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

Кваліфікаційна наукова
праця на правах рукопису

КОМАРОВ Максим Юрійович

УДК 004.056.5:005:004.3:004.4

ДИСЕРТАЦІЯ

МЕТОД ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРВПЛИВІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.05 – «Комп'ютерні системи та компоненти»

Галузь знань – інформаційні технології

Подається на здобуття наукового ступеня кандидата технічних наук

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

_____ М.Ю. Комаров

Науковий керівник: Гончар Сергій Феодосійович, доктор технічних наук, старший дослідник

Київ – 2021

АНОТАЦІЯ

Комаров М.Ю. Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2021.

Дисертаційна робота присвячена підвищенню рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації.

Проаналізовано сучасні методи та засоби моніторингу, виявлення та протидії кіберзагрозам інформаційно-телекомунікаційних систем. Показано, що забезпечення кіберзахисту інформаційних мереж підприємства електроенергетики при реалізації заходів протидії сучасним кіберзагрозам є невід'ємною частиною політики безпеки інформації підприємств енергетичної галузі. Аналізуючи загальні загрози безпеці інформації при розробці політики безпеки на підприємстві енергетичного сектору, необхідно враховувати специфіку його функціонування, а також брати до уваги технологічну та функціональну специфіку обробки інформації, що циркулює на відповідних об'єктах інформаційної діяльності.

Проаналізовано основні вразливості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури, удосконалено основні підходи до захисту від кіберзагроз інформаційно-телекомунікаційних мереж об'єктів критичної інфраструктури, а також розроблено класифікацію кіберзагроз інформаційно-телекомунікаційним мережам об'єктів критичної інфраструктури.

Розроблено таксономію кіберзагроз інформаційно-телекомунікаційним мережам об'єктів критичної інфраструктури. У запропонованій таксономії розвивається комбінований підхід до вирішення задачі класифікації. Однак

на відміну від попередніх робіт вводиться ієрархічна структура відносин з деревовидним розкриттям категорій. Як самостійний окремий об'єкт вводиться важливе поняття «етап атаки», що дозволяє, на відміну від попередніх підходів, досить природним чином описувати багатоетапні атаки, які на сьогоднішній день отримали дуже широку розповсюдженість.

Складено матрицю залежності інформаційних об’єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз.

Розроблено модель бази даних кіберзагроз інформаційним об’єктам захисту інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури.

Розроблено універсальний інструментарій, що включає у себе набір методів та засобів забезпечення стійкої кібербезпеки інформаційних об’єктів захисту інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури від якомога широкого кола загроз інформації.

Ключові слова: захист інформації, кібервплив, комп’ютерна система, мережа, кібербезпека, інформаційна система, об’єкт критичної інфраструктури.

ABSTRACT

Komarov M. Method and means of protecting information from cyber influences in computer systems and networks of critical infrastructure objects. – Manuscript.

Thesis for a Candidate of Technical Sciences degree in specialty 05.13.05 «Computer systems and components». – Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertations are assigned to the advancement of information on the basis of cyber fuels in computer systems and systems of critical information infrastructure, a gateway to the gateway of such an information method.

Analyzed the current methods for monitoring, detecting and countering cyber threats to information and telecommunication systems. It is shown that the cyber defense of the information network of the electric power industry in the course of the implementation of calls in against the current cyberthreats and the inadequate part of the policy of the information security. Analyze the external contamination without special information when developing the security policy for the energy sector, it is necessary to ensure the specifics of its function, as well as to respect the technological and functional specifics.

The main vulnerabilities of information and telecommunication systems of critical infrastructure objects are analyzed, the main approaches to protection against cyber threats of information and telecommunication networks of critical infrastructure objects are improved, and the classification of cyber threats to information and telecommunication networks of critical infrastructure objects is developed.

A taxonomy of cyber threats to information and telecommunication networks of critical infrastructure facilities has been developed. The proposed taxonomy develops a combined approach to solving the problem of classification. However, in contrast to previous works, a hierarchical structure of relations with a tree-like disclosure of categories is introduced. As an independent individual object, the important concept of "attack stage" is introduced, which allows, in contrast to previous approaches, to describe quite naturally multi-stage attacks, which today have become very common.

A matrix of dependence of information objects of protection on the type of potential threats that may affect them and susceptibility to specific threats.

The model of the database of cyberthreats to information objects of protection of information and telecommunication systems of objects of critical infrastructure is developed.

A universal toolkit has been developed, which includes a set of methods and means of ensuring sustainable cybersecurity of information objects to protect information and telecommunication systems of critical infrastructure objects from

the widest possible range of information threats.

Keywords: information protection, cyber influence, computer system, network, cybersecurity, information system, critical infrastructure object.

Список публікацій здобувача:

1. М. Комаров, С. Гончар, «Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури», *Національна академія наук України. Інститут проблем моделювання в енергетиці. Моделювання та інформаційні технології. Збірник наукових праць. Випуск 81, С. 12-19, 2017.*
2. 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.*
3. М. Комаров, С. Гончар, «Аналіз та дослідження загроз для захищеного вузлу Інтернет доступу», *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 29 (68). № 4, 2018. С. 165 - 168.*
4. 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.*
5. М. Комаров, «Підсистема управління доступом системи управління базами даних ORACLE DATABASE 12C ENTERPRISE EDITION», *Моделювання та інформаційні технології, №84, С. 87-96, 2018.*
6. 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.*

7. М. Комаров, «Загальні характеристики підприємства електроенергетики і елементи їх вразливості технологічного походження», *Електронне моделювання. Том 41. 1. С. 93 – 104 2019.*
8. М. Комаров, «Огляд кібератак на об’єкти критичної інфраструктури», *Національна академія наук України. Інститут проблем моделювання в енергетиці. Електронне моделювання. Т 41 № 6, 2019, С. 91 – 106.*
9. M. Komarov, A. Davydiuk, A. Onyskova, V. Tkachenko, S. Honchar “Critical Infrastructure Facilities and Analysis of Existing Approaches” *Studies in Systems, Decision and Control in Energy I. vol. 346, p. 189-205.*
10. М. Комаров «Особливості оцінки рівня гарантій Г-3 коректності реалізації функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу», *Безпека інформації в інформаційно-телекомунікаційних системах: Міжнар. наук.-практ. конф., 2015, Київ, 2015, С. 52-53.*
11. М. Комаров, С. Гончар, Г. Леоненко, «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.*
12. М. Комаров, С. Гончар, «Практичні аспекти побудови комплексної системи захисту інформації», *Кібербезпека енергетики: Наук.-практ. конф., 2018, м. Одеса.*
13. М. Комаров, С. Гончар, «Застосування систем управління інформаційною безпекою на об’єктах критичної інфраструктури», *Інформаційна безпека України: Наук.-практ. конф. 2018, м. Київ.*
14. 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.*
15. В. Ткаченко, М. Комаров, «Основні підходи оцінювання ризиків інформаційної безпеки», *Комп’ютерні системи та мережні технології: конф., Київ, 2019.*

16. 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.*
17. М. Комаров, «Аналіз шкідливого програмного забезпечення, як кіберзброї, та методи протидії кібератакам», *Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн: конф., Житомир, 2019, С. 235 – 238.*
18. М.Ю. Комаров, А.В. Оніськова, С.Ф. Гончар, В.В. Ткаченко, С.М. Сергєєв «Розробка бази даних кіберзагроз об’єктів критичної інформаційної інфраструктури», *Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: XXXVIII наук-техн. конф. молодих вчених, Київ, 2020, С. 30 – 32.*
19. В.В. Ткаченко, М.Ю. Комаров, С.М. Сергєєв «Основні підходи до оцінки кібербезпеки SMART GRID систем» *Європейський університет, Національний авіаційний університет: Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна наук-практ. конф., Київ 2020, С. 99 – 104.*
20. М. Комаров, С. Гончар, А. Ониськова «Дослідження актуальних проблем забезпечення кібербезпеки Об’єднаної енергосистеми України в рамках впровадження концепції інтелектуальних мереж», *Матеріали Другої науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», Київ, 2020, С. 11.*
21. 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.
22. Мохор В.В., Гончар С.Ф., Комаров М.Ю., Чьочь В.В. База даних «Кіберзагрози об’єктів критичної інформаційної інфраструктури Об′єднаної енергосистеми України». *Свідоцтво про реєстрацію авторського права на твір № 95314 від 14.01.2020.*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АБД – адміністратор баз даних

АІС ЦБД ПН – автоматизована інформаційна система «Централізована база даних перенесених номерів»

АС – автоматизована система

АСУ ТП - автоматизована система управління технологічними процесами

БД – база даних

ДІВ – деструктивні інформаційні впливи

ДП – державне підприємство

ДСТУ – державний стандарт України

ЕОМ – електронно-обчислювальна машине

ЄС – Європейський союз

ІС – інформаційна система

ІТКМ ЗК – інформаційно-телекомунікаційна мережа загального користування

ІТС – інформаційно-телекомунікаційна система

КВ – кібервпливи

КЗ – контрольована зона

КЗЗ – комплекс засобів захисту

КІ – критична інфраструктура

КІВ – керуючі інформаційні впливи

КІІ – критична інформаційна інфраструктура

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації

НД – нормативний документ

ОЕС - Об’єднана енергетична система

ОЦОД – основний центр обробки даних

ОС – операційна система

ПЗ – програмне забезпечення

ППН – процес перенесення номерів

РС – робоча станція

РЦОД – резервний центр обробки даних

СУБД – система управління базами даних

СУІБ – система управління інформаційною безпекою

ТЗ – технічне завдання

ТЗІ – технічний захист інформації

ЦОД – центр обробки даних

ШПЗ – шкідливе програмне забезпечення

IEC – International Electrotechnical Commission

ISO – International Organization for Standardization

SCADA – Supervisory Control And Data Acquisition (система диспечерського управління і збору даних)

FTP – File Transfer Protocol

SMTP – Simple Mail Transfer Protocol

POP3 – Post Office Protocol Version 3

ICMP – Internet Control Message Protocol

TCP – Transmission Control Protocol

IP – Internet Protocol

HTTP - HyperText Transfer Protocol

IDS – Intrusion Detection Systems

CERT – Computer Emergency Response Team

CVE – Common Vulnerabilities an Exposures

EMS – Energy Management System

SQL – Structured Query Language

DPI – Deep Packet Inspection

UDP – User Datagram Protocol

ВСТУП

Актуальність. Події останніх років в Україні та світі показали нагальну потребу у забезпеченні інформаційної безпеки від кібервпливів комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури України в цілому та енергетичної галузі зокрема. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» (ст. 4) об'єктами кібербезпеки, серед іншого, є об'єкти критичної інфраструктури. Згідно зі статтею 6 цього ж закону Об'єктами критичної інфраструктури є підприємства, установи та організації незалежно від форми власності, які:

- провадять діяльність та надають послуги в галузі енергетики;
- надають послуги у сферах життєзабезпечення населення, зокрема у сфері постачання електричної енергії.

Згідно зі ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» функціонування національної системи кібербезпеки забезпечується, в тому числі, шляхом встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури.

Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» визначає Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури. Відповідно до п. 12 цієї Постанови організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури, серед іншого, повинні забезпечувати мережевий захист компонентів та інформаційних ресурсів об'єкта.

З огляду на вищезазначене тема роботи присвячена розробці методу та засобів захисту інформації від кібервпливів в комп'ютерних системах та

мережах об’єктів критичної інфраструктури.

Дослідженню проблем, пов’язаних із процесом захисту інформації від кібервпливів в комп’ютерних системах та мережах об’єктів критичної інфраструктури, що являється об’єктом дисертаційного дослідження присвячується значна частина публікацій вітчизняних і зарубіжних вчених, таких як: О. Корченко, С. Казмірчук, О. Архіпов, С. Гнатюк, О. Богданов, L.Daniel, Attanasio C. R., Markstein P. W., Phillips R. J. 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 основних положень дослідження пов’язана з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки», «Планом проведення ДержНДІ Спецзв’язку науково-дослідних та дослідно-конструкторських робіт за основними напрямами науково-технічної діяльності Держспецзв’язку в 2018 році (Зведений тематичний план. Частина 2)» №01/02/02-96т від 02.03.2018, «Планом проведення ДержНДІ Спецзв’язку науково-дослідних та дослідно-конструкторських робіт за основними напрямами науково-технічної діяльності Держспецзв’язку в 2019 році (Зведений тематичний план. Частина 2)» №01/02/02-117т від 27.03.2019, Стратегією національної безпеки України від 26.05.2015 № 287/2015, Стратегією кібербезпеки України від 15.03.2016 № 96/2016 та низкою науково-дослідних робіт. Результати досліджень відображені у звітах наступних науково-дослідних робіт: «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), в яких здобувач був виконавцем окремих розділів.

Мета та задачі дослідження. Метою дисертаційного дослідження є підвищення рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації.

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

- проаналізувати сучасні методи та засоби захисту інформації в комп'ютерних мережах та системах;
- розробити таксономію інформаційних загроз комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;
- скласти матрицю залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз;
- розробити модель бази даних загроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;
- розробити метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури
- розробити методику оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури;
- розробити структурну модель багаторівневої системи виявлення підозрілих впливів на ком'ютерні мережі та системи об'єктів критичної інформаційної інфраструктури;
- розробити алгоритм та програмний застосунок розрахунку кіберстйкості об'єктів критичної інформаційної інфраструктури.

Об'єктом дослідження є процеси захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури.

Предметом дослідження є методи та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної

інфраструктури.

Методи дослідження. Методи дослідження, що використовуються в роботі, базуються на методологічному базисі теорії захисту інформації та системному аналізі новітніх теоретичних та практичних розробок, що застосовуються в галузі інформаційної безпеки для ефективного вирішення відповідних проблем кібербезпеки. При складанні матриці залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз, використовувались елементи теорії ймовірності і випадкових процесів. При розробці моделі бази даних кіберзагроз інформаційним об'єктам захисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури, використовувались засоби об'єктно-орієнтовного програмування та система керування базами даних SQL Server. При розробці універсального інструментарію, що включає у себе набір методів та засобів забезпечення стійкої кібербезпеки інформаційних об'єктів захисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури від якомога широкого кола загроз інформації, застосовувались елементи теорії алгоритмів, експерименту, об'єктно-орієнтоване програмування, а також імітаційне моделювання інформаційних процесів і структур. Методи дослідження застосовані коректно. Достовірність теоретичних результатів перевірена експериментально. Результати моделювання добре узгоджуються з отриманими експериментальним шляхом.

Наукова новизна одержаних результатів полягає в тому, що:

– *вперше* розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання ієрархічної структури відносин з деревовидним розкриттям категорій, дозволяє описувати багатоетапні атаки, які на сьогоднішній день отримали дуже широку розповсюдженість;

– *вперше* розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної

інформаційної інфраструктури, яка за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії та параметрів властивостей інформації, що підлягає захисту, дозволяє розробити базу даних кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;

– *вперше* розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, який за рахунок поєднання сигнатурного методу та методу виявлення аномалій, дозволяє розширити спектр виявлених кіберзагроз.

Практичне значення одержаних результатів. Практична цінність роботи полягає у наступному:

– розроблено алгоритмичне забезпечення на основі запропонованого комбінованого методу розпізнавання кіберзагроз для реалізації відповідного програмного засобу, що дозволяє здійснювати атоматизоване розпізнавання кіберзагроз та здійснбвати захист від них;

– розроблено алгоритмичне забезпечення на основі запропонованої методики оцінювання кіберстійкості для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість;

– на основі запропонованих алгоритмів розроблений програмний застосунок, що використовує запропоновану методику для захисту інформації в компютерних мережах та системах обєктів критичної інфраструктури.

