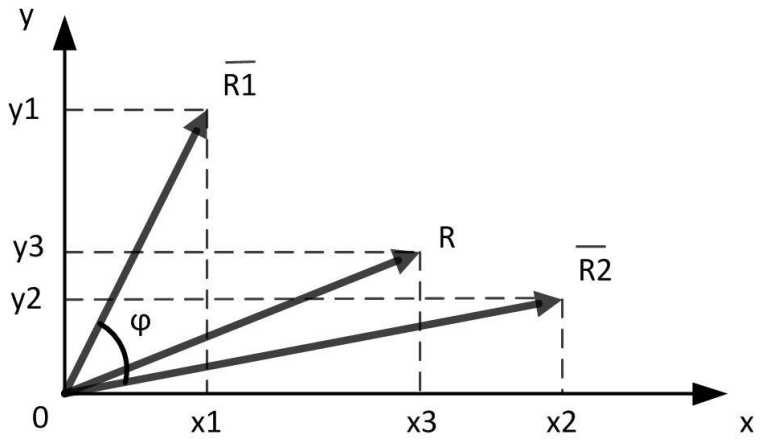


Рис. 4.1. Представлення ризиків в евклідовому векторному просторі

Скалярний добуток векторів ризиків $\overline{R_1}$ і $\overline{R_2}$, які подані у вигляді:

$$\overline{R_1} = (x_1, y_1), \tag{4.5}$$

$$\overline{R_2} = (x_2, y_2), \tag{4.6}$$

може бути визначений у вигляді:

$$(R_1, R_2) = \left|\overline{R_1}\right| \cdot \left|\overline{R_2}\right| \cdot \cos\{\varphi\}, \tag{4.7}$$

або

$$(R_1, R_2) = x_1 \cdot x_2 + y_1 \cdot y_2. \tag{4.8}$$

Використовуючи вирази (4.5) - (4.8), доведемо для об'єктивного та суб'єктивного ризиків справедливість аксіом евклідового простору:

- аксіома (1):

$$(R_1, R_2) = \left|\overline{R_1}\right| \cdot \left|\overline{R_2}\right| \cdot \cos\{\varphi\} = \left|\overline{R_2}\right| \cdot \left|\overline{R_1}\right| \cdot \cos\{\varphi\} = (R_2, R_1); \tag{4.9}$$

- аксіома (2):

$$\begin{gathered}(R_1 + R_2, R) = (x_1 + x_2) \cdot x_3 + (y_1 + y_2) \cdot y_3 = \\ = x_1 \cdot x_3 + x_2 \cdot x_3 + y_1 \cdot y_3 + y_2 \cdot y_3 = \\ = \left(x_1 \cdot x_3 + y_1 \cdot y_3\right) + \left(x_2 \cdot x_3 + y_2 \cdot y_3\right) = (R_1, R) + (R_2, R);\end{gathered} \tag{4.10}$$

- аксіома (3):

$$(a \cdot R_1, R_2) = (a \cdot x_1) \cdot x_2 + (a \cdot y_1) \cdot y_2 = a \cdot (x_1 \cdot x_2 + y_1 \cdot y_2) = a \cdot (R_1, R_2); \tag{4.11}$$

- аксіома (4):

$$(R, R) = \left|\overline{R}\right| \cdot \left|\overline{R}\right| \cdot \cos\{\varphi\} = \left|\overline{R}\right| \cdot \left|\overline{R}\right| \cdot \cos\{0\} = \left|\overline{R}\right| \cdot \left|\overline{R}\right| > 0, \tag{4.12}$$

у випадку $R \neq 0$.

Виходячи з отриманих результатів, можна констатувати, що для векторного простору, у якому представлені 2-мірні геометричні вектори ризиків $\overline{R_1}$ і $\overline{R_2}$, заданий скалярний добуток цих векторів і справедливі аксіоми, характерні для евклідового простору. Це означає, що зазначений векторний простір являється 2-мірним евклідовим простором.

Отримані результати дозволяють стверджувати, що довжина вектору визначається, як корінь квадратний його скалярного квадрату:

$$\left|\overline{R_1}\right| = \sqrt{x_1^2 + y_1^2}, \tag{4.13}$$

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:

$$\cos\{\varphi\} = \frac{\overline{R_1} \cdot \overline{R_2}}{\left|\overline{R_1}\right| \cdot \left|\overline{R_2}\right|}, \tag{4.14}$$

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

$\overline{R_1} \neq 0$, $\overline{R_2} \neq 0$,

а у випадку координатного представлення векторів:

$$\cos\{\varphi\} = \frac{x_1 \cdot x_2 + y_1 \cdot y_2}{\sqrt{\left(x_1^2 + y_1^2\right) \cdot \left(x_2^2 + y_2^2\right)}}. \tag{4.15}$$

Скористаємося властивістю ортогональних векторів евклідового

простору, у відповідності до якої два вектори $\overline{R_1}$ і $\overline{R_2}$ евклідового простору називаються ортогональними, якщо їх скалярний добуток дорівнює нулю. Виходячи з цього, можна констатувати, що два ненульові вектори ортогональні у випадку, якщо косинус кута між ними дорівнює нулю, а кут між ними відповідно дорівнює $\frac{\pi}{2}$.

Врахування даного факту відкриває можливість застосування однієї з властивостей ортогональних векторів, що взаємно ортогональні ненульові вектори лінійно незалежні. Як було показано вище, об'єктивний та суб'єктивний ризики лінійно незалежні, а це означає, що їх необхідно представляти ортогональними векторами у евклідовому просторі.

Як уже зазначалося вище, лінійним (векторним) простором називають довільну непусту множину елементів (векторів), на якій задані операції додавання цих елементів і множення елементу на число, при цьому, повинні виконуватися аксіоми лінійного (векторного) простору.

Такою множиною може бути, наприклад, множина звичайних геометричних векторів у просторі, множина матриць розміром $m \times n$, множина неперервних функцій тощо. Однак, незважаючи на різну природу елементів множин, операції додавання та множення на число мають спільні властивості. Таким чином, доцільно розглянути для множин елементів будь-якої природи виконання додавання цих елементів один до одного та множенням елементів на будь-яке дійсне число.

Дослідимо справедливість аксіом лінійного (векторного) простору для представлення ризиків, у якості елементів двомірного простору R^2, у якому задано множину ризиків:

$$R_1 = p_1 \cdot h_1, \tag{4.16}$$

$$R_2 = p_2 \cdot h_2, \tag{4.17}$$

…

$$R_J = p_J \cdot h_J . \qquad (4.18)$$

Використаємо для розрахунку суми ризиків метод наслідків повного знищення інформаційного активу, запропонованого у розділі 3.

Визначимо значення наслідків повного знищення інформаційного активу h_{1m} і h_{2m} для кожного із ризиків R_1 і R_2 відповідно. Значення сумарного наслідку повного знищення інформаційного активу буде дорівнювати сумі наслідків повного знищення інформаційного активу для кожного із ризиків $h_m = h_{1m} + h_{2m}$. Ймовірності виникнення подій, що призводять до наслідків повного знищення інформаційного активу в умовах дій ризиків R_1 і R_2, визначаються відповідно:

$$p_{1m} = \frac{R_1}{h_{1m}} \quad \text{і} \quad p_{2m} = \frac{R_2}{h_{2m}},$$

де $h_{1m} \neq 0$, $h_{2m} \neq 0$.

Ймовірність події, що призводить до дії ризиків R_1 і R_2 з наслідками повного знищення інформаційного активу h_{1m} і h_{2m} в умовах дії кожного ризику відповідно, визначається, як сума ймовірностей цих сумісних подій без ймовірності їх добутку:

$$p_m = p_{1m} + p_{2m} - p_{1m} \cdot p_{2m} .$$

Сумарний ризик дії ризиків R_1 і R_2 буде визначатися виразом:

$$R = h_m \cdot p_m .$$

Розглянемо виконання операцій додавання ризиків R_1, R_2 і помноження

ризику R_1 на число:

$$R_1 + R_2 = \left(h_{1m} + h_{2m}\right) \cdot \left(\left[p_{1m} + p_{2m}\right] - \left[p_{1m} \cdot p_{2m}\right]\right), \tag{4.19}$$

$$\alpha \cdot R_1 = \alpha \cdot h_{1m} \cdot p_{1m}, \tag{4.20}$$

де h_{1m} – наслідки повного знищення інформаційного активу від ризику R_1,

h_{2m} – наслідки повного знищення інформаційного активу від ризику R_2,

p_{1m} – ймовірність наслідків повного знищення інформаційного активу h_{1m},

p_{2m} – ймовірність наслідків повного знищення інформаційного активу h_{2m},

α – будь-яке дійсне число.

Дослідимо виконання аксіом лінійного (векторного) простору:

- перестановочна властивість суми ризиків

$$R_1 + R_2 = \left(h_{1m} + h_{2m}\right) \cdot \left(\left[p_{1m} + p_{2m}\right] - \left[p_{1m} \cdot p_{2m}\right]\right) =$$

$$= \left(h_{2m} + h_{1m}\right) \cdot \left(\left[p_{2m} + p_{1m}\right] - \left[p_{2m} \cdot p_{1m}\right]\right) = R_2 + R_1, \tag{4.21}$$

- сполучна властивість суми ризиків

$$\left(R_1 + R_2\right) + R_3 = \left(\left[h_{1m} + h_{2m}\right] + h_{3m}\right) \cdot \left(\left\{\left[p_{1m} + p_{2m} - p_{1m} \cdot p_{2m}\right] + p_{3m}\right\} -\right.$$

$$\left. - \left\{\left[p_{1m} + p_{2m} - p_{1m} \cdot p_{2m}\right] \cdot p_{3m}\right\}\right) = \left(h_{1m} + h_{2m} + h_{3m}\right) \times$$

$$\times \left(p_{1m} + p_{2m} + p_{3m} - p_{1m} \cdot p_{2m} - p_{1m} \cdot p_{3m} - p_{2m} \cdot p_{3m} + p_{1m} \cdot p_{2m} \cdot p_{3m}\right) =$$

$$= \left(h_{1m} + \left[h_{2m} + h_{3m}\right]\right) \cdot \left(\left\{p_{1m} + \left[p_{2m} + p_{3m} - p_{2m} \cdot p_{3m}\right]\right\} -\right.$$

$$-\left\{p_{1m}\cdot\left[p_{2m}+p_{3m}-p_{2m}\cdot p_{3m}\right]\right\}\Big)=R_1+\left(R_2+R_3\right), \qquad (4.22)$$

- існування нульового ризику R_2 такого, що

$$R_1+0=\left(h_{1m}+0\right)\cdot\left(p_{1m}+0-p_{1m}\cdot 0\right)=h_{1m}\cdot p_{1m}=R_1, \qquad (4.23)$$

де ризик $R_2=0$ лише у випадку, коли $h_{2m}=0$ і $p_{2m}=0$,

- існування для будь-якого ризику R_1 протилежного ризику $-R_1$ такого, що

$$R_1+\left(-R_1\right)=\left(h_{1m}+\left[-h_{1m}\right]\right)\cdot\left(\left[p_{1m}+\left(-p_{1m}\right)\right]-\left[p_{1m}\cdot\left(-p_{1m}\right)\right]\right)=0, \qquad (4.24)$$

де $-R_1=-h_{1m}\cdot p_{1m}$ – ризик, протилежний ризику R_1, тобто ймовірність отримання прибутку,

- виконання операції множення на ризик R_2, рівний одиниці

$$R_1\cdot 1=h_{1m}\cdot p_{1m}\cdot\frac{1}{p_{2m}}\cdot p_{2m}=R_1, \qquad (4.25)$$

де $R_2=1$, тобто $h_{2m}\cdot p_{2m}=1$ і $h_{2m}=\dfrac{1}{p_{2m}}$, $p_{2m}\neq 0$;

- сполучна властивість відносно числового множника

$$\alpha\cdot\left(\beta\cdot R_1\right)=\alpha\cdot\left(\beta\cdot h_{1m}\cdot p_{1m}\right)=(\alpha\cdot\beta)\cdot h_{1m}\cdot p_{1m}=(\alpha\cdot\beta)\cdot R_1. \qquad (4.26)$$

де α, β – будь-які дійсні числа,

- розподільча властивість відносно числових множників

$$(\alpha+\beta)\cdot R_1=(\alpha+\beta)\cdot\left(h_{1m}\cdot p_{1m}\right)=$$

$$=\alpha\cdot\left(h_{1m}\cdot p_{1m}\right)+\beta\cdot\left(h_{1m}\cdot p_{1m}\right)=\alpha\cdot R_1+\beta\cdot R_1, \qquad (4.27)$$

де α, β – будь-які дійсні числа,

- розподільча властивість відносно суми ризиків

$$\alpha\cdot\left(R_1+R_2\right)=\alpha\cdot\left[\left(h_{1m}+h_{2m}\right)\cdot\left(p_{1m}+p_{2m}-p_{1m}\cdot p_{2m}\right)\right]=$$

$$=\left(\alpha\cdot h_{1m}+\alpha\cdot h_{2m}\right)\cdot\left(p_{1m}+p_{2m}-p_{1m}\cdot p_{2m}\right)=$$

$$=\left(\alpha\cdot h_{1m}\cdot p_{1m}\right)+\left(\alpha\cdot h_{2m}\cdot p_{2m}\right)=\alpha\cdot R_1+\alpha\cdot R_2. \qquad (4.28)$$

де α – будь-яке дійсне число.

Вирази (4.19), (4.20) показують, що двом ризикам R_1 і R_2 протиставлена у відповідність сума цих ризиків, ризику R_1 і числу α протиставлений у відповідність добуток $\alpha\cdot R_1$. Вирази (4.21) – (4.28) задовольняють аксіомам векторного простору. Тому, можна стверджувати, що множина ризиків (4.16) – (4.18) може бути представлена множиною геометричних векторів і являти двомірний лінійний (векторний) простір R^2.

Розглянемо лінійний (векторний) простір, представлений множиною ризиків у вигляді геометричних векторів. Якщо у такому просторі будь-яким двом векторам ризиків поставлено у відповідність дійсне число, яке називають скалярним добутком цих векторів, то такий простір називають евклідовим простором. При цьому, повинні виконуватися аксіоми евклідового простору.

Дослідимо справедливість аксіом евклідового простору для представлення векторів ризиків, у якості елементів двомірного простору R^2.

Нехай є деякий 2-мірний простір R^2, у якому задано множину ризиків

(4.16)–(4.18) у вигляді геометричних векторів. Скалярний добуток векторів ризиків $\overline{R_1}$ і $\overline{R_2}$ у цьому просторі буде визначатися наступним чином:

$$\left(\overline{R}_1, \overline{R}_2\right) = \left|\overline{R}_1\right| \cdot \left|\overline{R}_2\right| \cdot \cos\{\varphi\} = h_{1m} \cdot p_{1m} \cdot h_{2m} \cdot p_{2m} \cdot \cos\{\varphi\}, \qquad (4.29)$$

де $\left|\overline{R}_1\right| = h_{1m} \cdot p_{1m}$ – абсолютне значення ризику R_1,

$\left|\overline{R}_2\right| = h_{2m} \cdot p_{2m}$ – абсолютне значення ризику R_2,

φ – кут між векторами $\overline{R_1}$ і $\overline{R_2}$.

Дослідимо виконання аксіом евклідового простору:

- комутативна властивість скалярного добутку

$$\left(\overline{R}_1, \overline{R}_2\right) = \left|\overline{R}_1\right| \cdot \left|\overline{R}_2\right| \cdot \cos\{\varphi\} = h_{1m} \cdot p_{1m} \cdot h_{2m} \cdot p_{2m} \cdot \cos\{\varphi\} =$$

$$= h_{2m} \cdot p_{2m} \cdot h_{1m} \cdot p_{1m} \cdot \cos\{\varphi\} = \left|\overline{R_2}\right| \cdot \left|\overline{R_1}\right| \cdot \cos\{\varphi\} = \left(\overline{R}_2, \overline{R}_1\right), \qquad (4.30)$$

- дистрибутивна властивість скалярного добутку відносно додавання

$$\left(\left(\overline{R_1 + R_2}\right), \overline{R}_3\right) = \left|\overline{R_1 + R_2}\right| \cdot \left|\overline{R}_3\right| \cdot \cos\{\varphi\} = \left(h_{12m} \cdot p_{12m}\right) \cdot \left(h_{3m} \cdot p_{3m}\right) \cdot \cos\{\varphi\} =$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \left(h_{12m} \cdot p_{12m}\right) =$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \sqrt{(R_1 \cos\{\alpha\} + R_2 \cos\{\beta\})^2 + (R_1 \sin\{\alpha\} + R_2 \sin\{\beta\})^2} =$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \sqrt{\begin{array}{l} {R_1}^2 \cos^2\{\alpha\} + {R_2}^2 \cos^2\{\beta\} + 2R_1 \cos\{\alpha\} R_2 \cos\{\beta\} + \\ + {R_1}^2 \sin^2\{\alpha\} + {R_2}^2 \sin^2\{\beta\} + 2R_1 \sin\{\alpha\} R_2 \sin\{\beta\} = \end{array}}$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \sqrt{\begin{matrix} R_1{}^2(\cos^2\{\alpha\} + \sin^2\{\alpha\}) + R_2{}^2(\cos^2\{\beta\} + \sin^2\{\beta\}) + \\ + 2R_1R_2(\cos\{\alpha\}\cos\{\beta\} + \sin\{\alpha\}\sin\{\beta\}) = \end{matrix}}$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \sqrt{R_1{}^2 + R_2{}^2 + 2R_1R_2\cos\{\alpha - \beta\}}.$$

де α - кут нахилу вектору ризику R_1 до горизонтальної осі; β - кут нахилу вектору ризику R_2 до горизонтальної осі.

Співвідношення під коренем буде максимальним, якщо $\alpha = \beta$, тобто, якщо $\cos\{\alpha - \beta\}$=1. Тоді

$$h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \sqrt{R_1{}^2 + R_2{}^2 + 2R_1R_2\cos\{\alpha - \beta\}} =$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot \sqrt{(R_1 + R_2)^2} = h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot (R_1 + R_2) =$$

$$= h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot R_1 + h_{3m} \cdot p_{3m} \cdot \cos\{\varphi\} \cdot R_2, \qquad (4.31)$$

- розподільча властивість скалярного добутку

$$\left(\alpha \cdot \overline{R}_1, \overline{R}_2\right) = \alpha \cdot h_{1m} \cdot p_{1m} \cdot h_{2m} \cdot p_{2m} \cdot \cos\{\varphi\} =$$

$$= \alpha \cdot \left(h_{1m} \cdot p_{1m} \cdot h_{2m} \cdot p_{2m} \cdot \cos\{\varphi\}\right) = \alpha \cdot \left(\overline{R}_1, \overline{R}_2\right), \qquad (4.32)$$

де α – будь-яке дійсне число,

- позитивна визначеність скалярного добутку

$$\left(\overline{R}_1, \overline{R}_1\right) = h_{1m} \cdot p_{1m} \cdot h_{1m} \cdot p_{1m} \cdot \cos\{\varphi_0\} = \left(h_{1m} \cdot p_{1m}\right)^2 = \left(\left|\overline{R}_1\right|\right)^2. \qquad (4.33)$$

Причому, $\left(\overline{R}_1,\overline{R}_1\right)=0$ тоді, і тільки тоді, коли $\overline{R}_1=0$, і $\left(\overline{R}_1,\overline{R}_1\right)>0$ у всіх інших випадках, коли $\overline{R}_1\neq 0$.

Виходячи з отриманих результатів (4.29) – (4.33), можна констатувати, що для 2-мірного лінійного (векторного) простору, у якому представлені вектори ризиків $\overline{R_1}$ і $\overline{R_2}$, заданий скалярний добуток цих векторів і справедливі аксіоми, характерні для евклідового простору. Це означає, що зазначений лінійний (векторний) простір являється 2-мірним евклідовим простором. Наявність скалярного добутку дозволяє ввести довжину вектору, кут між векторами, поняття проекції вектору на вісь, поняття ортогональності векторів.

Отримані результати дозволяють стверджувати, що довжина вектору ризику може визначатися, як корінь квадратний його скалярного квадрату:

$$\left|\overline{R_1}\right|=\sqrt{x_1^2+y_1^2}\,, \tag{4.34}$$

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:

$$\cos\{\varphi\}=\frac{\left(\overline{R}_1,\overline{R}_2\right)}{\left|\overline{R}_1\right|\cdot\left|\overline{R}_2\right|}, \tag{4.35}$$

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.4.2.

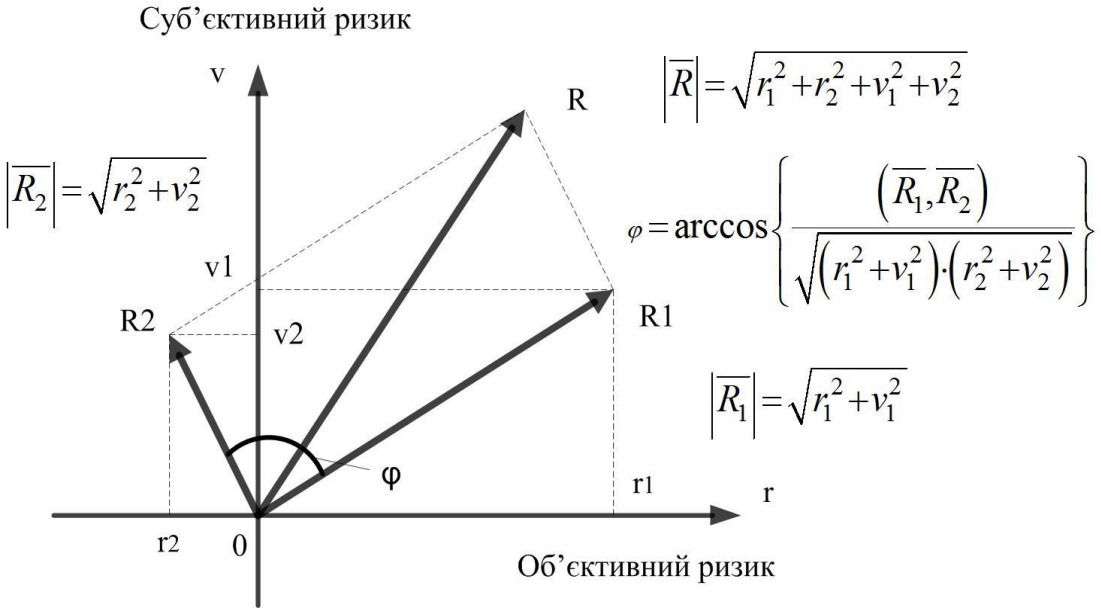


Рис. 4.2. Векторна модель ризику

4.3. Модель комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури

Реальний і уявний ризики можуть бути як позитивними, так і негативними. Дослідники зазначають, що прийняття рішень у сфері ризик-менеджменту надзвичайно залежить від усвідомлення ризику, тобто – сприйняття чи відчуття ризику. В якості універсальної характеристики можливих результатів будь-яких втрат використовуються гроші, оскільки вони є мірою вартості товарів і послуг, грають роль загального еквівалента,

висловлюють вартість всіх інших товарів і обмінюються на будь-який з них [16, 17].

Залежно від можливого результату (ризикової події) ризики поділяють на дві великі групи: чисті і спекулятивні [19, 20]. Чистий ризик означає можливість отримання негативного чи нульового результату, тобто це ризик, який може привести до погіршення ситуації (поміняти в гіршу сторону продукт, збільшити терміни виконання робіт, підвищити вартість робіт, знизити якість і т.д.). У цьому випадку ризик буде позитивним. До таких ризиків відносяться: природні, природні, екологічні, політичні, транспортні, частина комерційних ризиків (майнові, виробничі і торгові).

Спекулятивні ризики виражаються в можливості отримання як позитивного, так і негативного результату [19, 20]. До них можна віднести фінансові ризики, які є частиною комерційних ризиків. Негативний ризик - це ризик, що тягне за собою можливість поліпшити продукт, скоротити терміни виконання робіт, знизити їх вартість, підвищити якість і т.д., тобто - ймовірність отримання прибутку. Негативні ризики також можуть виникати, коли відбувається усвідомлення суб'єктом існування позитивних ризиків, тобто коли суб'єктом адекватно сприймається реальний ризик.

Очевидно, що ймовірність отримання прибутку теж може бути представлена в комплексному вигляді, тобто, включаючи реальну і уявну складові.

В [21] наводиться визначення "Ризик - об'єктивно-суб'єктивна категорія, яка пов'язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору і відображає міру (ступінь) досягнення очікуваного результату, невдачі і відхилення від цілей з урахуванням впливу контрольованих і неконтрольованих чинників при наявності прямих і зворотних зв'язків". Згідно з таким визначенням можна говорити, що ризик виникає внаслідок невизначеності.

Використовуючи векторну модель ризиків, розглянемо модель комплексного ризику, (рис. 4.3), та змістовну інтерпретацію комплексного ризику в залежності від φ.

У разі $0 \le \varphi < \frac{\pi}{2}$ вектор повного ризику знаходиться в I чверті, рис. 4.4. 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 виникнення матеріальних збитків), величина якого визначається значенням *r*; існує суб'єктивний ризик) величиною *v*.

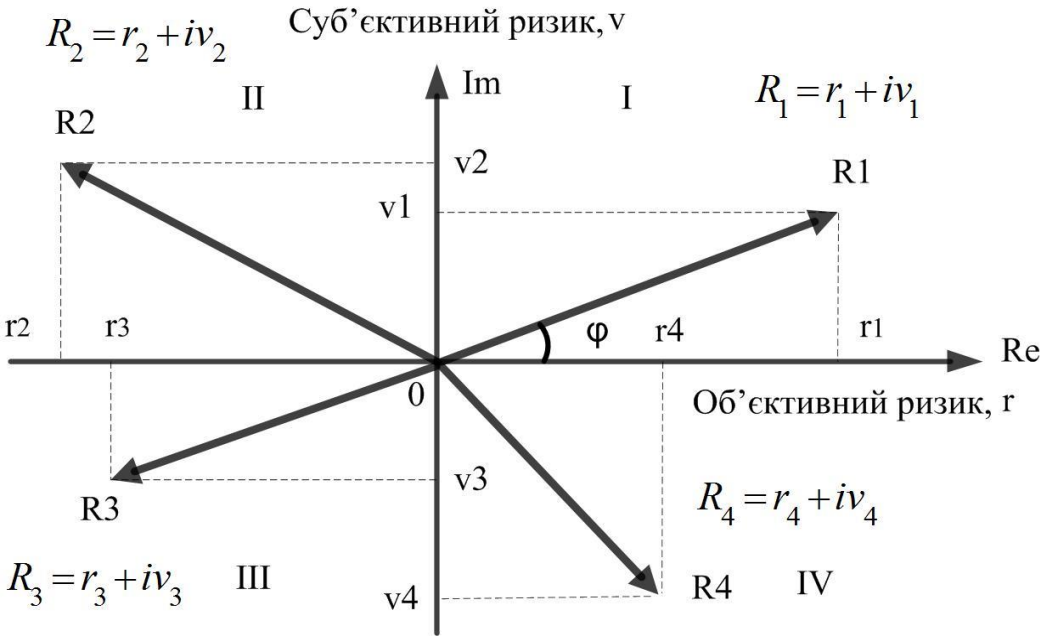


Рис. 4.3. Модель комплексного ризику

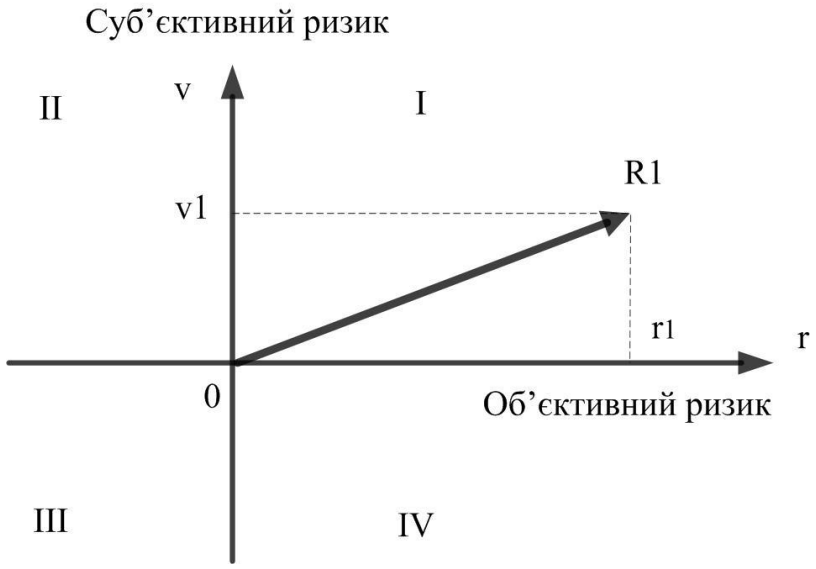


Рис. 4.4. Вектор повного ризику в I чверті

У випадку $\frac{\pi}{2} < \varphi \le \pi$ вектор повного ризику знаходиться в II чверті, рис.4.5. При цьому, об'єктивний ризик $r < 0$, суб'єктивний ризик $v > 0$, аргумент комплексного ризику $\varphi = arctg \frac{|v|}{-|r|} < 0$, де $|r| \neq 0$.

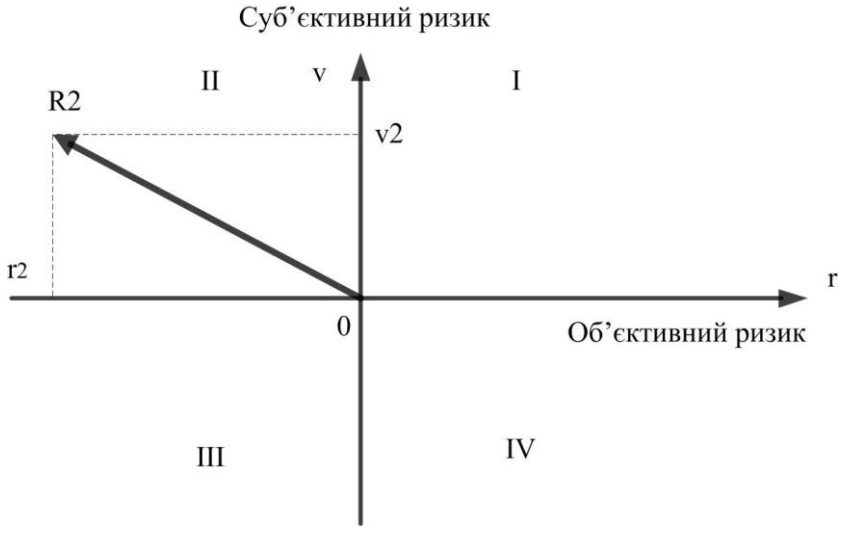


Рис. 4.5. Вектор повного ризику в II чверті

На практиці такий випадок має наступну інтерпретацію: існує реальна ймовірність отримання прибутку, величина якого визначається значенням $|r|$; існує суб'єктивний ризик (ймовірність виникнення моральних збитків) величиною *v*.

У випадку $0 \le \varphi < \frac{\pi}{2}$ вектор повного ризику знаходиться в III чверті, рис.4.6. 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'єктивна ймовірність отримання прибутку величиною *v*.

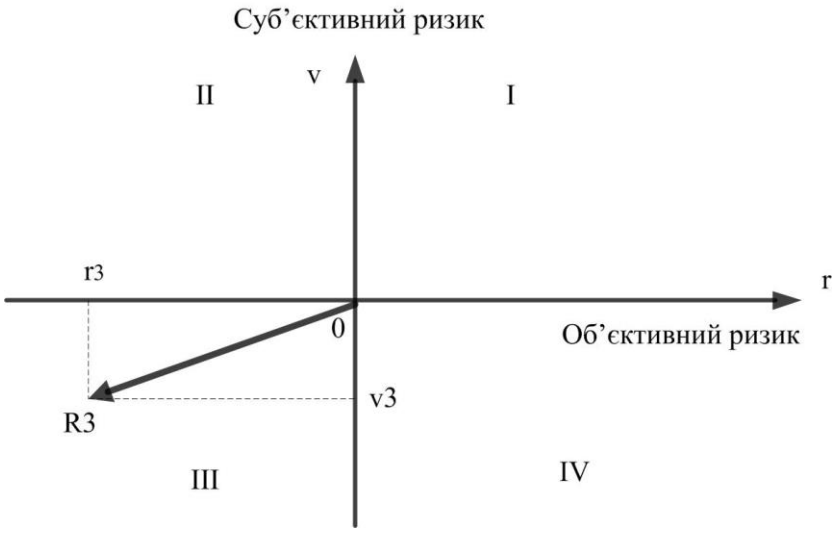


Рис. 4.6. Вектор повного ризику в III чверті

У випадку $0 \le \varphi < \frac{\pi}{2}$ вектор повного ризику знаходиться в IV чверті, рис.4.7. При цьому, реальний ризик $r > 0$, суб'єктивний ризик $m < 0$, аргумент комплексного ризику $\varphi = arctg \frac{-|v|}{|r|} < 0$. На практиці такий випадок має

наступну інтерпретацію: існує реальний ризик, величина якого визначається значенням *r*; на думку суб'єкта існує реальна ймовірність отримання прибутку величиною |*v*|; адекватність сприйняття суб'єктом реальної ситуації визначається значенням φ.

У випадку $0 \le \varphi < \frac{\pi}{2}$ вектор повного ризику знаходиться в IV чверті, рис.4.7. 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 реальний ризик (ймовірність виникнення збитків), величина якого визначається значенням *r*; існує суб’єктивна ймовірність отримання прибутку величиною *v*.

Таким чином, в разі розташування вектора комплексного ризику в II і в III чвертях вказує на реальну можливість отримання прибутку, а в I і в I чвертях - на реальний ризик.

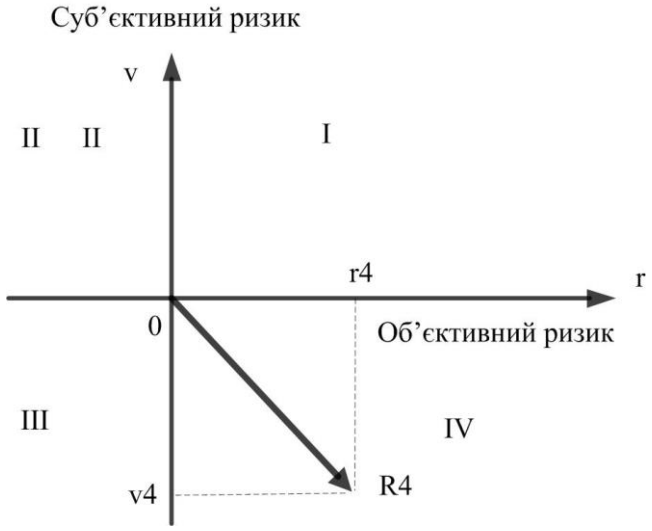


Рис. 4.7. Вектор повного ризику в IV чверті

Функція аргументу комплексного ризику $\varphi = arctg\left(\frac{v}{r}\right)$ періодична функція з періодом π, повертає коректні значення тільки в інтервалі $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Значення аргументів φ_1 і φ_3 комплексних ризиків R_1 і R_3, вектори яких знаходяться в I і в III чвертях, будуть рівними. Аналогічно, значення аргументів φ_2 і φ_4 комплексних ризиків R_2 і R_4, вектори яких знаходяться в II і в IV чвертях, також будуть рівними. Тоді, для аргументів комплексних ризиків, вектори яких розміщені в II і III чвертях, необхідно враховувати поправки на π та $-\pi$ відповідно.

Розглянемо випадок $v = r$. При цьому $\varphi = \pi/4$ і $\varphi = 5\pi/4$, вектор комплексного ризику R знаходиться на прямій a, і це значить, що суб'єкт адекватно сприймає реальний ризик, помилок управління ризиком, пов'язаних з неадекватним сприйняттям ризику, не виникає. У будь-якому іншому випадку, якщо $v \neq r$, виникає похибка сприйняття ризику, що знижує оптимальність прийнятих рішень з управління ризиком.

Якщо $v = -r$, то сприйняття ризику протилежно реальному ризику. При цьому $\varphi=3\pi/4$ і $\varphi = 7\pi/4$. У 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 практиці, 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.

При наближенні φ до значень $\pi/2$ і $3\pi/2$ реальний ризик прагне до нульового значення або до максимальної невизначеності при певному значенні уявного ризику. На практиці такий випадок може мати такі інтерпретації:

- реальний ризик можна зменшувати, але не можна звести до нуля;

- велике значення уявного ризику при низькому рівні реального ризику може означати навмисне завищення ризику суб'єктом з метою залучення ресурсів або з метою демонстрації результатів своєї роботи і подальшим вимогою підвищення оплати.

При $v = r$, що відповідає умові $\varphi = arctg\left(\frac{v}{r}\right) = \frac{\pi}{4}$, суб'єкт адекватно сприймає реальний ризик, при $v < r$ суб'єкт недооцінює реальний ризик, а при $v > r$ – переоцінює його. При $(-v)=(-r)$, що відповідає умові $\varphi = arctg\left(\frac{-v}{-r}\right) = \frac{5\pi}{4}$, суб'єкт адекватно сприймає реальну ймовірність отримання прибутку. Таким чином, аргумент φ комплексного ризику R є показником адекватності сприйняття ризику або показником адекватності сприйняття ймовірності отримання прибутку.

У всіх випадках, коли не виконуються умови: $\varphi = \frac{\pi}{4}$ и $\varphi = \frac{5\pi}{4}$, повний ризик зростає і, відповідно, необхідно вживати заходів по його зниженню.

Узагальнимо інтерпретації показника адекватності сприйняття ризику для кожного сектора комплексної площині:

$\varphi = 0$ – невизначеність: існує реальний ризик, але інформація про нього або не доводять до суб'єкта або не сприймається суб'єктом (ігнорування, відсутність знань, досвіду і т.д.);

$0 < \varphi < \pi/4$ – недооцінка реального ризику;

$\varphi = \pi/4$ – адекватне сприйняття ризику;

$\pi/4 < \varphi < \pi/2$ – переоцінка реального ризику;

$\pi/2 < \varphi < \pi$ – психологічний внутрішній або зовнішній вплив: суб'єкт помилково сприймає наявність ризику при наявності реальної можливості отримання прибутку;

$\varphi = \pi$ – невизначеність: існує реальна ймовірність отримання прибутку, але інформація про неї або не доводиться до суб'єкта або не сприймається суб'єктом (ігнорування, відсутність знань, досвіду і т.д.);

$\pi < \varphi < 5\pi/4$ – недооцінка реальної ймовірності отримання прибутку;

$\varphi = 5\pi/4$ – адекватне сприйняття ймовірності отримання прибутку;

$5\pi/4 < \varphi < 3\pi/2$ – переоцінка реальної ймовірності отримання прибутку;

$3\pi/2 < \varphi < 2\pi$ – психологічний внутрішній або зовнішній вплив: суб'єкт помилково сприймає наявність ймовірності отримання прибутку при наявності реального ризику.

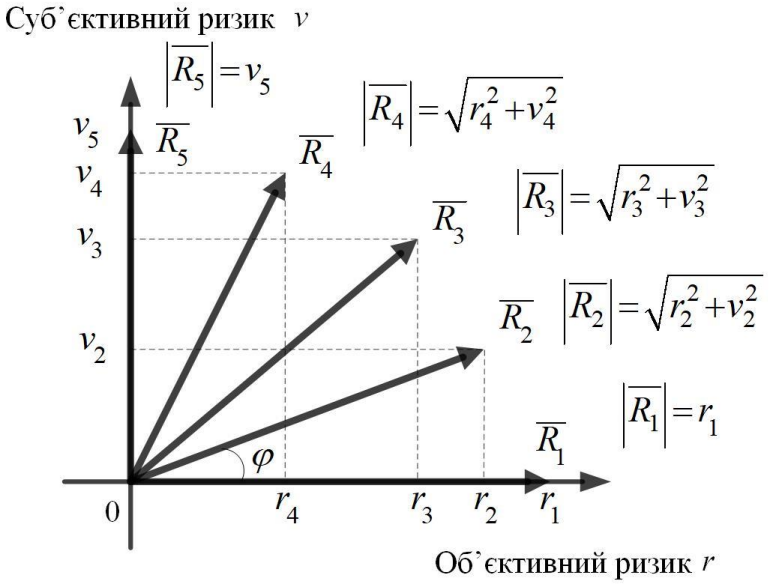


Рис. 4.8. Інтерпретація комплексного ризику

Аналіз векторної моделі ризику, рис. 4.2, та моделі комплексного ризику, рис. 4.3, дозволяє здійснити інтерпретацію комплексного ризику, у

залежності від кута нахилу вектору ризику до осі абсцис, рис. 4.8. У випадку відсутності суб'єктивної складової комплексного ризику, тобто $v_1 = 0$, величина комплексного ризику дорівнює величині об'єктивного ризику, тобто $\left|\overline{R_1}\right| = r_1$. Якщо існує об'єктивний ризик, наприклад r_2 і суб'єктивний ризик v_2, то наявність суб'єктивного ризику буде збільшувати величину комплексного ризику $\left|\overline{R_2}\right|$. Із збільшенням величини суб'єктивного ризику, збільшується абсолютне значення комплексного ризику, на рис. 4.8 $\left|\overline{R_3}\right|$ та $\left|\overline{R_4}\right|$. У випадку відсутності об'єктивної складової комплексного ризику, тобто $r_5 = 0$, величина комплексного ризику дорівнює величині суб'єктивного ризику, тобто $\left|\overline{R_5}\right| = v_5$.

Ступінь сприйняття ризику суб'єктом буде залежати від його темпераменту - сукупності психофізіологічних особливостей особистості, пов'язаних з динамічними, а не змістовними аспектами діяльності. Темперамент становить основу формування і розвитку характеру. З фізіологічної точки зору темперамент обумовлений типом вищої нервової діяльності людини і проявляється в характері поведінки людини, в ступені його життєвої активності [22].

Наприклад, недооцінювати реальний ризик схильні люди, яким притаманні безтурботність і недбалість, а переоцінювати - люди, яким притаманні необґрунтовані хвилювання, переживання, тривоги, страх.

4.4. Метод розрахунку комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Використовуючи векторну модель ризиків та модель комплексного ризику комплексний ризик можна представити у вигляді комплексного числа:

$$R = r + i\,v, \tag{4.36}$$

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

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

$i = \sqrt{-1}$.

У виразі (4.36) об’єктивний ризик r визначається, як добуток об’єктивної ймовірності $p_{об}$ настання події, що призводить до ризику, і величини реальних наслідків від настання такої події $h_{об}$. Суб’єктивний ризик v у виразі (4.36) визначається, як добуток суб’єктивної ймовірності $p_{суб}$ настання події, що призводить до ризику, і величини суб’єктивних наслідків від настання такої події $h_{суб}$. Під суб'єктивною ймовірністю настання події розуміємо припущення щодо її настання, що базується на особистому досвіді. Під об'єктивною ймовірністю настання 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: $\varphi_S = arctg\dfrac{v}{r}$, де $r \neq 0$, являється показником превалювання однієї складової ризику над іншою.

Не складними перетвореннями можна отримати вираз для косинуса кута між вектором об’єктивного ризику та вектором повного ризику:

$$\cos\{\varphi\} = \frac{r}{\sqrt{r^2 + v^2}} = \frac{r}{R}. \tag{4.37}$$

У виразі (4.37) значення $\cos\{\varphi\}$ визначає, яку частину повного ризику складає об'єктивний ризик, тобто той ризик, який показує величину реальних втрат. Для $\cos\{\varphi\}$ запропоновано термін «коефіцієнт ризику».

Враховуючи, що:

$$r = |R| \cdot \cos\varphi; \tag{4.38}$$

$$v = |R| \cdot \sin\varphi, \tag{4.39}$$

комплексний ризик можна представити в тригонометричній формі:

$$R = |R| \cdot (\cos\varphi + i \cdot \sin\varphi), \tag{4.40}$$

і в показниковій формі:

$$R = |R| \cdot e^{i \cdot \varphi}. \tag{4.41}$$

На підставі виразів (4.38), (4.39) можна записати:

$$\cos\varphi_S = \frac{r}{|R|}, \tag{4.42}$$

де $|R| \neq 0$.

У виразі (4.42) $\cos\varphi_S$ показує, яку частину повного ризику складає об'єктивний ризик.

Схематичне відображення методу обчислення комплексного ризику зображено на рис. 4.9.

Як було показано вище, кожний суб'єкт має свою систему цінностей, цілей і оцінок, і його поведінка в умовах ризику визначається саме цією системою, а не однаковими для усіх логіко-методологічними стандартами [13]. Ризик визначається сукупністю понять: суб'єкт, рішення, ймовірність,

втрати. Таким чином, ризик являється наслідком рішення і завжди пов'язаний із суб’єктом. Отже, при прийнятті рішення суб’єктом в умовах ризику визначальним буде не об’єктивний ризик, а суб’єктивний ризик.

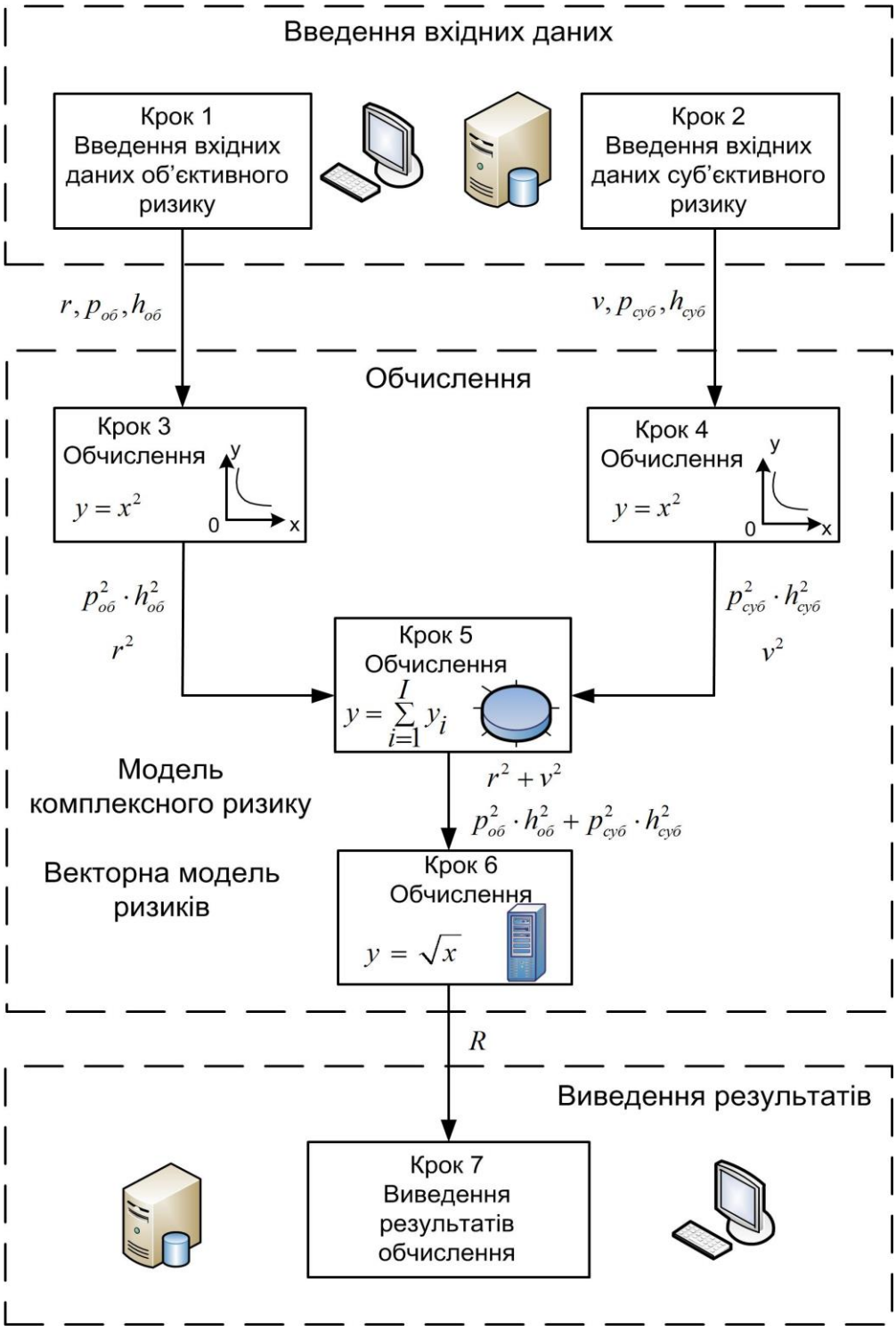


Рис. 4.9. Схематичне відображення методу обчислення комплексного ризику

Розглянемо представлення суб’єктивного ризику в полярних координатах, рис. 4.10.

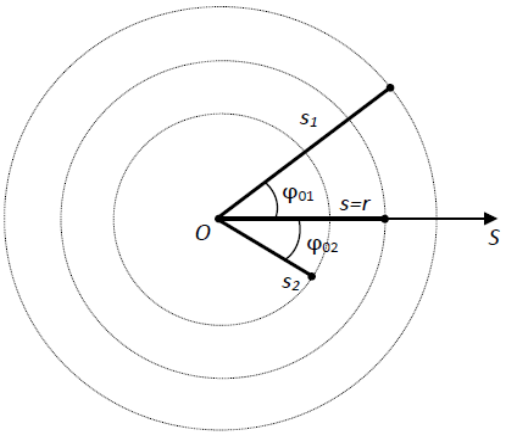


Рис. 4.10. Ризик в полярних координатах

Радіальна координата буде визначатися величиною суб’єктивного ризику *v*, а кутова координата – показником адекватності сприйняття суб'єктом об’єктивного ризику. Кутова координата у випадку адекватного сприйняття суб’єктом об’єктивного ризику, тобто *v* = *r*.

В [6] показано, що у випадку виконання умови *v* = *r* суб’єкт адекватно сприймає об’єктивний ризик. При цьому, показник адекватності сприйняття суб'єктом об’єктивного ризику:

$$\varphi_A = arctg\left(\frac{s}{r}\right) = \frac{\pi}{4}. \qquad (4.42)$$

Тоді, кутова координата φ_0 буде визначатися наступним чином:

$$\varphi_0 = \varphi - \varphi_A = arctg\left(\frac{v}{r}\right) - \frac{\pi}{4}. \qquad (4.43)$$

Розглянемо інтерпретацію ризику для кожного сектору полярної системи координат, рис. 4.11.

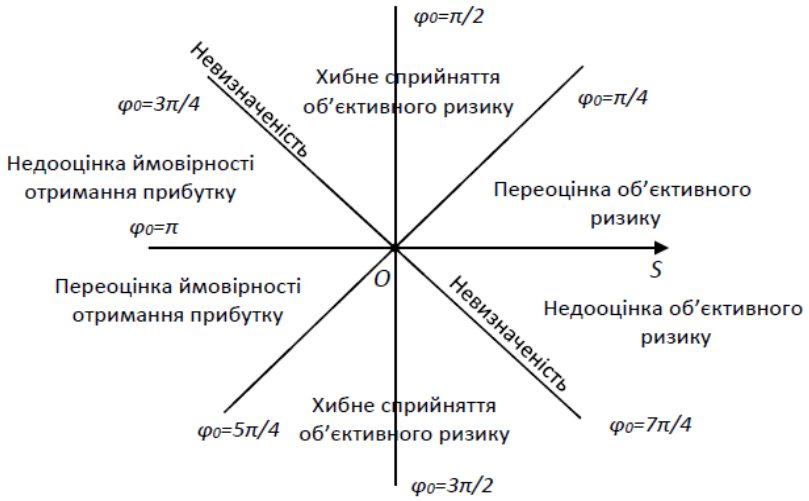


Рис. 4.11. Інтерпретація ризику в полярних координатах

В залежності від показника адекватності сприйняття суб'єктом об’єктивного ризику, провести його класифікацію по якісному рівню, а також сформулювати рекомендації щодо здійснення його подальшої обробки, табл.4.1.

Як можна бачити з табл. 4.1, у випадку, якщо суб’єктивний ризик має велике значення, а показник адекватності сприйняття суб'єктом об’єктивного ризику φ<0, тобто об’єктивний ризик недооцінений, то можемо казати, що об’єктивний ризик буде неприпустимим. У цьому випадку необхідно застосовувати способи обробки ризику: ухилення, зменшення, передача. Якщо суб’єктивний ризик має мале значення, а показник адекватності сприйняття суб'єктом об’єктивного ризику φ>0, тобто об’єктивний ризик переоцінений, то можемо казати, що об’єктивний ризик буде прийнятним. У цьому випадку можна застосовувати прийняття ризику. Якщо суб’єктивний ризик має мале значення, при цьому, показник адекватності сприйняття суб'єктом об’єктивного ризику φ<0, тобто об’єктивний ризик недооцінений, або ж якщо суб’єктивний ризик має велике значення, при цьому, показник адекватності сприйняття суб'єктом об’єктивного ризику φ>0, тобто об’єктивний ризик переоцінений, то у таких випадках можемо казати, що об’єктивний ризик буде виправданий. У цьому випадку можна застосовувати способи обробки ризику: зменшення, передача.

Таблиця 4.1

Класифікація ризику по якісному рівню

Суб’єктивний ризик	Великий	Малий
Недооцінений об’єктивний ризик, φ<0	Неприпустимий	Виправданий
Переоцінений об’єктивний ризик, φ>0	Виправданий	Прийнятний

З урахуванням викладеного вище, можна запропонувати схематичне відображення методу оцінювання якісного рівня об’єктивного ризику на підставі аналізу показника адекватності сприйняття суб'єктом об’єктивного ризику φ, якісного рівня суб’єктивного ризику, а також, формулювання рекомендацій щодо заходів по обробці зазначеного ризику, рис.4.12.

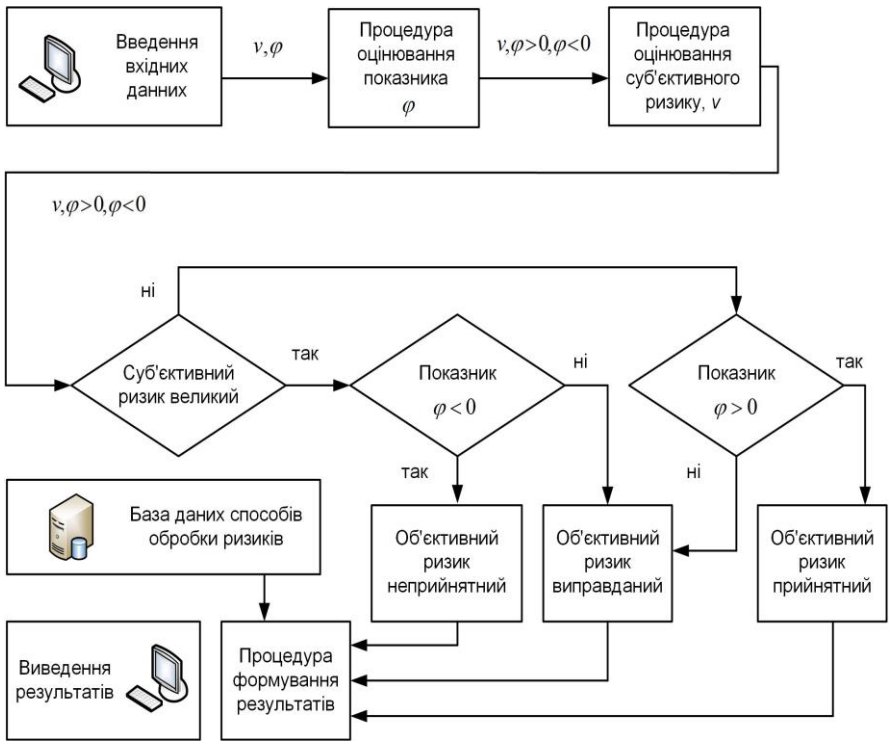


Рис. 4.12. Схематичне відображення методу оцінювання якісного рівня об’єктивного ризику

4.5. Висновки до четвертого розділу

1. У результаті проведених досліджень правомірності подання ризиків у векторному евклідовому просторі встановлено виконання аксіом евклідового простору для подання у ньому векторів об'єктивного та суб'єктивного ризиків, показано, що для лінійного (векторного) простору, у якому представлені 2-мірні геометричні вектори ризиків, заданий скалярний добуток цих векторів, можливе введення метрики у відношенні до векторного представлення ризиків, таких як, як довжина вектору, кут між векторами, проекція вектору на вісь, ортогональність векторів.

2. 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 ввести метрику векторів ризиків та здійснювати векторні операції над ними.

3. 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.

4. Проведені дослідження відкривають перспективи побудови моделей поводження з ризиками на основі застосування апарату теорії лінійної алгебри, аналітичної геометрії, функцій комплексної змінної.

Основні результати дисертаційної роботи, представлені в розділі 4, опубліковані в працях автора [7, 15].

Список використаних джерел до четвертого розділу

1. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation // European Journal of Operational Research, 2016, Vol. 253, Issue 1, p.1—13.

2. Jain P., Pasman H. J., Waldram S. et al. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management // Journal of Loss Prevention in the Process Industries, 2018, Vol. 53, p. 61–73.

3. Eling M., Wirfs J. What are the actual costs of cyber risk events? // European Journal of Operational Research, 2019, Vol. 272, Issue 3, p.1109—1119.

4. Mokhor V., Bakalynskyi O., Bohdanov O., Tsurkan V. Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry // Information technology and security, 2017, Vol. 5, Issue 1, p.71—82.

5. Bochkovskyi A., Gogunskii V. Development of the method for the optimal management of occupational risks // Eastern-European Journal of Enterprise Technologies, 2018, Vol. 1, № 3 (97), p.6—13.

6. Prokopenko T., Grigor O. Development of the comprehensive method to manage risks in projects related to information technologies // Ibid, 2018, № 2 (92), p.37— 43.

7. Гончар С.Ф. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом // Захист інформації, 2014, Т.16, № 1, С.40-46.

8. Schneier B. The Psychology of Security // SecurityLab. 2008. URL: https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html. Дата звернення: 15.01.2019.

9. Диев В. С. Риск: оценка и принятие решений // Философия науки, 2010, №4 (47), с. 15–32.

10. Моргенштерн О., Дж. фон Нейман. Теория игр и экономическое поведение / М. Книга по Требованию, 2012, 708с.

11. Rowe W. D. An Anatomy of Risk. Washington: Environmental

Protection Agency. 1975, 125p.

12. Цвігун Т. В. Поняття «ризик»: сучасний погляд // Вісник Східноукраїнського національного ун-ту ім. Володимира Даля, 2011, №3 (157), Ч. 2. URL: http://www.nbuv.gov.ua/portal/soc_gum/vsunu/2011_3_2/Cvigun.pdf. Дата звернення: 19.01.2019.

13. Ременников В. Б. Управленческие решения: учебное пособие для вузов. М.: ЮНИТИ-ДАНА, 2005, 144 с.

14. Новаков А. А. Концепция векторного представления риска в современной вариативной экономике // Управление экономическими системами: электронный научный журнал, 2011, № 34, с.1—38.

15. Мохор В. В., Гончар С. Ф. Идея построения алгебры рисков на основе теории комплексных чисел // Електрон. моделювання, 2018, 40, №4, с.107—111.

16. Bruce Schneier. The Psychology of Security. Part 1. [Електронний ресурс] // SecurityLab. – 2008. – Режим доступу до ресурсу: URL: https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html.

17. Bruce Schneier. The Psychology of Security. Part 2. [Електронний ресурс] // SecurityLab. – 2008. – Режим доступу до ресурсу: URL: https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se2.html

18. Мохор В.В., Гончар С.Ф. Идея построения алгебры рисков на основе теории комплексных чисел // Электронное моделирование. 2018, 40, № 4, с. 107–111.

19. Ременников В.Б. Разработка управленческого решения: учебное пособие для вузов / В. Б. Ременников. –М.: ЮНИТИ-ДАНА, 2000. –140с.

20. Ременников В.Б. Управленческие решения: учебное пособие для вузов / В. Б. Ременников. - 2-е изд., перераб. и доп. –М.: ЮНИТИ-ДАНА, 2005. –144 с.

21. Вітлінський В.В., Наконечний С.І. Ризик у менеджменті. – К.: ТОВ “Борисфен-М”, 1996. – 336 с.

22. Небылицын В. Д. Темперамент. // Психология индивидуальных различий. Тексты. / Под ред. Ю. Б. Гиппенрейтер, В. Я. Романова. — М.: Изд-во МГУ, 1982. — С. 153—159.

РОЗДІЛ 5
СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

5.1. Етапи реалізації методології оцінювання ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури

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

Визначення базових параметрів.

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

- Введення вхідних даних.

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

- Обчислення суми ризиків об'єктивної складової.

Обчислення суми ризиків об'єктивної складової здійснюється методом максимальних наслідків:

$$R_{S_{об}} = h_{m_{об}} \cdot p_{m_{об}}. \qquad (5.1)$$

- Обчислення суми ризиків суб'єктивної складової.

Обчислення суми ризиків суб'єктивної складової здійснюється методом максимальних наслідків:

$$R_{S_{суб}} = h_{m_{суб}} \cdot p_{m_{суб}} . \quad (5.2)$$

- Визначення суми ризиків об’єктивної і суб’єктивної складових.

Визначення суми ризиків об’єктивної і суб’єктивної складових здійснюється з використанням теорії комплексних чисел:

$$R_S = \sqrt{\left(R_{S_{об}}\right)^2 + \left(R_{S_{суб}}\right)^2} . \quad (5.3)$$

- Візуалізація результатів обчислень.

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

Розглянемо обчислення суми ризиків запропонованою методологією для випадку двох ризиків, $n = 2$ [1].

Нехай існує два ризики, які визначаються наступним чином:

$$R_1 = p_1 \cdot h_1; \quad R_2 = p_2 \cdot h_2 . \quad (5.4)$$

Визначимо максимальні значення наслідків h_{1m} і h_{2m} для кожного із ризиків R_1 і R_2 відповідно.

Значення сумарного наслідку повного знищення інформаційного активу буде дорівнювати сумі наслідків повного знищення інформаційного активу для кожного із ризиків, без урахування синергетичного ефекту:

$$h_m = h_{1m} + h_{2m} . \quad (5.5)$$

Ймовірності виникнення подій, що призводять до наслідків повного знищення інформаційного активу в умовах дій ризиків R_1 і R_2 ,

визначаються відповідно:

$$p_{1m} = \frac{R_1}{h_{1m}}; \qquad p_{2m} = \frac{R_2}{h_{2m}}. \tag{5.6}$$

Ймовірність виникнення події, що призводить до дії ризиків R_1 і R_2 з наслідками повного знищення інформаційного активу h_{1m} і h_{2m} в умовах дії кожного ризику відповідно, визначається, як сума ймовірностей цих подій без ймовірності їх добутку:

$$p_m = p_{1m} + p_{2m} - p_{1m} \cdot p_{2m}. \tag{5.7}$$

Сумарний ризик дії ризиків R_1 і R_2, на підставі виразів (15) і (16) буде визначатися виразом:

$$R = h_m \cdot p_m. \tag{5.8}$$

З урахуванням виразу (5.6) вираз (5.7) можна представити у вигляді:

$$p_m = \frac{R_1}{h_{1m}} + \frac{R_2}{h_{2m}} - \frac{R_1 \cdot R_2}{h_{1m} \cdot h_{2m}} = \frac{R_1 \cdot h_{2m} + R_2 \cdot h_{1m} - R_1 \cdot R_2}{h_{1m} \cdot h_{2m}}. \tag{5.9}$$

Підставивши вирази (5.5) і (5.9) у вираз (5.8), отримаємо вираз для визначення сумарного ризику:

$$R = \left(h_{1m} + h_{2m}\right) \cdot \left(\frac{R_1 \cdot h_{2m} + R_2 \cdot h_{1m} - R_1 \cdot R_2}{h_{1m} \cdot h_{2m}} \right), \tag{5.10}$$

або після перетворень:

$$R = R_1 + R_2 + R_1 \cdot \frac{h_{2m}}{h_{1m}} + R_2 \cdot \frac{h_{1m}}{h_{2m}} - R_1 \cdot R_2 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right). \qquad (5.11)$$

На підставі (5.11), з урахуванням (5.4) і (5.7) отримаємо вираз для визначення наслідків, у випадку дії сумарного результуючого ризику R:

$$h = \frac{R_1 + R_2 + R_1 \cdot \frac{h_{2m}}{h_{1m}} + R_2 \cdot \frac{h_{1m}}{h_{2m}} - R_1 \cdot R_2 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right)}{p_1 + p_2 - p_1 \cdot p_2}. \qquad (5.12)$$

Нехай наслідки повного знищення інформаційного активу h_{1m} і h_{2m} ризиків R_1 і R_2 будуть однаковими, тобто $h_{1m} = h_{1m} = h_m$. Тоді вираз (5.11) можна представити у вигляді:

$$R = 2 \cdot \left(R_1 + R_2 - \frac{R_1 \cdot R_2}{h_m} \right). \qquad (5.13)$$

У випадку рівності ризиків, тобто $R_1 = R_2 = R_0$, вираз (5.11) можна представити у вигляді:

$$R = R_0 \cdot \left(2 + \frac{h_{2m}}{h_{1m}} + \frac{h_{1m}}{h_{2m}} - R_0 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right) \right), \qquad (5.14)$$

де $h_{1m} \neq 0$ і $h_{2m} \neq 0$.

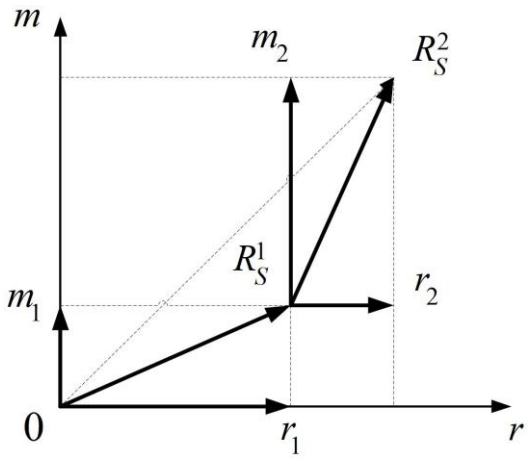
У випадку рівності насідків повного знищення інформаційного активу, тобто $h_{1m} = h_{1m} = h_m$, і рівності ризиків, тобто $R_1 = R_2 = R_0$, вираз (5.11)

можна представити у вигляді:

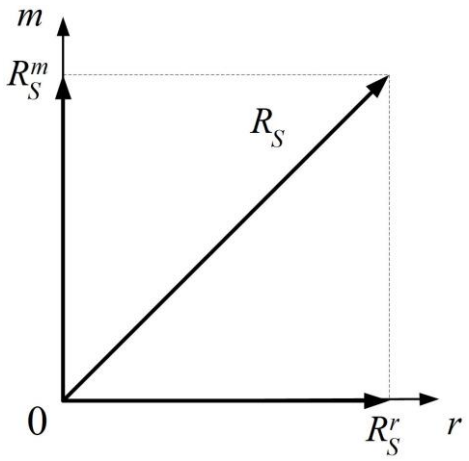
$$R = 2 \cdot R_0 \cdot \left(2 - \frac{R_0}{h_m} \right), \tag{5.15}$$

де $h_m \neq 0$.