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

– «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).

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв’язку та захисту інформації України, Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Державного підприємства «Український державний центр радіочастот», Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, ПрАТ «Фарлеп-Інвест», ТОВ "ІНТЕСИС".

Особистий внесок здобувача. Основні положення та результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних як у співавторстві, так і самостійно, автору належать: [1, 2, 10, 12] – дослідження нормативної бази та практичних аспектів побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури; [11] – розгляд практичних аспектів побудови комплексної системи захисту інформації в інформаційно-телекомунікаційних системах об’єктів критичної інфраструктури; [3, 4, 13] – розробка моделі загроз та моделі порушника для захищеного вузлу Інтернет доступу; [7, 8] – огляд загальних характеристик об’єктів критчної інфраструктури та кібератак на об’єкти критичної інфраструктури; [5, 6, 18] – аналіз механізмів безпеки системи управління базами даних Oracle Database 12C Enterprise Edition та розробка бази даних кіберзагроз об’єктів критичної інформаційної інфраструктури; [9, 14] – аналіз та розробка деяких підходів оцінювання ризиків інформаційної безпеки; [15, 16] – основні підходи до оцінювання ризиків та методика оцінки кіберстійкості об’єктів критичної інфраструктури; [17] – аналіз шкідливого програмного забезпечення; [19, 20] – основні підходи до оцінки кібербезпеки та дослідження актуальних проблем забезпечення кібербезпеки. З робіт, опублікованих самостійно та 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 таких наукових конференціях: XVII Міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2015 р., 2018 р.); VI Міжнародна наукова конференція «Моделювання-2018» (Київ, 2018 р.); Всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019 р.); науково-практична конференція «Кібербезпека енергетики» (Одеса, 2018 р., 2019 р.); науково-технічна конференція «Інформаційна безпека України» (Київ, 2018р.); XII Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 2019 р.); всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019); науково-практична конференція «Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн» (Житомир, 2019р.), науково-практична конференція «Безпека енергетики в епоху цифрової трансформації» (Київ, 2020 р.).

Публікації. Основні положення дисертаційного дослідження опубліковано у 22 наукових працях, у тому числі: 9 наукових статей у наукових журналах та збірниках наукових праць [1-9], з яких 4 наукові статі у виданнях, що входять до міжнародних баз даних [3, 4, 7, 8], 4 наукових статей у вітчизняних фахових наукових журналах та збірниках наукових праць [1, 2, 5, 6], 1 патент України на корисну модель [21], 1 свідоцтво про реєстрацію авторського права на твір [22], а також 11 матеріалів та тез доповідей конференцій [10-20].

Структура та обсяг роботи. Дисертаційна робота складається з анотації, списку скорочень, вступу, змісту, чотирьох розділів, висновків, додатків, списку використаних джерел, та містить 152 сторінки основного тексту, 22 рисунка, 17 таблиць, 18 сторінок додатків. Список використаних джерел налічує 102 найменування на 11 сторінках. Загальний обсяг дисертаційної роботи складає 171 сторінку.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРВПЛИВІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Нормативно-правове забезпечення кібербезпеки та захисту інформації в комп'ютерних системах та мережах об'єктів критичної інфраструктури

Основними нормативно-правовими документами, які регламентують питання забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури в Україні, є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017р. [23], Рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», введене в дію Указом Президента України від 15 березня 2016 року № 96 [24], 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 [25], Постанова Кабінету Міністрів України від 23.08.2016 № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [26], Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [27], Постанова Кабінету Міністрів України від 9 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» [28], Постанова Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури» [29], Постанова Кабінету Міністрів України від 11 листопада 2020 року №1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» [30], Стратегія національної безпеки України від 26

травня 2015 року № 287/2015 [31], Доктрина інформаційної безпеки України від 25 лютого 2017 року №47/2017 [32], Наказ Адміністрації Держспецзв′язку від 15 січня 2021 року № 23 «Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури» [33] та інші нормативно-правові акти.

Закон України «Про основні засади забезпечення кібербезпеки України» [23] 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 є об’єктами кібербезпеки, а об’єкти критичної інформаційної інфраструктури є 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.

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» (ст. 4) об’єктами кібербезпеки, серед іншого, є об’єкти критичної інфраструктури. Згідно зі статтею цього ж закону Обєктами критичної інфраструктури є 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.

Згідно зі ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» функціонування національної системи кібербезпеки забезпечується, в тому числі, шляхом:

- Встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;
- Залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;
- Розвитку та вдосконалення системи технічного і криптографічного захисту інформації.

Рішенням Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [24] затверджено та введено в дію Стратегію кібербезпеки України. У документі визначена мета Стратегії кібербезпеки України – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Наведено заходи для досягнення поставленої мети. У розділі 2 Стратегії наведено негативні чинники, що призводять до актуалізації загроз кібербезпеці держави. Розділ 3 Стратегії містить відомості

про призначення та завдання національної системи кібербезпеки. Також наведені функції та завдання суб'єктів забезпечення кібербезпеки, якими, зокрема, є Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Наведені основні пріоритети та напрями забезпечення кібербезпеки України. Зокрема наведені заходи, які становлять основу кіберзахисту китичної інфраструктури.

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 [25], 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 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [26], 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 інформаційнотелекомунікаційні 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 інформаційнотелекомунікаційну систему. Такими негативними наслідками є [26]:

- 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 [26].

Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [27], 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. Згідно з вимогами Постанови, які є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури, заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Відповідно до п. 12 Постанови Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» організаційні та технічні заходи з кіберзахисту, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, серед іншого, повинні забезпечувати мережевий захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури 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».

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 9 жовтня 2020 року № 943 «Деякі питання об’єктів критичної інформаційної інфраструктури» [28] розроблена у відповідності до статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» [23] та затверджує Порядок формування переліку об’єктів критичної інформаційної інфраструктури, а також Порядок внесення об’єктів критичної інформаційної інфраструктури до державного реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Постанова Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури» [29] розроблена у відповідності до статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» [23] та затверджує:

- Порядок віднесення об’єктів до об’єктів критичної інфраструктури;
- перелік секторів (підсекторів), основних послуг критичної інфраструктури держави;

– Методику категоризації об’єктів критичної інфраструктури.

Постанова Кабінету Міністрів України від 11 листопада 2020 року №1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» [30] розроблена у відповідності до статті 27 Закону України «Про національну безпеку України» та затверджує Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Цей Порядок визначає організаційні засади проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. У Порядку наведені такі терміни: «життєво важливі послуги та функції (основні послуги)», «кіберстійкість критичної інформаційної інфраструктури», «суб’єкт критичної інформаційної інфраструктури» та інші. Також у Прядку наведено мету, задля якої здійснюється огляд стану кіберзахисту, завдання, які мають бути вирішені під час огляду, принципи, на яких ґрунтується проведення огляду, а також результати заходів, на підставі яких здійснюється огляд стану кіберзахисту критичної інформаційної інфраструктури. Визначені суб’єкти та об’єкти огляду стану кіберзахисту критичної інформаційної інфраструктури. Наведено основні етапи огляду та заходи, які реалізуються під час виконання кожного етапу.

Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 [31], 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 [32] 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 інформаційнокомунікаційних 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 завдання 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.

Аналіз відкритих джерел показує, що наряду з такими важливими питаннями забезпечення захисту інформації від кібервпливів на об’єктах критичної інфраструктури, як визначення актуальних загроз безпеці інформації [3, 4, 14, 17, 18, 22, 34 – 37, 39 – 43] та оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури [15, 44 – 63], не менш важливими є питання розробки сучасних методів та засобів захисту інформації [1, 2, 10, 12, 19, 21, 64 – 66, 81, 84 – 86, 89, 90, 94 – 50].

1.2. Аналіз існуючих робіт та можливі підходи щодо таксономії загроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури

Кількість комп'ютерних атак, що постійно збільшується, призводить до необхідності створення організованих (або таких, що здатні самоорганізовуватись) структур, які призначені для забезпечення та надання актуальної інформації про виявлені кіберзагрози, кібератаки та кібервразливості системи, їх оперативне усунення, створення систем виявлення та запобігання вторгнень, та інших заходів. З цієї причини існують дуже великі масиви інформації щодо актуальних комп'ютерних атак та вразливостей комп'ютерних мереж та систем. Однак часто ця інформація (особливо, що стосується атак) є дуже різнорідною, неструктурованою та мало придатною для подальшого аналізу. Як наслідок, в даному випадку виникає необхідність в розробці моделі та інструментарію, які за своїм призначенням направлені на можливість упорядкування та систематизації накопичених знань. Іншими словами – створення таксономії.

Крім змістовного і систематичного опису комп'ютерних атак, на практиці таксономія атак потрібна для їх подальшого аналізу з метою акумулювання знань при оцінці ризиків і створення моделей загроз та моделей порушника на етапах проектування критично важливих систем, в тому числі інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури. А також для розробки політики безпеки та, зрештою, для створення засобів активного аудиту.

Взагалі слово «таксономія» має грецьке походження: (taxinomia) походить від грецького taxis – order (порядок) та nomos – law (закон).

За визначенням, яке дають John D. Howard, Thomas A. Longstaff у своїй книжці «A common language for computer security incidents» [69], *таксономія – абстрактна структура категорованих екземплярів, що включає комплексне дослідження предметної області та створення теоретичної моделі повної множини об'єктів, які досліджуються, що дозволяє визначити*

ознаки, які можуть бути покладені в основу тієї чи іншої класифікації.

Суворе сучасне визначення, яке буде використовуватись в даній роботі, можна знайти в Словнику стандартів з електротехніки та електроніці (The IEEE standard dictionary of electrical and electronics terms. Sixth edition. John Radatz. editor. Institute of Electrical and Electronics Engineers. New York, 1996) [70]: *таксономія – класифікаційна схема, яка розділяє сукупність знань та визначає взаємозв'язок частин.*

Визначення терміну «атака» теж візьмемо з праці «A common language for computer security incidents» [69] авторів John D. Howard, Thomas A. Longstaff. Отже, *атака – послідовність дій, здійснюваних будь-ким для досягнення несанкціонованого результату, тобто дій, направлених на порушення правил функціонування системи, які встановлені її власником.*

Суб'єкт, що здійснює такі дії, у даній роботі називається *атакуючим*, а система, на яку здійснюється атака – *об'єктом атаки.*

Для того щоб таксономія була придатна для вирішення описаних раніше основних завдань, вона повинна задовольняти деяким природним і розумним вимогам.

Списки таких вимог були викладені в багатьох роботах з класифікації атак. Нижче наведено об'єднаний список, отриманий на основі аналізу цих робіт. Ці вимоги не є абсолютно чіткими, і в повній мірі задовольнити всім їм складно. Як буде показано нижче, на практиці таксономія в більшій мірі є деяким компромісом між ними. Основні вимоги до таксономії приведені нижче:

- Взаємне виключення

Таксономія повинна бути влаштована таким чином, щоб вибір одної категорії виключав всі інші. Іншими словами, категорії таксономії, як атрибути / ідентифікатори множин, що складаються з атак, які до них відносяться, не перетинаються. Ця вимога необхідна, щоб мало сенс поняття «клас атаки».

- Повнота

Таксономія покриває собою всі можливі атаки і дозволяє їх класифікувати. Цілком природна вимога того, щоб таксономія покривала всю область комп'ютерних атак, а не лише якусь її частину. Об'єднуючи ці дві вимоги можна сказати, що категорії класифікації повинні утворювати розбиття множини атак.

- Детермінованість

Необхідною умовою є той факт, що сама процедура (або класифікаційна схема), за допомогою якої можна класифікувати атаки, повинна бути чітко визначена.

- Чіткість термінів

Всі терміни, використовувані в таксономії, повинні бути чітко визначені і пояснені з тим, щоб не виникало нерозуміння або розбіжностей в розумінні того чи іншого терміна.

- Об’єктивність

В таксономії повинні розглядатися тільки ті відомості про атаку, які можуть бути отримані виходячи з властивостей об'єкта в результаті неупередженого спостереження.

- Застосовність (useful)

Таксономія повинна являти собою систему, яку можна використовувати для отримання інформації про поле дослідження. Наприклад, виходячи з класу атаки, можна отримати конструктивну інформацію про неї саму.

- Зрозумілість (comprehensible)

Окрім спеціалістів, таксономія повинна бути доступна для розуміння окремих осіб, які не є експертами в області інформаційної безпеки.

- Однозначність (unambigious)

Кожна категорія має бути визначена настільки чітко, щоб була однозначність щодо того, до якої з категорій дана атака повинна бути віднесена.

- Узгодженість (conforming)

Термінологія, яка використовується в таксономії, повинна бути узгоджена з загальноприйнятою термінологією в області інформаційної безпеки.

- Повторюваність результатів (repeatable)

Ця вимога означає, що при класифікації одного і того ж об'єкта двома різними особами повинен виходити один і той же результат.

Однак, як можна помітити, деякі вимоги з перерахованого переліку перетинаються за змістом, деякі є наслідком інших. З цієї причини є доцільним такі вимоги поєднати або, відповідно, видалити. Більш того, вимоги за змістом можна розділити на дві групи: основні вимоги, як вимоги безпосередньо до сенсу і структури категорій, що вводяться, і другорядні, які стосуються радше форми викладу таксономії. Після внесення описаних змін список вимог прийме наступний вигляд.

Основні вимоги: взаємне виключення, повнота, застосовність, детермінованість, об'єктивність, розширюваність.

Додаткові вимоги: чіткість термінів, доступність / зрозумілість, узгодженість.

До основних вимог додано ще одну, нову вимогу – розширюваність (або можливість розширення). Це вимога того, щоб будова таксономії, по-перше, допускала можливість додавання нових категорій, а, по-друге, щоб вони органічно в неї вбудовувалися, а саме – для їх внесення потрібні були б мінімальні зміни основного каркасу таксономії. Це є важливою вимогою до таксономії в силу того, що інформаційно-телекомунікаційна сфера розвивається дуже динамічно, постійно з'являються нові технології, і, як наслідок, нові способи і технічні засоби проведення атак. З цієї причини неможливо розробити таксономію (досить детальну), яка б не вимагала доробок і змін з плином часу.

Питанням класифікації та розробки таксономії кіберзагроз присвячені роботі таких зарубіжних вчених, як Річард Аттанасіо, Пітер Маркштейн, Рей

Філіпс, Сем Канер, Джеймс Андерсон, Пітер Нойман, Дон Паркер, Саймон Хансман, Климовський та інших [71 – 76, 95]

Існує кілька підходів до проблеми класифікації кібератак. Традиційно атаки ділять на категорії в залежності від ефекту, який вони створюють: порушення конфіденційності інформації, порушення цілісності інформації, відмова в обслуговуванні (порушення доступності інформації) та порушення спостережності системи. Основним недоліком такого ділення є його слабка інформативність (і, як наслідок, застосовуваність), так як за інформацією про клас атаки ми практично нічого не можемо сказати про її особливості. Однак, зрозуміло, ефект атаки є важливою її властивістю і цей параметр в тому чи іншому вигляді використовується в багатьох таксономіях.