Графічне відображення розробленої методології для випадку двох об'єктивних і двох суб'єктивних ризиків представлено на рис. 5.1.



а)



б)

Рис. 5.1. Графічне відображення розробленої методології оцінки ризику

Структурно-аналітичне відображення розробленої методології представлено на рис. 5.2.

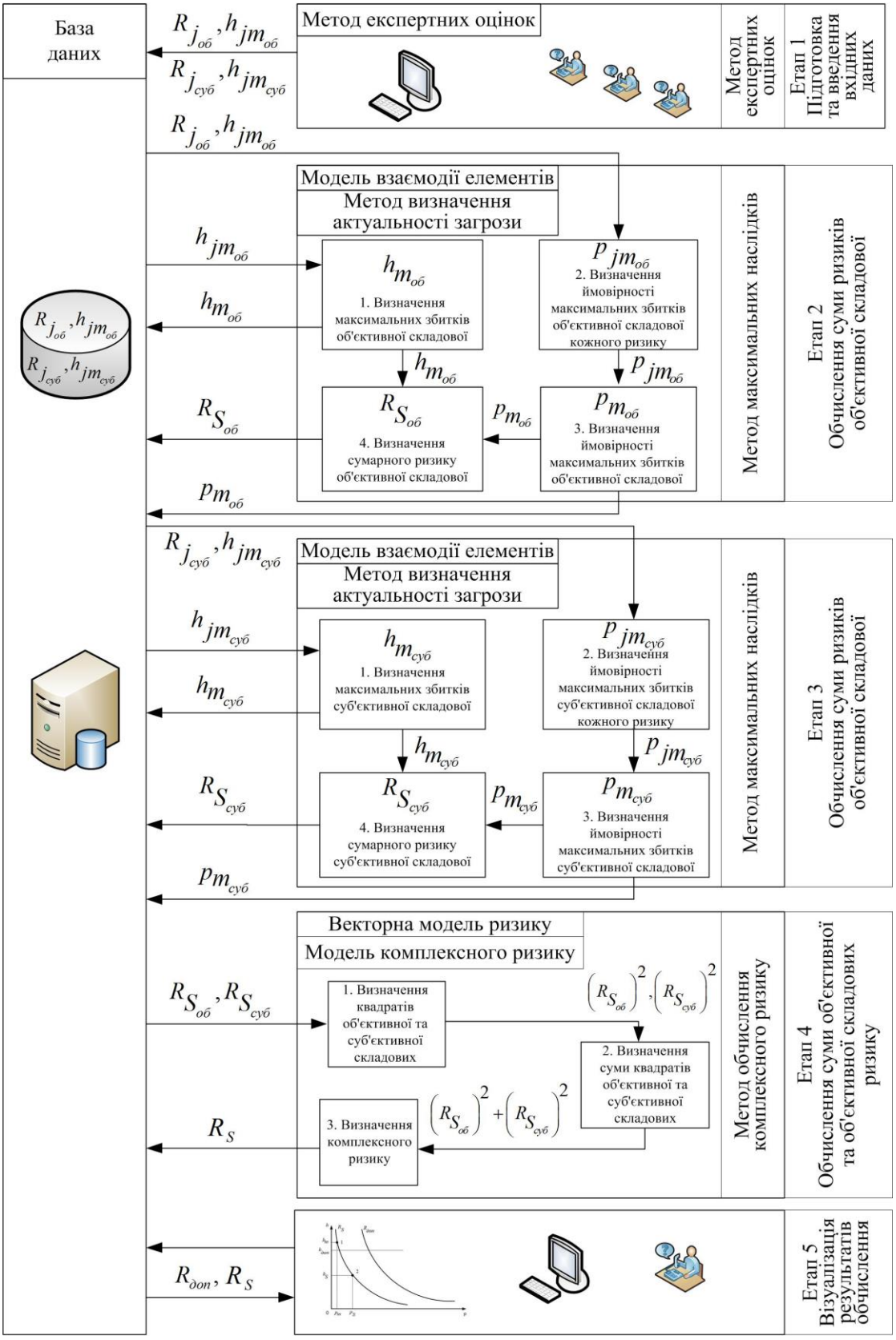


Рис. 5.2. Структурно-аналітичне відображення розробленої методології оцінки ризиків

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

Структурне рішення апаратно-програмного комплексу оцінки та аналізу ризику, робота якого базується на запропонованій методології, приведена на рис. 5.3 [2].

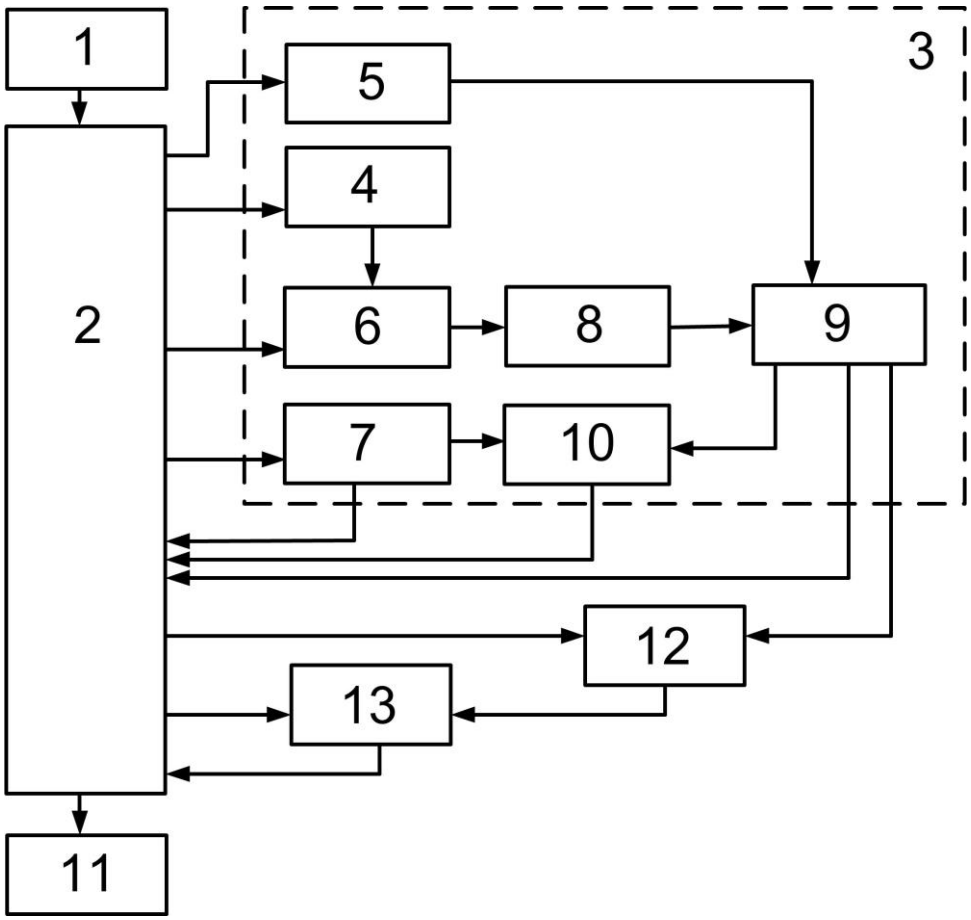


Рис. 5.3. Апаратно-програмний комплекс оцінки та аналізу ризику

Апаратно-програмний комплекс оцінки та аналізу ризику відноситься до спеціалізованих апаратно-програмних пристроїв обчислювальної техніки для автоматизованого розрахунку і аналізу ризиків з представленням варіантів рішень щодо вибору методів обробки ризику, і являє собою

апаратно-програмний комплекс, що містить модулі і зв'язки між ними, що знаходяться в функціонально-конструктивній єдності.

Розглянемо та дослідимо існуючі пристрої для оцінки ризику проекту, а також проаналізуємо їх недоліки.

Відомий пристрій для автоматизованої експертної оцінки факторів ризику проекту [3], що містить блок введення багатокомпонентних даних, блок обробки і аналізу даних, блок діалогового інтерфейсу, блок пам'яті і блок генерації анкети експертного опитування, який забезпечує формування на підставі кількох експертних оцінок для кожного об'єкта узагальненої величина ймовірності і негативних наслідків факторів ризику. Порядок експертної оцінки факторів ризику заснований на розрахунку середнього значення від всіх експертних оцінок одного і того ж фактору ризику для одного і того ж об'єкта оцінки. На підставі кількох експертних оцінок для кожного об'єкта формується узагальнена величина ймовірності і негативних наслідків факторів ризику.

Недоліком даного пристрою є відносно вузькі функціональні можливості, обумовлені тим, що враховуються тільки показники, пов’язані з факторами обмеженої кількості ризиків.

Крім того, відомий пристрій розрахунку ризику [4], що містить блок обчислення ризику, блок визначення стану, блок визначення умов та блок управління. Блок обчислення ризику включає в себе модуль управління параметрами і модуль обчислення індексу ризику. Пристрій забезпечує розрахунок ризику ймовірних збитків організації у випадку передачі власних даних за межі організації. При розрахунку ризику використовують три фактори ризику: виплата відшкодування, зниження конкурентоспроможності через вплив комерційної таємниці, втрата прибутку внаслідок вилучення клієнта.

Недоліком даного пристрою є відносно вузькі функціональні можливості, обумовлені тим, що враховуються тільки показники, пов’язані з вирішенням конкретно поставленої задачі.

Також, відомий апаратно-програмний комплекс розрахунку сумарного ризику [5], містить модуль введення початкових даних, блок пам’яті, модуль обчислення і аналізу даних, модуль виведення та візуалізації інформації і призначений для обчислення значень сумарного ризику.

Недоліком даного комплексу є відносно недостатні функціональні можливості, обумовлені тим, що не здійснюється аналіз розрахованих ризиків і не передбачено надання варіантів рішень щодо вибору методів обробки ризику.

Завданням запропонованого у даному розділі пристрою є вдосконалення відомого рішення шляхом введення додаткових функціональних модулів для забезпечення можливості автоматизованого розрахунку і аналізу ризиків з представленням варіантів рішень щодо вибору методів обробки ризику.

Поставлене завдання вирішується тим, що апаратно-програмний комплекс оцінки та аналізу ризику, який містить модуль введення початкових даних, блок пам’яті, модуль виведення та візуалізації інформації, модуль обчислення і аналізу даних, який складається з блоку формування масиву ризиків подій, блоку розрахунку значення максимальних збитків у результаті сумарного ризику, блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику, блоку визначення ймовірності сумарного ризику сумісних випадкових подій, блоку визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події, блоку розрахунку сумарного ризику в умовах дії множини ризиків, блоку розрахунку збитків при сумарному результуючому ризику, перший, другий, третій, четвертий входи блоку пам’яті з’єднані відповідно з виходом модуля введення початкових даних, виходом блоку визначення ймовірності сумарного ризику сумісних випадкових подій, другим виходом блоку розрахунку сумарного ризику в умовах дії множини ризиків та виходом блоку розрахунку збитків при сумарному результуючому ризику, перший,

другий, третій, четвертий та п’ятий виходи блоку пам’яті з’єднані відповідно з входом блоку розрахунку значення максимальних збитків у результаті сумарного ризику, входом блоку формування масиву ризиків подій, першим входом блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику, входом блоку визначення ймовірності сумарного ризику сумісних випадкових подій та модуля виведення та візуалізації інформації, вихід блоку формування масиву ризиків подій з’єднаний з другим входом блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику, вихід якого з’єднаний з входом блоку визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події, вихід якого є першим входом блоку розрахунку сумарного ризику в умовах дії множини ризиків, другий вхід якого з’єднаний з виходом блоку розрахунку значення максимальних збитків у результаті сумарного ризику, другий вихід блоку визначення ймовірності сумарного ризику сумісних випадкових подій та перший вихід блоку розрахунку сумарного ризику в умовах дії множини ризиків з’єднані з першим та другим входами блоку розрахунку збитків при сумарному результуючому ризику, додатково містить модуль аналізу гранично-допустимого значення ризику, модуль аналізу методів обробки ризику, шостий вихід блоку пам’яті та третій вихід блоку розрахунку сумарного ризику в умовах дії множини ризиків з’єднаний відповідно з першим та другим входами модуля аналізу гранично-допустимого значення ризику, вихід якого з’єднаний з другим входом модуль аналізу методів обробки ризику, перший вхід якого з’єднаний з сьомим виходом блоку пам’яті, а вихід з п’ятим входом блоку пам’яті.

Технічним результатом являється розширення функціональних можливостей пристрою в частині здійснення аналізу розрахованого ризику та надання варіантів рішень щодо вибору методів обробки ризику.

Апаратно-програмний комплекс розрахунку сумарного ризику містить,

рис. 5.3, 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 максимальних збитків у результаті сумарного ризику 5, блок формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, блок визначення ймовірності сумарного ризику сумісних випадкових подій 7, блок визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, блок розрахунку сумарного ризику в умовах дії множини ризиків 9, блок розрахунку збитків при сумарному результуючому ризику 10, блок аналізу гранично-допустимого значення ризику 12, блок аналізу методів обробки ризику 13. Перший, другий, третій, четвертий входи блоку пам’яті 2 з’єднані відповідно з виходом модуля введення початкових даних 1, виходом блоку визначення ймовірності сумарного ризику сумісних випадкових подій 7, другим виходом блоку розрахунку сумарного ризику в умовах дії множини ризиків 9 та виходом блоку розрахунку збитків при сумарному результуючому ризику 10, перший, другий, третій, четвертий та п’ятий виходи блоку пам’яті 2 з’єднані відповідно з входом блоку розрахунку значення максимальних збитків у результаті сумарного ризику 5, входом блоку формування масиву ризиків подій 4, першим входом блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, входом блоку визначення ймовірності сумарного ризику сумісних випадкових подій та модуля виведення та візуалізації інформації 11, вихід блоку формування масиву ризиків подій 4 з’єднаний з другим входом блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, вихід якого з’єднаний з входом блоку визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, вихід якого є першим входом

блоку розрахунку сумарного ризику в умовах дії множини ризиків 9, другий вхід якого з'єднаний з виходом блоку розрахунку значення максимальних збитків у результаті сумарного ризику 5, другий вихід блоку визначення ймовірності сумарного ризику сумісних випадкових подій 7 та перший вихід блоку розрахунку сумарного ризику в умовах дії множини ризиків 9 з'єднані з першим та другим входами блоку розрахунку збитків при сумарному результуючому ризику 10, шостий вихід блоку пам'яті 2 та третій вихід блоку розрахунку сумарного ризику в умовах дії множини ризиків 9 з'єднаний відповідно з першим та другим входами модуля аналізу гранично-допустимого значення ризику 12, вихід якого з'єднаний з другим входом модуль аналізу методів обробки ризику 13, перший вхід якого з'єднаний з сьомим виходом блоку пам'яті 2, а вихід з п'ятим входом блоку пам'яті 2.

Пристрій містить елементи, охарактеризовані на функціональному рівні, і описувана форма їх реалізації передбачає використання, зокрема, програмованих (налаштовуваних) багатофункціональних засобів, тому нижче при описі роботи пристрою подано відомості, що підтверджують можливість виконання такими засобами конкретних завдань.

Апаратно-програмний комплекс розрахунку сумарного ризику працює наступним чином.

Для досліджуваного об'єкта (об'єктів) попередньо визначають множину подій, ймовірність їх настання та наслідки (збитки), до яких може призвести кожна така подія, а також максимально можливі збитки.

Максимальні значення наслідків можуть бути визначені, наприклад експертним шляхом, як максимальні збитки, що можуть бути завдані активам компанії (матеріальні, нематеріальні, людські).

Після запуску апаратно-програмного комплексу через модуль введення початкових даних 1, вводять вищезазначені дані, формуючи базу даних, яку зберігають у блоці пам'яті 2.

У блоці формування масиву ризиків ймовірних подій 4, на основі вхідних даних, отриманих з блоку пам'яті 2 , формують масив із n ризиків, де

кожний ризик визначають ймовірністю або можливістю настання випадкової події, що може призвести до певних наслідків.

На блок розрахунку значення максимальних збитків у результаті сумарного ризику 5 подають множину максимальних значень наслідків для кожного ризику з блоку пам’яті 2.

У випадку дії *n* ризиків значення сумарного наслідку не буде перевищувати суми максимальних наслідків для кожного із *n* ризиків, без урахування синергетичного ефекту.

В блоці формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, формують масив ймовірностей виникнення кожної події, що призводить до відповідних максимальних наслідків в умовах дії ризиків.

Дія одного або декількох ризиків не виключає дії інших ризиків у той же період часу. З огляду на це, можемо констатувати, що події, які призводять до ризиків є сумісними подіями. На підставі цього, ймовірність виникнення події, що призводить до дії *n* ризиків з максимальними наслідками для кожного ризику, визначають у блоці визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, як суму ймовірностей цих подій без ймовірності їх добутку.

Сума дії *n* ризиків визначають у блоці розрахунку суми ризиків в умовах дії множини ризиків 9.

Ймовірність суми дії *n* ризиків визначають у блоці визначення ймовірності суми ризиків сумісних випадкових подій 7.

Таким чином, величину наслідків у випадку дії суми ризиків визначають у блоці розрахунку збитків при сумарному результуючому ризику 10.

Розраховане значення ризику у блоці розрахунку сумарного ризику в умовах дії множини ризиків 9 аналізують та порівнюють в блоці аналізу гранично-допустимого значення ризику 12 з гранично-допустимим значенням ризику, яке подають з блоку пам’яті 2.

Результат аналізу розрахованого ризику та порівняння його з гранично-допустимим значенням ризику з блоку аналізу гранично-допустимого значення ризику 12 подають на блок аналізу методів обробки ризику 13, де здійснюють аналіз отриманих результатів, порівняння та визначають пропозицію щодо методів обробки ризику.

Проміжні та кінцеві результати розрахунків зберігають у блоці пам’яті 2 та виводять у цифровому та/або графічному вигляді на модуль виведення та візуалізації інформації 11.

Таким чином, запропонований апаратно-програмний комплекс оцінки та аналізу ризику має розширені функціональні можливості в частині аналізу розрахованого значення ризику з гранично-допустимим значенням та надання варіантів рішень щодо вибору методів обробки ризику, і може бути використаний як система підтримки прийняття рішень.

Модуль виведення та візуалізації інформації 11 на рис. 5.3 являє собою апаратно-програмний комплекс, що містить модулі і зв'язки між ними, що знаходяться в функціонально-конструктивній єдності. Структурне рішення апаратно-програмного комплексу візуалізації ризику приведено на рис. 5.4 [6].

Апаратно-програмний комплекс візуалізації ризику працює наступним чином.

Для досліджуваного об’єкта (об’єктів) попередньо визначають множину подій, ймовірність їх настання та наслідки (збитки), до яких може призвести кожна така подія, а також крок дискретизації ймовірності.

Вибір кроку дискретизації ймовірності залежить від точності візуалізації ризику, яку необхідно досягти.

Після запуску апаратно-програмного комплексу через модуль введення початкових даних 1, вводять вищезазначені дані, формуючи базу даних, яку зберігають у блоці пам’яті 2.

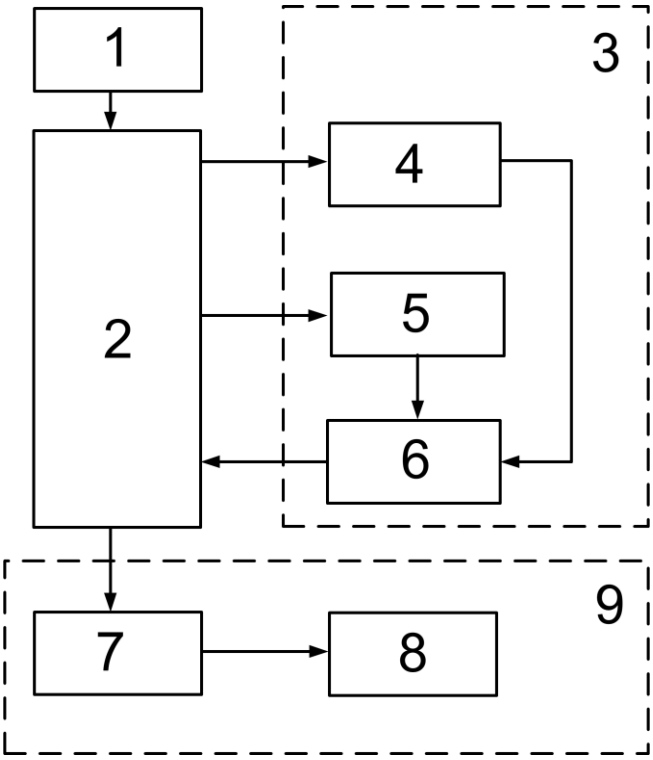


Рис. 5.4. Апаратно-програмний комплекс візуалізації ризику

Як ми уже зазначали, одне з визначень ризику R – ймовірність p випадкової події, що призводить до певних наслідків h, і може визначатися за формулою:

$$R = p \cdot h.$$

У блоці розрахунку значення поточного ризику 5 на підставі виразу (1) здійснюється обчислення значення ризику на основі вхідних даних, отриманих з блоку пам’яті 2.

У блоці формування значень горизонтальної координати 4 формується масив значень ймовірності від 0 до 1 з кроком дискретизації, заданим у модулі введення початкових даних 1.

На підставі виразу (1) залежність наслідків h в результаті настання деякої події від ймовірності p її настання можна представити у вигляді:

$$h(p) = \frac{R}{p} \ ,$$

де $p \neq 0$.

У блоці обчислення та формування значень вертикальної координати 6, на основі вхідних даних, отриманих з блоку формування значень горизонтальної координати 4 та з блоку розрахунку значення поточного ризику 5, формують масив із n значень ймовірностей настання випадкових подій та наслідків від їх настання.

Проміжні та кінцеві результати розрахунків зберігають у блоці пам'яті 2. З блоку пам'яті 2 кінцеві результати у вигляді координат задання ризику подаються на блок формування зображення 7 та виводяться у цифровому та/або графічному вигляді на блок виведення та візуалізації інформації 8.

Таким чином, при використанні «безперервних карт ризику» інформаційної безпеки знімаються практично всі недоліки «дискретних карт», ставатиме значно легше отримувати адекватні результати, якісно змінюється можливість в отриманні точних і коректних результати при будь-якому кроці зміни рівня ризику або величини можливої втрати. Це дає нові можливості для розрахунку ризиків, і як наслідок, для подальших дій по їх обробці. Використання такого підходу дає можливість підвищити адекватність існуючих моделей СУІБ, за допомогою яких було б можливо трансформувати ризик-апетит власника активу у співставні, прозорі та зрозумілі характеристики.

Запропонований апаратно-програмний комплекс візуалізації ризику дозволяє здійснити розрахунки та побудувати безперервну карту ризиків, що усуває проблему дискретності і нерівномірності кроку значень ризиків, врахувавши усі ризики в процесі їх оцінки, а також дозволяє легше отримувати адекватні, точні і коректні результати оцінки ризику при будь-якому кроці зміни рівня ризику, ймовірності виникнення подій, що призводять до ризику або величини можливих наслідків їх реалізації.

З урахуванням того, що у даній дисертаційній роботі ми розробляємо методологію оцінювання ризику кібербезпеки інформаційних систем об'єктів

критичної інфраструктури, розглянемо спосіб виявлення кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури.

Структурне рішення системи, яка реалізує спосіб виявлення кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури представлене на рис. 5.5 [7].

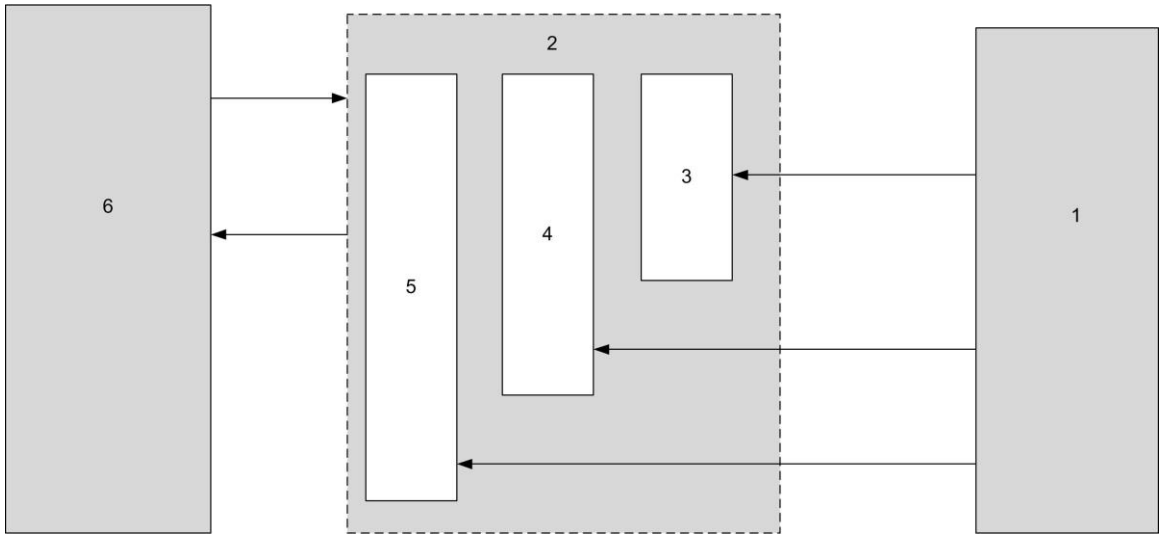


Рис. 5.5. Структурне рішення системи виявлення кібератак

Система належить до галузі захисту інформаційно-телекомунікаційних систем та мереж від підозрілих впливів на них та несанкціонованого доступу до їх ресурсів, а саме до способів, які забезпечують моніторинг, аналіз, обробку та класифікацію мережевого трафіку, що надходить до відомчої інформаційно-телекомунікаційної системи з глобальної мережі Інтернет, з метою виявлення комп'ютерний атак та захисту від них.

Однією з загроз є кібератаки (підозрілі впливи) на інформаційну (комунікаційну або технологічну) систему об'єкта критичної інфраструктури, яка безпосередньо вплине на стале функціонування об'єкту критичної інфраструктури.

Відомий спосіб виявлення атак [8], який передбачає нагляд за тотальним мережевим трафіком, накопичення даних, перевірку даних за

заданими правилами і вживання відповідних дій при виявлені даних, що відповідають цим правилам.

Недоліком такого способу виявлення атак є те, що він на мережевому рівні не дозволяє виявляти атаки, що спрямовані на спеціалізовані інформаційні системи для отримання несанкціонованого доступу. До того ж він не забезпечує виявлення зловживань незареєстрованими абонентами під час роботи з ресурсами інформаційної системи. А також, у зв'язку з необхідністю обробки великого обсягу даних мережевих з'єднань, даний спосіб не забезпечує своєчасного виявлення атак та реагування на них.

Аналогічне рішення передбачає використання сигнатурного аналізу для фільтрації вхідних пакетів [9, 10].

Крім недоліків попереднього способу, спосіб [9, 10] не забезпечує виявлення нових, не відомих комп'ютерних атак на інформаційні ресурси.

Спосіб виявлення атак, який реалізовано у [11], включає спостереження за трафіком пакетів даних, що надходять абоненту, перевірку цих пакетів за заданими правилами і подачу сигналу для прийняття заходів захисту від несанкціонованого доступу, коли перевірка виявляє відповідність вказаним правилам. Він орієнтований на спостереження за поведінкою зареєстрованих користувачів мереж і виявлення спроб несанкціонованого доступу до ресурсів мережі з їхньої сторони. Особливістю даного способу є те, що для виявлення спроб несанкціонованого доступу від обманно присвоєного імені іншого абонента мережі, проводять спостереження за трафіком адресованих абоненту пакетів даних, що включає постійно поновлюваний підрахунок числа пакетів, що виконується в межах серії пакетів, що надходять підряд один за одним через проміжки часу, не більші заданого значення. При цьому перевірку пакетів даних, що надходять, виконують кожен раз на відповідність заданим правилам, коли розмір чергової серії досягає критичного числа пакетів.

Недоліком даного способу є те, що хоч дана система забезпечує збір даних в реальному часі, проте потім, при послідовному аналізі сеансів

мережевих з'єднань, виявлення несанкціонованих дій в комп'ютерній мережі відбувається з неминучим запізненням по відношенню до початку таких дій. У багатьох випадках, запізнення з прийняттям заходів по припиненню несанкціонованих дій може приводити до непоправних наслідків і робити захист малоефективним. Відомий також спосіб виявлення атак [12], що передбачає спостереження за діями абонентів шляхом отриманням даних з системних журналів інформаційної системи, що містять інформацію про запити абонента на доступ до ресурсів, або аналізом трафіку, який надходить від абонентів до інформаційної системи. Дані про дії абонентів перевіряються за заданими правилами. За результатами аналізу видаються сигнали для прийняття заходів захисту інформаційної системи. Для своєчасного реагування на атаку аналіз трафіку виконується безперервно, а аналіз накопичених даних виконується через невеликий інтервал часу, величина якого вибирається залежно від інтенсивності роботи абонентів з ресурсами інформаційної системи і необхідним часом реагування на виявлену атаку.

Недоліком способів, реалізованих в [8-12] є те, що вони не забезпечують в режимі реального часу виявлення всіх типів комп'ютерних атак, а в основному направлені на виявлення атак зі сторони зареєстрованих користувачів мереж, тобто окремих типів атак. Також відомі рішення не забезпечують виявлення нових, не відомих комп'ютерних атак на інформаційні ресурси

Відомий сигнатурний спосіб моніторингу інформаційно-телекомунікаційних мереж [13], який полягає у використанні спеціалізованого антивірусного програмного забезпечення для виявлення та нейтралізації шкідливого програмного забезпечення (вірусів), це програмне забезпеченням певного типу, що працює на обчислювальних машинах. Антивірусне програмне забезпечення для аналізу використовує множину відомих вірусів, інформація про які внесена до власної бази даних, виконує перегляд файлів або пакетів на комп’ютері, перевіряючи наявність чи

відсутність у базі даних відомих вірусів. У випадку відповідності будь-якої ділянки коду програми, що перевіряється, відомому коду (сигнатурі) віруса в базі даних, антивірусне програмне забезпечення здійснює один із наступних заходів: знищує інфікований файл; переносить файл до «карантину» - забезпечуючи його недоступність для виконання з метою недопущення подальшого розповсюдження вірусу; намагається відновити файл, видаляючи вірус з тіла файлу.

Сигнатурний спосіб є надійним і забезпечує високу швидкодію. Тривале застосування способу дозволило напрацювати основні механізми та засоби ефективного виявлення та знешкодження найбільш розповсюджених вірусних програм. Сучасні обчислювальні ресурси дозволяють здійснювати порівняння коду програми з сигнатурами антивірусних баз з високою точністю та оперативністю.

Але через лавиноподібне зростання кількості нових вірусів та їх мінливість, бази сигнатур збільшуються до надзвичайних розмірів, що призводить до зниження швидкодії.

Відомий спосіб евристичного пошуку шкідливих програм [14], суть якого полягає в аналізі поведінки всіх програм, які запускаються на виконання. Якщо в процесі роботи системи виявляється підозріла поведінка додатку, тобто програма починає виконувати дії, які не стосуються її функціонального призначення та які раніше не виконувались, то спрацьовує сигналізація про небезпеку та евристичний модуль повідомляє користувачу про потенційну загрозу.

Спосіб евристичного пошуку шкідливих програм є перспективним, сучасні тенденції розвитку обчислювальних систем та технологій штучного інтелекту дозволяють спрогнозувати підвищення рівня захищеності як програмних, так і апаратних засобів обробки інформації за рахунок використання евристичного модуля, який спроможний реагувати на загрози, про які відсутня інформація в базі сигнатур.

Разом з цим, спосіб евристичного пошуку шкідливих програм може

спричинити помилкове реагування на безпечні події, враховуючи людський фактор, це може призвести до того, що користувач, після декількох помилкових спрацювань, може відключити евристичний модуль, що, в свою чергу, неминуче призведе до зниження рівня захисту інформаційної системи. Крім того, евристичний модуль може є використовувати значні обчислювальні потужності, невиправдано великі об’єми пам’яті та ресурси процесору, що призводить до погіршення робочих характеристик інформаційної системи в цілому, як наслідок – відключення евристичного модуля користувачем.

Відомий спосіб моніторингу інформаційно-телекомунікаційних мереж [15], який базується на застосуванні міжмережевих екранів. Механізм захисту в ранніх версіях міжмережевих екранів ґрунтувався на налаштованому заздалегідь знанні додатків, мережевих взаємозв'язків між ними і механізму примусової підтримки існуючих взаємозв'язків. В цьому випадку обмінюватися даними можуть тільки підтверджені хости і додатки. У більш пізніх версіях міжмережевих екранів було додано механізм Deep Packet Inspection (DPI), який привів до появи гібрида брандмауера / антивіруса, який забезпечує перевірку характеристик даних, що проходять через міжмережевий екран. Численні програми та додатки для встановлення з’єднання з віддаленими комп’ютерами або серверами можуть використовувати небезпечні методи, залишаючи «отвори» та вразливості для проникнення ззовні.

Суть роботи міжмережевого екрану полягає в контролі як вхідного, так і вихідного трафіку шляхом обмеження можливості встановлювати з’єднання з визначеними віддаленими ресурсами. Найрозповсюдженіший метод захисту – білі та чорні списки мережевих ресурсів. Чорний список – це список мережевих ресурсів, на які не можна заходити. Білий список – це список ресурсів, на які тільки можна заходити. Вочевидь метод білого списку є більш безпечним, але з іншого боку він суттєво обмежує можливості користувача та додатків.

Налаштування міжмережевого екрану дозволяє забезпечити можливість мережевої взаємодії тільки з перевіреними ресурсами, відокремлюючи всі потенційно небезпечні та неперевірені мережеві ресурси. Крім того, міжмережевий екран може бути встановлений на мережевому шлюзі локальної мережі, тобто на сервері, що надає доступ до мережі Інтернет комп'ютерам, що входять до єдиної локальної мережі установи, не витрачаючи при цьому обчислювальні ресурси машин користувачів.

Як і попередні способи, даний спосіб також має свій недолік, який логічно витікає з його переваги: персонал, який експлуатує та обслуговує міжмережевий екран, повинен мати досить велику кваліфікацію та глибокі знання мережевих протоколів та особливостей роботи мережевих додатків. При роботі з міжмережевим екраном на перший план виходить рівень кваліфікації технічного персоналу, тому що екран, який працює з налаштуваннями «за замовченням» має дуже низьку ефективність.

В основу корисної моделі поставлено задачу розробки способу виявлення кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури, який дозволить здійснювати ефективний моніторинг, виявлення, обробку та аналіз підозрілих впливів на мережеві об'єкти інформаційно-телекомунікаційної системи за рахунок застосування трьох рівнів моніторингу та фільтрації трафіку, забезпечуючи виявлення і відсічення більш широкого спектру загроз, порівняно з вищенаведеними існуючими способами захисту від мережевих атак.

Поставлена задача вирішується тим, що спосіб виявлення кібератак на інформаційно-телекомунікаційні системи, згідно з яким здійснюють моніторинг мережевого трафіку, накопичення даних, перевірку та аналіз даних в режимі реального часу за заданими правилами і вживання відповідних дій при виявлені даних, що відповідають цим правилам, причому для моніторингу, перевірки та аналізу трафіку використовують апаратно-програмний модуль виявлення підозрілих впливів, за допомогою якого фіксують у відповідні бази даних підозрілі та небезпечні IP-адреси та

інформацію про віруси, забезпечують виконання аналізу та фільтрації трафіку щонайменше на трьох рівнях послідовно, на першому рівні здійснюють автоматичне сканування трафіку та визначення типу протоколу мережевої взаємодії і у разі виявлення підозрілих впливів на порти системи модуль виявлення підозрілих впливів надсилає повідомлення про це адміністратору системи та здійснює блокування вхідного трафіку від визначеної IP-адреси і одночасно фіксує її у базі даних підозрілих та небезпечних IP-адрес, на другому рівні проводять аналіз та виявлення небезпечних впливів на мережеве обладнання інформаційно-телекомунікаційної системи, таких як відмови в обслуговуванні та/або підміни IP-адрес та/або вразливості протоколів мережевої взаємодії та/або вразливості додатків, на третьому рівні проводять виявлення небезпечних впливів на додатки інформаційно-телекомунікаційної системи таких як, спроби підбору пароля та/або захоплення чи привласнення привілей та/або спроби впровадження шкідливого програмного забезпечення типу «троянські коні» та/або скриті дії та/або аудит мережі та фіксують інформацію про віруси у відповідну базу даних небезпечних впливів.

За рахунок застосування послідовно трьох рівнів виявлення підозрілих впливів забезпечують:

- на першому рівні захист портів на предмет виявлення підозрілої активності від зовнішнього мережевого обладнання; на цьому рівні реалізований також механізм захисту від підозрілих спроб визначення типів протоколів взаємодії об’єкта захисту (ІТС, що підлягає захисту) з зовнішньою мережею (в разі виявлення спроб сканування портів інформаційно-телекомунікаційної системи модуль виявлення підозрілих впливів повідомляє про це адміністратору та блокує вхідний трафік від IP-адреси, з якої здійснюється спроба впливу, одночасно такі IP-адреси заносяться до «чорного списку», який являє собою базу небезпечних IP-адрес);

- на другому рівні захист мережевого обладнання інформаційно-

телекомунікаційної системи від потенційної атаки типу «відмови в обслуговуванні» (DDoS) (в разі виявлення різкого збільшення звернень до ресурсів інформаційно-телекомунікаційної системи система виявлення кібератак блокує вхідний трафік від IP-адрес, з яких здійснюються спроби впливів, одночасно такі IP-адреси заносяться до «чорного списку», який являє собою базу небезпечних IP-адрес);

- на третьому рівні захист додатків від впливів типу атаки на пароль, спроб захоплення привілеїв, «троянські коні», аудит мережі, скриті дії (захист реалізується за допомогою класичного сигнатурного способу антивірусного захисту).

Спосіб здійснюють таким чином.

На першому рівні проводять виявлення підозрілих впливів шляхом здійснення контрзаходів від зловмисного сканування портів. Як правило, зловмисники вдаються до сканування TCP- і UDP-портів віддаленого комп'ютера, щоб встановити, які з них знаходяться в стані очікування запитів. Тому виявити факт сканування - значить, встановити, в якому місці і ким буде зроблено спробу злому. В основу принципу виявлення сканування портів покладені сучасні методи виявлення факту сканування з використанням спеціальної програми, призначеної для виявлення вторгнень на рівні мережі (IDS) – NFR. На цьому рівні реалізований також механізм захисту від підозрілих спроб визначення типів протоколів взаємодії об’єкта захисту (ІТС, що підлягає захисту) з зовнішньою мережею.

На другому рівні програмно-апаратний модуль виявлення підозрілих впливів здійснює аналіз вхідного трафіку на предмет потенційної атаки типу «відмови в обслуговуванні» (DDoS). На цьому рівні апаратно-програмний модуль виявлення підозрілих впливів аналізує впливи за наступними напрямами:

- Атака на мережевий пристрій. При атаці безпосередньо на мережевий пристрій (Network Device level), можуть бути використані помилки або недоліки програмного забезпечення або особливості апаратної реалізації

обладнання, при яких може наступати вичерпування його апаратних ресурсів. Одним з найпростіших прикладів атак на мережевий пристрій є переповнення його буфера, під час процедури автентифікації користувача за паролем. Використовуючи дану уразливість, зловмисник нейтралізує можливість підключення до пристрою за допомогою протоколів telnet або ssh.

- Атаки на операційну систему (OS level) зловмисники проводяться за допомогою використання особливостей реалізації ОС. Наприклад, до цієї категорії DDoS відноситься атака Ping of Death. У цій атаці ICMP exo-запити (echo request) мають загальний розмір, що перевищує максимальний розмір IP-пакета, відправляється потенційній жертві. Дана атака часто призводить до збою роботи операційної системи, так як пов'язана з особливостями реалізації стека протоколів TCP / IP.
- Атаки на додатки (Application-based attacks) намагаються взаємодіяти з робочими станціями або сервісами на предмет використання їхніх помилок на рівні мережевих додатків, які працюють на хостах пристроїв, що піддаються атаці або використовувати ці додатки для утилізації ресурсів потенційної жертви (пошук точок високої алгоритмічної складності та використання їх з метою утилізації доступних ресурсів віддаленого хоста). Одним із прикладів атак на рівні мережного додатки є finger bomb - коли зловмисник може викликати рекурсивну маршрутизацію на хост жертви.
- Застосовуючи на рівні каналу (Data Flooding), зловмисник намагається утилізувати доступну смугу пропускання мережі, хоста або пристрою, пересилаючи великі кількості даних, що тягне за собою переповнення (забивання) каналу зв'язку. В даному випадку, атакуючий просто використовує бомбардування доступної смуги пропускання, великими безглуздими пакетами з підробленим адресою джерела. Прикладом може служити атака типу ping flood.

- Атака на протокол (protocol fiture attack) використовує стандартні функції протоколу. Наприклад, деякі атаки використовують той факт, що IP адреса відправника може бути підмінений. Деякі, сфокусовані на DNS і атакують кеш DNS серверів. Зловмисник, який має свій сервер імен, може змусити атакується DNS помістити в свій кеш неправдиву запис, яка не буде відповідати адресою призначення.

З метою запобігання вищенаведеним впливам на інформаційно-телекомунікаційну систему апаратно-програмний модуль виявлення підозрілих впливів використовує механізм захисту на кордоні мережі. Даний метод дозволяє забезпечити ефективний захист від DDoS в межах існуючої смуги пропускання. В разі виявлення хоча б одної з вищенаведених ознак підозрілого впливу апаратно-програмний модуль виявлення підозрілих впливів інформує адміністратора системи про небезпеку та блокує вхідний трафік, який надходить від джерела небезпеки.

На третьому рівні апаратно-програмний модуль виявлення підозрілих впливів реалізує моніторинг підозрілих дій щодо системних параметрів та налаштувань додатків. На цьому рівні система реалізує виявлення наступних підозрілих впливів: атаки на пароль, захоплення привілей, «троянські коні», аудит мережі, скриті дії.

На даному рівні апаратно-програмний модуль виявлення підозрілих впливів діє за принципом чорного списку – виявлення хоча б однієї ознаки спроби небезпечної дії призводить до блокування вхідного трафіку від джерела небезпеки та інформування адміністратора.

Запропонований спосіб виявлення кібератак на інформаційно-телекомунікаційні системи, що передбачає багаторівневе виявлення підозрілих впливів, дозволяє реалізувати політику інтелектуального моніторингу та аналізу вхідного трафіку в реальному часі, який розповсюджується на широке коло системних та функціональних характеристик інформаційно-телекомунікаційної системи, що підлягає захисту. Розподілені за трьома рівнями механізми виявлення кібератак

(підозрілих впливів) охоплюють собою широкий спектр мережевих характеристик, що призводить до нейтралізації практично всіх відомих «слабких місць» в захисті мережевої інфраструктури – від вхідного порту до операційних систем.

Схематичне відображення способу виявлення кібератак (підозрілих впливів) на інформаційну систему об’єкту критичної інфраструктури представлено на рис. 5.6.

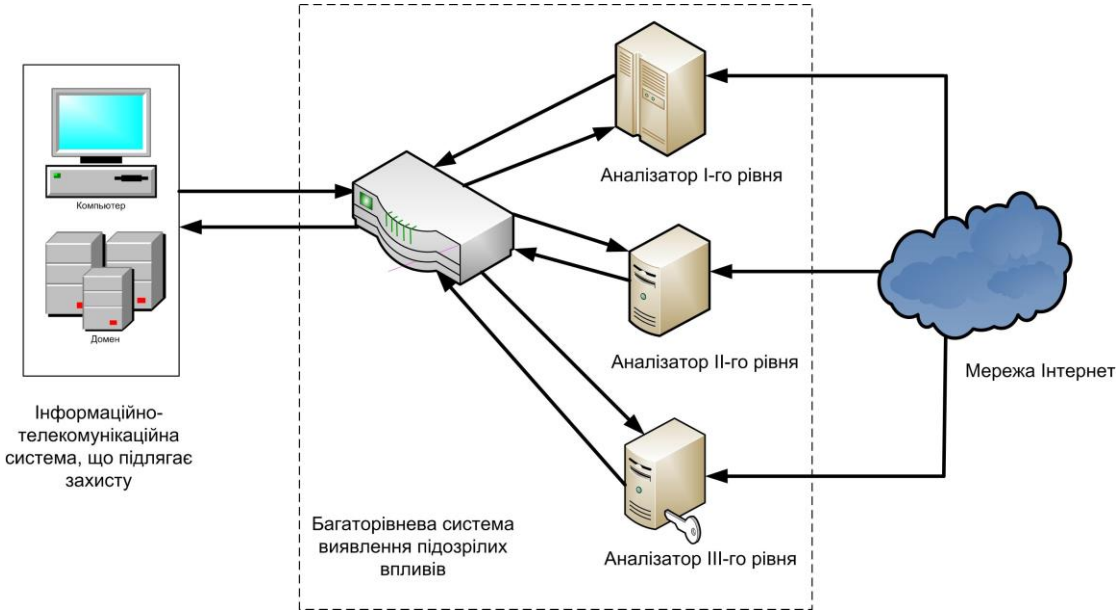


Рис. 5.6. Схематичне відображення способу виявлення кібератак

В основу дії багаторівневої системи виявлення підозрілих впливів покладений принцип розподіленого моніторингу. Фактично, для того, щоб зловмисник отримав змогу проникнути до інформаційно-телекомунікаційної системи, для захисту якої застосовано запропонований спосіб виявлення кібератак на інформаційно-телекомунікаційні системи, йому буде необхідно подолати трирівневий захисний рубіж. Такий підхід до захисту інформаційно-телекомунікаційної системи об’єктів критичної інфраструктури значно (фактично в три рази) підвищить витрати на проникнення, що в багатьох випадках зробить такі дії нерентабельними.

5.2. Структурна модель (рішення) обчислювальної системи розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури

На підставі даної методології вперше розроблено структурне рішення обчислювальної системи оцінки ризику кібербезпеки інформаційних систем, «Калькулятор ризиків», що реалізує запропоновані у даній дисертаційній роботі методи, рис. 5.7 [5].

Апаратно-програмний комплекс розрахунку суми ризиків відноситься до спеціалізованих апаратно-програмних пристроїв обчислювальної техніки, може бути використаний для визначення суми ризиків в умовах дії множини ризиків, і являє собою апаратно-програмний комплекс, що містить модулі і зв'язки між ними, що знаходяться в функціонально-конструктивній єдності.

Розглянемо та дослідимо існуючі пристрої для оцінки суми ризиків, а також проаналізуємо їх недоліки.

Відомий пристрій для автоматизованої експертної оцінки факторів ризику проекту [16], що містить блок введення багатокомпонентних даних, блок обробки і аналізу даних, блок діалогового інтерфейсу, блок пам'яті і блок генерації анкети експертного опитування, який забезпечує формування на підставі кількох експертних оцінок для кожного об'єкта узагальненої величина ймовірності і негативних наслідків факторів ризику. Порядок експертної оцінки факторів ризику заснований на розрахунку середнього значення від всіх експертних оцінок одного і того ж фактору ризику для одного і того ж об'єкта оцінки. На підставі кількох експертних оцінок для кожного об'єкта формується узагальнена величина ймовірності і негативних наслідків факторів ризику.

Недоліком даного пристрою є відносно вузькі функціональні можливості, обумовлені тим, що враховуються тільки показники, пов’язані з факторами обмеженої кількості ризиків.

Відомий пристрій розрахунку ризику [17], що містить блок обчислення

ризику, блок визначення стану, блок визначення умов та блок управління. Блок обчислення ризику включає в себе модуль управління параметрами і модуль обчислення індексу ризику. Пристрій розраховує ризик ймовірних збитків організації у випадку передачі власних даних за межі організації. При розрахунку ризику використовується три фактори ризику: виплата відшкодування, зниження конкурентоспроможності через вплив комерційної таємниці, втрата прибутку внаслідок вилучення клієнта.

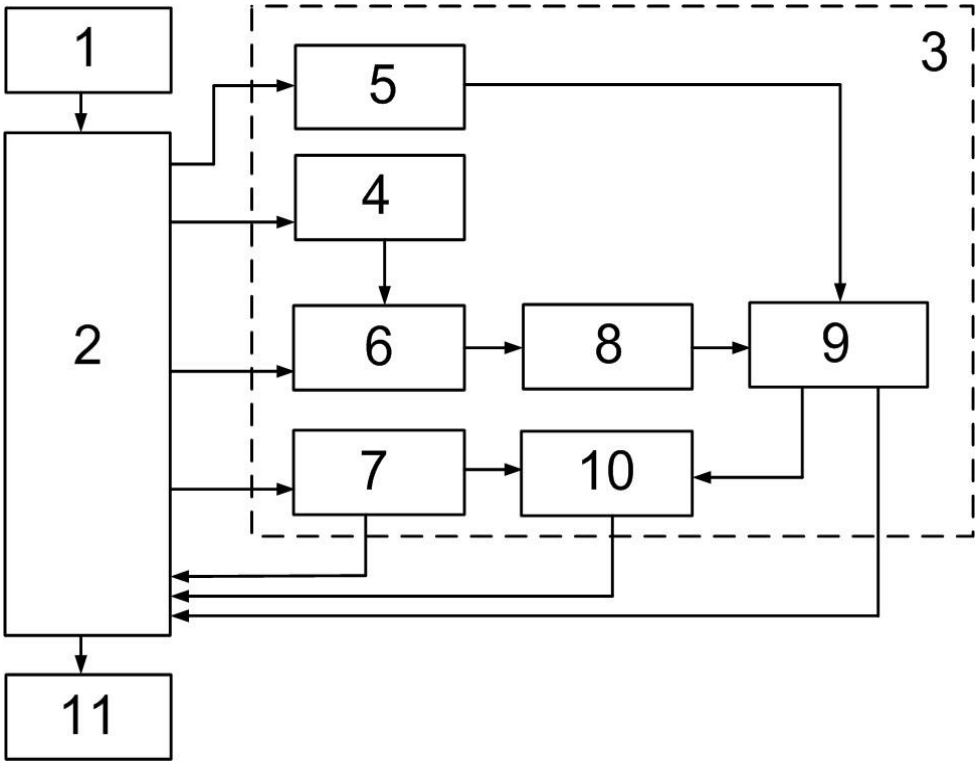


Рис. 5.7. Структурне рішення обчислювальної системи «Калькулятор ризиків»

Недоліком даного пристрою є відносно вузькі функціональні можливості, обумовлені тим, що враховуються тільки показники, пов’язані з вирішенням конкретно поставленої задачі.

Завданням запропонованого пристрою є забезпечення можливості автоматизованого розрахунку і аналізу наслідків множини ризиків з урахуванням показників, таких як ймовірність виникнення подій, що призводять до негативних наслідків, та величина негативних наслідків

(збитків).

Поставлене завдання вирішується тим, що апаратно-програмний комплекс розрахунку сумарного ризику, рис. 5.7, який містить модуль введення початкових даних 1, блок пам’яті 2, модуль обчислення і аналізу даних 3, модуль виведення та візуалізації інформації 11, причому, модуль обчислення і аналізу даних 3 містить блок формування масиву ризиків подій 4, блок розрахунку значення максимальних збитків у результаті сумарного ризику 5, блок формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, блок визначення ймовірності сумарного ризику сумісних випадкових подій 7, блок визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, блок розрахунку сумарного ризику в умовах дії множини ризиків 9, блок розрахунку збитків при сумарному результуючому ризику 10, входи блоку пам’яті 2 з’єднані з виходами модуля введення початкових даних 1, блоку визначення ймовірності сумарного ризику сумісних випадкових подій 7, блоку розрахунку сумарного ризику в умовах дії множини ризиків 9 та блоку розрахунку збитків при сумарному результуючому ризику 10, виходи блоку пам’яті 2 з’єднані з входами блоків формування масиву ризиків подій 4, розрахунку значення максимальних збитків у результаті сумарного ризику 5, формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, визначення ймовірності сумарного ризику сумісних випадкових подій 7 та модуля виведення та візуалізації інформації 11, вихід блоку формування масиву ризиків подій 4 з’єднаний з входом блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, вихід якого з’єднаний з входом блоку визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, вихід якого є одним з входів блоку розрахунку сумарного ризику в умовах дії множини ризиків 9, другий вхід якого

з’єднаний з виходом блоку розрахунку значення максимальних збитків у результаті сумарного ризику 5, виходи блоків визначення ймовірності сумарного ризику сумісних випадкових подій 7 та розрахунку сумарного ризику в умовах дії множини ризиків 9 з’єднані з входами блоку розрахунку збитків при сумарному результуючому ризику 10.

Технічним результатом являється розширення функціональних можливостей пристрою в частині здійснення розрахунку більшої кількості ризиків та вирішення ширшого класу задач.

Апаратно-програмний комплекс розрахунку сумарного ризику містить 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 максимальних збитків у результаті сумарного ризику 5, блок формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, блок визначення ймовірності сумарного ризику сумісних випадкових подій 7, блок визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, блок розрахунку сумарного ризику в умовах дії множини ризиків 9, блок розрахунку збитків при сумарному результуючому ризику 10, входи блоку пам’яті 2 з’єднані з виходами модуля введення початкових даних 1, блоку визначення ймовірності сумарного ризику сумісних випадкових подій 7, блоку розрахунку сумарного ризику в умовах дії множини ризиків 9 та блоку розрахунку збитків при сумарному результуючому ризику 10, виходи блоку пам’яті 2 з’єднані з входами блоків формування масиву ризиків подій 4, розрахунку значення максимальних збитків у результаті сумарного ризику 5, формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, визначення ймовірності сумарного ризику сумісних випадкових подій 7 та модуля виведення та візуалізації інформації 11, вихід блоку формування масиву

ризиків подій 4 з'єднаний з входом блоку формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, вихід якого з'єднаний з входом блоку визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, вихід якого є одним з входів блоку розрахунку сумарного ризику в умовах дії множини ризиків 9, другий вхід якого з'єднаний з виходом блоку розрахунку значення максимальних збитків у результаті сумарного ризику 5, виходи блоків визначення ймовірності сумарного ризику сумісних випадкових подій 7 та розрахунку сумарного ризику в умовах дії множини ризиків 9 з'єднані з входами блоку розрахунку збитків при сумарному результуючому ризику 10.

Пристрій містить елементи, охарактеризовані на функціональному рівні, і описувана форма їх реалізації передбачає використання, зокрема, програмованих (налаштовуваних) багатофункціональних засобів, тому нижче при описі роботи пристрою подано відомості, що підтверджують можливість виконання такими засобами конкретних завдань.

Апаратно-програмний комплекс розрахунку сумарного ризику працює наступним чином.

Для досліджуваного об'єкта (об'єктів) попередньо визначають множину подій, ймовірність їх настання та наслідки (збитки), до яких може призвести кожна така подія, а також максимально можливі збитки.

Максимальні значення наслідків можуть бути визначені, наприклад експертним шляхом, як максимальні збитки, що можуть бути завдані активам компанії (матеріальні, нематеріальні, людські).

Після запуску апаратно-програмного комплексу через модуль введення початкових даних 1, вводять вищезазначені дані, формуючи базу даних, яку зберігають у блоці пам'яті 2.

У блоці формування масиву ризиків ймовірних подій 4, на основі вхідних даних, отриманих з блоку пам'яті 2, формують масив із n ризиків, де кожний ризик визначають ймовірністю або можливістю настання випадкової

події, що може призвести до певних наслідків.

На блок розрахунку значення максимальних збитків у результаті сумарного ризику 5 подають множину максимальних значень наслідків для кожного ризику з блоку пам’яті 2.

У випадку дії *n* ризиків значення сумарного наслідку не буде перевищувати суми максимальних наслідків для кожного із *n* ризиків, без урахування синергетичного ефекту.

В блоці формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, формують масив ймовірностей виникнення кожної події, що призводить до відповідних максимальних наслідків в умовах дії ризиків.

Дія одного або декількох ризиків не виключає дії інших ризиків у той же період часу. З огляду на це, можемо констатувати, що події, які призводять до ризиків є сумісними подіями. На підставі цього, ймовірність виникнення події, що призводить до дії *n* ризиків з максимальними наслідками для кожного ризику, визначають у блоці визначення ймовірності події, що призводить до сумарного ризику з максимальними наслідками для кожної події 8, як суму ймовірностей цих подій без ймовірності їх добутку.

Сумарний ризик дії *n* ризиків на підставі виразів (5) і (7) визначають у блоці розрахунку сумарного ризику в умовах дії множини ризиків 9.

Ймовірність сумарної дії *n* ризиків визначають у блоці визначення ймовірності сумарного ризику сумісних випадкових подій 7.

Таким чином, величину наслідків у випадку дії сумарного результуючого ризику визначають у блоці розрахунку збитків при сумарному результуючому ризику 10.

Проміжні та кінцеві результати розрахунків зберігають у блоці пам’яті 2 та виводять у цифровому та/або графічному вигляді на модуль виведення та візуалізації інформації 11.

Структурно-аналітичне відображення обчислювальної системи «Калькулятор ризиків» представлено на рис. 5.8.

Таким чином, запропонований апаратно-програмний комплекс розрахунку сумарного ризику має розширені функціональні можливості в частині забезпечення автоматизованого розрахунку негативних наслідків (збитків) від дії множини сумісних подій, з урахуванням показників, таких як ймовірність виникнення подій, що призводять до негативних наслідків, та величина негативних наслідків (збитків), і може бути використаний як частина системи підтримки прийняття рішень.

5.3. Структурна модель (рішення) обчислювальної системи розрахунку комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури

На підставі представленої методології вперше розроблено структурне рішення обчислювальної системи розрахунку комплексного ризику кібербезпеки інформаційних систем, «Калькулятор комплексного ризику», що реалізує запропонований у даній дисертаційній роботі метод, рис. 5.9 [18].

Апаратно-програмний комплекс розрахунку комплексного ризику відноситься до спеціалізованих апаратно-програмних пристроїв обчислювальної техніки, може бути використана для визначення комплексного ризику як об'єктивно-суб'єктивної категорії, і являє собою апаратно-програмний комплекс, що містить модулі і зв'язки між ними, що знаходяться в функціонально-конструктивній єдності.

Розглянемо та дослідимо існуючі пристрої для оцінки ризику, а також проаналізуємо їх недоліки.

Відомий пристрій для автоматизованої експертної оцінки факторів ризику проекту [19], що містить блок введення багатокомпонентних даних, блок обробки і аналізу даних, блок діалогового інтерфейсу, блок пам'яті і блок генерації анкети експертного опитування, який забезпечує формування на підставі кількох експертних оцінок для кожного об'єкта узагальненої величина ймовірності і негативних наслідків факторів ризику. Порядок

експертної оцінки факторів ризику заснований на розрахунку середнього значення від всіх експертних оцінок одного і того ж фактору ризику для одного і того ж об'єкта оцінки. На підставі кількох експертних оцінок для кожного об'єкта формується узагальнена величина ймовірності і негативних наслідків факторів ризику.

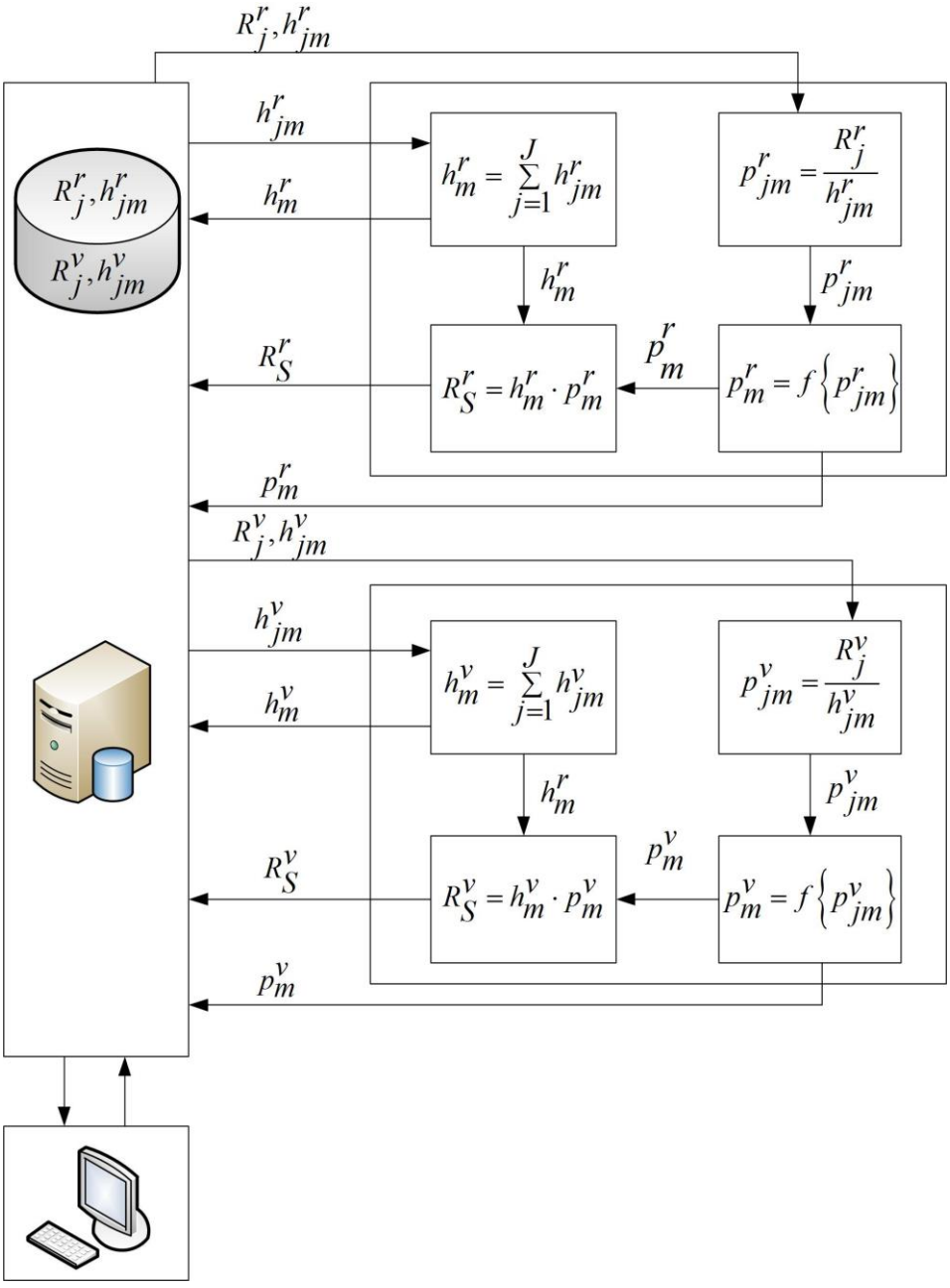


Рис. 5.8. Структурно-аналітичне відображення обчислювальної системи «Калькулятор ризиків»

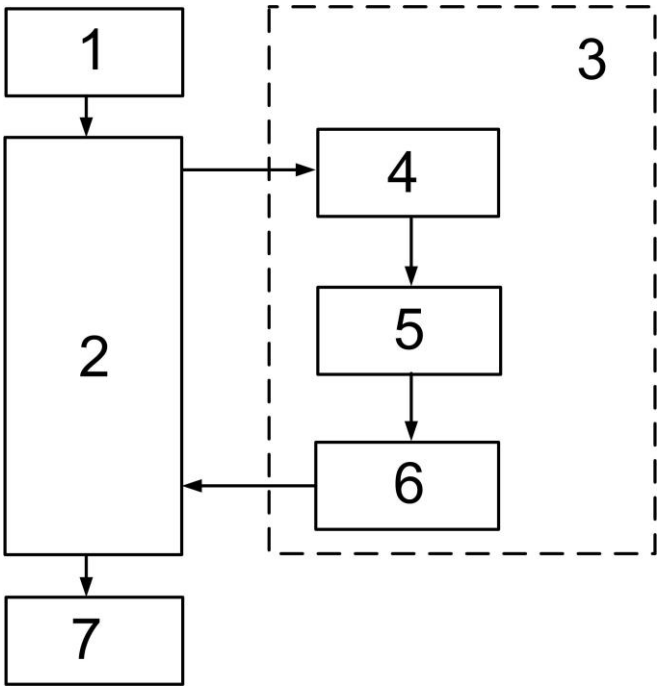


Рис. 5.9. Структурна модель (рішення) обчислювальної системи «Калькулятор комплексного ризику»

Недоліком даного пристрою є відносно вузькі функціональні можливості, обумовлені тим, що враховуються тільки показники, пов’язані з факторами обмеженої кількості ризиків.

Відомий пристрій розрахунку ризику [20], що містить блок обчислення ризику, блок визначення стану, блок визначення умов та блок управління. Блок обчислення ризику включає в себе модуль управління параметрами і модуль обчислення індексу ризику. Пристрій забезпечує розрахунок ризику ймовірних збитків організації у випадку передачі власних даних за межі організації. При розрахунку ризику використовують три фактори ризику: виплата відшкодування, зниження конкурентоспроможності через вплив комерційної таємниці, втрата прибутку внаслідок вилучення клієнта. Недоліком даного пристрою є відносно вузькі функціональні можливості, обумовлені тим, що враховуються тільки показники, пов’язані з вирішенням конкретно поставленої задачі.

Загальним недоліком подібних рішень є те, що при визначенні ризику враховують лише показники, пов’язані з факторами об’єктивних ризиків і не враховують фактори суб’єктивних ризиків. Завданням запропонованої корисної моделі є забезпечення можливості автоматизованого розрахунку комплексного ризику з урахуванням об’єктивної та суб’єктивної його складових.