Іншим підходом до класифікації кібератак є класифікація вразливостей апаратного і програмного забезпечення комп'ютерних мереж та систем. Однією з перших робіт в цьому напрямку є робота Атанасіо, Маркштейна і Філліпса (Penetrating an operating system: a study of VM/370 integrity. IBM System Journal, 15(1), 1976. P. 102–116) [71]. Часткове розподілення за типом вразливості було використано Джоном Ховардом та Томасом Лонгстаффом в роботі «A common language for computer security incidents» [69].

Далі цей підхід отримав продовження, і в роботі Giri Vijayaraghavan, Cem Kaner "Bug Taxonomies" [72] розвита вже досить детальна класифікація вразливостей. Однак цей підхід є занадто вузьким і часто не відображає в повній мірі характер атаки, тому застосовується в основному лише для спеціальних класів задач (наприклад, при тестуванні програмного забезпечення).

Одним з можливих варіантів є поділ виходячи з початкового доступу, яким володіє атакуючий. Найвідоміший приклад подібного підходу – це матриця Андерсона. У своїй роботі [73] Джеймс Андерсон (James P. Anderson) запропонував покласти в основу класифікації можливість, або неможливість доступу атакуючого до комп'ютера або до його компоненту. Таким чином, категорія, до якої належить атака, залежить від того, які

початкові привілеї мав атакуючий. Таким чином, можна скласти наступну матрицю 2 × 2:

Таблиця 1.1 – Матриця Андерсона

	Атакуючий не має права запуску / використання програми / інформації	Атакуючий має право запуску / використання програми / інформації
Атакуючий не має доступу до комп'ютера	Категорія A Зовнішнє вторгнення	-
Атакуючий має доступ до комп'ютера	Категорія B Внутрішнє вторгнення	Категорія C Зловживання повноваженнями

З наведеної таблиці можна помітити, що всі атаки розбиваються на три категорії, тому що випадок, коли атакуючий не має доступу до комп'ютера (такий доступ йому не дозволено), проте при цьому йому дозволено використовувати дані, що зберігаються на комп'ютері, і запускати програми, неможливий. Категорія B підрозділяється Андерсоном ще на 3 підкатегорії, в залежності від атакуючого. Таким чином, повний список категорій має нижченаведений вигляд.

A. Зовнішнє вторгнення.

B. Внутрішнє вторгнення.

i. Помилковий користувач (masquerader).

ii. Легальний користувач (legitimate user).

iii. Прихований користувач (clandestine user).

C. Зловживання повноваженнями.

Відмінність між хибним користувачем, легальним користувачем і прихованим користувачем полягає в тому, що хибний користувач маскується під легального користувача і, наприклад, з точки зору системи, не відрізняється від нього. Прихований ж користувач діє так, щоб залишитися непоміченим механізмами виявлення або якимось чином уникає їх.

Наприклад, якщо атакуючий зміг дізнатися пароль легального користувача і скористався ним для отримання доступу, то він діяв як хибний користувач. Якщо він підмінив частину системних файлів для отримання доступу, то він діяв як прихований користувач.

Простежуючи подальший розвиток підходів, можна помітити, що деякі автори у своїх роботах спробували не відштовхуватись від будь-яких властивостей і параметрів атак, а скласти загальний список типів атак. Найвідоміші роботи, представлені в цьому напрямку – це роботи Ноймана і Паркера (“A summary of computer misuse techniques”) [74]. Такі ж в цілому ідеї були використані Симоном Хансманом в роботі “A taxonomy of network and computer attacks methodologies. University of Canterbury. New Zealand, November 2003” [75]. Безперечною перевагою підходу, заснованого на виділенні списку типових атак, є добра відповідність вимоги застосовності, так як в більшості випадків тип атаки дає суттєво більше інформації ніж знання будь-яких її властивостей. Однак область застосування такого підходу дуже обмежена в силу того, що при його використанні дуже важко задовольнити першим двом дуже значним вимогам – повноті і взаємному виключенню. В зв’язку з цим часто такі списки містять категорії атак, які сильно перетинаються, а питання про їх повноту також залишається відкритим.

В роботі Пітера Ноймана і Дональда Паркера (Peter Neumann, Donald Parker) представлені 9 категорій технік вторгнення (табл. 1.2).

Таблиця 1.2 – Категорії технік вторгнень

1.	Зовнішнє
2.	Апаратне
3.	Маскування
4.	Шкідливі програми
5.	Обхід механізмів безпеки
6.	Активне зловживання
7.	Пасивне зловживання
8.	Інертне зловживання
9.	Непряме зловживання

На їх основі Нойман розробив типи атак, які представлені в табл. 1.3.

Таблиця 1.3 – Типи атак

Зовнішні	
Візуальне спостереження	Спостереження за клавіатурою або монітором
Обман	Обман операторів і користувачів

Витяг сміття	Витяг інформації з віртуальних кошиків
Апаратні (hardware)	
Логічне відновлення	Витяг інформації з викинутих або вкрадених носіїв
Прослуховування	Перехоплення даних
Втручання	
Фізична атака	Руйнування або пошкодження обладнання, джерел живлення
Фізичне видалення	Вилучення обладнання і сховищ даних
Маскування	
Імітування	Використання помилкових ідентифікаторів
Узурпування ліній зв'язку або хостів	
Атаки з підміною параметрів	
Сплутування мереж	Маскування фізичного розташування або маршруту
Шкідливі програми	*Створення можливості подальших зловмисних дій*
Троянські коні	Впровадження шкідливого коду
Логічні бомби (Logic bombs)	Різновид троянських коней
Черви	Оволодіння розподіленими ресурсами
Віруси	Прикріплення до програм і розмноження
Обхід	Обхід механізмів безпеки
Експлуатація вразливостей	
Злом паролів	
Активне зловживання	
Основні	
Інкрементальні атаки	Поступова ескалація привілеїв, повільне просування до мети
Відмова в обслуговуванні	Вчинення масивних атак
Пасивне зловживання	
Огляд	Випадковий або вибірковий пошук
Збір і виведення даних	Використання баз даних та аналіз трафіку
Приховані канали	Використання прихованих каналів або інші способи витоку інформації
Інертне зловживання	
Непряме зловживання	

Перший спосіб полягає в тому, щоб рознести окремо всі параметри, що аналізуються, і вважати їх незалежними. Такий підхід був реалізований в

роботі Хансмана, де автор використовує так звану концепцію «вимірів», основна ідея якої полягає в тому, що властивості атаки розшаровуються на кілька незалежних вимірювань, в кожному з яких є свій список (або дерево) категорій.

У своїй роботі Симоном Хансманом (Simon Hansman) запропонована таксономія мережевих і комп'ютерних атак, в основі якої лежить спосіб поділу параметрів атаки на кілька вимірів. Автором запропоновано чотири основні виміри і кілька допоміжних.

- **Перший вимір** – це список типів атак (наприклад, відмова в обслуговуванні).
- **Другий вимір** – це мета (цільовий об'єкт) атаки. Якщо у атаки кілька об'єктів нападу, то в цьому вимірі має бути кілька записів.
- **Третій вимір** – це уразливості, що використовуються в процесі атаки. За словами автора, це вимір зазвичай містить CVE-описи вразливостей (Common Vulnerabilities an Exposures), причому якщо використовується декілька вразливостей, то в цьому вимірі присутні кілька записів.
- **Четвертий вимір** – це, фактично, результат або мета атаки.

Опишемо всі ці виміри більш докладно.

Перший вимір наведений в таблиці 1.4.

Таблиця 1.4 – Перший вимір кібератак

Віруси:	Інфікуючи файли	
	Інфікуючи системні/завантажувальні сектори	
	Макровіруси	
Хробаки:	Використовують масову розсилку	
	Розпізнають стан мережі	
Троянські програми:	Логічні бомби	
Переповнення буфера:	Переповнення стека	

	Переповнення сховища	
Відмова в обслуговуванні	Локальний (host based):	Вичерпання ресурсів
		Вивід з ладу
	Мережевий (network based):	TCP- флуд
		UDP-флуд
		ICMP-флуд
	Розподілені	
Мережеві атаки	Підміна пакетів	
	Перехоплення сесії	
	Бездротові атаки:	Злам крипто алгоритмів бездротових мереж
	Атаки на веб-додатки:	Використання зловмисних веб-сценаріїв (Cross Site Scripting)
		Підбір параметрів
		Використання некоректних cookies
		Атаки на бази даних
		Використання скритих полів
Фізичні атаки:	Прості	
	Енергетична зброя:	HERF
		LERF
		EMP
	Van Eck	
Атаки на паролі	Вгадування	Атака методом грубої сили
		Атака за словником
	Використовуючи вразливість в реалізації	
Атаки – збір інформації	Прослуховування	Прослуховування пакетів
	Виявлення структури мережі	
	Сканування	

Другий вимір наведений в таблиці 1.5.

Таблиця 1.5 – Другий вимір кібератак

Апаратне забезпечення:	Комп’ютер:	Жорсткі диски			
		…			
	Мережеве обладнання:	Хаб			
		Кабель			
		…			
	Периферійне обладнання:	Монітор			
		Клавіатура			
		Миша			
		Принтер			
		…			
Програмне забезпечення:	Операційна система:	Сімейство Windows:	Windows 10		
			Windows Server 2016		
			…		
		Сімейство Linux:	Linux	2.2	
				2.4	
				…	
			FreeBSD	4.8	
				5.1	
				…	
			…		
		Сімейство MacOS:	MacOS X	10.1	
				10.2	
				…	
			…		
		…			
	Додатки:	Серверні додатки:	Бази даних		
			Поштовий сервер		
			Веб-сервер	IIS	4.0
					5.0
			…		

		Користувальницький додаток:	Текстовий редактор	MS Word	2000
					XP
					…
			Поштовий клієнт	…	
			…		
		…			
Мережа:	Протокол:	Транспортний рівень:	IP		
			…		
		Мережевий рівень:	TCP		
			…		
		…			

Третій вимір

Як уже було відзначено вище, третій вимір містить в собі стандартні описи вразливостей, які використовуються в атаці. У зв'язку з цим для нього необхідність опису будь-якої спільної схеми, як для перших двох, відпадає.

Четвертий вимір

Четвертий вимір служить для класифікації атак, які здійснюються не тільки для досягнення своєї головної мети. Наприклад, хробак окрім свого прямого призначення – зараження комп'ютера, може служити для віддаленого управління або знищення якихось файлів. Четвертий вимір складається з п'яти категорій:

- безпосередня (номінальна) мета атаки;
- порушення цілісності інформації;
- порушення конфіденційності інформації;
- захоплення ресурсів;
- отримання контролю над частиною системи для подальшого використання.

Інші виміри

Інші виміри, як пише Хансман, можуть бути додані для поліпшення і розвитку таксономії. Як варіанти подальшої деталізації пропонуються

наступні категорії:

- збитки, який описує шкоду, завдану атакою;
- вартість відновлення, яка описує загальну вартість відновлення системи після атаки до початкового стану;
- поширення, яке описує швидкість і спосіб поширення атаки; ця категорія підходить найбільше для атак, що поширюються, на зразок вірусів і черв'яків;
- способи захисту.

Другий спосіб заснований на тій же ідеї, проте є більш гнучким, так як має на увазі деревоподібну структуру категоріальних класів з найвищого рівня. Реалізацію цього підходу можна знайти в роботі Джеффрі Андеркоффера і Джона Пінкстона (Jeffrey Undercoffer, John Pinkston) Modeling computer attacks: a target-centric ontology for intrusion detection. University of Maryland Baltimore Country [76].

У своїй роботі Джеффрі Андеркоффер і Джон Пінкстон дотримуються структурного підходу до класифікації. У графічному поданні (рис. 1.1) розроблена ними таксономія є деревом, коренем якого є вторгнення. Ребра цього дерева мають мітки та несуть смислове навантаження: наприклад, з кореня дерева виходять два ребра, які означають «здійснено з допомогою» і «мало результат». Пунктирна стрілка виражає відношення «є підкласом» між вершинами, які вона з'єднує і, для того щоб надмірно не навантажувати малюнок, цей напис опущений. Можна помітити, що застосування таких способів хоча і дає більш детальний опис атаки, проте не може відобразити деякі її структурні особливості, сценарій атаки. Зазначена обставина є суттєвими недоліком, з огляду на постійне вдосконалення сучасних систем захисту і, як наслідок, тенденції до все більш складних і витончених методів атак.

Третій спосіб - це комбінування властивостей з внесенням структури. Такий підхід був застосований в роботі Джона Ховарда і Томаса Лонгстаффа (John D. Howard, Thomas A. Longstaff) «A common language for computer

security incidents» [69]. Основна його ідея полягає в тому, що вводиться ієрархія понять: основним в даній роботі вважається поняття «інцидент», в нього включається поняття «атака», а в поняття «атака» включається поняття «дія». При цьому інцидент може складатися з декількох атак, а кожна атака з декількох дій.

Джон Ховард і Томас Лонгстафф не тільки створили таксономію, а й розробили «Спільну мову для інцидентів в області комп'ютерної безпеки». Як сказано у вступі до «A common language for computer security incidents» [69], «Ця спільна мова не є спробою створення всеохоплюючого словника термінів в області комп'ютерної безпеки. Замість цього ми створили мінімальний набір високорівневих термінів, разом зі структурою, що відображає їх взаємозв'язок (таксономією)».

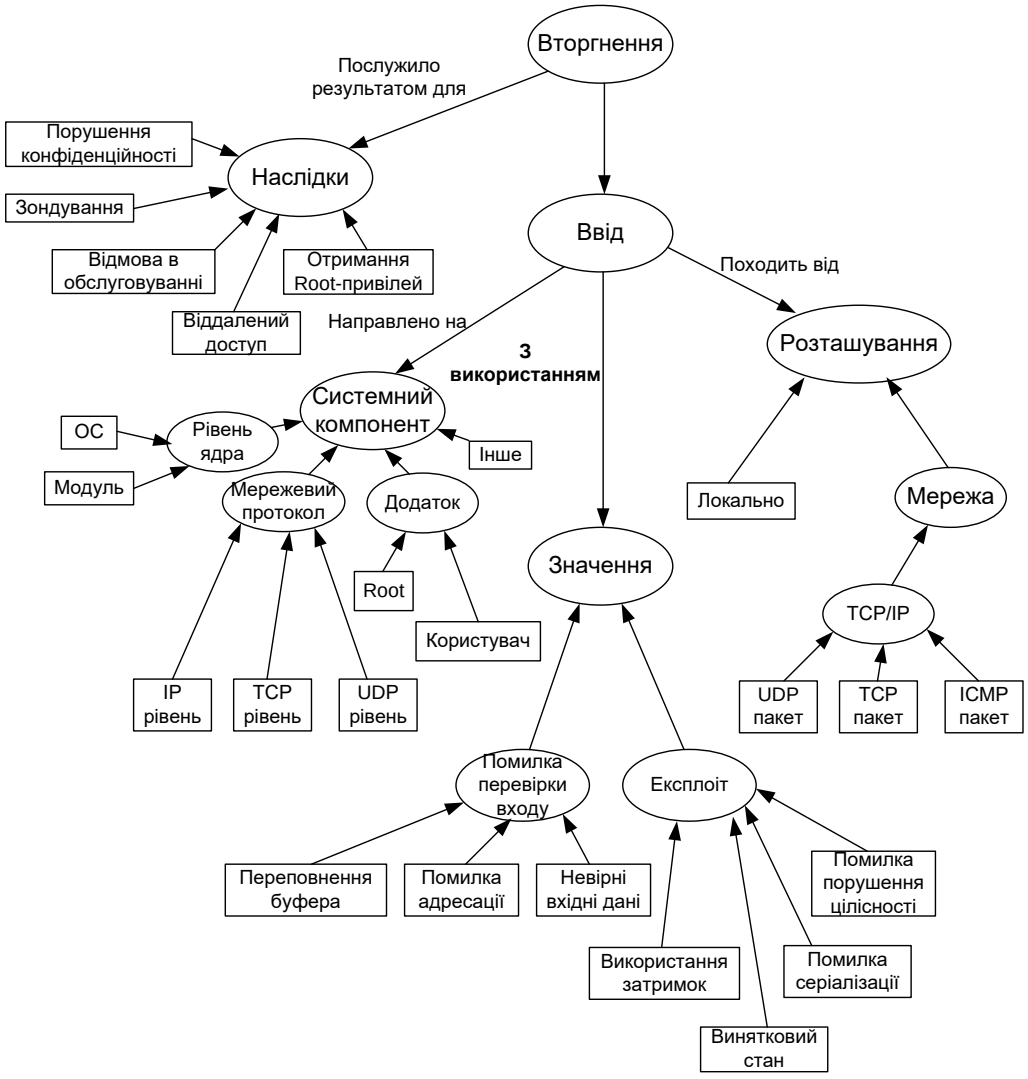

Рис. 1.1 – Вторгнення

Таксономія, розроблена цими авторами, являє собою наступну діаграму (рис. 1.2). Основним поняттям в цій таксономії є поняття «інцидент», так як автори поділяють два поняття – інцидент та атака. У поняття інцидент входить атакуючий, атака і мета атаки. Під атакою розуміються ті сутності, які відносяться безпосередньо до процесу здійснення атаки: інструмент, вразливість, дія, цільовий об'єкт і несанкціонований результат. Інструмент – це засіб, який використовував атакуючий при нападі. Сукупність дії і цільового об'єкта називається подією.

Запропонована авторами таксономія відрізняється від описаних вище тим, що в ній присутні структурні елементи: інцидент, атака, подія і закладена можливість комбінування цих подій. Так в одному інциденті може бути вкладена послідовність атак. Дана властивість в якійсь мірі дозволяє описувати неатомарні (багатоходові) складні атаки і враховувати їх сценарій.

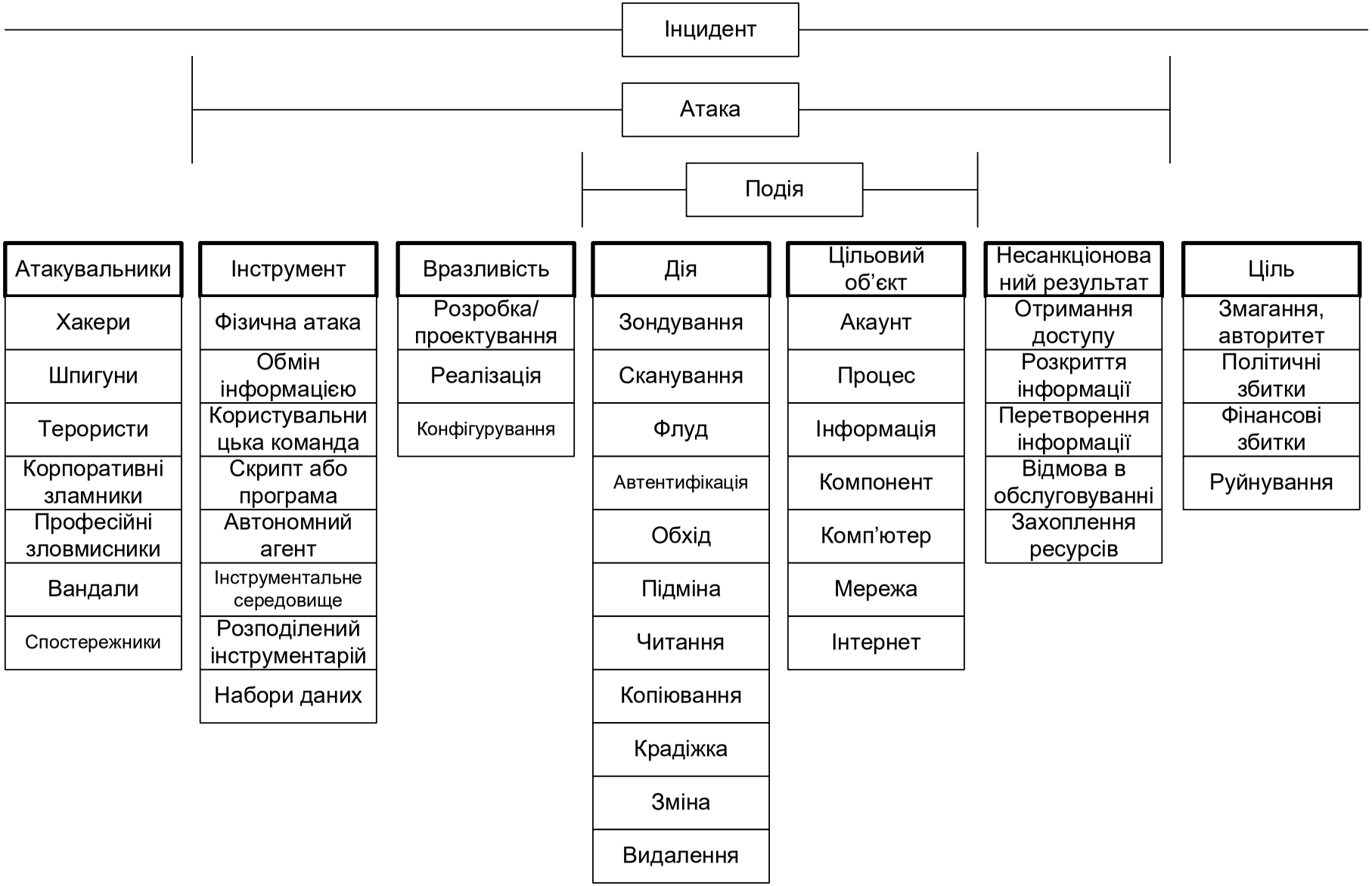

Рис. 1.2 – Інцидент

Порівняльна таблиця підходів до розробки таксономій кіберзагроз наведена у таблиці 1.6.

Таблиця 1.6 – Порівняльна таблиця підходів до розробки таксономій кіберзагроз

Властивості / підходи до класифікації	Застосовуваність (інформативність)	Повнота	Детермінованість	Взаємне виключення	Чіткість термінів	Об’єктивність	Зрозумілість	Однозначність	Узгодженість	Повторюваність результатів
За ефектом впливу на властивості інформації	-	+	+	-	-	+	-	-	+	-
Вразливості апаратного та програмного забезпечення	+	-	+	+	+	+	+	+	-	-
Загальний список атак	+	-	-	-	+	+	-	-	+	-
Комбінований підхід	+	+	+	+	+	+	+/-	+	+	+

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 мети і наукових задач досліджень

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

Метою дисертаційного дослідження є підвищення рівня захисту інформації від кібервпливів в комп’ютерних мережах та системах об’єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації.

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

– проаналізувати сучасні методи та засоби захисту інформації в комп’ютерних мережах та системах;
– розробити таксономію інформаційних загроз комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури;
– скласти матрицю залежності інформаційних об’єктів захисту від типу

потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз;

- розробити модель бази даних загроз інформаційним об’єктам захисту комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури;
- розробити метод розпізнавання кіберзагроз інформаційній безпеці комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури
- розробити методику оцінювання кіберстійкості комп’ютерних систем та мереж об’єктів критичної інформаційної інфраструктури;
- розробити структурну модель багаторівневої системи виявлення підозрілих впливів на ком’ютерні мережі та системи об’єктів критичної інформаційної інфраструктури;
- розробити алгоритм та програмний застосунок розрахунку кіберстйкості об’єктів критичної інформаційної інфраструктури.

1.4. Висновки до першого розділу

1. Проаналізовано сучасні методи та засоби захисту інформації в комп’ютерних мережах та системах. Встановлено, що дослідженню проблем, пов’язаних із процесом захисту інформації від кібервпливів в комп’ютерних системах та мережах об’єктів критичної інфраструктури, 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 щодо забезпечення кібербезпеки та захисту інформації в комп’ютерних системах та мережах об’єктів критичної інфраструктури дають можливість визначити основні складові частини систем захисту інформації, сформулювати основні завдання із забезпечення безпеки інформації та визначити основні напрямки

забезпечення інформаційної безпеки компютерних систем та мереж об'єктів критичної інфраструктури.

3. Результати аналізу показують відсутність таксономії загроз інформаційній безпеці комп’ютерних мереж та систем об’єктів критичної інфраструктури, яка б дозволяла описувати багатоетапні атаки, які на сьогоднішній день отримали дуже широку розповсюдженість.

РОЗДІЛ 2
МОДЕЛЬ БАЗИ ДАНИХ ЗАГРОЗ ІНФОРМАЦІЙНИМ ОБ'ЄКТАМ ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Таксономія кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури

У запропонованій таксономії розвивається комбінований підхід до вирішення задачі класифікації. Однак, на відміну від попередніх робіт, вводиться ієрархічна структура відносин з деревовидним розкриттям категорій. Як самостійний окремий об'єкт вводиться важливе поняття «етап атаки», що дозволяє, на відміну від попередніх підходів, досить природним чином описувати багатоетапні атаки, які отримали високу розповсюдженість на сьогоднішній день.

Атака

На рис. 2.1 приведена загальна схема атаки.

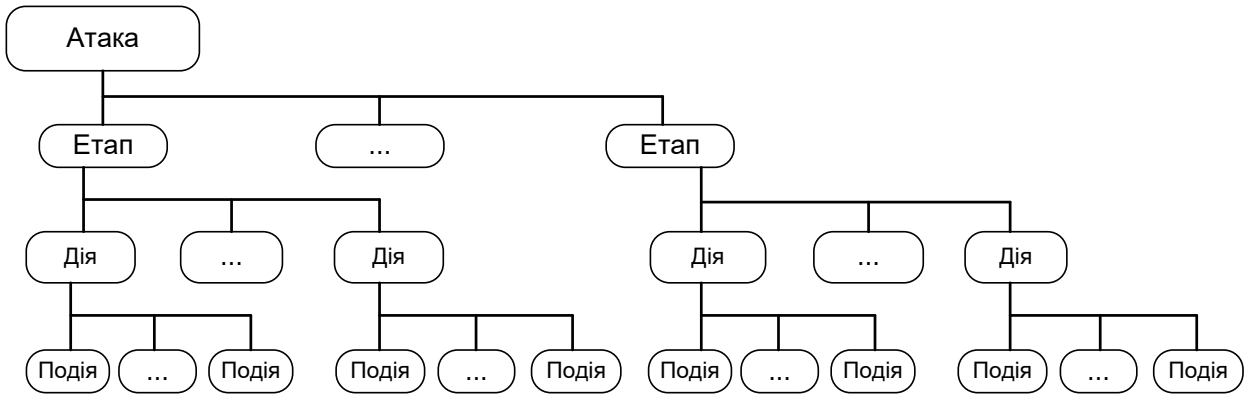

Рис. 2.1 – Загальна структура атаки

Атака може складатися з декількох етапів, етап, в свою чергу, з декількох дій, дія – з декількох подій. Наприклад, злом через pro-ftpd може бути частиною одного з етапів атаки і складається з чотирьох подій, які можуть відбуватися в різному порядку.

Крім вкладеності в поняття більш високого рівня, кожне з цих чотирьох понять розкривається за допомогою дерева підкатегорій, тобто має свій

власний набір атрибутів.

Поняттям самого верхнього рівня є атака. Функціональна схема атаки наведена на рис. 2.2.

Поняття атаки має такі атрибути, як глобальна мета / результат, властивості атаки, об'єкт атаки і атакуючий. Кожен з перерахованих атрибутів теж має свої атрибути і є піддеревом дерева атрибутів атаки. Важливо відзначити, що мета поділяється на дві компоненти: інформаційну складову і соціально значущу складову. Інформаційна складова відображає інформаційний аспект наслідків впливу атаки на систему: порушення конфіденційності інформації (яка поділяється на порушення конфіденційності з метою розвідки або з метою розголошення), порушення доступності інформації / ресурсів системи (яка поділяється на порушення з метою блокування системи захисту або з метою порушення функціонування самої системи) і порушення цілісності інформації (з метою втручання і отримання контролю). Соціально значуща складова, на відміну від інформаційної, відображає поза інформаційні аспекти наслідків атаки. Проілюструємо такі наслідки на прикладі захоплення комп'ютерів інформаційно-обчислювального середовища атомної електростанції і проведення теракту з метою створення техногенної катастрофи шляхом виведення з ладу реактора. В даному випадку, інформаційною складовою мети є захоплення комп'ютерів, а соціально значущою – створення надзвичайної ситуації за допомогою виведення з ладу реактора.

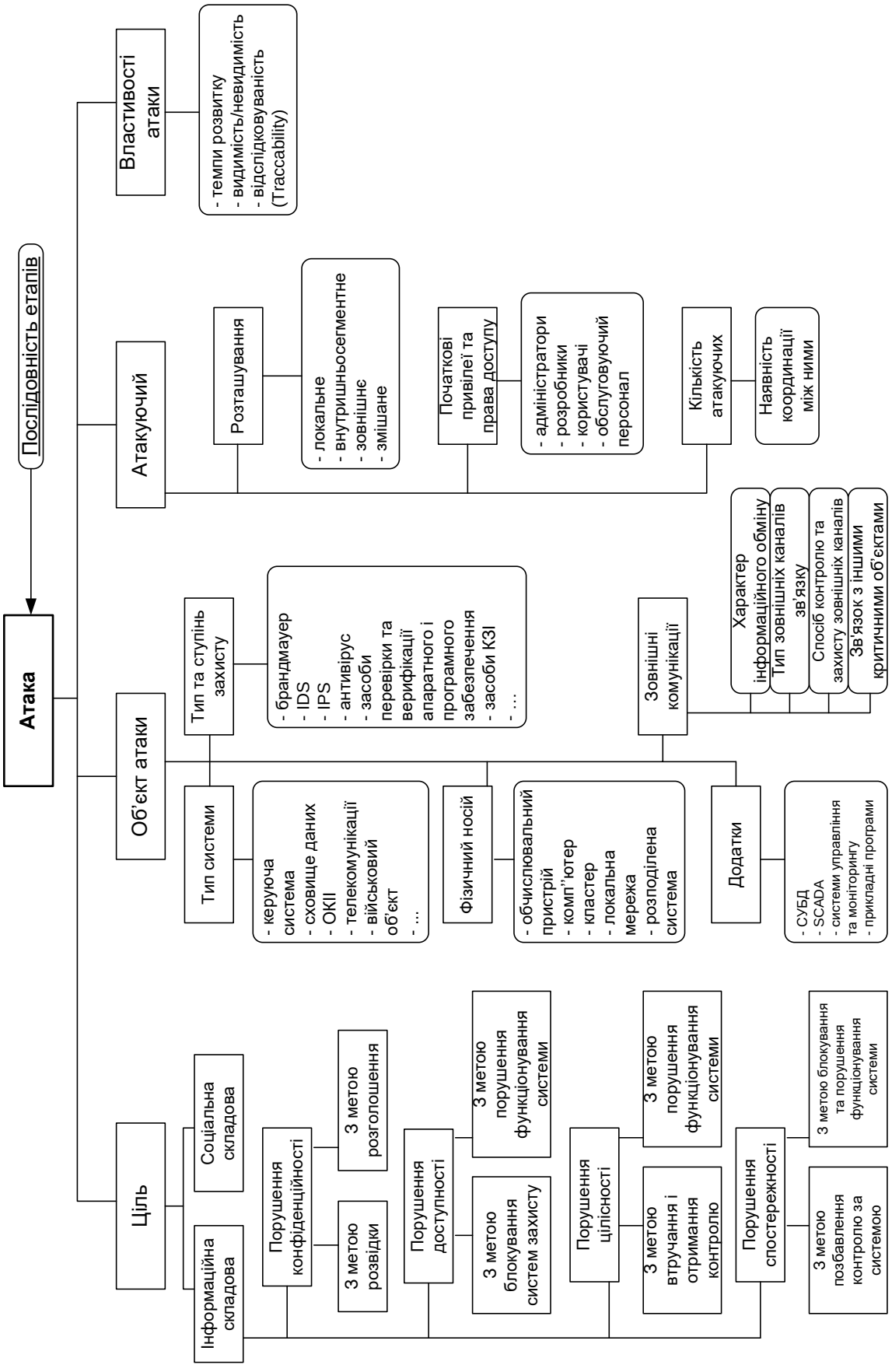

Рис. 2.2 – Функціональна схема атаки

Іншим важливим атрибутом є об'єкт атаки, так як атаки на об'єкти різної функціональності і категорійності мають, як правило, різний характер. Тут виділяються такі властивості об'єкта атаки, як тип системи, яку атакують, її фізичний носій (обладнання, яке формує інформаційно-обчислювальну середу системи), тип засобів захисту, які використовуються в системі, і ступінь захищеності (рівень жорсткості правил безпеки), а також зовнішні комунікації системи.