Поставлене завдання вирішується тим, що апаратно-програмний комплекс розрахунку комплексного ризику, який містить модуль введення початкових даних, модуль пам’яті, модуль обчислення даних, модуль виведення та візуалізації інформації, вихід модуля введення початкових даних з’єднаний з входом модуля пам’яті, вихід модуля пам’яті з’єднаний з входом модуля виведення та візуалізації інформації, причому модуль обчислення даних містить блок формування проміжних даних суб’єктивного ризику, блок формування проміжних даних об’єктивного ризику, суматор проміжних даних суб’єктивного і об’єктивного ризиків, блок розрахунку комплексного ризику, другий вихід модуля пам’яті з’єднаний з входом блоку формування проміжних даних суб’єктивного ризику, третій вихід модуля пам’яті з’єднаний з входом блоку формування проміжних даних об’єктивного ризику, виходи блоків формування проміжних даних об’єктивного та суб’єктивного ризиків зв’язані з першим та другим входами суматора проміжних даних суб’єктивного і об’єктивного ризиків, вихід якого з’єднаний з входом блоку розрахунку комплексного ризику, вихід якого з’єднаний з другим входом модуля пам’яті. Технічним результатом являється розширення функціональних можливостей пристрою в частині здійснення автоматизованого розрахунку повного (комплексного) ризику, з урахуванням об’єктивної та суб’єктивної його складових, з використанням теорії векторної алгебри та комплексних чисел.

Апаратно-програмний комплекс розрахунку комплексного ризику містить модуль введення початкових даних 1, модуль пам’яті 2, модуль обчислення даних 3, модуль виведення та візуалізації інформації 8, модуль

обчислення і аналізу даних 3 містить блок формування проміжних даних суб'єктивного ризику 4, блок формування проміжних даних об'єктивного ризику 5, суматор проміжних даних суб'єктивного і об'єктивного ризиків 6, блок розрахунку комплексного ризику 7, другий вихід модуля пам'яті 2 з'єднаний з в ходом блоку формування проміжних даних суб'єктивного ризику 4, треті й вихід модуля пам'яті 2 з'єднаний з в ходом блоку формування проміжних даних об'єктивного ризику 5, виходи блоків формування проміжних даних об'єктивного 5 та суб'єктивного 4 ризиків зв'язані з першим та другим входами суматора проміжних даних суб'єктивного і об'єктивного ризиків 6, вихід якого з'єднаний з входом блоку розрахунку комплексного ризику 7, вихід якого з'єднаний з другим входом модуля пам'яті 2.

Пристрій містить елементи, охарактеризовані на функціональному рівні, і описувана форма їх реалізації передбачає використання, зокрема, програмованих (налаштовуваних) багатофункціональних засобів, тому нижче при описі роботи пристрою подано відомості, що підтверджують можливість виконання такими засобами конкретних завдань.

Структурно-аналітичне відображення обчислювальної системи «Калькулятор комплексного ризику» представлено на рис. 5.10.

Апаратно-програмний комплекс розрахунку комплексного ризику працює наступним чином.

Для досліджуваного об'єкта (об'єктів) попередньо визначають об'єктивний і суб'єктивний ризики. Після запуску апаратно-програмного комплексу через модуль введення початкових даних 1, вводять вищезазначені дані, які зберігають у модулі пам'яті 2. З модуля пам'яті 2 на модуль обчислення даних 3, а саме на в ходи блоків формування проміжних даних суб'єктивного 4 та об'єктив ного 5 ризиків подають відповідно значення суб'єктивного та об'єктивного ризиків, де здійснюють обчислення їх квадратів, одержані дані подають на входи суматора проміжних даних суб'єктивного і об'єктивного ризиків 6, отримуючи значення суми квадратів

суб’єктивного та об’єктивного ризиків, яку подають на вхід блоку розрахунку комплексного ризику 7, де здійснюють розрахунок квадратного кореня суми квадратів об’єктивного і суб’єктивного ризиків.

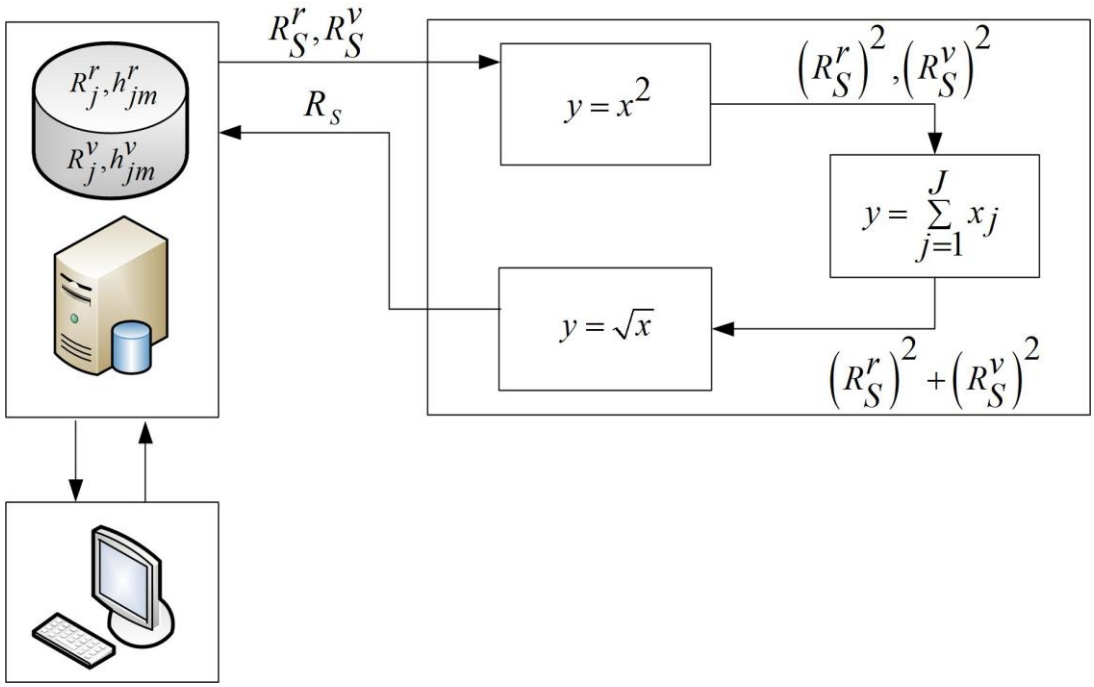


Рис. 5.10. Структурно-аналітичне відображення обчислювальної системи «Калькулятор комплексного ризику»

При цьому, модуль комплексного ризику визначає дійсну характеристику повного (комплексного) ризику, а аргумент комплексного ризику являється показником превалювання однієї складової ризику над іншою.

Проміжні та кінцеві результати розрахунків зберігають у блоці пам’яті 2 та виводять у цифровому та/або графічному вигляді на модуль виведення та візуалізації інформації 8.

Таким чином, запропонований апаратно-програмний комплекс розрахунку комплексного ризику має розширені функціональні можливості в частині забезпечення автоматизованого розрахунку і дозволяє здійснювати автоматизований розрахунок повного ризику, з урахуванням об’єктивної та

суб’єктивної його складових, з використанням теорії векторної алгебри та комплексних чисел, і може бути використаний як частина системи підтримки прийняття рішень.

5.4. Висновки до п’ятого розділу

1. Розроблено методологію оцінки ризику кібербезпеки інформаційних систем 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 інформаційних систем об’єктів критичної інфраструктури.

2. Запропоновано структурні рішення обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури, які, за рахунок використання розроблених методів та методології, дозволяють розробити засоби для розрахунку суми ризиків та обчислення комплексного ризику з урахуванням об’єктивної та суб’єктивної складових.

Основні результати дисертаційної роботи, представлені в розділі 5, опубліковані в працях автора [1, 2, 5, 6, 7, 18].

Список використаних джерел до п’ятого розділу

1. Гончар С.Ф. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури / Мохор В.В., Дибач О.М. // Ядерна та радіаційна безпека. – 2019. – №2(82). – С.57-61.

2. Пат. № 136947 України, МПК G06Q 90/00, G06F 17/00. Апаратно-програмний комплекс оцінки та аналізу ризику / Мохор В.В., Гончар С.Ф., Бакалінський О.О.; заявник та патентовласник ІПМЕ ім. Г.Є. Пухова НАН України. - № u201908305; заявл. 16.07.2019; опубл. 10.09.2019, Бюл. № 12.

3. Патент RU 182 968 U1; G06Q 10/06 (2012.01), G06F 17/00 (2006.01); Устройство для автоматизированной экспертной оценки факторов риска

проекта / Молоканов Г. Г. (RU), Ролдугин В. Д. (RU), Казарин В. Е. (RU), Залесков А. С. (RU). - Автономная некоммерческая организация "Научно-инновационный центр ракетно-космических технологий" (RU). - Заяв. 2018117169, 08.05.2018. - Опубл. 06.09.2018, Бюл. № 25.

4. Заявка JP2018142284 (A); G06F17/30, G06Q10/06; Risk calculation device, risk determination device mounted with risk calculation device and risk calculation method / Inventor(s): Katayama Shoko; Terauchi Atsushi; Applicant(s): Nippon Telegraph & Telephone. – заявл. 28.02.2017.

5. Пат. № 135456 України, МПК G06Q 90/00, G06F 17/00. Апаратно-програмний комплекс розрахунку сумарного ризику / Мохор В.В., Гончар С.Ф., Бакалінський О.О., заявник та патентовласник ІПМЕ ім. Г.Є. Пухова НАН України. - №u201903831; заявл. 15.04.2019; опубл. 25.06.2019, Бюл. № 12.

6. Пат. № 136949 України, МПК G06Q 90/00, G06F 17/00. Апаратно-програмний комплекс візуалізації ризиків / Мохор В.В., Бакалінський О.О., Гончар С.Ф.; заявник та патентовласник ІПМЕ ім. Г.Є. Пухова НАН України. - № u201908431; заявл. 17.07.2019; опубл. 10.09.2019, Бюл. № 12.

7. Гончар С.Ф., Мохор В.В., Комаров М.Ю. Спосіб виявлення кібернетичних атак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури : пат. 132581 Україна : МПК H04W 12/08, G06F 21/55. № u201813077; заявл. 29.12.2018; опубл. 25.02.2019, Бюл. №4.

8. Патент US 5796642 A від 18.08.1998 р.

9. Патент RU 2285287; Способ защиты информационно-вычислительных сетей от компьютерных атак / О.Е. Куликов, В.А. Липатніков, Р.В. Максимов, О.А. Можаєв, заявл. 04.04.2005.

10. Патент UA 110330; G06F 12/14 (2006.01). Спосіб запобігання комп'ютерним атакам у мережі за допомогою фільтрації вхідних пакетів / І.А. Жуков, С.В. Балакін //; заявл. 09.03.2016; № u201602196; опубл. 10.10.2016, Бюл. № 19.

11. Патент RU 2179738 C2; G06F 12/14, G06F 11/00; Способ обнаружения удаленных атак в компьютерной сети / И.О. Вильчевский, В.С. Заборовский, В.Е. Клавдиев, В.А. Лопота, А.В. Маленкова // від 24.04.2002 р.

12. Патент UA 9182; G06F 12/14; Спосіб виявлення віддалених атак на інформаційну систему / С.А. Криштоп, М.Ф. Логвиненко, В.Я. Пєвнєв, О.А., Серков, Г.Л. Чурюмов // заявл. 10.02.2005, № u200501204; опубл. 15.09.2005, Бюл. 55 № 9.

13. Безруков, Н. Н. Компьютерные вирусы / Н.Н. Безруков. – Москва : Наука, 2000. – 345 с.

14. Кораблев Н.М. Модель эвристического анализатора вредоносных программ на основе искусственной иммунной сети / Н.М. Кораблев, М.В. Кушнарев // Системи обробки інформації: зб. наук. праць. – 2013. – Вип. 8 (115). – С. 216-222.

15. Новиков Е.А. Сравнительный анализ методов обнаружения вторжений / Е.А. Новиков, А.А. Краснопевцев // Безопасность информационных технологий. – 2012. – № 1. – С. 47-50.

16. Патент RU 182 968 U1; G06Q 10/06 (2012.01), G06F 17/00 (2006.01); Устройство для автоматизированной экспертной оценки факторов риска проекта / Молоканов Г. Г. (RU), Ролдугин В. Д. (RU), Казарин В. Е. (RU), Залесков А. С. (RU). - Автономная некоммерческая организация "Научно-инновационный центр ракетно-космических технологий" (RU). - Заяв. 2018117169, 08.05.2018. - Опубл. 06.09.2018, Бюл. № 25.

17. Заявка JP2018142284 (A); G06F17/30, G06Q10/06; Risk calculation device, risk determination device mounted with risk calculation device and risk calculation method / Inventor(s): Katayama Shoko; Terauchi Atsushi; Applicant(s): Nippon Telegraph & Telephone. – заявл. 28.02.2017.

18. Пат. № 136792 України, МПК G06Q 90/00, G06F 17/00. Апаратно-програмний комплекс розрахунку комплексного ризику / Мохор В.В., Гончар С.Ф., Бакалінський О.О.; заявник та патентовласник ІПМЕ ім. Г.Є. Пухова НАН України. - № u201906995; заявл. 24.06.2019; опубл. 27.08.2019, Бюл. №

12.

19. Патент RU 182 968 U1; G06Q 10/06 (2012.01), G06F 17/00 (2006.01); Устройство для автоматизированной экспертной оценки факторов риска проекта / Молоканов Г. Г. (RU), Ролдугин В. Д. (RU), Казарин В. Е. (RU), Залесков А. С. (RU). - Автономная некоммерческая организация "Научно-инновационный центр ракетно-космических технологий" (RU). - Заяв. 2018117169, 08.05.2018. - Опубл. 06.09.2018, Бюл. № 25.

20. Заявка JP2018142284 (A); G06F17/30, G06Q10/06; Risk calculation device, risk determination device mounted with risk calculation device and risk calculation method / Inventor(s): Katayama Shoko; Terauchi Atsushi; Applicant(s): Nippon Telegraph & Telephone. – заявл. 28.02.2017.

РОЗДІЛ 6
ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ СИСТЕМ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

6.1. Розробка алгоритмів та програмного застосунку обчислення сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури

На базі запропонованої методології та структурного рішення обчислювальної системи розроблено алгоритмічне забезпечення для реалізації відповідного програмного забезпечення і на їх основі розроблено прикладні програмний застосунок, що реалізує запропоновані у даній дисертаційній роботі методи.

На підставі аналітичного методу максимальних наслідків розробляємо алгоритм обчислення сумарного ризику. Схему алгоритму представлено на рис. 6.1.

Представлений алгоритм передбачає введення початкових даних, які характеризують ризики: ймовірність реалізації та збитки від їх реалізації. На наступному етапі розраховуються значення ризиків, як добуток ймовірності реалізації та збитків від їх реалізації. Далі обчислюються значення ймовірності виникнення подій, що призводять до максимальних наслідків, після чого розраховується значення ймовірність виникнення сумарних максимальних наслідків і власне самі максимальні наслідки дії суми ризиків. На наступному етапі здійснюється обчислення значення ймовірності виникнення події, що призводить до сумарного ризику і, далі, розрахунок власне величини сумарного ризику. У разі необхідності розраховуються значення збитків, які можуть мати місце при сумарному ризику. Виведення результатів обчислень здійснюється у числовому вигляді і у графічному.

Результат у графічному вигляді дає можливість наочної візуалізації розрахунків.

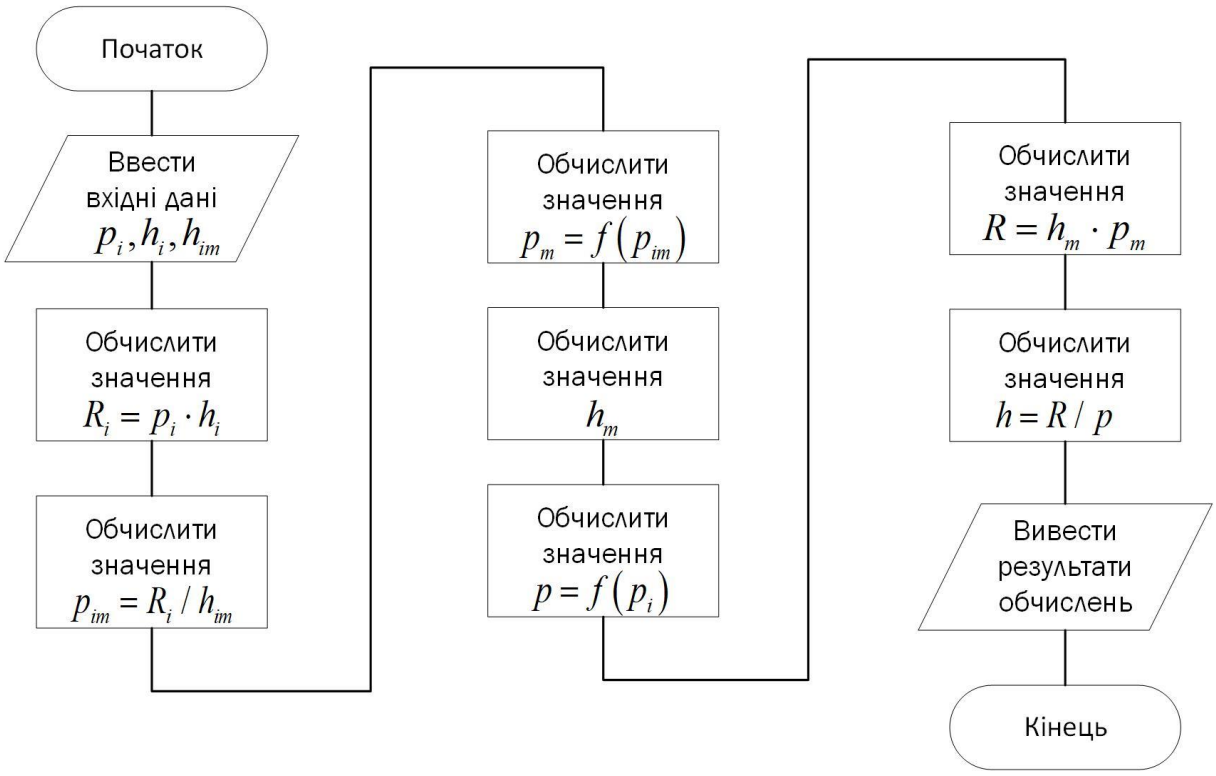


Рис. 6.1. Схема алгоритму обчислення сумарного ризику

На підставі методу обчислення комплексного ризику розробляємо алгоритм обчислення комплексного ризику. Схему алгоритму представлено на рис. 6.2.

Представлений алгоритм передбачає введення вхідних даних, якими являються значення об’єктивного та суб’єктивного ризиків. На наступному етапі здійснюється обчислення квадрату значень об’єктивного ризику а далі суб’єктивного ризику. Після цього визначається сума квадратів значень об’єктивного та суб’єктивного ризиків. Наступним етапом визначається квадратний корінь із отриманого на попередньому кроці значення і візуалізація результатів розрахунків. Виведення результатів обчислень здійснюється у числовому вигляді.

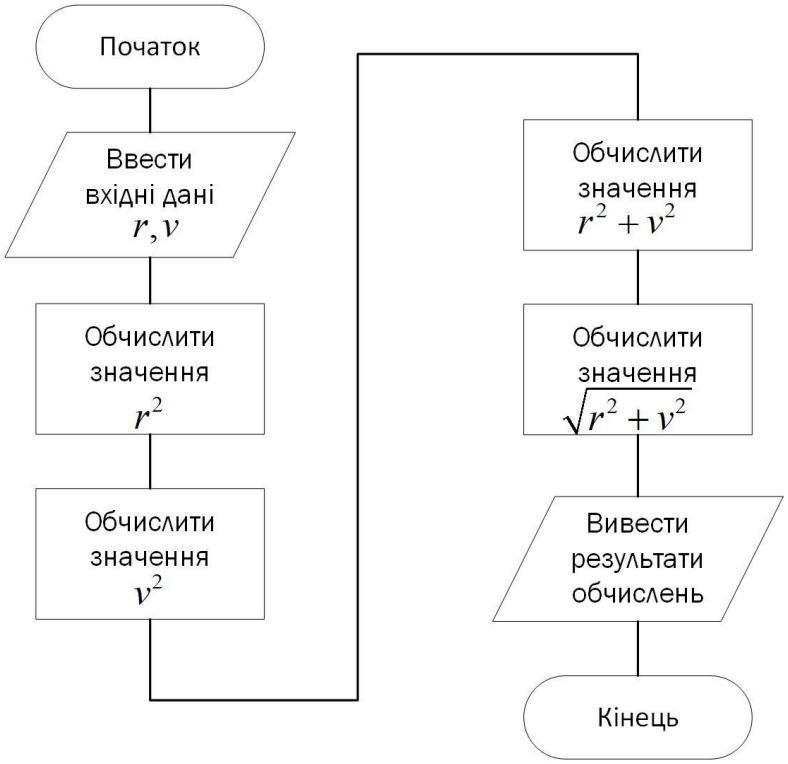


Рис. 6.2. Схема алгоритму обчислення комплексного ризику

На базі представлених алгоритмів розроблено програмний застосунок запропонованих у даній дисертаційній роботі методів.

Оскільки написання програми розрахунку не містить специфічних вимог, то зазначена програма була написана на об'єктно-орієнтованій мові програмування C#, яка має зручний інтерфейс розробника, більш ніж достатні можливості для вирішення даної задачі. Розроблений програмний застосунок займає близько 20 кбайт дискового простору.

Інтерфейс програмної системи розрахунку суми ризиків, наслідків від цих ризиків, ймовірності настання цих наслідків, представлена на рис. 6.3.

Введення вхідних даних здійснюється в правому блоці інтерфейсного вікна програми у віконці «Додати ризик». Вхідними даними при цьому являються характеристики ризиків, які є об'єктами обчислення, а саме ймовірність реалізації, збитки та максимальні збитки у разі їх реалізації. Вхідні дані формуються методом експертних оцінок. При цьому, ймовірність визначається у діапазоні від 0 до 1, а збитки можуть виражатися у відносних

одиницях, відносно максимального значення. Натискаючи кнопку «Додати ризик» можливо вводити параметри необхідної кількості ризиків. Після завершення введення вхідних даних, після натискання внизу справа інтерфейсного вікна програми кнопки «Розрахунок», справа внизу у віконці «Результати розрахунків» появляться результати розрахунку.

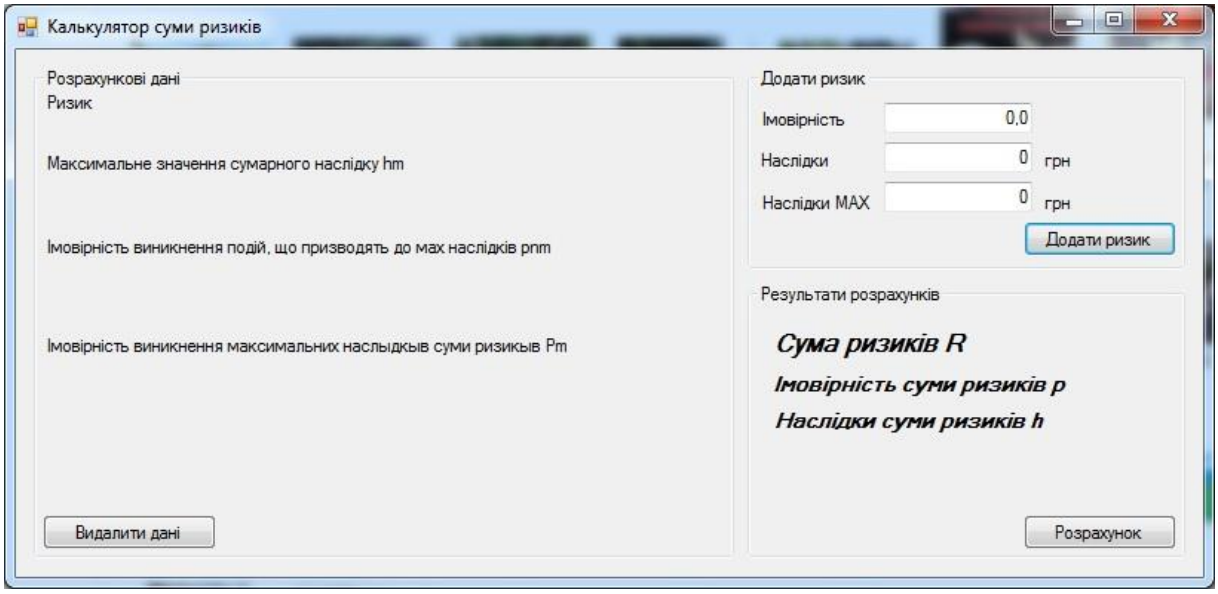


Рис. 6.3. Інтерфейс програми

Лістинг (коди) програмного застосунку приведено у додатку Б дисертаційної роботи.

6.2. Дослідження систем розрахунку сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури

Експериментальні дослідження розробленого програмного застосунку здійснювалися з метою перевірки адекватності реагування розроблених моделей та методів відносно тих чи інших ініціалізуючих величин шляхом практичного використання.

Практичне застосування програмного застосунку проводилось при створенні комплексної системи захисту інформації атомних електростанцій

та інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест» [1, 2].

Приведемо більш детально практичне застосування програмного застосунку при створенні комплексної системи захисту інформації а інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест».

У ході проведення обстеження середовища функціонування інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест» було досліджено об’єкти захисту, потенційні загрози інформації, розроблено модель порушника та модель загроз для інформації даної інформаційно-телекомунікаційної системи.

ЗВІД-ФАРЛЕП призначений для надання органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним та фізичним особам (далі – споживачам) послуг зв’язку, послуг захищеного доступу до ресурсів та сервісів мережі Інтернет – [PAI].

Розглянемо загальну структуру ЗВІД-ФАРЛЕП. Функціональна схема ЗВІД-ФАРЛЕП складається з наступних елементів (рис. 6.4):

Пристрої мережевого захисту:

- система моніторингу та реєстрації аварій в Магістральній мережі (HP OpenView);

- програмний DDoS аналізатор;

Комутаційне обладнання:

- LSR-маршрутизатор Cisco 7600 (з інтегрованими функціями міжмережевого екрану);

- EDGE 3 - маршрутизатор Cisco 7600 (з інтегрованими функціями міжмережевого екрану);

- ядро комутації (core 0) на базі Cisco 7600;

- ядро комутації (core 1) на базі Cisco 7206;

- комутатори агрегації Cisco 3750G (6 шт.);

- комутатор Cisco 3750E;

- комутатор Cisco 4500X;

Серверне обладнання:

- DNS-сервери (ОС FreeBSD 10.1).

АРМ адміністраторів:

- Адміністратор безпеки: ПЕОМ на базі cpu Intel Core 2 duo 2,66, mem 8Gb, hdd 2000Gb (ОС Windows 10 Enterprise 2016 LTSB);

- Системний адміністратор: ПЕОМ на базі Cpu Intel core 2 quad 3.0, mem 8Gb, hdd 500Gb (ОС Windows 7 Enterprise SP1).

Антивірусне програмне забезпечення - “FortiGuard Security Services”.

Склад програмного та апаратного забезпечення детально наведено в документі «Паспорт-формуляр».

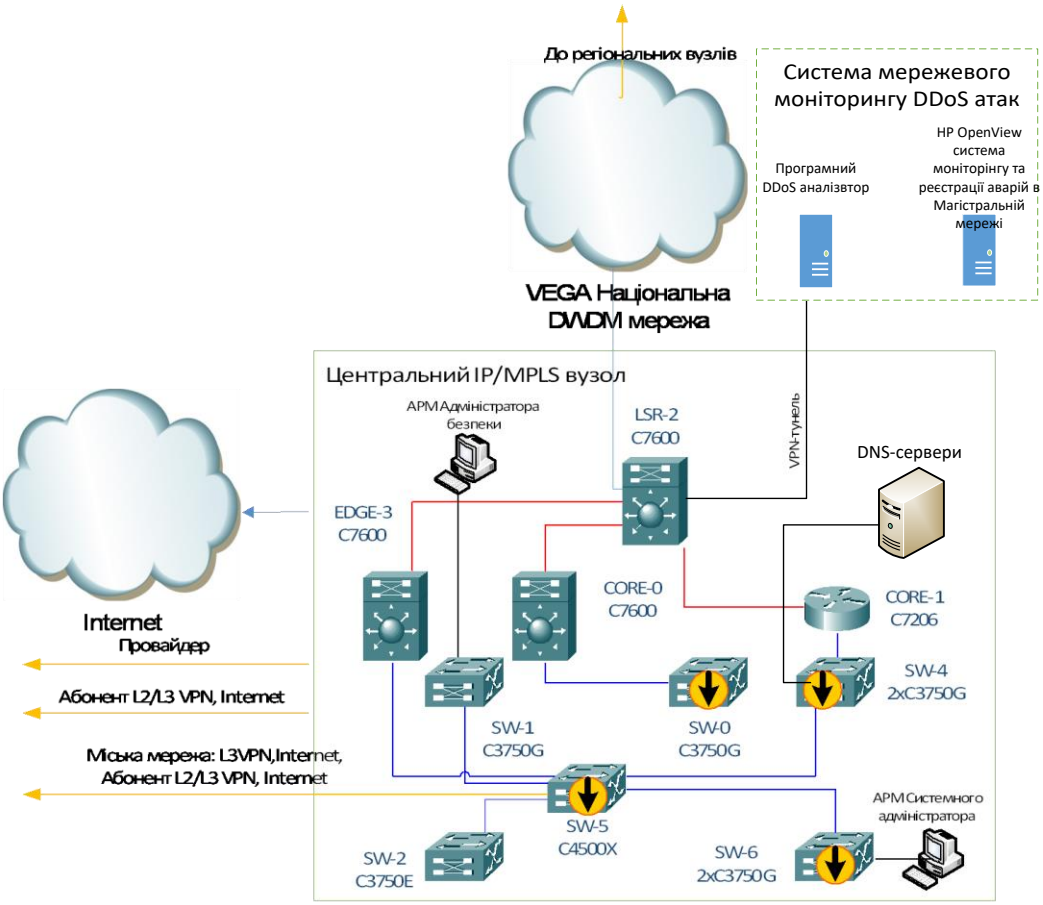


Рис. 6.4. Функціональна схема ЗВІД-ФАРЛЕП

Вимоги до робочих станцій фізичних і юридичних осіб, які є користувачами загальнодоступної інформації WEB-сторінки, та їхнього ПЗ не висуваються.

Розглянемо режими функціонування ЗВІД-ФАРЛЕП. Функціонування ЗВІД-ФАРЛЕП передбачає декілька режимів:

- основний робочий режим – в цьому режимі КЗЗ у повний мірі виконує свої функції щодо забезпеченню виконання послуг безпеки;
- аварійний режим роботи – стан аварійного призупинення роботи ОС, під час якого зупиняється більшість процесів, що виконувались у режимі функціонування. Надалі ОС переходить у режим роботи одного користувача та очікує відповідні дії від адміністратора щодо відновлення системи після збоїв. При цьому, здійснюється запис у системний журнал щодо факту переходу до режиму роботи одного користувача. Повернення до робочого стану ОС можливе тільки після вводу паролю адміністратора та усунення причини збою;
- режим технічного обслуговування – стан технічного обслуговування (або адміністрування) передбачають такі стадії: налаштовування КЗЗ, дії в аварійних ситуаціях, налаштовування та вибіркове відновлення певних пакетів або інсталяція ОС. Інсталяція, налаштування КЗЗ та ручне відновлення пошкодженої системи виконується системним адміністратором у присутності адміністратора безпеки. Дії щодо інсталяції, відновлення та конфігурації КЗЗ описані в інструкції адміністратора.

Здійснимо опис послуги, що надається через ЗВІД-ФАРЛЕП. Послуга РАІ (захищений доступу споживача до ресурсів та сервісів мережі Інтернет) надається в частині передачі даних між ресурсами мережі Інтернет (загальнодоступна інформація WEB-сторінок, HTLM-документ тощо) і користувачами ЗВІД-ФАРЛЕП.

Послуга РАІ передбачає:

Права адміністратора ЗВІД-ФАРЛЕП керувати потоками інформації від ресурсів мережі Інтернет через ЗВІД-ФАРЛЕП до його користувачів (згідно з

політикою адміністративної конфіденційності присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію).

Розглянемо характеристики інформації, що обробляється в ЗВІД-ФАРЛЕП. Відповідно до функціонального призначення в ЗВІД-ФАРЛЕП передбачається обробка та зберігання інформації, яка за своїм функціональним призначенням може бути віднесена до наступних видів:

1) відкрита інформація;

2) технологічна інформація.

До відкритої інформації відноситься інформація, вимоги до захисту якої висуваються у частині цілісності та доступності, зокрема:

- програмне забезпечення ЕОМ (у вигляді файлів) – операційні системи, прикладне програмне забезпечення, антивірусне програмне забезпечення;
- транзитна інформація, що передається між мережею клієнта та мережею Інтернет через засоби ЗВІД.

До технологічної інформації ЗВІД-ФАРЛЕП відноситься технологічна інформація КСЗІ та технологічна інформація щодо адміністрування та управління обчислювальною системою і засобами обробки інформації – дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів, інформація журналів реєстрації дій користувачів, інша інформація КЗЗ, встановлені робочі параметри окремих механізмів або засобів захисту, інформація про профілі обладнання та режими його функціонування, робочі параметри функціонального ПЗ тощо.

Технологічна інформація призначена для використання тільки уповноваженими адміністраторами і технічним обслуговуючим персоналом, що забезпечує функціонування системи. Вимоги до захисту технологічної інформації висуваються в частині забезпечення її конфіденційності, цілісності та доступності.

За рівнем доступу технологічна інформація відноситься до конфіденційної.

В разі появи в межах технологічного циклу ЗВІД-ФАРЛЕП інформації інших категорій доступу, що передбачають відмінні від викладених в даному ТЗ вимоги до забезпечення її захисту, зміни та доповнення до ТЗ на КСЗІ ЗВІД-ФАРЛЕП вносяться в порядку, передбаченому розділом 8 даного ТЗ.