Ще одним атрибутом атаки є атакуючий. Основними властивостями, які його характеризують, є розташування щодо системи, початкові привілеї і права доступу. Якщо атакуючих декілька, то в цьому випадку виникає ворожа багатоагентна система, тому стає вкрай важливим їх кількість, наявність і характер координації між атакуючими.

З перелічених властивостей, імовірно, найбільше значення має розташування атакуючого щодо об'єкта атаки. Атакуючий може здійснювати атаку з того ж комп'ютера, на якому знаходиться інформація, яка є його метою. Прикладом локальної атаки може бути підвищення привілеїв за допомогою переповнення буфера в одній з програм, які виконують частину операцій в привілейованому режимі, і отримання доступу до даних. Приклад внутришньосегментної атаки – це атака, коли атакуючий починає атаку з комп'ютера, який знаходиться в одному сегменті мережі, що дозволяє йому використовувати експлоіти для сервісів, порти яких фільтруються ззовні фаєрволом, і таким чином захопить комп'ютер-жертву. Зовнішня атака – це атака, проведена атакуючим віддалено, наприклад, атака суперкомп'ютерного центру Сан-Дієго, описана Медведовским І. Д., Семьяновим П. В. та Платоновим В. В. в книзі «Атака через Internet» [77]. Крім вищезазначених існує і змішаний тип атак, які зазвичай проводяться узгоджено групою атакуючих. Прикладом може служити атака, що проводиться двома користувачами за допомогою створення прихованого каналу. суть полягає в тому, що один користувач знаходиться всередині сегмента мережі та певним чином отримує доступ до необхідної інформації і передає її іншому

користувачеві зовні за допомогою прихованого каналу. Атаку можуть проводити кілька атакуючих з різних місць, в цьому випадку атака називається розподіленою за атакуючими (про що говорить параметр «кількість атакуючих»), найпростіший приклад – DdoS-атака.

Останнім атрибутом, представленим на діаграмі (рис. 2.2), є атрибут «властивості атаки». Для зменшення ризику бути виявленими атаки іноді тривають по кілька місяців, а інших випадках, кілька секунд (щоб, наприклад, виключити можливість втручання адміністратора системи, яку атакують). В силу цих обставин темп розвитку атаки являє собою важливу для класифікації властивість атаки. Інші дві властивості – видимість і можливість простежити джерело атаки (відстеженість). Видимість означає, що сценарій атаки роблений таким чином, що передбачається, що під час проведення атака не буде виявлена засобами виявлення. Відстеженість означає, що після проведення атаки при проведенні розслідування існує можливість простежити джерело атаки. Слід зазначити, що ці дві властивості сильно пов'язані одна з одною. Значення кожного з неї залежить, в першу чергу, від поставленої зловмисником мети, і вони сильно впливають на вибір стратегії, використовуваної при атаці. Наприклад, якщо завдання зловмисника непомітно проникнути в систему і викрасти конфіденційну інформацію, то при виборі стратегії він цілком може використовувати сценарії, які невидимі, проте відслідковуються (наприклад, редагування або стирання лог-файлів робить атаку істотно більш помітною, але менш відслідковуваною).

Етап

Атака складається з етапів, які, в свою чергу, теж мають свої атрибути. Поняття етап відображає (див. Рис. 2.3) окрему частину атаки та має свою локальну мету. Наведемо приклад: одним з етапів атаки може бути етап-розвідка – сканування підмереж певної організації, яку атакують. Мета цього етапу – по можливості непомітно, не викликаючи підозр, дослідити топологію і внутрішній устрій мережевого сегменту об'єкта атаки для

знаходження слабких місць системи захисту і подальшого вторгнення. Для досягнення цієї мети існує велика кількість різних і досить нетривіальних способів.

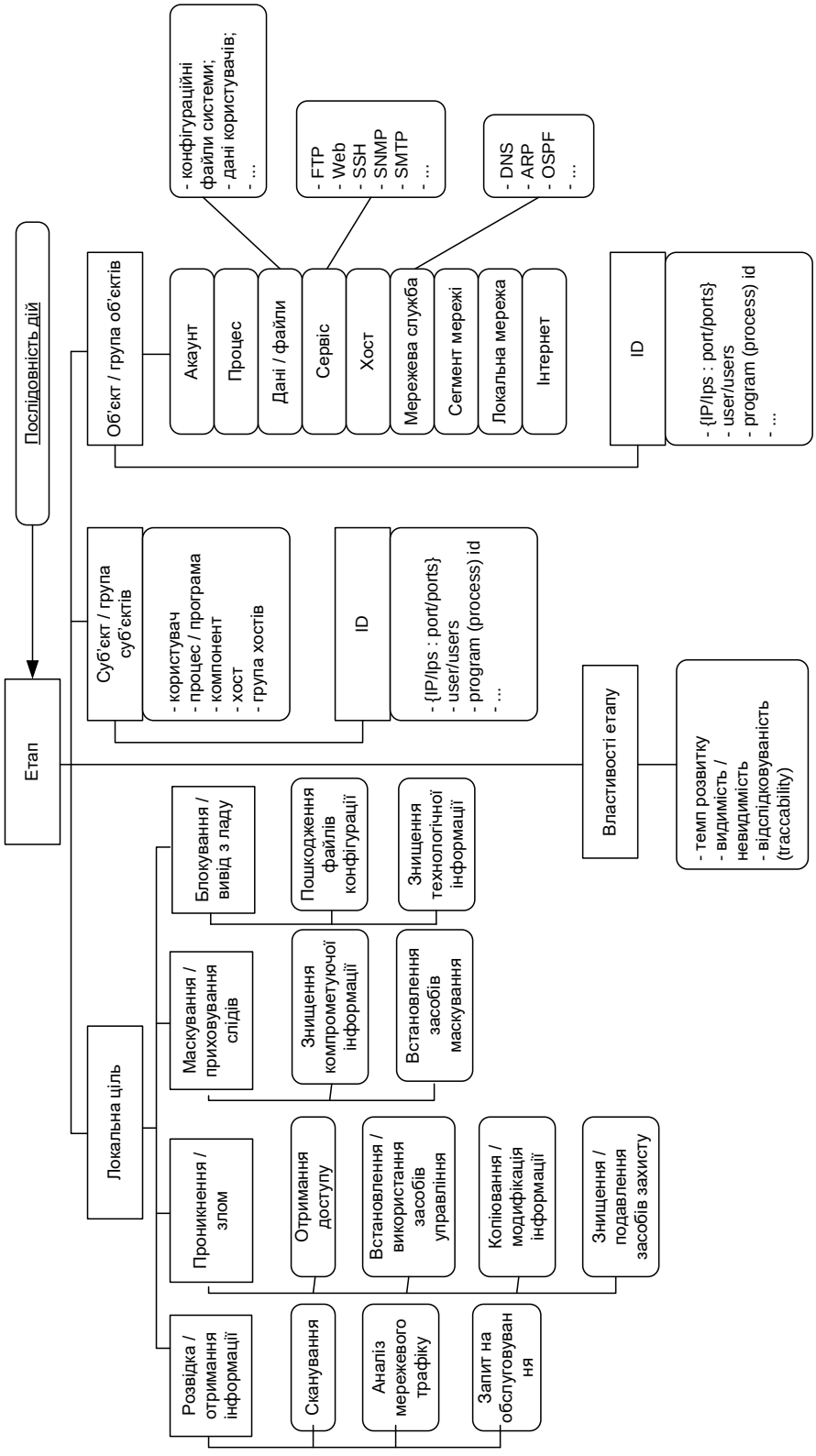

Рис. 2.3 – Функціональна схема етапу

Дія

Етап складається з дій. Дія являє собою, в деякому сенсі, «атомарну» атаку (наприклад, сканування портів або використання програмних вразливостей). Дія теж має атрибути: тип дії, суб'єкт, об'єкт, наслідки дії, результат. Фактично, вона є мінімальним смисловим кроком атаки.

Розглянемо атрибути цього поняття (рис. 2.4).

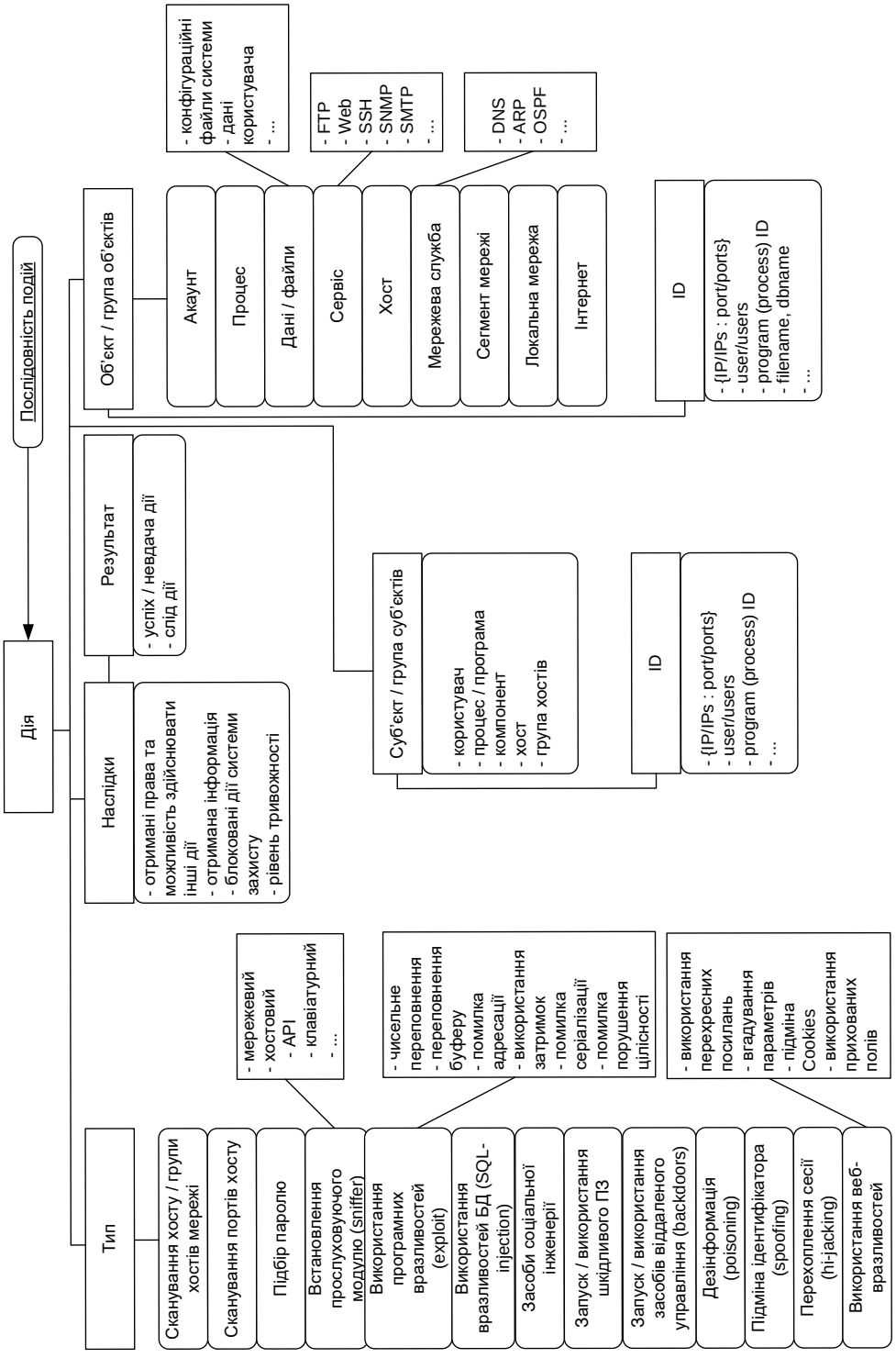

Рис. 2.4 – Функціональна схема дії

Атрибут «тип дії» описує безпосередньо саму дію, що відбувається на даному етапі атаки. Цей атрибут є найбільш важливим і інформативним. У деякому сенсі, список можливих дій схожий на перелік типових атак. З цієї причини йому теж властива відсутність повноти і, можливо, при застосуванні таксономії на практиці, представлений на рисунку список буде потребувати розширення (в залежності від специфіки області застосування). «Об'єкт / група об'єктів» - це те (програма, комп'ютер або мережа), на що дана дія направлена. «Суб'єкт / група суб'єктів» - це те, що спричиняє дану дію. Наприклад, якщо при зломі мережі атакуючому вдалося захопити один з вузлів мережі (хост А), і надалі він проводить сканування портів іншого хоста (назвемо його В) від імені захопленого комп'ютера, то суб'єктом дії буде хост А, а об'єктом - хост В. Параметр «наслідки» характеризує наслідки дії, а саме, отримані атакуючим права і привілеї в об'єкті атаки, інформацію, до якої він отримав доступ в результаті цієї дії тощо. Цей параметр містить також інформацію про рівень тривожності даної дії (безумовно, рівень тривожності є вельми суб'єктивною величиною і сильно залежить від передісторії і від оточення, в якому відбувається дія, тому тут мається на увазі деяке апріорне мірило оцінок тривожності).

Подія

Зауважимо, що з точки зору системи дія є далеко не атомарною. Сканування портів, наприклад, це ланцюжок дій, який може сильно варіюватися. З цієї причини, для більш детального розгляду атаки, необхідно ввести ще один, найнижчий рівень абстракції - рівень подій (рис. 2.5).

Подією є мінімальний (на заданому рівні деталізації) крок з точки зору системи. Подія має наступні атрибути: тип, результат, час, суб'єкт та об'єкт.

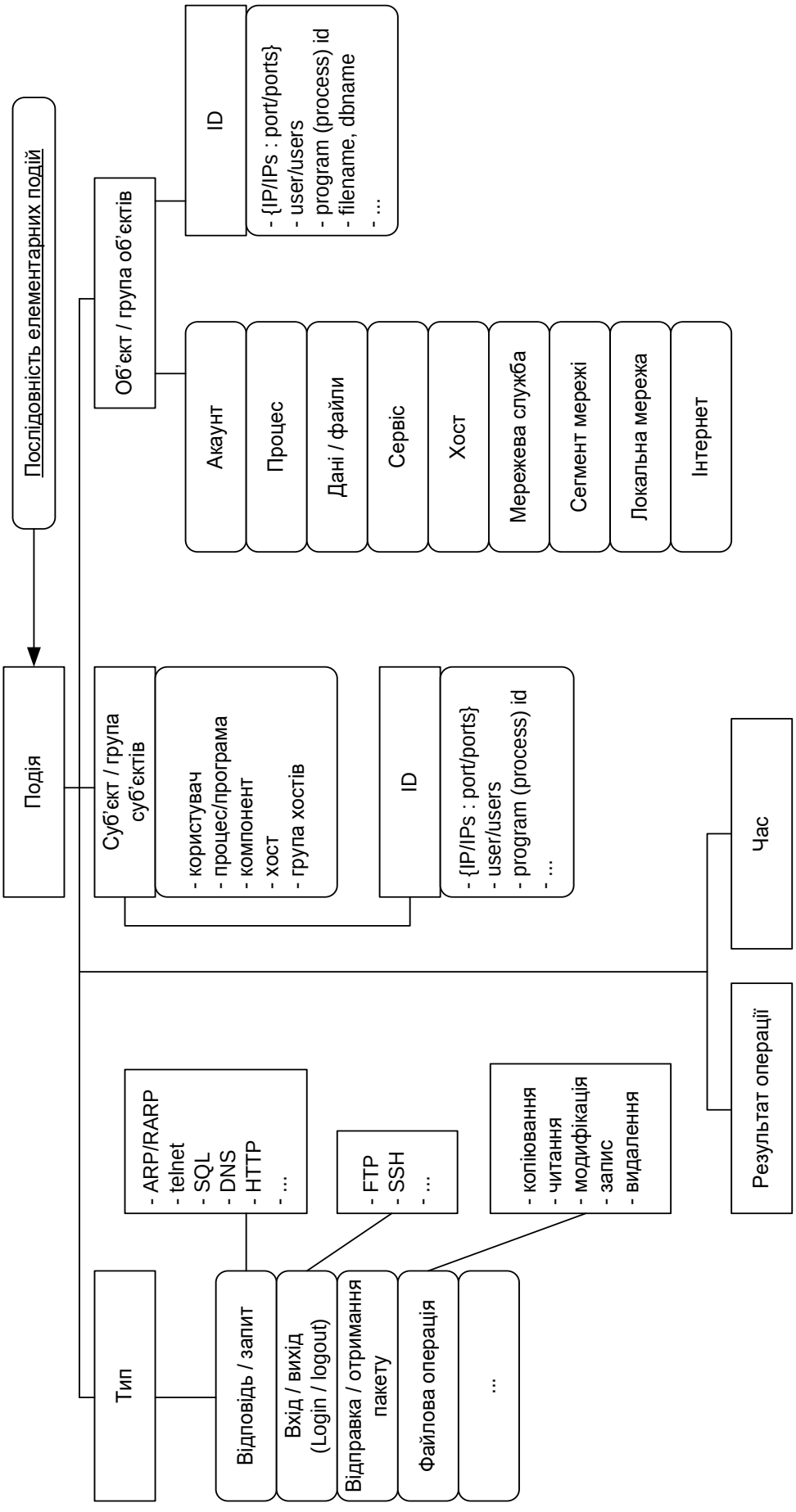

Рис. 2.5 – Функціональна схема події

2.2. Матриця залежності інформаційних об’єктів захисту від типу потенційних загроз

Проведений аналіз існуючих систем захисту інформації [5, 6, 9, 11, 13, 20, 79, 80, 83, 91, 92, 93] та вищенаведені класифікації та таксономії кіберзагроз дають змогу побудувати первинну матрицю кіберзагроз для програмних та апаратних засобів об’єктів критичної інформаційної інфраструктури. Матриця наведена у вигляді таблиці та включає загрози програмного та апаратного забезпечення, кіберзагрози прикладного ПЗ та кіберзагрози операційної системи (табл. 2.1)

Таблиця 2.1 - Матриця кіберзагроз для програмних та апаратних засобів об’єктів критичної інформаційної інфраструктури

Об’єкти / загрози	Кабельна система	Мережеве обладнання	Засоби мережевого захисту	Технологічна інформація захисту активного мережевого обладнання	Технологічна інформація захисту хостів (робочих станцій та серверів)	Дані, що передаються мережею	Програмне забезпечення	Файли	Записи баз даних	Обчислювальні ресурси
Мережеві загрози										
Відсутність фізичного з’єднання	+	+								
Помилки та непрацездатність активного мережевого обладнання (АМО)		+	+							
Розголошення даних про мережу				+	+					
Перехоплення (сніффінг) пакетів				+	+	+				
Підміна отримувача (спуфінг пакетів)				+	+					
Відмова в обслуговуванні (DoS)				+	+		+			
Дзеркалювання трафіку					+	+				
Непрацездатність мережевих застосувань							+	+	+	
Створення альтернативних несанкціонованих точок доступу до мережі (бекдор)		+	+	+			+	+		+

Об’єкти / загрози	Кабельна система	Мережеве обладнання	Засоби мережевого захисту	Технологічна інформація захисту активного мережевого обладнання	Технологічна інформація захисту хостів (робочих станцій та серверів)	Дані, що передаються мережею	Програмне забезпечення	Файли	Записи баз даних	Обчислювальні ресурси
Віддалене захоплення (боти, ботнети)				+	+		+			+
Сканування системи		+	+	+						
Встановлення з’єднання від імені користувача, що заслуговує довіру (фітинг, маскарад)				+	+		+	+	+	+
Соціальна інженерія	+	+	+	+	+	+	+	+	+	+
Цільова кібератака (розвинута стійка загроза (advanced persistent threat, APT))		+	+	+	+	+				
Загрози прикладного ПЗ										
Помилка, збій та відмова прикладного ПЗ							+	+	+	+
Виконання недокументованих функцій					+			+	+	
Розповсюдження вірусів та хробаків					+		+	+	+	+
Несумісність версій ПЗ							+			
Перехоплення інформації					+					
Підміна або дезорганізація							+			
Злам					+		+			

Об’єкти / загрози	Кабельна система	Мережеве обладнання	Засоби мережевого захисту	Технологічна інформація захисту активного мережевого обладнання	Технологічна інформація захисту хостів (робочих станцій та серверів)	Дані, що передаються мережею	Програмне забезпечення	Файли	Записи баз даних	Обчислювальні ресурси
Використання вразливостей та слабких місць (експлоіт)					+		+	+	+	+
Фіксація дій на пристроях вводу інформації (кейлогер)					+			+	+	
Атака під час реєстрації (login attack)					+		+	+	+	
Захоплення облікового запису (account takeover, ATO)					+		+	+	+	
Загрози операційних систем										
Помилка, збій та відмова системного ПЗ							+	+		+
Перехоплення технологічної інформації захисту					+					
Пошкодження файлів ОС					+		+			
Збирання «сміття»					+			+		
Втручання в роботу ОС з мережі					+		+	+		
Руткіт (rootkit)					+		+	+	+	+
Атака нульового дня							+	+		+

2.3. Розробка моделі бази даних загроз інформаційним об’єктам захисту комп’ютерних систем та мереж об’єктів критичної інфраструктури

База даних «Кіберзагроз об’єктів критичної інформаційної інфраструктури Об’єднаної енергосистеми України в рамках впровадження концепції інтелектуальних мереж» (далі – БД) призначена для використання в автоматизованій системі розпізнавання несанкціонованого впливу на режими роботи об'єктів критичної інфраструктури. Кластерна структура бази даних орієнтована на зберігання параметрів елементів та об’єктів Об’єднаної енергосистеми, розрахункових параметрів режиму і інформації, отриманої від SCADA (існуючі системи управління і збору інформації) і EMS (Energy Management System) в реальному часі. При побудові моделі бази даних було використано загальні принципи побудови баз даних [5, 6, 82].

1. Функціональні режими БД.

Доступність даних. Надання уповноваженому користувачеві можливості вставляти, редагувати, видаляти та виймати дані із БД.

Метаопис даних. Система управління базою даних (далі - СУБД) повинна надавати системний каталог, в якому міститься:

- опис даних, які зберігаються в БД;
- опис зв’язків між даними;
- обмеження цілісності даних;
- реєстраційні дані користувачів;
- інша службова інформація.

Завдяки метаданим БД стає доступною для зовнішніх додатків, спрощується розуміння сенсу даних, посилюються заходи безпеки, виконуються передумови для аудиту інформації.

Управління паралельністю. Реалізація механізму одночасного багатокористувачевого (паралельного) доступу до даних, що обробляються, з гарантією їх коректного оновлення.

Обробка даних в рамках транзакції. БД даних завжди повинна

знаходитись у непротирічному стані в незалежності від будь-яких збоїв при проведенні операцій оновлення даних. Для цього операції з даними (в першу чергу вставки, редагування, видалення) об’єднуються у єдиний блок, який називається транзакцією. Всі оператори транзакції повинні бути виконані коректно та повністю, тільки в такому випадку в БД будуть зафіксовані зміни. В іншому випадку здійснюється автоматичний відкат транзакції, тобто стан БД буде відновлений на момент часу, який передував виклику транзакції.

Забезпечення цілісності даних. Всі дані, які містяться в БД, мають бути коректними та непротирічними. Це означає, що дані в таблицях можуть модифікуватися тільки у відповідності з затвердженими правилами. В загальному випадку мається на увазі три правила підтримки цілісності даних:

- цілісність доменів;
- цілісність відношень;
- цілісність зв’язків між відношеннями.

Відновлення даних. У випадку непередбачуваних помилок та збоїв, які призвели до пошкодження або руйнуванню даних, СУБД повинна мати можливість відновлювати постраждалі дані. В першу чергу ця функція реалізована за допомогою процедур резервного копіювання.

Обмін даними. СУБД повинна підтримувати сучасні технології та надавати доступ до БД віддаленим персональним комп’ютерам.

Контроль за доступом до даних. Доступ до даних можуть здійснювати тільки зареєстровані користувачі у відповідності із призначеними адміністратором СУБД їм правами.

2. Узагальнена структурна схема моделі бази даних.

Для того щоб СУБД виявилась в змозі надавати послуги, перелічені вище, вона повинна складатися із набору компонентів, наведених на рис. 2.6.

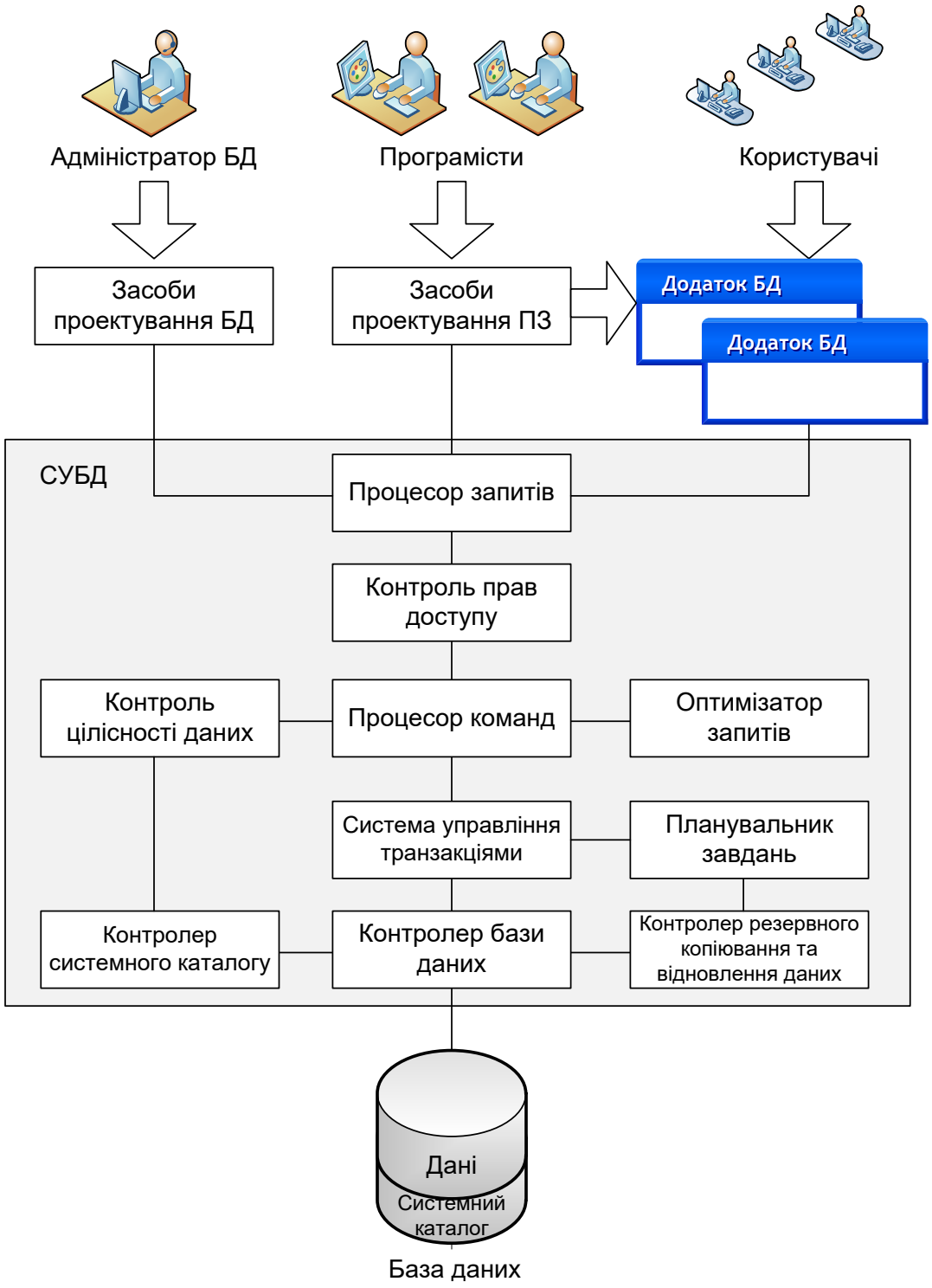

Рис. 2.6 – Узагальнена структура моделі бази даних

Над верхнім рівнем моделі БД розташовані споживачі послуг БД:

- адміністратор БД;
- програмісти;
- користувачі.

Адміністратор БД відповідає за планування та фізичну реалізацію проекту. Він створює основні об’єкти БД, визначає правила підтримки цілісності та не протиріччя і даних, керує політикою безпеки, аналізує процес експлуатації проекту, контролює ефективність системи.

Програмісти практично реалізують концепцію БД, розробляючи клієнтські додатки та звіти. Основним інструментом прикладного програмування є різні середовища проектування та розробки не нижче 4-го покоління.

Користувачами послуг БД виступають фахівці в сфері кібербезпеки, а також обслуговуючий персонал об’єктів критичної інформаційної інфраструктури.

Засобом взаємодії між користувачами та БД є структурована мова запитів SQL. Засоби проектування БД, ПЗ та клієнтські додатки надсилають до СУБД інструкції на мові SQL. Ці команди поступають на процесор запитів, який перетворює їх у набір низькорівневих команд, доступних ядру СУБД.