Розглянемо вимоги до ролей користувачів ЗВІД-ФАРЛЕП. Щодо повноважень та прав доступу до інформації, що зберігається та циркулює в ЗВІД-ФАРЛЕП, визначаються наступні ролі користувачів:

Адміністратори – технічний персонал, який забезпечує функціонування ЗВІД-ФАРЛЕП:

1. Адміністратор безпеки (Ad1) – обслуговуючий персонал, який виконує наступні обов’язки:

- здійснює загальний контроль за станом безпеки в ЗВІД-ФАРЛЕП;
- контролює відповідність налаштувань програмних та технічних засобів прийнятій політиці безпеки;
- здійснює реєстрацію нових користувачів та видалення старих користувачів в/із ЗВІД-ФАРЛЕП;
- здійснює призначення атрибутів доступу користувачів та об’єктів захисту;
- надає користувачам права доступу до об’єктів захисту;
- здійснює аудит подій щодо автентифікації і авторизації користувачів в ЗВІД-ФАРЛЕП, доступу до об’єктів захисту, а також оброблення та аналіз зареєстрованої інформації про критичні з погляду безпеки події.

2. Системний адміністратор ЗВІД-ФАРЛЕП (Ad2) – обслуговуючий персонал, який виконує наступні обов’язки:

- забезпечує працездатність компонентів ЗВІД-ФАРЛЕП в цілому;
- проводить налаштування апаратного і програмного забезпечення ЗВІД-ФАРЛЕП;

- здійснює технічне обслуговування апаратного і програмного забезпечення ЗВІД-ФАРЛЕП;
- проводить резервування та відновлення працездатності ЗВІД-ФАРЛЕП;
- здійснює аналіз журналів реєстрації подій;
- проводить моніторинг стану ЗВІД-ФАРЛЕП.

3. Фахівці організацій, які підтримуються ЗВІД-ФАРЛЕП (Ad3) - користувачі з функціональними обов'язками адміністраторів мережевого обладнання, адміністраторів ресурсів DNS (Domain Name System), PROXY, FTP (File Transfer Protocol), адміністраторів-постачальників ПЗ, користувачів сторонніх організацій, що підтримують справне та безвідмовне функціонування основного та допоміжного обладнання ІТС, тощо.

4. Користувачі, яким надано право доступу тільки до загальнодоступної інформації WEB-сайтів (Us).

Зазначені категорії осіб повинні мати дозвіл на доступ до відомостей, які містяться в програмній і технічній документації на ЗВІД-ФАРЛЕП або окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

Вимоги до користувачів, яким надається право доступу до загальнодоступної інформації WEB-сторінки, не висуваються.

Користувачі загальнодоступної інформації одержують доступ до WEB-сторінки у відповідності до діючих у мережі Інтернет правил та регламенту.

Дослідимо об'єкти захисту інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест».

В КСЗІ ЗВІД-ФАРЛЕП виділяються наступні інформаційні об'єкти, що підлягають захисту:

ОЗ.1 Об'єкти, що містять робочі дані.

Об'єкти, що містять відкриту інформацію представлені у вигляді:

- сильно-зв'язних об'єктів баз даних (таблиці, записи, поля бази даних, які містять інформацію, що підлягає захисту);

• окремих об’єктів файлової системи різних форматів (файли, логічні пристрої, каталоги).

Об’єкти відносяться до наступних компонентів ЗВІД-ФАРЛЕП:

• серверів (об’єкти ЗВІД-ФАРЛЕП введено у відповідності до розділу 5.3.1: (О1.2, О1.3);

• робочих станцій (О3.1.2, О3.2.2).

О3.2 Об’єкти, що містяться у IP-пакетах транзитних потоків

Об’єкти, що містять відкриту та технологічну інформацію представлені у вигляді:

• пакетів протоколів стеку TCP\IP, що містять дані, що підлягають захисту

Об’єкти відносяться до наступних компонентів ЗВІД-ФАРЛЕП:

• комутаторів (О2.1.5);

• маршрутизатору (О2.2.5)

• міжмережевих екранів (О2.3.5).

О3.3 Об’єкти, що містять виконуваний код програмного забезпечення ЗВІД-ФАРЛЕП (ПЗ прикладних систем ЗВІД-ФАРЛЕП, ОС тощо) .

Виконуваний код, що підлягає захисту:

• ОС серверів ЗВІД-ФАРЛЕП (О1.1);

• ПЗ активного мережевого обладнання та засобів мережевого захисту:

- комутаторів (О2.1.1);
- маршрутизаторів (О2.2.1)
- міжмережевих екранів (О2.3.1);

• ПЗ робочих станцій (О3.1.1, О3.2.1).

О3.4 Об’єкти, що містять конфігураційні налаштування ПЗ та обладнання компонентів ЗВІД-ФАРЛЕП і засобів захисту.

Об’єкти, що містять технологічну інформацію представлені у вигляді файлів конфігурацій:

• ОС серверів ЗВІД-ФАРЛЕП (О1.5);

• ПЗ активного мережевого обладнання та засобів мережевого захисту:

- комутаторів (О2.1.2);
- маршрутизаторів (О2.2.2)
- міжмережевих екранів (О2.3.2).

• ПЗ робочих станцій (О3.1.3, О3.2.3).

О3.5 Об’єкти, що містять атрибути доступу користувачів і адміністраторів ЗВІД-ФАРЛЕП і визначають їх права в системі.

Об’єкти, що містять технологічну інформацію представлені у таких компонентах:

• ОС серверів ЗВІД-ФАРЛЕП (О1.4);

• активному мережевому обладнанні та засобах мережевого захисту:

- комутаторів (О2.1.3);
- маршрутизаторів (О2.2.3)
- міжмережевих екранів (О2.3.3).

• ОС робочих станцій (О3.1.3, О3.2.3).

О3.6 Об’єкти, що містять дані журналів функціонування компонентів ЗВІД-ФАРЛЕП.

Об’єкти, що містять технологічну інформацію представлені у вигляді файлів журналів:

- ОС серверів ЗВІД-ФАРЛЕП(О1.6);
- активного мережевого обладнання та засобів мережевого захисту:
  - комутаторів (О2.1.4);
  - маршрутизаторів (О2.2.4)
  - міжмережевих екранів (О2.3.4).
- ОС робочих станцій (О3.1.5, О3.2.5).

З огляду на сферу можливої дії, а також причини виникнення, загрози інформації ЗВІД-ФАРЛЕП доцільно розбити на наступні класи:

1) природні загрози;

2) відмови та збої (ненавмисні техногенні загрози);

3) мережеві загрози;

4) загрози прикладного ПЗ;

5) загрози ОС.

Дослідимо потенційні загрози інформації інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест».

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) [3, 4] за результатом впливу на інформацію та систему її обробки загрози поділяються на чотири класи:

1. Порушення конфіденційності інформації (отримання доступу до інформації з обмеженим доступом);

2. Порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав'язування хибної інформації);

3. Порушення доступності інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації);

4. Втрата спостереженості або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

В КСЗІ ЗВІД-ФАРЛЕП висуваються вимоги щодо забезпечення конфіденційності, цілісності, доступності технологічної інформації та забезпечення цілісності та доступності відкритої інформації.

Розробимо модель порушника інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест».

За локалізацією джерела, загрози поділяються на внутрішні та зовнішні. До зовнішніх відносяться загрози, джерело яких знаходиться поза межами ЗВІД-ФАРЛЕП. Внутрішні загрози реалізуються в межах контрольованої зони, в приміщеннях, де розташовані засоби обробки та

збереження інформації ЗВІД-ФАРЛЕП. Відповідно до цього розрізняються два види порушників: зовнішній та внутрішній.

1. Зовнішній порушник (ЗП) – це порушник, що діє із зовнішнього, відносно ЗВІД-ФАРЛЕП, боку. У цій моделі розглядається як особа, що не має доступу до приміщень, у яких розташовані засоби обчислювальної техніки, і не є авторизованим користувачем. Зовнішній порушник має можливість реалізувати загрозу інформації тільки впливаючи на інформацію з боку інших автоматизованих систем (що не входять до складу ЗВІД-ФАРЛЕП).

Категорії осіб, які можуть бути зовнішніми порушниками:

- сторонні особи, що знаходяться за межами контрольованої території ЗВІД-ФАРЛЕП;

- відвідувачі;

- представники організацій, що взаємодіють з питань обслуговування ЗВІД-ФАРЛЕП та підтримки його функціональності.

2. Внутрішній порушник (ВП) – це порушник, що діє зсередини ЗВІД-ФАРЛЕП. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки ЗВІД-ФАРЛЕП. Внутрішній порушник має можливість реалізувати загрозу інформації, й може бути як авторизованим користувачем, так і не авторизованим.

Внутрішнім порушником може бути особа з наступних категорій персоналу організації:

- технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЗВІД-ФАРЛЕП (Тр 1);

- користувачі ЗВІД-ФАРЛЕП;

- адміністратор безпеки;

- системний адміністратор ЗВІД-ФАРЛЕП;

- представники організацій, що взаємодіють з питань технічного забезпечення;

- фахівці організацій, що підтримуються ЗВІД-ФАРЛЕП.

Модель загальних загроз інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест» приведені в На підставі отриманих у табл. 6.1 – 6.4 даних (додатки В - Е), проведемо аналіз ризиків інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу ПрАТ «Фарлеп-Інвест».

У табл. 6.5 наведені профілі можливостей потенційного порушника, визначені у документі «ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технологій. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій» [5]. Розрахунок ефективного рівня загроз здійснюється за формулами, наведеними у тому ж документі.

Таблиця 6.5

Профілі можливостей порушника та величина ефективного рівня загроз

Позначення	Визначення категорії	Потенційний рівень загрози (T_{pot})	Характер дій порушника						Ефективний рівень загроз (T_{ef})
			Мотив порушення ($М_i$), *i*	Мета порушення ($Ц_i$), *i*	Кваліфікація ($К_i$), *i*	Можливості ($П_i$), *i*	Час дії ($Ч_i$), *i*	Місце дії ($Д_i$), *i*	
1	2	3	4	5	6	7	8	9	10
	Внутрішні по відношенню до ЗВІД-ФАРЛЕП								
ПВ1	Персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЗВІД-ФАРЛЕП, технічні засоби (інженери, техніки) (Тр1)	2	1	1,3	3	1, 2	1, 2	4–6	2,06

Продовження таблиці 6.5

ПВ2	користувачі, яким надано право доступу тільки до загальнодоступної інформації WEB-сайтів (Us)	2	1, 3	1, 3	1-3	1-4	3	4	2.19
ПВ3	Адміністратор безпеки (Ad1)	4	1	1	4	3	4	6	3.33
ПВ4	Системні адміністратори ЗВІД-ФАРЛЕП (Ad2)	4	1	1	4	3	4	5, 6	3.33
ПВ5	Фахівці організацій, що підтримуються ЗВІД-ФАРЛЕП (Ad3)	4	1, 3	1, 3	4	2-5	4	1-6	3.37
	Зовнішні по відношенню до ЗВІД-ФАРЛЕП								
ПЗ1	Сторонні особи, що знаходяться за межами контрольованої території вузлів ЗВІД-ФАРЛЕП	1	2, 3	2, 4	1–4	1	4	1	1.64
ПЗ2	Відвідувачі	2	3	2, 3	1–4	1, 3	4	2, 3	2.27
ПЗ3	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і т.і.)	2	1, 3	1	1	1	1, 2	2, 3	1.67
ПЗ4	Представники організацій, що взаємодіють з питань обслуговування ЗВІД-ФАРЛЕП та підтримки його функціональності	3	1, 3	1-3	3–6	1 – 5	1,4	3-6	2.82

В таблиці 6.6 представлені значення ризику для загроз ЗВІД-ФАРЛЕП.

Таблиця 6.6

Оцінка ризику

Ідентифікатор загрози	Назва загрози	Ймовірність реалізації загрози (p)	Величина збитків (h)	Значення ризику (R)
1	2	3	5	6
3.1.1	Пожежа	0.1	6.62	0.66
3.1.2	Руйнування	0.02	6.62	0.13
3.1.3	Затоплення	0.03	6.62	0.2
3.1.4	Забруднення	0.05	6.62	0.33
3.1.5	Перегрів	0.3	6.62	1.99
3.1.6	Вологість	0.2	6.62	1.32
3.1.7	Електромагнітні випромінювання	0.05	6.62	0.33
3.1.8	Поламки, відмови та збої апаратури	0.3	6.62	1.99
3.1.9	Нестача ресурсів	0.5	6.62	10.19
3.1.10	Навмисне пошкодження або крадіжка обладнання	0.2	8.86	5,23
3.1.11	Випадкове пошкодження обладнання	0.3	6.62	5,82
3.2.1	Відсутність фізичного з’єднання	0.1	8	2,32
3.2.2	Помилки та непрацездатність активного мережевого обладнання	0.2	11.29	7,34
3.2.3	Розголошення даних про мережу	0.2	3.73	2,13
3.2.4	Перехоплення (сніферінг) пакетів	0.1	3.73	1,04
3.2.5	Підміна отримувача (спуфінг пакетів)	0.1	6.62	1,85
3.2.6	Відмова в обслуговуванні (DoS)	0.2	3.32	1,46
3.2.7	Дзеркалювання трафіку	0.05	6.88	0,96
3.2.8	Непрацездатність мережевих застосувань	0.2	7,30	3,8
3.2.9	Створення альтернативних несанкціонованих точок доступу до мережі	0.5	4,5	5,67
3.3.1	Помилка, збій та відмова прикладного ПЗ	0.3	8,09	7,2
3.3.2	Виконання недоку-ментованих функцій	0.05	5,83	0,99
3.3.3	Розповсюдження вірусів та хробаків	0.5	8,86	13,64
3.3.4	Несумісність версій ПЗ	0.1	6,50	2,21
3.3.5	Перехоплення ТІЗ	0.2	3,87	1,82
3.3.6	Підміна або дезорганізація	0.05	6,5	0,84

Продовження таблиці 6.6

3.3.7	Злам	0.02	4,42	0,18
3.4.1	Помилка, збій та відмова системного ПЗ	0.3	7,97	6,77
3.4.2	Перехоплення ТІЗ	0.2	3,87	1,82
3.4.3	Пошкодження файлів ОС	0.2	6,25	3,87
3.4.4	Збирання «сміття»	0.02	2,63	0.13
3.4.5	Втручання в роботу ОС з мережі	0.2	6,47	4,01
3.5.1	Помилка користувача	0.2	10,10	5,76
3.5.2	Дезорганізація	0.05	7	1,05
3.5.3	Ненавмисне пошкодження БД	0.1	7	2,24
3.5.4	Відмова від авторства	0,2	7	1,68
3.5.5	Розголошення даних	0,3	10,10	4,75

Використовуючи запропоноване програмне забезпечення «Калькулятор ризиків» виконано обчислення суми ризиків: від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу.

В результаті роботи програмного засобу, рис. 6.5, здійснено розрахунок значення сум ризиків від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу. Також здійснено розрахунок значення наслідків при реалізації кожної з груп загроз і ймовірність виникнення цих наслідків.

Використовуючи запропоноване програмне забезпечення виконано обчислення суми ризиків: від загроз, що можуть виникнути під час мережевої взаємодії, табл. 6.7; від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, табл. 6.8; від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу «ЗВІД-ФАРЛЕП», табл. 6.9.

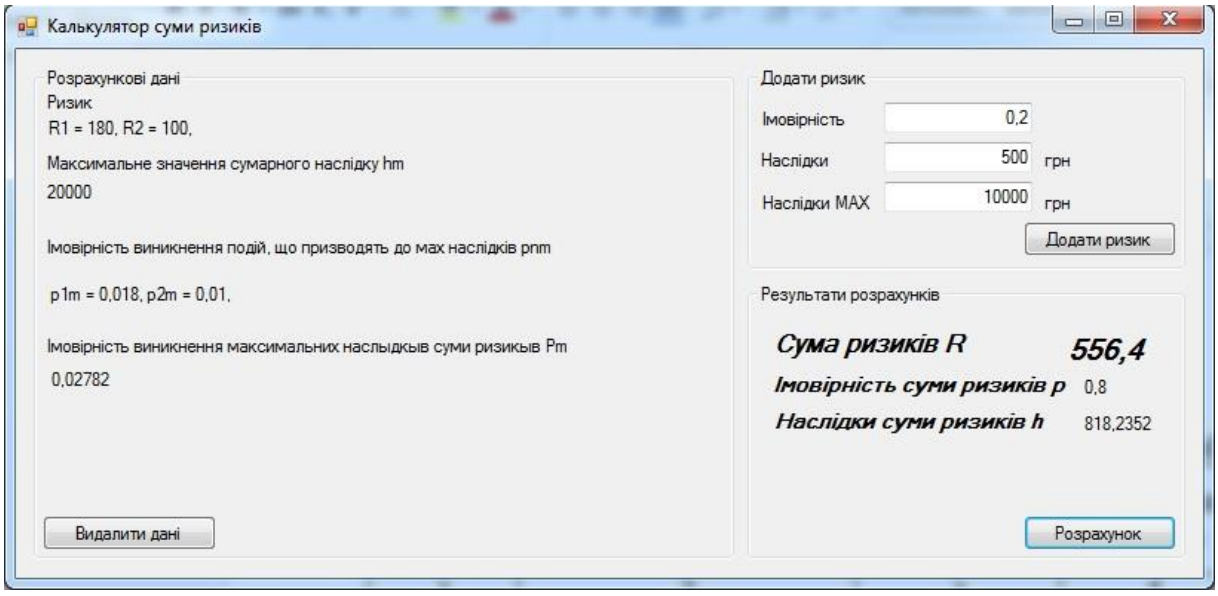


Рис. 6.5. Приклад розрахунку

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 максимально можливим збиткам. Зазначені параметри визначаються експертним шляхом.

Таблиця 6.7

Значення ризиків від загроз мережевої взаємодії

Іденти-фікатор загрози	Назва загрози	Ймовірність реалізації загрози	Величина збитків	Значення ризику
1	2	3	5	7
З.2.1	Відсутність фізичного з’єднання	0,1	8,0	0,80
З.2.2	Помилки та непрацездатність активного мережевого обладнання	0,2	9,8	1,96
З.2.3	Перехоплення (сніферінг) пакетів	0,1	3,7	0,37

Продовження таблиці 6.7

З.2.4	Відмова в обслуговуванні (DoS)	0,2	3,3	0,66
	Результати обчислення	0,48	27,80	13,34

Таблиця 6.8

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.3.1	Помилка, збій та відмова прикладного ПЗ	0,3	8,09	2,43
З.3.2	Виконання недокументованих функцій	0,05	5,83	0,29
З.3.3	Розповсюдження вірусів та хробаків	0,5	8,86	4,43
З.3.4	Несумісність версій програмного забезпечення	0,1	6,5	0,65
	Результати обчислення	0,7	35,23	24,66

Таблиця 6.9

Значення ризиків від загроз мережевих операційних систем

Іденти-фікатор загрози	Назва загрози	Ймовірність реалізації загрози	Величина збитків	Значення ризику
1	2	3	5	7
З.4.1	Помилка, збій та відмова системного програмного забезпечення	0,3	7,97	2,39
З.4.2	Перехоплення технологічної інформації	0,2	3,87	0,77
З.4.3	Пошкодження файлів операційної системи	0,2	6,25	1,25
З.4.4	Втручання в роботу операційної системи з мережі	0,2	6,47	1,29
	Результати обчислення	0,64	29,00	18,56

В графі «результати обчислення» (табл. 6.7 – табл. 6.9) відповідно приведено розраховані значення ризиків від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу «ЗВІД-ФАРЛЕП». Також приведено розраховані значення наслідків при реалізації кожної з груп загроз і ймовірність цих наслідків.

Із приведених розрахунків можна бачити, що ризик від загроз, які можуть виникнути під час мережевої взаємодії складає 13,39. При цьому, із урахуванням зазначених ймовірностей реалізації загроз складових ризиків та величин збитків при їх реалізації, сумарні збитки від реалізації даних загроз

будуть складати 27,8 з ймовірністю 0,48. Ризик від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням складає 24,68. При цьому, із урахуванням зазначених ймовірностей реалізації загроз складових ризиків та величин збитків при їх реалізації, сумарні збитки від реалізації даних загроз будуть складати 35,23 з ймовірністю 0,7. Ризик від загроз, що можуть виникнути в мережевих операційних системах складає 18,61. При цьому, із урахуванням зазначених ймовірностей реалізації загроз складових ризиків та величин збитків при їх реалізації, сумарні збитки від реалізації даних загроз будуть складати 29,0 з ймовірністю 0,64.

Використовуючи розроблені у дисертаційній роботі методи, розрахуємо ризик від усіх зазначених видів загроз, а саме: від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу «ЗВІД-ФАРЛЕП», табл. 6.10.

Таблиця 6.10

Значення ризиків від загроз

№ п/п	Вид загрози	Ймовірність реалізації	Величина збитків	Значення ризику
1	2	3	4	5
1	Загрози, що можуть виникнути під час мережевої взаємодії	0,48	27,80	13,34
2	Загрози, що можуть виникнути під час роботи з прикладним програмним забезпеченням	0,7	35,23	24,66

Продовження таблиці 6.10

3	Загрози, що можуть виникнути в мережевих операційних системах	0,64	29,0	18,56
	Результати обчислення	0,94	109,72	103,14

Після запуску програми калькулятора ризиків вводимо вхідні параметри для загроз, що можуть виникнути під час мережевої взаємодії за результатами розрахунків, приведеними в табл. 6.7. Демонстрація роботи програми розрахунку суми ризиків на цьому етапі показана на рис. 6.6.

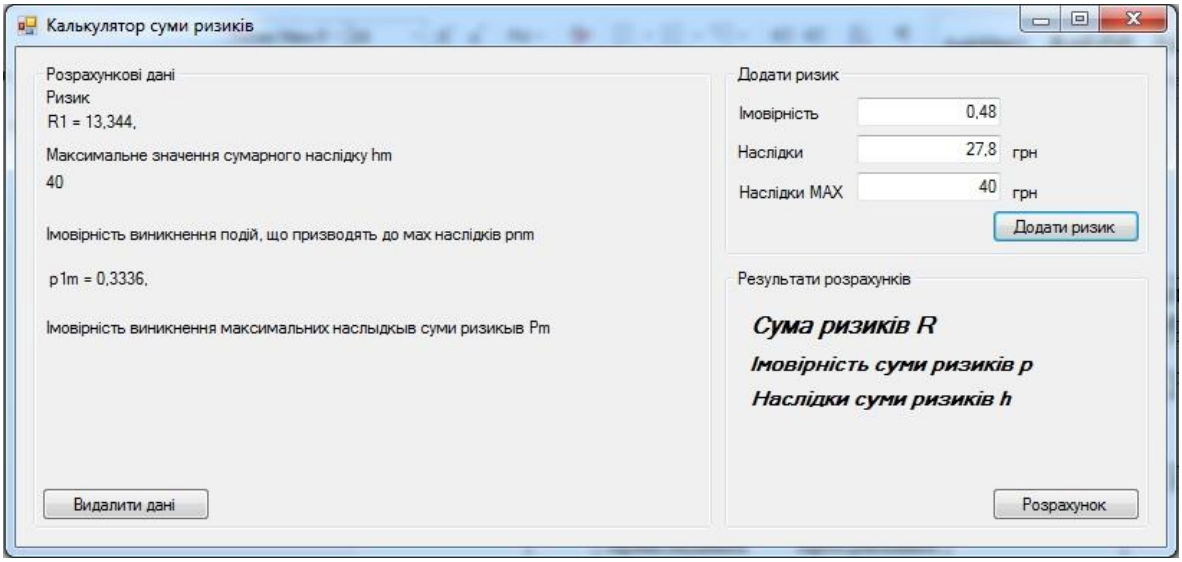


Рис. 6.6. Введення значень для першого ризику

Далі вводимо вхідні параметри для загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням за результатами розрахунків, приведеними в табл. 6.8. Демонстрація роботи програми розрахунку суми ризиків на цьому етапі показана на рис. 6.7.

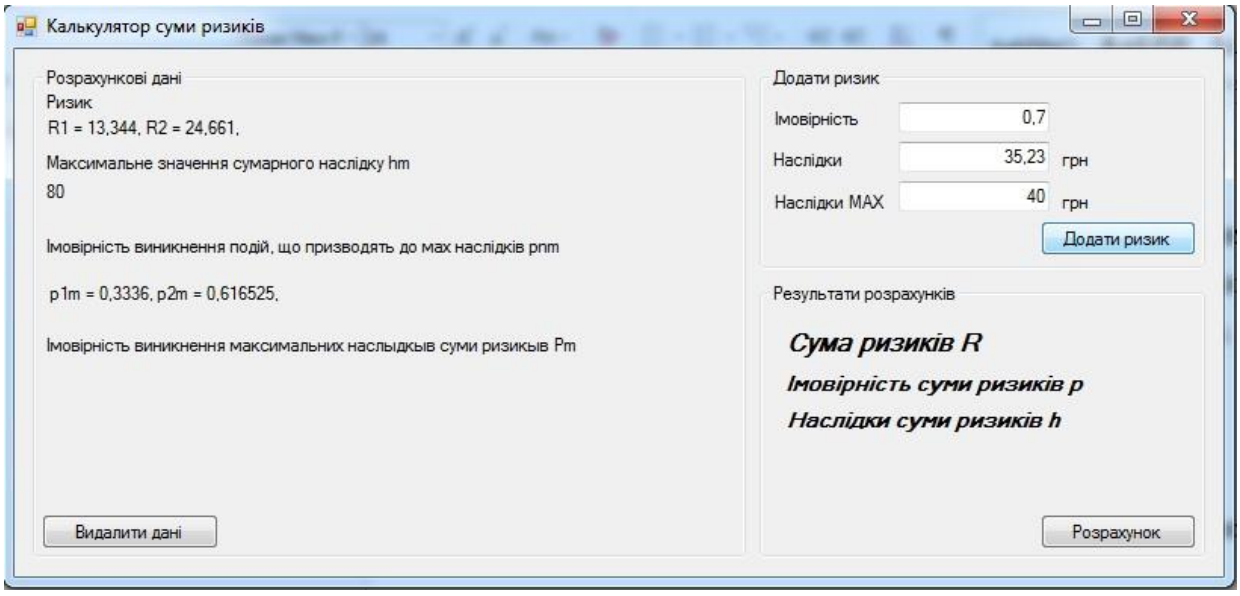


Рис. 6.7. Введення значень для другого ризику

Після цього вводимо вхідні параметри для загроз, що можуть виникнути в мережевих операційних системах за результатами розрахунків, приведеними в табл. 6.9. Демонстрація роботи програми розрахунку суми ризиків на цьому етапі показана на рис. 6.8.

Із приведених розрахунків, табл. 6.10, можна бачити, що ризик від кіберзагроз, які можуть виникнути в інформаційно-телекомунікаційній системі захищеного вузлу Інтернет доступу «ЗВІД-ФАРЛЕП» складає 103,14. При цьому, із урахуванням зазначених ймовірностей реалізації загроз складових ризиків та величин збитків при їх реалізації, сумарні збитки від реалізації даних загроз будуть складати 109,72 з ймовірністю 0,94. Аналогічно, знаючи значення ризику, можна розрахувати ймовірність виникнення будь-яких заданих збитків, які можуть бути максимально допустимими для власників інформаційної системи.

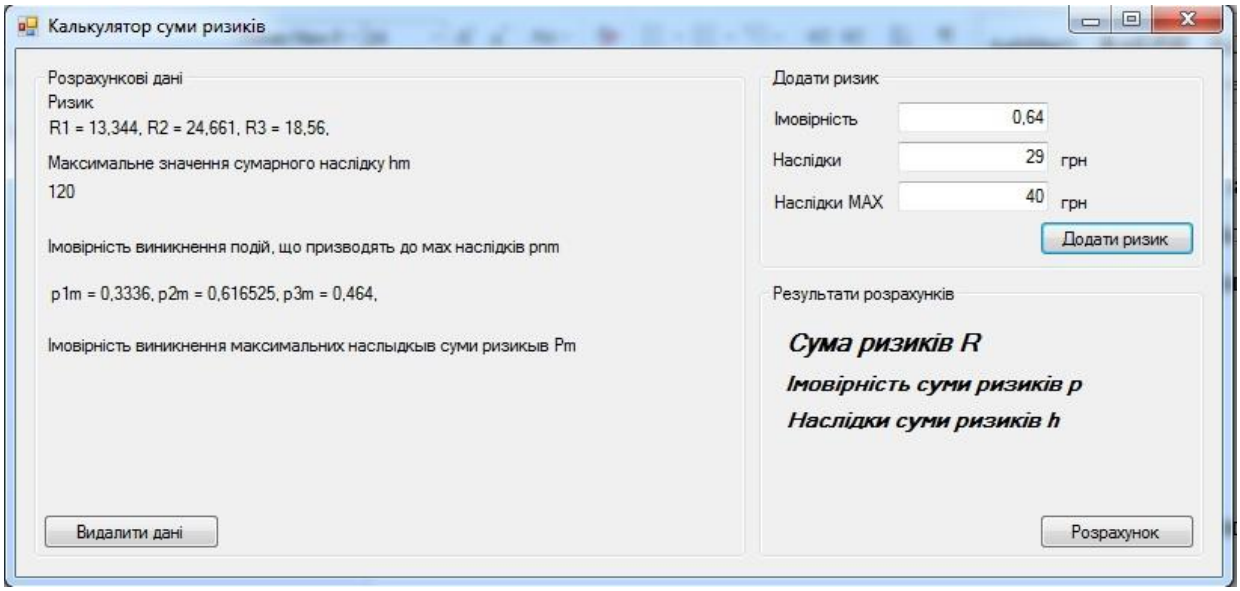
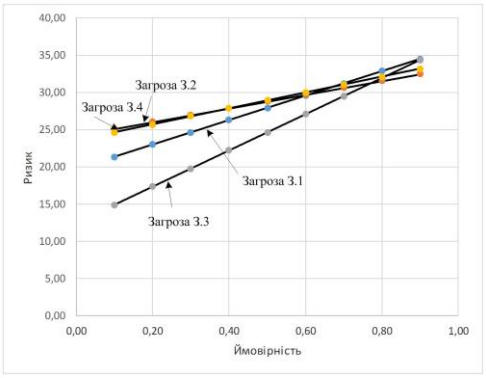
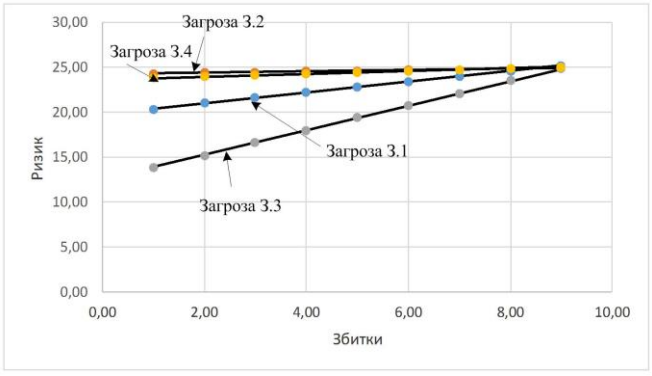


Рис. 6.8. Введення значень для третього ризику

За результатами експерименту, рис. 6.9 (а, б), видно, що система оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури «Калькулятор ризиків» адекватно реагує на зміну ініціалізуючих параметрів.



а)



б)

Рис. 6.9. Залежності ризику від ймовірності (а) та збитків (б)

Розглянемо застосування методу обчислення комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури на

прикладі оцінки ризику кібербезпеки газопроводів високого тиску, що являється об’єктом критичної інфраструктури.

У відповідності до керівних принципів кібербезпеки систем управління в галузі газопроводу [6], рекомендується створити і використовувати план корпоративних програм безпеки на основі оцінки ризику кожному оператору трубопровідної галузі для вирішення та документування політик та процедур безпеки організації, управління загрозами, інцидентами та реагуваннями на безпеку. В зазначений план необхідно включити розділ забезпечення кібербезпеки системи управління. Цей розділ плану, згідно з рекомендаціями [6], повинен включати політику, практику та процедури кібербезпеки системи управління. Плани кібербезпеки належної системи управління, як мінімум, стосуються питань визначення та надання доступу, захисту сервера та системи проникнення в систему, виявлення зловмисного коду, відновлення бізнесу та відновлення аварій. Вимоги щодо забезпечення кібербезпеки стосується великих систем SCADA у галузі передачі природного газу та локальних систем управління, які використовуються у всій трубопровідній системі, включаючи компресорні станції, виробничі станції, сховища, станції кондиціонування та зневоднення газу.

На даний час, на основі статистичного аналізу, в якості характерного значення ймовірності аварій газопроводу високого тиску внаслідок кібератак приймаються наступні значення:

- від кіберзагроз, що можуть виникнути під час мережевої взаємодії $p_{r1} = 0,24$;
- від кіберзагроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням $p_{r2} = 0,42$;
- від кіберзагроз, що можуть виникнути в мережевих операційних системах $p_{r3} = 0,35$.

У випадку реалізації кібератаки, здійснюється пошкодження газопроводу. При цьому, відбувається витік газу $h_r = 5000$ кг/с при

робочому значенні тиску 12 МПа і при протяжності лінійної ділянки між компресорними станціями 120 км.

Значення об'єктивного ризику кібербезпеки газопроводу високого тиску у даному випадку буде розраховуватися з виразів:

$$R_{r1} = h_r \cdot p_{r1} = 5000 \cdot 0,24 = 1200; \quad (6.1)$$

$$R_{r2} = h_r \cdot p_{r2} = 5000 \cdot 0,42 = 2100; \quad (6.2)$$

$$R_{r3} = h_r \cdot p_{r3} = 5000 \cdot 0,35 = 1750. \quad (6.3)$$

В той же час, досвід експлуатації газопроводів дозволяє фахівцям сформулювати вимоги до проектування і побудови газопроводів нового покоління. Такі газопроводи використовують комп'ютерно-інтегровані технології, що дає ряд переваг в аспектах управління та моніторингу. Одночасно, це створює уразливості таких систем до кібератак.

У такому випадку, на думку фахівців, ймовірність реалізації кібератак буде складати

- від кіберзагроз, що можуть виникнути під час мережевої взаємодії $p_{v1} = 0,45$;
- від кіберзагроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням $p_{v2} = 0,5$;
- від кіберзагроз, що можуть виникнути в мережевих операційних системах $p_{v3} = 0,6$.

При цьому, буде здійснюватися витік газу у такій же кількості і з такою ж інтенсивністю $h_v = 5000$ кг/с, при значенні тиску 12 МПа і при протяжності лінійної ділянки між компресорними станціями 120 км.

Суб'єктивний ризик кібербезпеки газопроводу високого тиску у даному випадку буде розраховуватися з виразів:

$$R_{v1} = h_v \cdot p_{v1} = 5000 \cdot 0,45 = 2250; \quad (6.4)$$

$$R_{v2} = h_v \cdot p_{v2} = 5000 \cdot 0,5 = 2500; \quad (6.5)$$

$$R_{v3} = h_v \cdot p_{v3} = 5000 \cdot 0,6 = 3000. \quad (6.6)$$

Використовуючи метод обчислення комплексного ризику, а також значення об'єктивного (6.1), (6.2), (6.3) та суб'єктивного (6.4), (6.5), (6.6) ризиків, знаходимо значення копмлексного ризику:

- від кіберзагроз, що можуть виникнути під час мережевої взаємодії:

$$R_1 = \sqrt{R_{r1}^2 + R_{v1}^2} = \sqrt{1200^2 + 2250^2} =$$
$$= \sqrt{1440000 + 5062500} = \sqrt{6502500} = 2550;$$

- від кіберзагроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням:

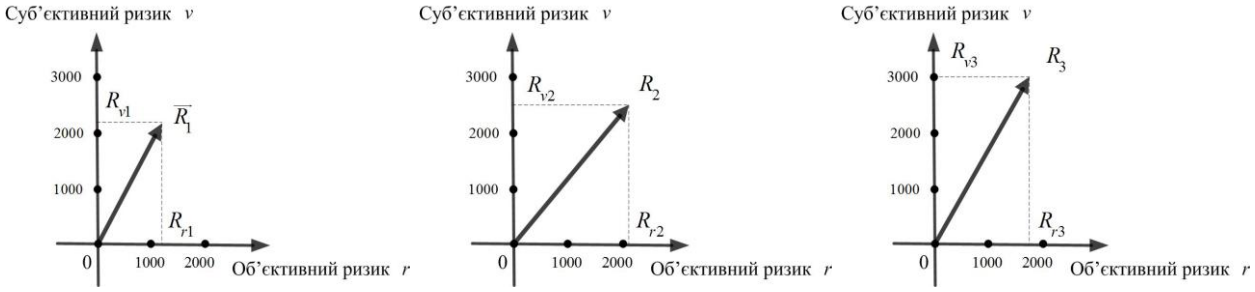
$$R_2 = \sqrt{R_{r2}^2 + R_{v2}^2} = \sqrt{2100^2 + 2500^2} =$$
$$= \sqrt{4410000 + 6250000} = \sqrt{6691000} \approx 2587;$$

- від кіберзагроз, що можуть виникнути в мережевих операційних системах:

$$R_3 = \sqrt{R_{r3}^2 + R_{v3}^2} = \sqrt{1750^2 + 3000^2} =$$
$$= \sqrt{3062500 + 9000000} = \sqrt{12062500} \approx 3473.$$

Використовуючи векторну модель ризику та модель комплексного ризику, зобразимо на комплексній площині розраховані об'єктивні, суб'єктивні та комплексні ризики від кіберзагроз, що можуть виникнути під час мережевої взаємодії, рис. 6.10(а), від кіберзагроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, рис. 6.10(б), від

кіберзагроз, що можуть виникнути в мережевих операційних системах, рис. 6.10(в).



а) б) в)

Рис. 6.10. Вектори на комплексній площині об'єктивних та суб'єктивних ризиків від різних кіберзагроз

Використовуючи векторну модель ризику та модель комплексного ризику, зобразимо розраховані об'єктивні та суб'єктивні ризики на комплексній площині, рис. 6.11.

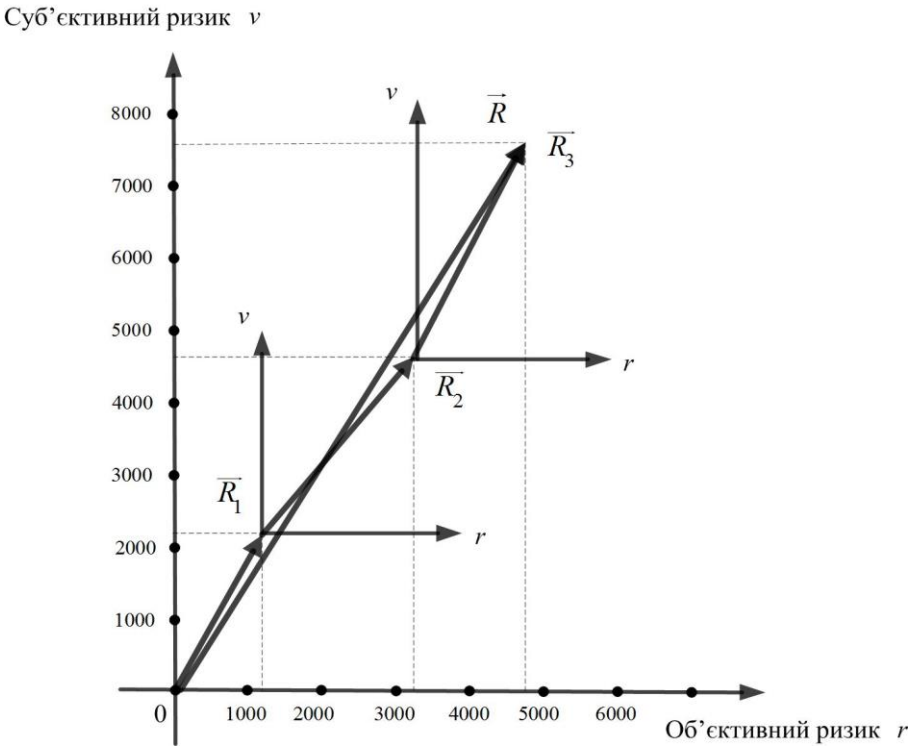


Рис. 6.11. Вектори об'єктивних та суб'єктивних ризиків на комплексній площині

Розрахунки показують, що об’єктивний ризик від кіберзагроз, що можуть виникнути під час мережевої взаємодії, під час роботи з прикладним програмним забезпеченням, що можуть виникнути в мережевих операційних системах буде складати $R_r = 5050$.

При цьому, суб’єктивний ризик від кіберзагроз, що можуть виникнути під час мережевої взаємодії, під час роботи з прикладним програмним забезпеченням, що можуть виникнути в мережевих операційних системах буде складати $R_v = 7750$.

Використовуючи метод обчислення комплексного ризику, а також розраховані значення об’єктивного та суб’єктивного ризиків, знаходимо значення комплексного ризику:

$$R = \sqrt{R_r^2 + R_v^2} = \sqrt{5050^2 + 7750^2} =$$

$$= \sqrt{25502500 + 60062500} = \sqrt{85565000} \approx 9250. \qquad (6.7)$$

Графік проекції функції комплексного ризику на площину *ph* можна представити у вигляді виразу

$$h(p) = \frac{R}{p}, \qquad (6.8)$$

де R - значення ризику, на рівні якого здійснюється переріз графіку функції;

$p \neq 0$.

Підставляючи у вираз (6.8) значення ймовірності від 0 до 1 отримуємо графік проекції функції комплексного ризику на площину *ph* для значення ризику:

- від кіберзагроз, що можуть виникнути під час мережевої взаємодії

$R_1 = 2550$, рис. 6.12;

- від кіберзагроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням $R_2 = 2587$, рис. 6.13;
- від кіберзагроз, що можуть виникнути в мережевих операційних системах $R_3 = 3473$, рис. 6.14.

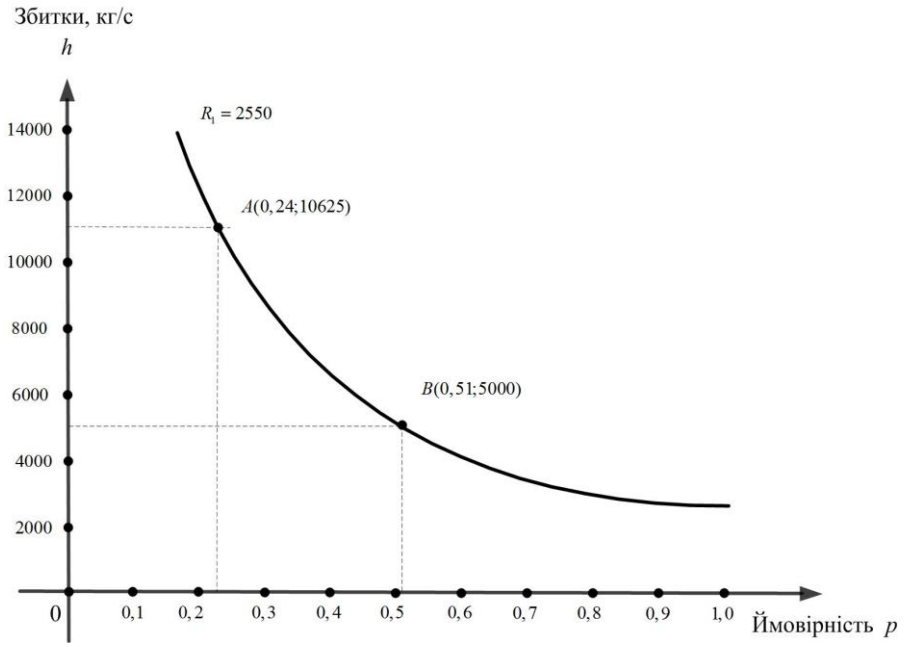


Рис. 6.12. Графік проекції функції комплексного ризику на площину *ph* для значення ризику $R_1 = 2550$

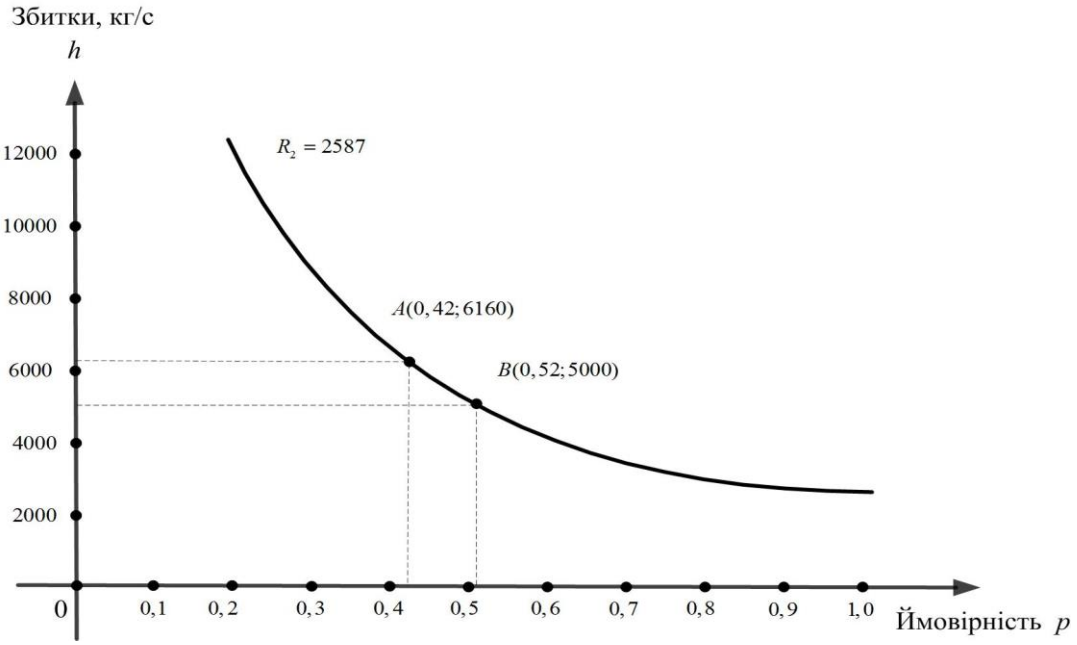


Рис. 6.13. Графік проекції функції комплексного ризику на площину *ph* для значення ризику $R_2 = 2587$

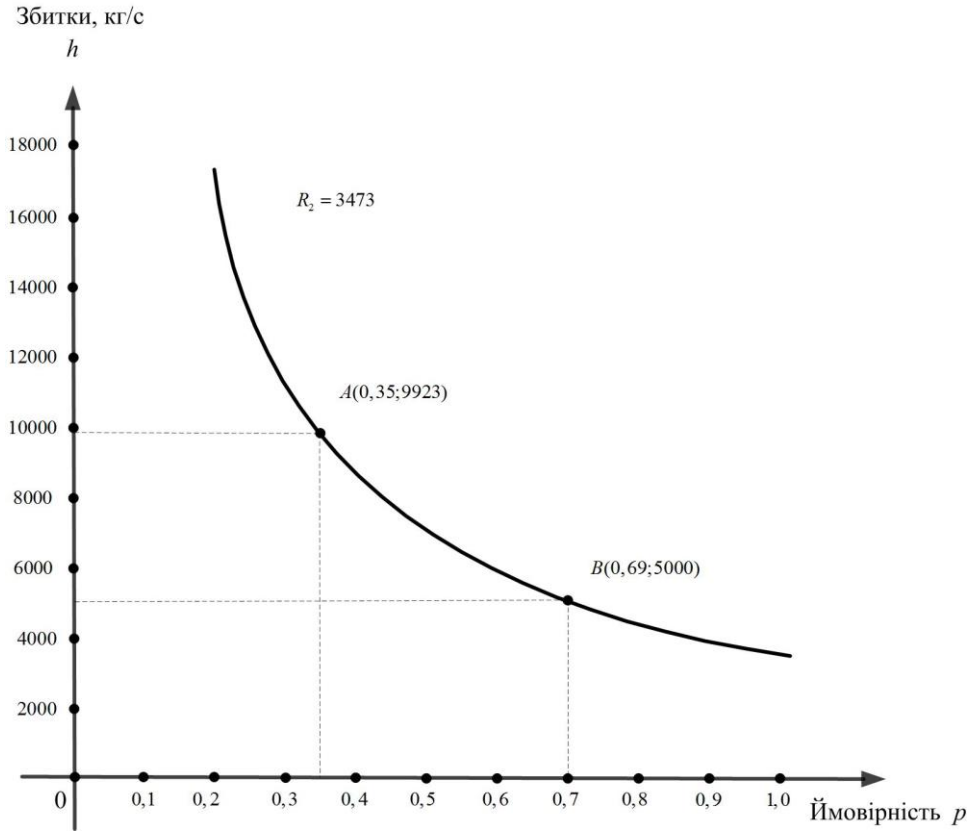


Рис. 6.14. Графік проекції функції комплексного ризику на площину *ph* для значення ризику $R_3 = 3473$

За результатами проведених розрахунків можна бачити, що у випадку:

- кіберзагроз, які можуть виникнути під час мережевої взаємодії:
  - ймовірність збитків $h = 5000$ збільшується у 2,12 раз;
  - збитки від кібератаки, ймовірність реалізації якої $p_1 = 0,24$, збільшуються у 2,12 раз;
- кіберзагроз, які можуть виникнути під час роботи з прикладним програмним забезпеченням:
  - ймовірність збитків $h = 5000$ збільшується у 1,23 рази;
  - збитки від кібератаки, ймовірність реалізації якої $p_2 = 0,42$, збільшуються у 1,23 рази;
- кіберзагроз, які можуть виникнути в мережевих операційних системах:
  - ймовірність збитків $h = 5000$ збільшується у 1,98 раз;

- збитки від кібератаки, ймовірність реалізації якої $p_3 = 0,35$, збільшуються у 1,98 раз.

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».

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

6.3. Висновки до шостого розділу

1. Розроблено алгоритмічне та програмне забезпечення обчислювальних систем для розрахунку суми ризиків та обчислення комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів.

2. Отримані результати підтверджують ефективність розроблених методів та методології забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, орієнтованої на створення відповідних методів та засобів розрахунку сумарних ризиків.

3. 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 по забезпеченню кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Результати дисертаційної роботи впроваджено у діяльність

Адміністрації Державної служби спеціального зв'язку та захисту інформації України (відгук від 20.03.2019р. № 05/02-295), 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), 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.).

Основні результати дисертаційної роботи, представлені в розділі 6, опубліковані в працях автора [1, 2].

Список використаних джерел до шостого розділу

1. Гончар С.Ф. Аналіз і дослідження загроз для захищеного вузла інтернет доступу / Комаров М.Ю., Гончар С.Ф. // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2018. – Т.29(68). Ч.1. – №4. – С. 165-168.

2. Гончар С.Ф. Аналіз та дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу / Комаров М.Ю., Ониськова А.В., Гончар С.Ф. // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2018. – Т.29(68). Ч.1. – №5. – С. 138-142.

3. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 за № 22.

4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 за № 22.

5. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технологій. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій.

6. Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry. INGAA Control Systems Cyber Security Guidelines : 2011. Control Systems Cyber Security Working Group.

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.).

Додаток А. Документи, що підтверджують впровадження результатів дисертації

Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

20.03.2019 № 05/02-295

Відгук

на результати виконання НДР «Методичні та нормативно-правові основи забезпечення кібернетичної безпеки функціонування енергетики України з урахуванням європейських вимог» та НДР «Розробка методів оцінювання чутливості об'єднаної енергосистеми України до кібернетичних впливів»

Розглянувши результати виконання НДР «Методичні та нормативно-правові основи забезпечення кібернетичної безпеки функціонування енергетики України з урахуванням європейських вимог» та НДР «Розробка методів оцінювання чутливості об'єднаної енергосистеми України до кібернетичних впливів», які виконувались Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Науково-технічна рада Адміністрації Держспецзв'язку рекомендує профільним підрозділам Адміністрації Держспецзв'язку використати результати розглянутих НДР при проведенні подальших наукових робіт з питань кіберзахисту об'єктів критичної інфраструктури України та при формуванні державної політики у сфері кіберзахисту об'єктів критичної інфраструктури.

Перший заступник Голови Служби О.М. Чаузов

ІПМЕ вх. 111
22.03.2019р

Прим. № 1

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національної академії Служби безпеки України
кандидат юридичних наук, доцент

_____ С. Фальченко

«18» березня 2019 року

АКТ
про впровадження результатів дисертаційного дослідження Гончара С.Ф. на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Комісія у складі: голови – начальника наукової лабораторії № 2 науково-організаційного центру Національної академії СБ України доктора юридичних наук Гребенюка В.М.; головного наукового співробітника наукової лабораторії № 2 НОЦ НА СБ України, доктора юридичних наук, старшого наукового співробітника Авдошина І.В.; доцента спеціальної кафедри № 2 Навчально-наукового інституту контррозвідувальної діяльності кандидата юридичних наук, доцента Манжул І.В.

ВСТАНОВИЛА:

основні наукові результати дослідження, отримані особисто автором у дисертації «Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури» впроваджені в наукову діяльність Національної академії СБ України, а саме у започаткуванні та провадженні науково-дослідної роботи «Організаційно-правові засади контррозвідувального захисту об'єктів критичної інфраструктури України» (державний реєстраційний номер 0117U000044Т, звіт за НДР реєстр. № 29/20-13463дск від 17.12.2019 року).

Зокрема, в межах зазначеної НДР була підготовлена монографія за участю дисертанта:

Системи забезпечення безпеки критичної інфраструктури : моногр. / О.Г. Корченко, С.В. Казмірчук, Є.В. Іванченко, А.О. Корченко, Ю.О. Дрейс , В.В. Мохор, С.Ф. Гончар, В.М. Гребенюк, І.В. Манжул, О.Є Юдін. – К. : ЦП «Компринт», 2018. – в 2-ох томах. – Том 1, 2018 – 540 с. – том 2, 2018. – 400 с.

Ця монографія рекомендована Вченою радою НА СБ України, протокол засідання № 11 від 29.11.18 р.

Отримані особисто здобувачем наукові результати мають теоретичне значення для розвитку науки, зокрема у сфері:

1) функціонування механізмів захисту об'єктів критичної інфраструктури;

2) оцінки стану та пропозицій поліпшення цієї діяльності.

Наукові здобутки автора використовуються при:

1) дослідженні шляхів протидії СБ України посяганням на критичну інфраструктуру України, її інформаційний сегмент зокрема;

2) підготовці науково-аналітичної продукції з проблем оптимізації захисту критичної інфраструктури, контрдиверсійної діяльності.

Результати дослідження Гончара С.Ф. мають теоретичну та практичну значущість для оптимізації оперативно-службової діяльності СБ України в сучасних умовах.

Голова комісії:
Начальник наукової лабораторії № 2
науково-організаційного центру
Національної академії Служби безпеки України
доктор юридичних наук

В. Гребенюк

«17» 09 2019 року

Члени комісії:

Головний науковий співробітник
наукової лабораторії № 2
науково-організаційного центру
Національної академії Служби безпеки України
доктор юридичних наук, старший науковий співробітник

І. Авдошин

«17» 09 2019 року

Доцент спеціальної кафедри № 2
Навчально-наукового інституту контррозвідувальної діяльності
Національної академії Служби безпеки України
кандидат юридичних наук, доцент

І. Манжул

«17» 09 2019 року

"ЗАТВЕРДЖУЮ"
Начальник Державного науково-дослідного інституту спеціального зв'язку та захисту інформації

Д.Д. Вергелес

"08" жовтня 2015р.

АКТ
впровадження результатів наукових досліджень
Гончара Сергія Феодосійовича
в Державному науково-дослідному інституті спеціального зв'язку та захисту інформації в науково-дослідній роботі "Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури"
(шифр "Інфраструктура" № 0114U000038д)

Комісія у складі:

голови комісії – першого заступника начальника ДержНДІ Спецзв'язку полковника Держспецзв'язку Леоненко Г.П.,

членів комісії – начальника науково-дослідного центру ДержНДІ Спецзв'язку полковника Держспецзв'язку Юдіна О.Ю., заступника начальника науково-дослідного центру ДержНДІ Спецзв'язку полковника Держспецзв'язку Бондаренка Д.М. з'ясувала що в Державній службі спеціального зв'язку та захисту інформації України в ході виконання науково-дослідної роботи "Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури" (шифр "Інфраструктура" № 0114U000038д) вперше впровадженні розроблені Гончаром Сергієм Феодосійовичем такі наукові результати:

- модель деструктивних дій обслуговуючого персоналу автоматизованих систем об'єктів критичної інфраструктури при умові наявності зовнішніх та/або внутрішніх дестабілізуючих впливів;
- схему життєвого циклу аналізу ймовірності реалізації загроз інформаційній безпеці автоматизованих систем управління технологічними процесами за запропонованими вихідними даними, що необхідні для цього аналізу;
- модель управлінського впливу на забезпечення захисту інформації на об'єктах критичної інфраструктури.

Ефект від впровадження набутих наукових результатів полягає в тому, що вони дозволяють розробляти адекватні рекомендації, методи та засоби щодо захисту інформації на об'єктах критичної інфраструктури.

Голова комісії
полковник Держспецзв'язку Леоненко Г.П.
"08" жовтня 2015 р.

Члени комісії:
полковник Держспецзв'язку Юдін О.Ю.
"8" жовтня 2015 р.

полковник Держспецзв'язку Бондаренко Д.М.
"8" жовтня 2015 р.

"ЗАТВЕРДЖУЮ"
Начальник Державного науково-дослідного інституту спеціального зв'язку та захисту інформації

Д.Д. Вергелес

"26" 11 2015р.

АКТ
впровадження результатів наукових досліджень
Гончара Сергія Феодосійовича
в Державному науково-дослідному інституті спеціального зв'язку та захисту інформації в науково-дослідній роботі "Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури"
(шифр "Інфраструктура" № 0114U000038д)

Комісія у складі:

голови комісії – першого заступника начальника ДержНДІ Спецзв'язку полковника Держспецзв'язку Леоненко Г.П.,

членів комісії – начальника науково-дослідного центру ДержНДІ Спецзв'язку полковника Держспецзв'язку Юдіна О.Ю., заступника начальника науково-дослідного центру ДержНДІ Спецзв'язку полковника Держспецзв'язку Бондаренка Д.М. з'ясувала що в Державній службі спеціального зв'язку та захисту інформації України в ході виконання науково-дослідної роботи "Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури" (шифр "Інфраструктура" № 0114U000038д) вперше впровадженні розроблені Гончаром Сергієм Феодосійовичем такі наукові результати:

- методологічний аспект розробки і впровадження систем захисту інформації об'єктів критичної інфраструктури;
- соціокультурний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури;
- підходи до визначення актуальних загроз інформації, яка циркулює на об'єктах критичної інфраструктури;
- пропозиції з удосконалення організаційної структури механізму забезпечення безпеки інформації, яка циркулює на об'єктах критичної інфраструктури;
- пропозиції з удосконалення науково-методичного забезпечення безпеки інформації, яка циркулює на об'єктах критичної інфраструктури;
- загальну модель загроз безпеці інформації в автоматизованих системах управління об'єктів критичної інфраструктури.

Ефект від впровадження набутих наукових результатів полягає в тому, що вони дозволяють розробляти адекватні рекомендації, методи та засоби щодо захисту інформації на об'єктах критичної інфраструктури.

Голова комісії
полковник Держспецзв'язку Леоненко Г.П.

Члени комісії:
полковник Держспецзв'язку Юдін О.Ю.

полковник Держспецзв'язку Бондаренко Д.М.

ДЕРЖАВНА ІНСПЕКЦІЯ
ЯДЕРНОГО РЕГУЛЮВАННЯ УКРАЇНИ

НАЦІОНАЛЬНА
АКАДЕМІЯ НАУК УКРАЇНИ

ДНТЦ ЯРБ ДЕРЖАВНЕ ПІДПРИЄМСТВО
"ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР
З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ"

вул. Василя Стуса, 35-37, м. Київ, 03142, Україна, а/с 124, тел.: (044)450-05-00, факс: (044) 452-89-90 e-mail: nrs@sstc.com.ua
П/р 26008000022515 в АТ "Укрексімбанк" в м. Києві МФО 322313 КОД ЄДРПОУ 14282338 www.sstc.com.ua

ЗАТВЕРДЖУЮ
Директор
Державного підприємства
«Державний науково-технічний
центр з ядерної та радіаційної
безпеки»
_____ І.А. Шевченко
_____ 2019 р.

Акт

впровадження результатів дисертаційної роботи
Гончара Сергія Феодосійовича
за темою «Методологія оцінки ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури», представленої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»

Комісія у складі:
голови – к.т.н., першого заступника директора Печериці О.В.,
членів комісії – д.т.н., головного наукового співробітника відділу аналізу безпеки керуючих та інформаційних систем АЕС Харківської філії ДНТЦ ЯРБ Ястребенецького М.О.
к.т.н., начальника відділу аналізу безпеки керуючих та інформаційних систем АЕС Харківської філії ДНТЦ ЯРБ Клевцова О.Л.

склала цей акт про те, що результати дисертаційної роботи Гончара С.Ф. впроваджено в діяльність ДНТЦ ЯРБ шляхом застосування результатів виконаних дисертантом наукових досліджень (методу розрахунку сумарного ризику кібербезпеки інформаційних та керуючих систем АЕС та методу оцінки ризику кібербезпеки інформаційних та керуючих систем, що враховує об'єктивну і суб'єктивну складові ризику) під час розробки регулюючих вимог з комп'ютерної безпеки інформаційних та керуючих систем АЕС.
Впроваджені результати дисертаційного дослідження є складовою частиною створення передумов побудови системи підтримки прийняття рішень щодо застосування заходів по зменшенню ризику кібербезпеки інформаційних і керуючих систем об'єктів атомної енергетики та можуть бути використані для ефективного вирішення завдань оцінки ризиків.
Дійсний акт не є підставою для отримання премій та інших винагород з фондів ДНТЦ ЯРБ.

Голова комісії:
к.т.н., перший заступник директора _____ О.В. Печериця

Члени комісії:
д.т.н, головний науковий співробітник відділу аналізу безпеки керуючих та інформаційних систем АЕС Харківської філії ДНТЦ ЯРБ _____ М.О. Ястребенецький

к.т.н., начальник відділу аналізу безпеки керуючих та інформаційних систем АЕС Харківської філії ДНТЦ ЯРБ _____ О.Л. Клевцов

«ЗАТВЕРДЖУЮ»
Директор Інституту проблем моделювання
в енергетиці ім. Г.Є. Пухова НАН України
член-кореспондент НАН України
д.т.н., професор В.В. Мохор

«____» _____ 2019 р.

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційної роботи
«Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури»
Гончара Сергія Феодосійовича
на здобуття наукового ступеню доктора технічних наук
за спеціальністю 05.13.21 – «Системи захисту інформації»

Комісія у складі голови комісії заступника директора Інституту, доктора технічних наук Чемериса Олександра Анатолійовича та членів комісії у складі: завідувача відділу, доктора технічних наук Винничука Степана Дмитровича та старшого наукового співробітника, кандидата технічних наук Гільгурта Сергія Яковича встановила, що програмна реалізація методології оцінювання ризиків, що є результатом досліджень Гончара С.Ф. реалізоване в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Розроблена методологія оцінки ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури використовує методи розрахунку суми ризиків і методу обчислення комплексного ризику. Методи обчислення суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, за рахунок використання значень максимальних наслідків від ризиків, дозволяють розраховувати суму декількох ризиків, загальні наслідки від реалізації цих ризиків та ймовірність їх реалізації, а метод обчислення комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, за рахунок врахування об'єктивної і суб'єктивної складових ризику, дозволяє здійснювати більш коректну оцінку зазначених ризиків.

Таким чином, результати, отримані Гончаром С.Ф. при написанні дисертаційної роботи, дозволили використовувати системи оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури з метою підвищення рівня автоматизації процесів управління ризиками при побудові комплексних систем захисту інформації і систем управління інформаційною безпекою.

Вказані результати було використано в ході виконання науково-дослідної роботи «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів», шифр «ВПЛИВ», № держреєстрації 0118U005320.

Даний акт не є підставою для проведення взаємних фінансових розрахунків.

Голова комісії:
заступник директора ІПМЕ ім. Г.Є. Пухова
НАН України
д.т.н., с.н.с. О.А. Чемерис

Члени комісії:
завідувач відділу ІПМЕ ім. Г.Є. Пухова
НАН України
д.т.н., с.н.с. С.Д. Винничук

старший науковий співробітник ІПМЕ ім. Г.Є. Пухова
НАН України
к.т.н., с.н.с. С.Я. Гільгурт

vega telecom

Вих. № 65/04-10
від «09» 07 2018 р.
На № 225/01-1-145 від 02.07.2018 р.

Директору Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України Мохору В.В.

ПрАТ «Фарлеп-Інвест» висловлює подяку за виконання робіт зі створення та проведення первинної державної експертизи комплексної системи захисту інформації захищеного вузла Інтернет доступу ПрАТ «Фарлеп-Інвест», які були виконані у повному обсязі та в терміни, визначені календарним планом.

Сподіваємось на подальшу співпрацю.

Генеральний директор
ПрАТ «Фарлеп-Інвест» **Мурат Чинар**

Вик. Чудінов Р.А.
050 364-40-97

НАЦІОНАЛЬНА КОМІСІЯ, ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ
РЕГУЛЮВАННЯ У СФЕРІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

УДЦР

ДЕРЖАВНЕ ПІДПРИЄМСТВО
«УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ЦЕНТР РАДІОЧАСТОТ»

03179, м. Київ, проспект Перемоги, 151, тел.: (044) 422-81-03, тел./факс: (044) 422-81-81,
e-mail: centre@ucrf.gov.ua, http://www.ucrf.gov.ua,
р/р 26009428584 в АТ «Райффайзен Банк Аваль», м. Київ, МФО 380805, код за ЄДРПОУ 01181765

«10» ЖОВ 2019 201__ р. № 80/14.2-55/847/13063 На № _____ від «___» _____ 201__ р.

Директору Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України Мохору В.В.

Шановний Володимире Володимировичу!

Державне підприємство «Український державний центр радіочастот» висловлює подяку за виконання робіт з проведення первинної державної експертизи комплексної системи захисту інформації в Автоматизованій інформаційній системі «Централізована база даних перенесених номерів» Державного підприємства «Український державний центр радіочастот» - автоматизована система класу «3», в якій циркулює інформація з обмеженим доступом. Роботи виконані у повному обсязі та в терміни, визначені календарним планом.

Сподіваємось на подальшу співпрацю.

З повагою,
Директор з інформаційно-телекомунікаційного напрямку **В.Ю. Трощенко**

Вик. БондаренкоВ.І.
Тел.422-85-81

«ЗАТВЕРДЖУЮ»
Директор Інституту проблем моделювання
в енергетиці ім. Г.Є. Пухова НАН України
член-кореспондент НАН України
д.т.н., професор В.В. Мохор

«_____» 2019 р.