В СУБД існує модуль, що відповідає за контроль прав доступу користувачів з різними правами доступу. Отримані під час реєстрації пароль та логін потенційного клієнта БД звіряються з обліковими записами, що зберігаються в системному каталозі.

Після вдалої процедури автентифікації та авторизації користувача модуль контролю прав доступу надає доступ до процесору команд. В першу чергу процесор команд перевіряє, що команда, яка поступила, не протирічить обмеженням цілісності даних. Це зона відповідальності модуля контролю цілісності даних.

Під час перевірки команди на відповідність обмеженням цілісності доменів, суттєвостей та зв’язків долучається до дії контролер системного каталогу. Він збирає метадані, які містять технічний опис БД.

Переконавшись, що загрози цілісності відсутні, процесор передає команду оптимізатору запитів. Задача оптимізатора – знайти найбільш

ефективний спосіб виконання команд, що поступають.

Оптимізована команда компілюється та передається до системи управління транзакціями. Система управління транзакціями відповідає за повне та коректне виконання блоку команд, а також сумісно з планувальником завдань забезпечує паралельну багатокористувачеву обробку даних.

Потім блок команд передається до контролеру бази даних. Задача модуля полягає в організації взаємодії СУБД з файлами БД та файлами системного каталогу. При цьому для здійснення стандартних операцій вводу/виводу залучаються можливості операційної системи.

Системний каталог служить для зберігання наступної інформації:

- опис типів даних, що підтримуються БД;
- опис розгорнутих БД (схеми даних) та об’єктів (домени, таблиці, представлення тощо), що входять до них;
- відомості про обмеження цілісності;
- імена та права користувачів, що мають доступ до даних;
- статистичні дані.

Системний каталог реалізується як окрема БД з системними таблицями за замовчуванням, які приховані від звичайних користувачів.

3. *Доступ до бази даних.*

В моделі бази даних передбачається клієнт-серверна архітектура доступу. Клієнт-серверна модель БД передбачає, що БД розміщується на окремому сервері, на якому також встановлена СУБД. На клієнтських станціях встановлено користувацьке ПЗ та налаштований мережевий доступ до серверу БД. Клієнтський комп’ютер надсилає серверу запит, побудований на основі мови SQL. Отримавши та опрацювавши інструкцію SQL, сервер повертає клієнтському комп’ютеру результати її виконання.

Узагальнена архітектура «клієнт-сервер» наведена на рис. 2.7.

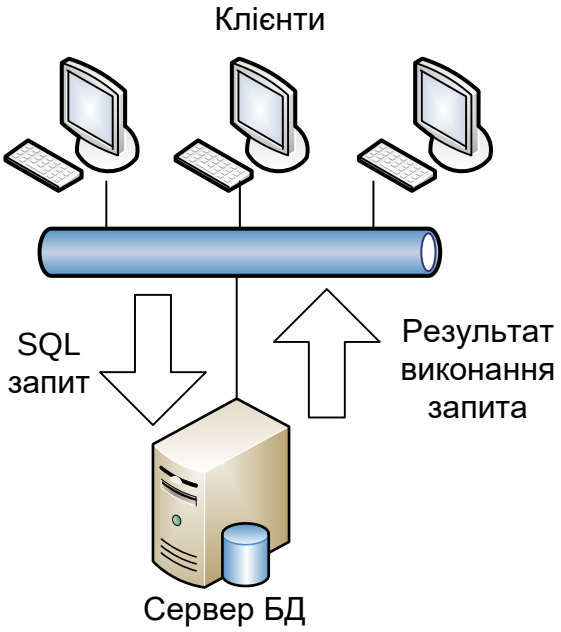

Рис. 2.7 – Узагальнена архітектура «клієнт-сервер»

Функціональні переваги клієнт-серверної архітектури моделі БД:

1) Підвищена доступність БД. Сервер являє собою відкриту систему, тому клієнтські комп'ютери можуть функціонувати під керуванням різних операційних систем та з різним ПЗ.
2) Виділений сервер СУБД в змозі забезпечити паралельну багатокористувачеву обробку даних.
3) Основні правила підтримки цілісності та непротирічності даних описуються на одному сервері СУБД. Ці правила актуальні для всіх клієнтських робочих станцій.
4) Гнучкий підхід до використання ресурсів комп'ютерних мереж.
5) Єдині правила безпеки для всіх учасників інформаційної взаємодії.
6) Наявність стандарту на основну мову взаємодії SQL забезпечує широкі можливості доступу до серверу БД від програмного забезпечення різних виробників.
7) Єдині правила обслуговування та адміністрування БД.

4. Адміністративний персонал та користувачі бази даних.

Передбачено наявність наступних категорій адміністративного

персоналу та користувачів БД:

1) Адміністратор даних, АД (Data Administrator, DA);
2) Адміністратор БД, АБД (Database Administrator, DBA);
3) Розробники БД;
4) Прикладні програмісти;
5) Користувачі.

На рис. 2.8 наведена узагальнена схема основних напрямів та видів діяльності персоналу при роботі з БД.

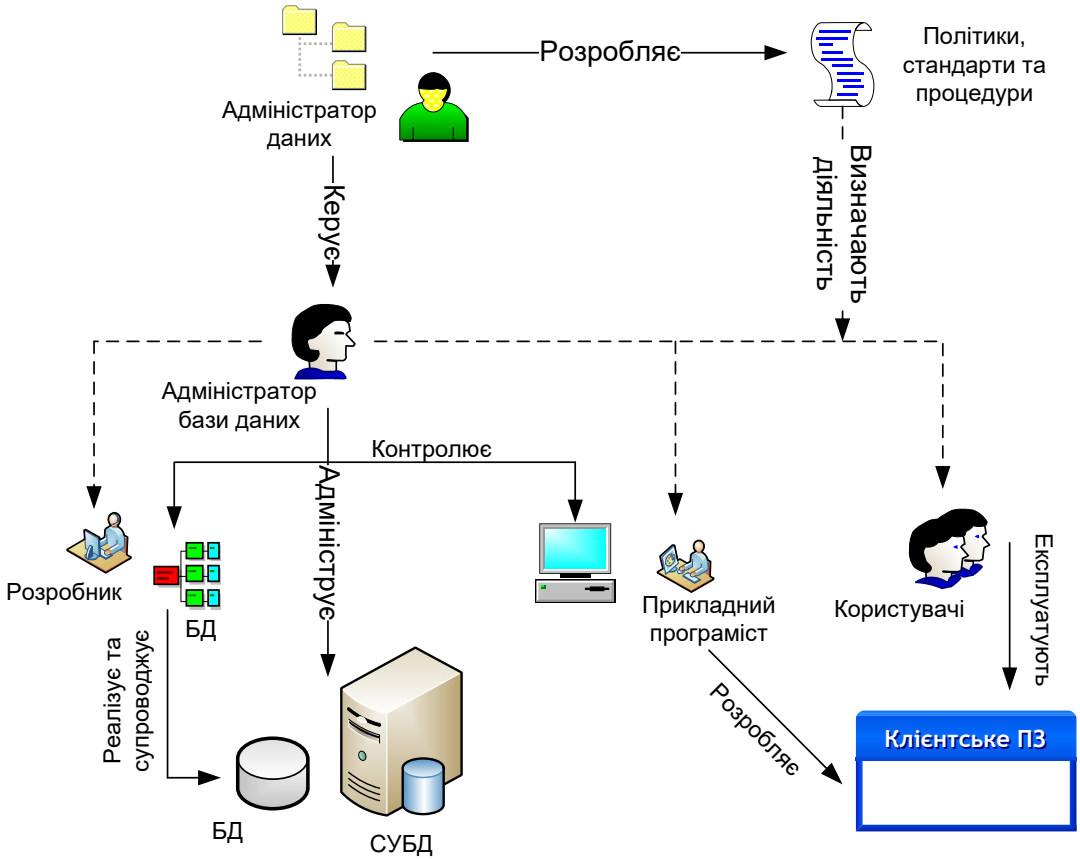

Рис. 2.8 – Загальні напрями та види діяльності персоналу при роботі з БД

Адміністратор даних виконує організаційні функції, а також відповідає за керування даними (планування БД, розробка стандартів та правил) та за концептуальне проектування БД.

Основні завдання адміністратора даних:

- надання допомоги у формуванні корпоративної стратегії побудови інформаційної системи (ІС);
- контроль за впровадженням та виконанням на всіх етапах життєвого циклу ІС політик, процедур та стандартів з коректного створення, використання та розповсюдження даних;
- розробка концептуальної моделі даних;
- планування процесу створення БД;
- надання вимог до даних, що використовуються;
- встановлення правил збору, зберігання та представлення даних;
- визначення політики інформаційної безпеки;
- розробка концептуальної та логічної моделей БД;
- взаємодія з АБД та програмістами з метою забезпечення відповідності БД, що розробляється, та клієнтських додатків існуючим стандартам та вимогам;
- контроль за модернізацією ІС та ПЗ;
- забезпечення повноти необхідної документації;
- взаємодія з користувачами БД.

Адміністратор бази даних відповідає за її реалізацію (в тому числі за фізичне проектування), забезпечення безпеки та цілісності даних, супроводження системи, а також за забезпечення оптимальної працездатності СУБД та додатків.

До завдань адміністратора бази даних відносяться:

- вибір цільової СУБД;
- розробка логічної моделі БД;
- забезпечення необхідного рівня захисту та цілісності даних;
- тестування БД;
- введення БД в експлуатацію;
- підготовка користувачів до роботи з БД;
- системне адміністрування СУБД;
- контроль працездатності;

- резервне копіювання;
- відновлення;
- реплікація;
- розмежування прав доступу користувачів;
- ведення технічної документації;
- супроводження БД.

Розробники бази даних, керуючись концептуальною моделлю даних та прийнятими політиками та стандартами, здійснюють розробку логічної, а потім фізичної моделі даних.

Прикладні програмісти здійснюють розробку та впровадження клієнтського ПЗ. До їх завдань входить:

- організація доступу клієнтського додатку до БД;
- проектування інтерфейсу користувача;
- наповнення додатку необхідним функціоналом;
- тестування та відладка додатків;
- супроводження додатків в період їх експлуатації.

Користувач є особою, що користується послугами БД, зокрема використовує інформації, що міститься в БД, у своїй повсякденній службовій діяльності.

Нижче наведені приклади сутностей таблиць бази даних.

Тип	Кіберзагроза
Threat	Spoofing
Specifications	Кількість виявлених IP-адрес у спам-базах
Specifications	Кількість спам-слів у темі
Specifications	Кількість спам-слів в повідомленні
Properties	Цілісність
Properties	Доступність
Properties	Спостережність
Protection	Налаштування управління доступом
Protection	Додаткова автентифікація (одноразовий пароль, криптографічна автентифікація)

Тип	Кіберзагроза
Threat	Sniffing
Specifications	Кількість пакетів з однаковою адресою відправника та отримувача
Specifications	Швидкість обробки запитів
Properties	Конфіденційність
Properties	Спостережність
Protection	Використання одноразових паролей
Protection	Встановлення програмних або апаратних засобів розпізнавання сниферів
Protection	Застосування засобів криптографічного захисту інформації

Тип	Кіберзагроза
Threat	Denial-of-Service, DoS
Specifications	Кількість одночасних підключень до серверу
Specifications	Кількість пакетів з однаковою адресою відправника та отримувача
Specifications	Швидкість обробки запитів
Specifications	Затримка між запитами від одного користувача
Properties	Доступність
Properties	Спостережність
Protection	Аналіз трафіку
Protection	Блокування шкідливих IP-адрес
Protection	Фільтрація трафіку
Protection	Адекватні апаратні потужності та канали зв’язку

Нижче наведена структура бази даних кіберзагроз об’єктів критичної інформаційної інфраструктури (рис. 2.9).

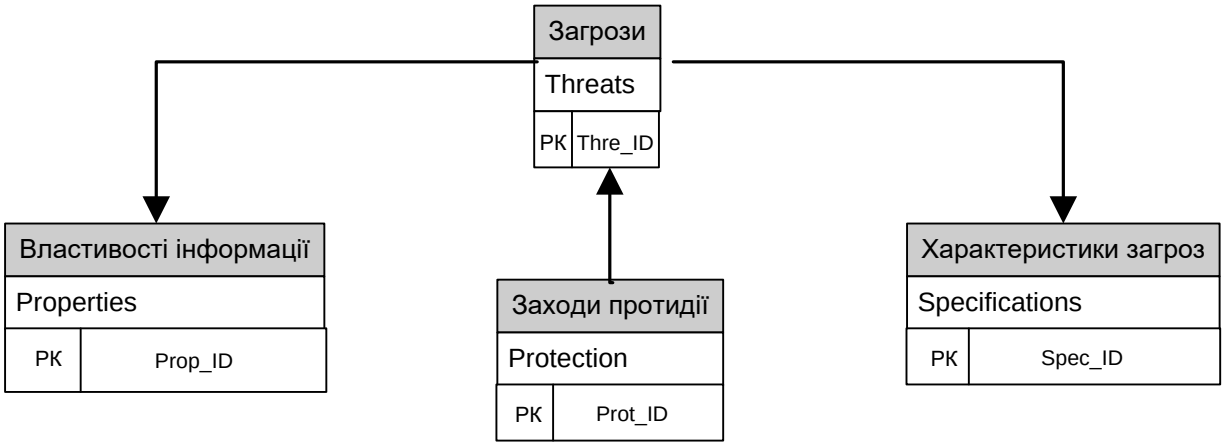

Рис. 2.9 – Структура бази даних кіберзагроз об’єктів критичної інформаційної інфраструктури

Фізичні характеристики логічних атрибутів наведені в таблиці 2.2.

Таблиця 2.2 – Фізичні характеристики логічних атрибутів

№	Назва атрибуту	Фіз. формат	Переклад назви атрибуту
1.	Threats	TXT	Назва загрози
2.	Properties	TXT	Властивості інформації
3.	Protection	TXT	Заходи протидії
4.	Specifications	TXT	Назва типу документу
5.	Thre_ID	BINARY	Ідентифікатор загрози
6.	Prop_ID	BINARY	Ідентифікатор властивості інформації
7.	Prot_ID	BINARY	Ідентифікатор заходу протидії
8.	Spec_ID	BINARY	Ідентифікатор характеристики загрози

2.4. Висновки до другого розділу

1. Виконано систематизацію кібератаки, як деревовидної структури, гілками якої є складові частини атаки – етап, дія, подія. Наведено структуру та зміст кожного з цих понять.

2. Приведена таксономія кіберзагроз, яка базується на комбінованому підході до вирішення задачі класифікації. У розробленій таксономії вводиться ієрархічна структура відносин з деревовидним розкриттям категорій. Як самостійний окремий об'єкт вводиться важливе поняття «етап атаки», що дозволяє природним чином описувати багатоетапні атаки, які отримали високу розповсюдженість на сьогоднішній день.

3. Проведено класифікацію кіберзагроз за об’єктами впливу. Результати класифікації покладено в основу розробленої матриці кіберзагроз для програмних та апаратних засобів об’єктів критичної інформаційної інфраструктури.

4. Удосконалено підходи до класифікації кіберзагроз, що дало змогу провести більш детальну їх класифікацію, розробити актуальну таксономію кіберзагроз, скласти матрицю кіберзагроз та розробити модель бази даних загроз інформаційним об’єктам захисту комп’ютерних систем та мереж

об’єктів критичної інфраструктури.