АКТ
впровадження у навчальний процес

Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України результатів дисертаційної роботи «Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури»
Гончара Сергія Феодосійовича
на здобуття наукового ступеню доктора технічних наук
за спеціальністю 05.13.21 – «Системи захисту інформації»

Комісія у складі голови комісії заступника директора Інституту, доктора технічних наук Чемериса Олександра Анатолійовича та членів комісії у складі: завідувача відділу, доктора технічних наук Винничука Степана Дмитровича та завідувача відділу, кандидата технічних наук Душеби Валентини Віталіївни склали цей акт про те, що результати дисертаційної роботи Гончара С.Ф. впроваджені у навчальний процес і використовуються у науково-навчальному центрі кіберфізичних систем Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України при викладанні наступних дисциплін: «Сучасні проблеми і тенденції розвитку комп'ютерних наук та інформаційних технологій» та «Філософські та методологічні проблеми теорії інформаційної безпеки».

Дані дисципліни викладаються при підготовці фахівців у сфері вищої освіти за третім (освітньо-науковим) рівнем зі спеціальності 122 – «комп'ютерні науки».

Даний акт не є підставою для проведення взаємних фінансових розрахунків.

Голова комісії:
заступник директора ІПМЕ ім. Г.Є. Пухова
НАН України
д.т.н., с.н.с. О.А. Чемерис

Члени комісії:
завідувач відділу ІПМЕ ім. Г.Є. Пухова
НАН України
д.т.н., с.н.с. С.Д. Винничук

завідувач відділу ІПМЕ ім. Г.Є. Пухова
НАН України
к.т.н., доцент В.В. Душеба

УКРАЇНА

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 132581

СПОСІБ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **25.02.2019.**

Заступник Міністра економічного розвитку і торгівлі України Ю.П. Бровченко

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ * ІДЕНТИФІКАЦІЙНИЙ КОД 37508596 *

УКРАЇНА

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 136947

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ОЦІНКИ ТА АНАЛІЗУ РИЗИКУ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **10.09.2019.**

Заступник Міністра розвитку економіки, торгівлі та сільського господарства України Д.О. Романович

УКРАЇНА

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 136792

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС РОЗРАХУНКУ КОМПЛЕКСНОГО РИЗИКУ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **27.08.2019.**

Заступник Міністра економічного розвитку і торгівлі України Ю.П. Бровченко

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ * ІДЕНТИФІКАЦІЙНИЙ КОД 37508596 *

УКРАЇНА

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 135456

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС РОЗРАХУНКУ СУМАРНОГО РИЗИКУ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **25.06.2019.**

Заступник Міністра економічного розвитку і торгівлі України Ю.П. Бровченко

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ * ІДЕНТИФІКАЦІЙНИЙ КОД 37508596 *

УКРАЇНА

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 136949

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ВІЗУАЛІЗАЦІЇ РИЗИКІВ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **10.09.2019.**

Заступник Міністра розвитку економіки, торгівлі та сільського господарства України — Д.О. Романович

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace WindowsFormsApp2

{
   public partial class Form1 : Form

   {
      public Form1()

      {
         InitializeComponent();
      }

      int kilk;//Лічильник кліків
      float Rizik;
      float Naslidki;
      float NaslidkiM;//Максимальні наслідки
      float ImovirPnm;//Імовірність виникнення подій, що призводить до
максимальних наслідків
      float SumImovirPnm;//Сума імовірностей
      float ProizImovirPnm = 1;//Добуток імовірностей
      float Pm;//
      float SumP;//Сума імовірностей
      float ProizP = 1;//Добуток імовірностей
      float P;//
      float H;//
      float RizikSum;//Сумарний ризик дії ризиків

      //List<float> imovir = new List<float>();
      //List<float> naslidki = new List<float>();
      //List<float> naslidkiM = new List<float>();
      //List<float> rizik = new List<float>();

      private void Form1_Load(object sender, EventArgs e)
```

```
        {
            //Загрузка форми і обнуління Label
            label15.Text = "";
            label9.Text = "";
            label8.Text = "";
            label12.Text = "";
            label14.Text = "";
            label18.Text = "";
            label19.Text = "";
        }

        private void Button1_Click(object sender, EventArgs e)

        {
            kilk++;//Збільшення лічильника на одиницю
            Rizik = (Convert.ToSingle(textBox1.Text)) *
(Convert.ToSingle(textBox2.Text));//Розрахунок ризику
            ImovirPnm = Rizik / Convert.ToSingle(textBox3.Text);//Розрахунок
імовірності Pnm
            SumImovirPnm += ImovirPnm;//Розрахунок суми Pnm
            ProizImovirPnm *= ImovirPnm;//Розрахунок добутка Pnm
            SumP+= Convert.ToSingle(textBox1.Text);//Розрахунок суми
імовірностей
            ProizP*= Convert.ToSingle(textBox1.Text);//Отримання добутку
імовірностей
            NaslidkiM += (Convert.ToSingle(textBox3.Text));//Отримання муми
максимальних наслідків

            //imovir.Add(Convert.ToSingle(textBox1.Text));
            //naslidki.Add(Convert.ToSingle(textBox2.Text));
            //naslidkiM.Add(Convert.ToSingle(textBox3.Text));
            //float rizik1 =(Convert.ToSingle(textBox1.Text) *
Convert.ToSingle(textBox2.Text));
            //rizik.Add(Convert.ToSingle(textBox1.Text)*
Convert.ToSingle(textBox2.Text));
            //Виведення результатів
            label15.Text += 'R' + Convert.ToString(kilk) + " = " +
Convert.ToString(Rizik)+", " ;// Виведення ризику R
            label8.Text += 'p' + Convert.ToString(kilk) + "m" + " = " +
Convert.ToString(ImovirPnm) + ", ";//Виведення імовірності Pnm
            label9.Text = Convert.ToString(NaslidkiM);//Виведення максимального
наслідку
        }
```

```
        private void Button3_Click(object sender, EventArgs e)
        {
            Pm = SumImovirPnm - ProizImovirPnm;
            RizikSum = Pm * NaslidkiM;
            P = SumP - ProizP;
            //Виведення на форму результатів розрахунків
            label12.Text = Convert.ToString(Pm);
            label14.Text = Convert.ToString(RizikSum);// Виведення суми ризикі R
            label18.Text = Convert.ToString(SumP); ;// Виведення імовірності суми ризиків p
            label19.Text = Convert.ToString(RizikSum/P);//Розрахунок і виведення наслідків суми ризиків
        }

        private void Button2_Click(object sender, EventArgs e)

        {
            // Видалення всіх результатів розрахунків
            kilk = 0;
            NaslidkiM = 0;
            ImovirPnm = 0;
            SumImovirPnm = 0;
            ProizImovirPnm = 1;
            Pm = 0;
            RizikSum = 0;
            SumP=0;
            ProizP = 1;
            //Обнуління Label
            label15.Text = "";
            label9.Text = "";
            label8.Text = "";
            label12.Text = "";
            label14.Text = "";
            label18.Text = "";
            label19.Text = "";

        }
    }
}
```

Додаток В. Загрози загального характеру

Таблиця 6.1

Загрози загального характеру, що можуть виникнути в ЗВІД-ФАРЛЕП

Іденти-фікатор загрози	Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкт загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використо-вуватися	Тип загрози
1	2	3	4	5	6	7	8	9
З.1.1	Пожежа	Виникнення полум’я та розповсюдження пожежі в приміщеннях, де знаходяться технічні засоби. Можуть бути пошкоджені об’єкти захисту, структурні компоненти, канали передачі даних, втрачена інформація.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середо-вище	-	Недотримання правил проти-пожежної безпеки, несправності електричної проводки, перевантаження електромережі	Відсутність системи пожежо-гасіння	Ц, Д, С
З.1.2	Руйнування	Руйнування приміщень та їх вмісту внаслідок вибуху, зсуву, урагану тощо. Можуть бути пошкоджені об’єкти захисту, структурні компоненти ЗВІД-ФАРЛЕП, канали передачі даних, втрачена інформація.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середовище	-	Невідповідність інженерних характеристик будівлі та приміщень	Відсутність географічно розподіленої системи резервування даних	Ц, Д, С
З.1.3	Затоплення	Заливання приміщень внаслідок аварій, стихійних лих у вигляді дощів, танення снігу, гасіння полум’я водою. Можуть бути пошкоджені об’єкти захисту, структурні компоненти ЗВІД-ФАРЛЕП.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середовище	-	Несправність інженерних конструкцій, систем водо постачання, пожежогасіння	Невідповід-ність умовам розміщення технічних засобів	Ц, Д, С

Продовження таблиці 6.1

З.1.4	Забруднення	Запиленість та забрудненість приміщень та технічних засобів. Наслідком можуть стати відмови та збої компонентів ЗВІД-ФАРЛЕП та окремих технічних засобів, пошкодження носіїв інформації.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середовище	-	Неповне та несистематичне прибирання приміщень та обслуговування технічних засобів	Невідповідність умовам розміщення технічних засобів	Ц, Д, С
З.1.5	Перегрів	Зміна температури повітря внаслідок погодних аномалій, порушення в роботі систем опалення та вентиляції. Наслідком можуть стати відмови та збої компонентів ЗВІД-ФАРЛЕП та окремих технічних засобів.	Технічні засоби ЗВІД-ФАРЛЕП	Зовнішнє середовище	-	Несправність систем вентиляції і опалення приміщень, захаращення вентиляційних отворів технічних засобів	Відсутність системи клімат-контролю, невідповідність умовам розміщення технічних засобів	Ц, Д, С
З.1.6	Вологість	Зміна вологості повітря внаслідок погодних аномалій, порушення систем вентиляції. Можуть бути пошкоджені носії інформації, електроконтакти, що спричинятиме відмови та збої компонентів ЗВІД-ФАРЛЕП та окремих технічних засобів.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середовище	-	Несправність систем вентиляції і опалення приміщень, порушення режиму прибирання приміщень, необережне поводження з водою	Відсутність системи клімат-контролю, невідповідність умовам розміщення технічних засобів	Ц, Д, С

Продовження таблиці 6.1

З.1.7	Електро-магнітні випромі-нювання	Магнітні наводки від потужних електроприладів (трансформатори, електродвигуни, динаміки), електромагнітні бурі. Можливе пошкодження носіїв інформації, відмови та збої технічних засобів.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середовище	-	Недотримання правил розміщення електроприладів	Невідповід-ність умовам розміщення технічних засобів	Ц, Д, С
З.1.8	Поламки, відмови та збої апаратури	Відмова та збої у роботі технічних засобів ЗВІД-ФАРЛЕП, вихід з ладу аппаратного забезпечення внаслідок техногенних аварій, порушення умов експлуатації, несвоєчасного діагностування проблеми. Наслідком може стати непрацездатність компонентів ЗВІД-ФАРЛЕП та окремих технічних засобів, втрата та перекручення інформації в процесі запису/зчитування.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Зовнішнє середовище, апаратні та програмні засоби	-	Порушення умов експлуатації, недотримання правил обслуговування технік-них засобів, недостатня кваліфікація користувачів, використання обладнання, що не пройшло перевірку на сумісність з іншим обладнанням	Порушення процедур перевірки працездат-ності компо-нентів ЗВІД-ФАРЛЕП, відсутність в календарному плані регла-ментних робіт, недостатньо глибоке проведення випробувань апаратури в умовах функціону-вання ЗВІД-ФАРЛЕП	Ц, Д, С

Продовження таблиці 6.1

З.1.9	Нестача ресурсів	Нестача ресурсів центрального процесору, оперативної пам’яті, місця на жорстких дисках, перепускної здатності каналів передачі даних. Може призводити до втрати та перекручення інформації, доступності ресурсів ЗВІД-ФАРЛЕП, непрацездатності компонентів ЗВІД-ФАРЛЕП та окремих технічних засобів.	Технічні засоби ЗВІД-ФАРЛЕП, носії інформації	Технічні засоби ЗВІД-ФАРЛЕП, Ad1-Ad3, Us	-	Помилкове конфігурування, неконтрольоване використання ресурсів	Відсутність квот на використання обчислювальних ресурсів, відсутність моніторингу використання ресурсів та заходів оперативного реагування на їх пере-вантаження.	Ц, Д, С
З.1.10	Навмисне пошкодження або крадіжка обладнання	Навмисний вивід з ладу обладнання, що може призвести до тимчасової або повної непрацездатності компонентів ЗВІД-ФАРЛЕП, крадіжка технічних засобів ЗВІД-ФАРЛЕП, що може мати як наслідок простій ЗВІД-ФАРЛЕП, розголошення технологічної інформації захисту (ТІЗ). Може проявлятися за можливості безпосереднього доступу до обладнання.	Технічні засоби ЗВІД-ФАРЛЕП	Ad1-Ad3, Us, Tp1	Деструктивні дії, що можуть призвести до пошкодження обладнання	-	Відсутність контролю доступу до приміщень, недостатня роз’ясню-вальна робота з персоналом, недостатність заходів при наданні допуску до роботи зі ЗВІД-ФАРЛЕП	К, Ц, Д, С

Продовження таблиці 6.1

З.1.11	Випадкове пошкодження обладнання	Ненавмисний вивід з ладу обладнання, що може призвести до тимчасової або повної непрацездатності компонентів ЗВІД-ФАРЛЕП. Може проявлятися за можливості безпосереднього доступу до обладнання.	Технічні засоби ЗВІД-ФАРЛЕП	Ad1-Ad3, Us, Tp1	-	Недостатня кваліфікація користувачів	Відсутність контролю доступу до приміщень, відсутність чіткого розмежування обов'язків користувачів ЗВІД-ФАРЛЕП, недостатня роз'яснювальна робота з персоналом, недостатність заходів при наданні допуску до роботи зі ЗВІД-ФАРЛЕП	Ц, Д

Додаток Г. Загрози інформації, що можуть виникнути під час мережевої взаємодії

Таблиця 6.2

Загрози інформації, що можуть виникнути під час мережевої взаємодії в ЗВІД-ФАРЛЕП

Ідентифікатор загрози	Назва загрози	Опис загрози та можливі наслідки реалізації	Об'єкти загрози	Суб'єкт загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використов	Тип загрози
1	2	3	4	5	6	7	8	9
З.2.1	Відсутність фізичного з'єднання	Створення з'єднань, що не відповідають проектній документації і/або приводять до порушення функціонування мережі. Порушення працездатності мережі внаслідок фізичного розз'єднання мережевих кабелів і/або вимкнення каналоутворюючого облад-нання, що може призвести до втрати пакетів	Кабельна система, мережеве обладнання	Ad1-Ad3, Тр1	Зловмисні дії з перекомутації кабелів та обладнання	Помилки при проектуванні, не передбачена проектом модернізація кабельної мережі, відсутність необхідної документації або її неадекватність	Відсутність контролю доступу до приміщень та обладнання, недостатня роз'яснювальна робота з персоналом	Ц, Д, С
З.2.2	Помилки та непрацездатність активного мережевого обладнання (АМО)	Помилкове функціонування мережі внаслідок помилок програмної або апаратної конфігурації АМО або помилок програмного забезпечення АМО. Загроза може мати місце при проектуванні, експлуатації та модернізації ЗВІД-ФАРЛЕП.	Комутатори, маршрутизатори, засоби мережевого захисту	Ad1-Ad3	Зловмисні дії порушника, спрямовані на зміну конфігурації захисту з метою отримання доступу	Неправильна конфігурація активного мережевого обладнання, недостатня кваліфікація мережевих адміністраторів	Відсутність політики мережевої безпеки, недостатньо глибоке проведення випробувань мережі, відсутність перевірок конфігурацій	К, Ц, Д, С

Продовження таблиці 6.2

3.2.3	Розголошення даних про мережу	Розголошення ТІЗ мережі, що є наслідком мережевої розвідки - збору інформації про мережу за допомогою загальнодоступних та спеціальних застосувань. На рівні мережі збирається інформація про структуру мережі, наявні сегменти мережі, хости. На рівні АМО збирається інформація про мережеві конфігурації та протоколи (зокрема, схему IP-адресації). На рівні хостів збирається інформація про відкриті порти, встановлене програмне забезпечення. На рівні застосувань збирається інформація про наявні вразливості.	ТІЗ АМО, хостів (робочих станцій та серверів)	Ad1-Ad3, Us	Застосування штатних програмних засобів для аналізу продуктивності та функціональності мере-жі (trace, ping, nslookup), спеціалізо-ваних засобів пошуку вразливостей (XSpider, Retina, Nessus, SATAN, Portscanner, тощо)	Помилки конфігурації мережевих засобів захисту, відсутність контролю за діями гостьових користувачів, використання незахищених протоколів керування	Вразливості мережевих протоколів (ICMP, протоколи динамічної маршрутизації, SNMP. Telnet), відсутність або недостатність мережевих засобів захисту, моніторингу мережевих подій та оперативного реагування, відсутність правил розповсюдження і використання ПЗ, недостатнє розмежувавння доступу на рівні віртуальних локальних мереж	К, С

Продовження таблиці 6.2

З.2.4	Перехоп-лення (сніферін г) пакетів	Розголошення ТІЗ, що є наслідком перехоплення мережевих пакетів (сніферингу). Сніфер пакетів являє собою прикладну програму, яка використовує мережеву карту, що працює в режимі promiscuous mode (у цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє застосуванню для обробки). При цьому сніфер перехоплює всі мережеві пакети, що передаються через розпо-ділене середовище. На кому-таторах сніферінг є малоефек-тивним в силу того, що пакети направляються лише на ті порти, яким дані пакети призначені. Проте за допо-могою спеціалізованих програмних утиліт, комутатор можна змусити спрямовувати всі пакети на всі порти у broadcast домені.	ТІЗ АМО, хостів (робочих станцій та серверів), дані, що переда-ються мережею	Ad1-Ad3, Us, адміністрат ори мережі оператора передачі даних (МОПД)	Навмисне підключен ня до каналів передачі даних, застосува ння сніферів та аналізатор ів пакетів (tcpdump, ethereal, Sniffer Pro, CAIN)	Помилки конфігурації мережевих засобів захисту, використання мережевих застосувань, що передають дані в незахищеному вигляді, апаратні збої	Вразливість мережевих протоколів (802.1Q, ARP), відсутність або недостатність мережевих за-собів захисту, моніторингу мережевих подій та опе-ративного реагування, відсутність правил роз-повсюдження і використання ПЗ, недостат-ність системи мережевої автентифікації	К, С

Продовження таблиці 6.2

3.2.5	Підміна отримувача (спуфінг пакетів)	Втрата даних внаслідок спуфінгу. Це відбувається, коли зловмисник, що знаходиться усередині ЗВІД-ФАРЛЕП або поза нею, видає себе за іншого користувача. В першому випадку, зловмисник може скористатися IP-адресою, що знаходиться в межах чужого діапазону санкціонованих IP-адрес, або авторизованою зовнішньою адресою, якій дозволяється доступ до визначених мережевих ресурсів. Атаки IP-спуфінгу часто є відправною точкою для інших атак (наприклад, DoS-атака, див. 3.2.6). Зазвичай IP-спуфінг обмежується вставкою помилкової інформації або шкідливих команд у звичайний потік даних, переданих між клієнтським і серверним застосуванням або каналами зв'язку між одноранговими пристроями.	АМО, хости (робочі станції, сервери)	Ad1-Ad3, Us	Застосування штатних програмних засобів для встановлення IP-адреси, генератори пакетів, що дозволяють формувати довільні заголовки пакетів	Помилки конфігурування АМО, розголошення інформації про карту мережі та схему адресації (див. 3.2.4)	Вразливості мережевих протоколів (ARP, протоко-ли динамічної маршрутизації), відсутність або недостатність мережевих засобів захисту, моніторингу мережевих подій та оперативного реагування, відсутність правил розпов-сюдження і використання ПЗ, недостатність системи мережевої автентифікації	Ц, Д, С

Продовження таблиці 6.2

3.2.6	Відмова в обслуговуванні (DoS)	Атака Denial of Services (DoS) робить мережу або окремі сервіси мережі недоступними для звичайного використання за рахунок перевищення припустимих параметрів функціонування мережі, ОС або застосування. У випадку DoS-атаки на мережу результатом є надмірне перевантаження каналів зв'язку, що призводить до блокування всіх сервісів у певному сегменті . У випадку використання серверних застосувань на хостах (таких як web-сервер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих застосувань, і тримати їх у зайнятому стані, не допускаючи обслуговування звичайних користувачів. У випадку комутаторів об'єктом DoS-атаки є такі характеристики обладнання як максимальний обсяг таблиці	АМО, хости (робочі станції, сервери), програмне забезпечення	Us	Застосування спеціальних генераторів пакетів, ураження вірусами, шкідливим ПЗ	Недостатність ресурсів обчислювальних та комунікаційних систем, неправильна конфігурація АМО та мережевих засобів захисту	Вразливості застосувань, відсутність або недостатність мережевих засобів захисту, вразливості мережевих протоколів (802.1Q, ARP, ICMP, протоколи динамічної маршрутизації)	Д, С

Продовження таблиці 6.2

3.2.7	Дзеркалю ва-ння трафіку	Для дзеркалювання трафіку (атаки типу Man-in-the-Middle) зловмиснику потріб-ний доступ до пакетів, переданим по мережі. Атака може бути проведена як через спуфінг пакетів, так і переналаштуванням комутаторів. Зловмисник може підключитися до SPAN-порту комутатора та віддзеркалювати трафік на потрібний хост з метою його подальшого аналізу за допомогою аналізаторів пакетів. Атаки проводяться з метою крадіжки інформації, пере-хоплення поточної сесії й одержання доступу до приватних мережевих ре-сурсів, для аналізу трафіку й одержання інформації про мережу і її користувачів, для проведення атак типу DoS, перекручування переданих даних і введення несанкціонованої інформації в мережеві сесії.	ТІЗ хостів (робочих станцій, серверів), дані, що передають-ся мережею	Ad1-Ad3, Us	Використа ння спуфінгу па-кетів (див. 3.2.5), пере-конфігуру ва-ння комута-торів та під-ключення до SPAN-порту	Помилки конфігурації мережевого обладнання АМО, недостатня кваліфікація адміністратора ЗВІД-ФАРЛЕП	Відсутність контролю доступу до приміщень, обладнання та каналів зв’язку, вразливість мережевих протоколів (802.1Q, ARP, ICMP, протоколи динамічної маршрути-зації)	К, Ц, С

Продовження таблиці 6.2

З.2.8	Непрацездатність мережевих застосувань	Атаки на рівні застосувань можуть проводитися декількома способами. Найпоширеніший з них полягає у використанні добре відомих вразливостей серверного ПЗ. Використовуючи дані вразливості, зловмисники можуть одержати доступ до комп'ютера від імені користувача (адміністратора), що працює із застосуванням. На рівні сервісів атаки можуть проводитися по відношенню до поштових серверів, DNS-серверів, серверів БД.	Прикладне ПЗ, слабота сильнозв'язані об'єкти	Ad1-Ad3, Us	Застосування спеціалізованих хакерських утиліт, генераторів пакетів, ураження вірусами, шкідливим ПЗ	-	Помилки при реалізації та конфігуруванні прикладного ПЗ, вразливості мережевих протоколів (UDP, DNS), відсутність або недостатність мережевих засобів захисту, недостатнє розмежуавння доступу на рівні віртуальних локальних мереж	К, Ц, Д, С
З.2.9	Створення альтернат-тивних несанкціо-нованих точок доступу до мережі	Існує можливість додзвону на модеми, що несанкціоновано підключені користувачами до робочих станцій	Прикладне та системне ПЗ, слабкозв'язані об'єкти, обчислювальні ресурси	Ad1-Ad3, Us, Tp1	-	Наявність широких повноважень користувачів робочих станцій	Відсутність контролю підключення зовнішніх пристроїв	К, Ц, С

Додаток Д. Загрози інформації, що можуть виникнути під час роботи з прикладним ПЗ

Таблиця 6.3

Загрози інформації, що можуть виникнути під час роботи з прикладним ПЗ в межах ЗВІД-ФАРЛЕП

Іденти-фікатор загрози	Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкт загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використов	Тип загрози
1	2	3	4	5	6	7	8	9
З.3.1	Помилка, збій та відмова прикладного ПЗ	Помилки та відмови прикладного ПЗ, що можуть виникати внаслідок непра-вильних налаштувань ПЗ, помилок розробників ПЗ, невідповідності системним вимогам тощо (ненавмисна загроза). Це може призводи-ти до втрати чи перекручення даних, відмови системного ПЗ та виходу з ладу компонентів ЗВІД-ФАРЛЕП, надмірного використання обчислю-вальних ресурсів.	Прикладне та системне ПЗ, слабко- та сильно-зв’язані об’єкти, обчислюва льні ресурси	Прикладне та системне ПЗ, зовнішнє середовищ е, Ad1-Ad3, Us	Вірусна атака	Використання неліцензійного та нерегламентованог о ПЗ, помилки при інсталяції та конфігуруванні ПЗ, недостатні періоди тестування ПЗ перед впровадженням у промислову експлуатацію	Відсутність або недостатність антивірусного захисту, порушення процедур інсталяції та використання ПЗ	К, Ц, Д, С
З.3.2	Виконанн я недоку-ментован их функцій	Маскування всередині коду модулів прикладного ПЗ програмних закладок, що здатні перехоплювати технологічну інформацію та здійснювати цілий ряд несанкціонованих операцій. Зазвичай закладка слугує відправною точкою для реалізації інших загроз.	ТІЗ робочих станцій та серверів, слабко- та сильно-зв’язані об’єкти	Ad1-Ad3	Навмисне впровадж ення шкідливог о коду в прикладне ПЗ	Використання неліцензійного та нерегламентованог о ПЗ, недостатні періоди тестування ПЗ перед впровадженням у промислову експлуатацію	Відсутність контролю аномальної поведінки ПЗ	К, Ц, С

Продовження таблиці 6.3

З.3.3	Розповсю д-ження вірусів та хробаків	Ураження і/або пошкодження файлів прикладного ПЗ (в т.ч. файлів журналів) комп'ютерними вірусами та хробаками. Може здійснюватися як навмисно, так і ненавмисно. Ураження вірусами може викликати втрату чи перекручення даних, неконтрольоване використання обчислювальних ресурсів, ініціювати помилки у ПЗ, збої та непрацездатність серверів, робочих станцій та інших компонентів ЗВІД-ФАРЛЕП.	ТІЗ робочих станцій та серверів, сильно-зв'язані та слабо-зв'язані об'єкти, системне і прикладне ПЗ, обчислюва льні ресурси	Ad1-Ad3, Us	Навмисне впровадж ення шкідливог о ПЗ всередині мережі, надсиланн я уражених вірусами поштових повідомле нь	Використання зовнішніх носіїв інформації	Неефектив-ність засобів антивірусного захисту, несвоєчасне оновлення антивірусних баз, відсутність або порушення інструкцій щодо анти-вірусного захисту, протидії вторгненням, захисту поштових сервісів	К, Ц, Д, С
З.3.4	Несуміс-ність версій ПЗ	Несумісність різних версій/типів ПЗ, що може спричинити збої в роботі прикладних АС, загрози цілісності та доступності інформації.	Системне і прикладне ПЗ	Ad1-Ad3, прикладне ПЗ	-	Помилки розробників та адміністраторів ЗВІД-ФАРЛЕП	Відсутність системи керування оновленнями та контролю версій	Ц, Д

Продовження таблиці 6.3

З.3.5	Перехоплення ТІЗ	Підглядання атрибутів доступу, автоматичний підбір паролів за допомогою спеціалізованих програмних засобів (закладки типу „троянський кінь” – див. З.3.2, З.3.3), перехоплення логінів і паролів за допомогою перехоплювачів клавіатури (keyloggers)	ТІЗ робочих станцій і серверів	Us-Us3, Тр1	Підглядання, впровадження програмних та апаратно-програмних перехоплювачів клавіатури	Необхідність введення атрибутів доступу у відкритому вигляді, недбалість користувачів ЗВІД-ФАРЛЕП	Порушення політики безпеки щодо розповсюдження паролів (використання тривіальних паролів), відсутність контролю за встановленням ПЗ та обладнання	К, С
З.3.6	Підміна або дезорганізація	Порушення цілісності ПЗ внаслідок підміни елементів програм, динамічних бібліотек, модулів ПЗ, даних аудиту, або дезорганізації структури ПЗ. Може викликати непрацездатність ЗВІД-ФАРЛЕП або її компонентів, перекручення даних.	Прикладне ПЗ	Ad1-Ad3, Us	Зловмисні дії щодо порушення цілісності ПЗ	Неблокування робочих станцій під час відсутності користувачів, недбалість користувачів ЗВІД-ФАРЛЕП	Недостатній контроль цілісності ПЗ, порушення правил розмежування доступу, недостатність аудиту подій	Ц, Д, С
З.3.7	Злам	Обхід чи злам механізмів захисту шляхом аналізу програмного коду за допомогою спеціалізованих програмних засобів з подальшим несанкціонованим отриманням доступу до даних та конфігур.	ТІЗ робочих станцій, прикладне ПЗ	Us	Дизасемблювання ПЗ	-	Відсутність правил розповсюдження і використання ПЗ, порушення правил розмежування доступу	К, Ц, С

Додаток Е. Загрози інформації, що можуть виникати в мережевих ОС

Таблиця 6.4

Загрози інформації, що можуть виникати в мережевих ОС ЗВІД-ФАРЛЕП

Іденти-фікатор загрози	Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкт загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використов	Тип загрози
1	2	3	4	5	6	7	8	9
З.4.1	Помилка, збій та відмова системного ПЗ	Помилки та відмови системного ПЗ, що можуть виникати внаслідок неправильних налаштувань ОС, помилок розробників ОС, невідповідності системним вимогам (ненавмисна загроза). Це може призводити до втрати чи перекручення даних, відмови прикладного ПЗ та виходу з ладу компонентів ЗВІД-ФАРЛЕП, надмірного використання обчислювальних ресурсів.	Прикладне та системне ПЗ, слабозв’язані об’єкти, обчислювальні ресурси	Системне ПЗ, зовнішнє середовище, Ad1-Ad3, Us	Вірусна атака, застосування шкідливого ПЗ	Використання неліцензійного та нерегламентованого ПЗ, помилки при інсталяції та конфігуруванні ОС	Відсутність або недостатність антивірусного захисту, порушення процедур інсталяції та використання ОС, відсутність правил розповсюдження і використання ПЗ	К, Ц, Д, С
З.4.2	Перехоплення ТІЗ	Підглядання атрибутів доступу, автоматичний підбір паролів за допомогою спеціалізованих програмних засобів (закладки типу „троянський кінь” – див. З.3.2, З.3.3, З.3.5), перехоплення логінів і паролів за допомогою перехоплювачів клавіатури (keyloggers)	ТІЗ робочих станцій і серверів	Us, Тр1	Підглядання, впровадження програмних та апаратно-програмних перехоплювачів клавіатури	Необхідність введення атрибутів доступу у відкритому вигляді, недбалість користувачів ЗВІД-ФАРЛЕП	Порушення політики безпеки щодо розповсюдження паролів, від-сутність конт-ролю за встановленням ПЗ та обладнання	К, С

Продовження таблиці 6.4

З.4.3	Пошкодже-ння файлів ОС	Порушення цілісності файлів системного ПЗ (в т.ч. системних журналів) внаслідок необережності або навмисних дій.	ТІЗ робочих станцій і серверів, системне ПЗ	Ad1-Ad3, Us, прикладне ПЗ	Вірусна атака, використання нерегламентованого ПЗ	Неблокування серверу або робочої станції під час відсутності користувачів, недбалість користувачів	Недостатність антивірусного захисту, недос-татній конт-роль цілісності, порушення правил розме-жування досту-пу, недостат-ність аудиту подій, відсут-ність резерв-ного копіюван-ня системних файлів	Ц, Д, С
З.4.4	Збирання «сміття»	Відновлення знищеної користувачем або сеансової інформації (так званого «сміття») шляхом аналізу тимчасових каталогів ОС, оперативної пам’яті, тощо.	ТІЗ робочих станцій і серверів, слабо-зв’язані об’єкти	Ad1-Ad3, Us	Несанкціо-нований отримання фізичного доступу до робочих станцій, застосування спеціалізо-ваного ПЗ	Використання функції fast user switching, неблокування робочої станції під час відсутності користувачів	Відсутність контролю дос-тупу до примі-щень, відсут-ність правил розповсюд-ження і вико-ристання ПЗ, порушення правил розмежування доступу	К, С

Продовження таблиці 6.4

З.4.5	Втручання в роботу ОС з мережі	Зовнішнє втручання в роботу з боку інших користувачів ОС, що спричиняє загрози керова-ності, цілісності, доступності, а також конфіденційності ТІЗ. Зловмисник може використовувати як відомі вразливості ОС, так і штатні засоби комунікацій.	ТІЗ робочих станцій і серверів, слабо-зв’язані об’єкти, прикладне і системне ПЗ	Ad1-Ad3, Us	Застосування спеціалізо-ваного ПЗ, засобів віддаленого доступу ОС (Remote Desktop)	Розподілення та спільне використання ресурсів в рамках мережі	Наявність відкритих не-задіяних мере-жевих портів, відсутність або недостатність захисту від ме-режевих загроз, недосконаліст ь доменної полі-тики ОС, не-достатнє роз-межування доступу на рівні віртуаль-них локальних мереж, відсут-ність системи контролю і розповсюд-ження онов-лень ОС, існу-ючі вразлив-ості ОС	К, Ц, Д, С