5. Розроблена модель бази даних загроз інформаційним об’єктам захисту комп’ютерних систем та мереж об’єктів критичної інфраструктури за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії, параметрів властивостей інформації, що підлягає захисту, дозволяє розробити базу даних кіберзагроз інформаційній безпеці комп’ютерних мереж та систем об’єктів критичної інфраструктури.

6. Результати розробки моделі бази даних зареєстровано, як твір, про що отримано відповідне свідоцтво [22].

РОЗДІЛ 3
СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОМ'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури

Теоретичні та практичні дослідження, пов'язані з забезпеченням кібербезпеки інформаційно-телекомунікаційних систем, в тому числі об'єктів критичної інфраструктури взагалі та підприємств електроенергетики зокрема, проводяться такими вітчизняними та іноземними вченими, як: В. Мохор, С. Гончар, Г. Кравцов, О. Богданов, В. Шаньгін, О. Замула, К. Монаппа, Б. Андерсон, Д. Мак-Грю та інші. За результатами аналізу науково-технічної літератури [7, 8, 38, 78, 87, 88, 93, 96] та спираючись на існуючий практичний досвід побудови систем захисту інформації розроблено метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури.

Метод ґрунтується на способі моніторингу трафіку, що надходить до відомчої інформаційно-телекомунікаційної системи з глобальної мережі Інтернет. Метод призначений для застосування у багаторівневій системі виявлення підозрілих впливів, яка здійснює моніторинг, аналіз та обробку покажчиків вхідного трафіку. Метод реалізує три рівня аналізу впливів:

1) Автоматичне сканування трафіку, визначення типу протоколу мережевої взаємодії;
2) Аналіз та виявлення таких підозрілих факторів, як відмова в обслуговуванні, підміна IP-адрес, вразливості (слабкі місця) протоколів мережевої взаємодії, вразливості (слабкі місця) додатків;
3) Атака (спроба підбору) на пароль, захоплення (привласнення) привілей, спроби впровадження шкідливого програмного забезпечення типу «троянські коні», аудит (моніторинг) мережі, скриті дії.

Відомий сигнатурний спосіб моніторингу інформаційно-

телекомунікаційних мереж, в основі якого покладено спеціалізоване програмне забезпечення виявлення та нейтралізації шкідливого програмного забезпечення – антивірусне програмне забезпечення, яке є програмним забезпеченням певного типу, що працює на обчислювальній машині. Антивірусне програмне забезпечення для аналізу використовує множину відомих вірусів, які занесені до власної бази даних. Антивірусна програма, переглядає файл або пакет на комп'ютері, звертається до власної бази даних, в яку занесені відомі віруси. У випадку відповідності будь-якої ділянки коду програми, що переглядається, відомому коду (сігнатурі) віруса в базі, антивірусне програмне забезпечення здійснює один із наступних заходів:

- знищує інфікований файл;
- переносить файл до «карантину» - робить його недоступним для виконання з метою недопущення подальшого розповсюдження вірусу;
- намагається відновити файл, видалив сам вірус з тіла файлу.

Даний спосіб має декілька переваг:

1) Відпрацьована надійність. Спосіб застосовується протягом тривалого періоду, що дозволило напрацювати основні механізми та засоби ефективного виявлення та знешкодження найбільш розповсюджених вірусних програм.
2) Висока швидкодія. Сучасні обчислювальні ресурси дозволяють здійснювати порівняння коду програми з сигнатурами антивірусних баз з високою точністю та оперативністю.

Недоліками відомого способу є:

1) Проблема лавиноподібного зростання сигнатур. Причиною цього явища є зростання кількості нових вірусів та їх особливість змінюватись. Як результат бази сигнатур збільшуються до надзвичайних розмірів, що призводить до нівелювання другої переваги способу – швидкодії. Як варіант вирішення проблеми розглядають застосування спеціальних оптимізацій, коли одна

сигнатура описує багато вірусів. Однак при цьому зменшується перша перевага.

2) Проблема виявлення нових вірусів. Вважається, що самі користувачі вносять занадто маленький внесок у збільшення бази даних вірусів. Тобто виявлення нових вірусів зазвичай вважається проблемою розробників антивірусу. Однак такий підхід порушує принцип «безпека стосується кожного». Разом з цим, як було зазначено вище, збільшення антивірусних баз неминуче призводить до втрати швидкодії обробки інформації.

Відомий спосіб евристичного пошуку шкідливих програм, 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.

Перевагами даного способу можна вважати:

1) Спосіб являє собою перспективний напрямок розвитку. Враховуючи сучасні тенденції розвитку обчислювальних систем та технологій штучного інтелекту, в майбутньому можливості евристичного модулю будуть тільки зростати, що неминуче призведе до підвищення рівня захищеності як програмних так і апаратних засобів обробки інформації.
2) На відміну від першого способу евристичний модуль має змогу реагувати на загрози, про які відсутня інформація в базі сигнатур.

Разом з цим у даного способу є декілька недоліків:

1) Помилкове спрацювання, як реакція 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 рівню захисту інформаційної системи.

2) Однією з особливостей роботи евристичного модулю є проблема надлишкового споживання обчислювальних потужностей. Тобто антивірусне програмне забезпечення займає невиправдано великі об’єми пам’яті та ресурсів процесору, що призводить до погіршення робочих характеристик інформаційної системи в цілому. Як наслідок відбувається подія, що була описана вище – відключення користувачем евристичного модуля.

Відомий спосіб моніторингу інформаційно-телекомунікаційних мереж, яка 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 має можливість перевіряти характеристики даних, що проходять через міжмережевий екран.

Багато програм 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.

Перевагами міжмережевого екрану є:

1) Налаштування міжмережевого екрану дозволяють забезпечити можливість мережевої взаємодії тільки з перевіреними ресурсами, відокремлюючи всі потенційно небезпечні та неперевірені мережеві ресурси.
2) 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 організації, 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 методу поставлено задачу розробки системи моніторингу та інтелектуального виявлення підозрілих впливів на мережеві об'єкти інформаційно-телекомунікаційної системи. Застосовуючи три рівні моніторингу та фільтрації трафіку, з'являється можливість відсікати більш широкий спектр загроз, порівняно з вищенаведеними існуючими способами захисту від мережевих атак.

Поставлена задача вирішується наявністю в системі виявлення підозрілих впливів трьох рівнів аналізу та фільтрації трафіку, які були наведені вище.

3.2. Структурна модель багаторівневої системи виявлення підозрілих впливів на ком'ютерні системи та мережі об'єктів критичної інфраструктури

Як зазначалося у попередньому пункті розроблений метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та

мереж об’єктів критичної інфраструктури реалізує трирівневий механізм сканування трафіку, запобігання проникненню на рівні додатків та системного програмного забезпечення, а також шкідливому програмному забезпеченню.

На основі зазначеного методу розроблено багаторівневу систему виявлення підозрілих впливів на комп’ютерні системи та мережі об’єктів критичної інфраструктури. За результатами розробки багаторівневої системи виявлення підозрілих впливів отримано Патент на корисну модель «Спосіб виявлення кібернетичних атак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури» [21].

На рис. 3.1 зображено структурну схему багаторівневої системи виявлення підозрілих впливів.

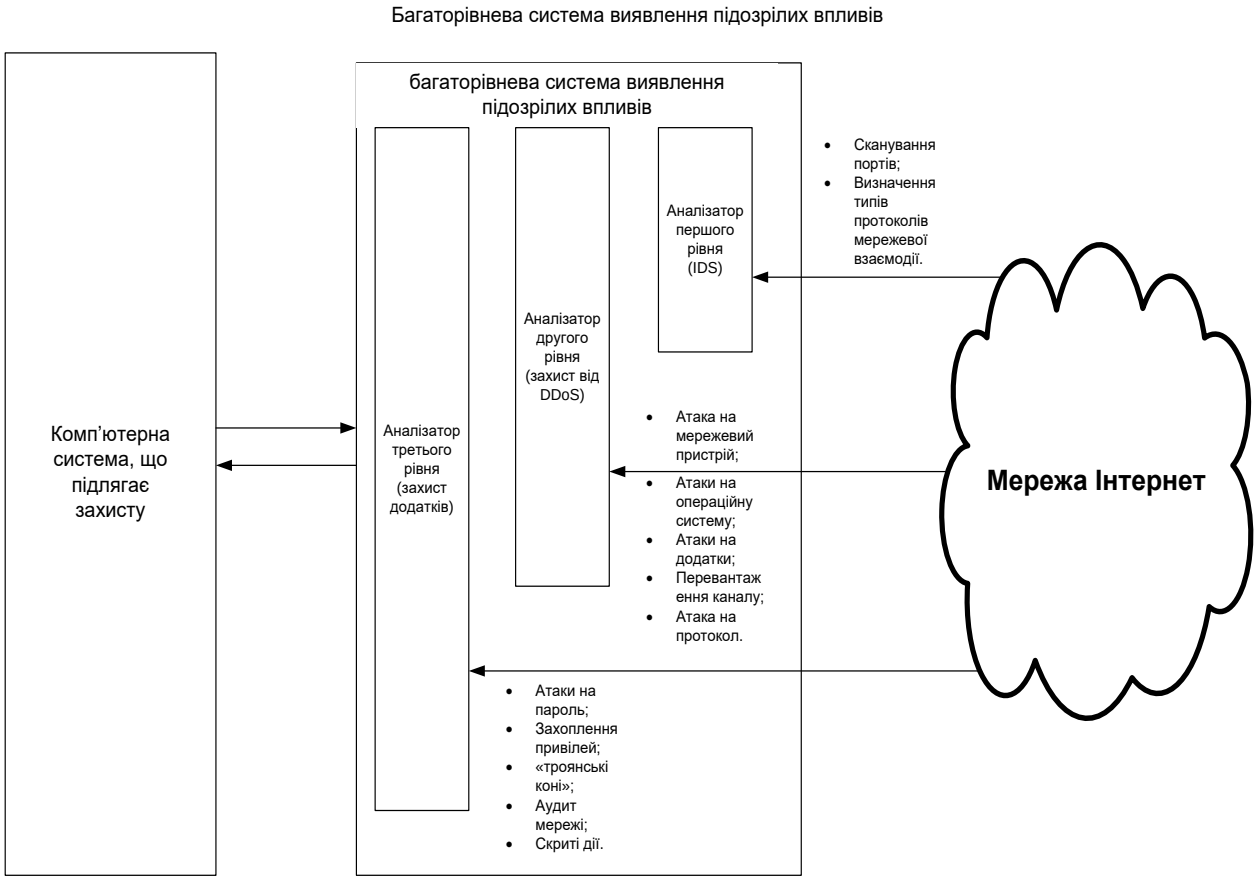

Рис. 3.1 – Структурна схема багаторівневої системи виявлення підозрілих кібервпливів

На першому рівні система виявлення підозрілих впливів реалізує контрзаходи 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). 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 система виявлення підозрілих впливів здійснює аналіз вхідного трафіку на предмет потенційної атаки типу «відмови в обслуговуванні» (DDoS). На цьому рівні система 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 аутентифікації користувача за паролем. Використовуючи дану уразливість, зловмисник нейтралізує можливість підключення до пристрою за допомогою протоколів telnet або ssh.
- Атаки на операційну систему (OS level) 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 багаторівнева система 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 система виявлення сигналізує адміністратора про

небезпеку та блокує вхідний трафік, який надходить від джерела небезпеки.

На третьому рівні система виявлення небезпечних 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 система діє за принципом чорного списку – виявлення хоча б однієї ознаки спроби небезпечної дії призводить до блокування вхідного трафіку від джерела небезпеки та сигналізації адміністратору.

Запропонована багаторівнева система виявлення підозрілих впливів дозволяє реалізовувати політику інтелектуального моніторингу та аналізу вхідного трафіку в реальному часі. Корисна дія такого моніторингу розповсюджується на широке коло системних та функціональних характеристик інформаційно-телекомунікаційної системи, що підлягає захисту. Розподілені за трьома рівнями механізми виявлення 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. В основу дії багаторівневої системи виявлення підозрілих впливів покладений принцип розподіленого моніторингу. Фактично, для того, щоб зловмисник отримав змогу проникнути до інформаційно-телекомунікаційної системи, що захищена за допомого багаторівневої системи виявлення підозрілих впливів, йому буде необхідно подолати трирівневий захисний рубіж. Такий підхід до захисту інформаційної системи значно (фактично в три рази) підвищить витрати на проникнення, що в багатьох випадках зробить такі дії нерентабельними.

3.3. Методика оцінювання кіберстійкості комп’ютерних систем та мереж об’єктів критичної інфраструктури

Функціонування об'єктів КІІ у кіберпросторі пов’язане з вразливостями систем захисту від кібервпливів (далі – КВ) і кіберзагрозами, та вимагає розробки нового інструментарію забезпечення стійкості функціонування в умовах кібератак. Управління стійкістю функціонування об’єктів КІІ ґрунтується на знаннях про стан об'єктів захисту, стан середовища функціонування і впливи, які відбуваються. Невід'ємним елементом систем управління об’єктів КІІ є низка підсистем підтримки прийняття рішень. Можливості системи управління безпосередньо залежать від здатності підсистеми підтримки прийняття рішень забезпечити відповідальну особу, яка приймає рішення, достовірною інформацією, що характеризує реальні і прогнозовані стани об'єктів критичної інфраструктури, та запропонувати обґрунтований вибір того чи іншого інструментарію, заходів та механізмів захисту, які дозволять забезпечити захист інформаційної системи від КВ на необхідному рівні.

Нижче приведена методика оцінки кіберстійкості об’єктів КІІ.

Запропонована методика [16] полягає в оцінці складних технічних систем, що мають високий ступінь критичності. Дану методику можливо застосовувати для підвищення ефективності управління критичною інфраструктурою, а також для обґрунтування нових методів і засобів захисту інформації від КВ.

Високий ступінь автоматизації управління і глобалізації інформаційних систем через всесвітню мережу Інтернет призвів до формування глобального інформаційного суспільства, яке функціонує в такому специфічному середовищі, як кіберпростір. Це ставить об'єкти КІІ, серед іншого, в залежність від ступеня захищеності інформаційно-телекомунікаційних систем, за допомогою яких вони функціонують.

Аналіз відкритих джерел [26 – 30, 33], що присвячені забезпеченню безпеки КІІ, надійності та стійкості функціонування АС об'єктів КІІ показав,

що в них практично не розглянуті питання, пов'язані:

- з розробкою моделей, методів та засобів реалізації систем оцінки стану об'єктів КІІ;
- з розробкою моделей, методів та засобів адаптивного управління КІІ, що враховують поточний і прогнозований стан об'єктів КІІ в умовах КВ;
- з розробкою науково-методичного апарата побудови автоматичної системи збору та приведення до єдиного вигляду інформації, що характеризує стан КІІ в умовах КВ.

Під поняттям кіберживучості розуміється здатність інформаційної системи виконувати свої функції в умовах здійснення КВ, які виникають внаслідок протиборства щонайменше двох сторін. Під час інформаційної взаємодії з метою здійснення КВ відбувається спільне використання загального ресурсу (глобального інформаційного простору), управління яким має розглядатися як цілеспрямований вплив двох (і більше) підсистем управління, які прагнуть поширити керуючий вплив одна на одну (Рисунок 3.2).

Незважаючи на суттєве спрощення та ідеалізацію, модель, наведена на Рисунку 3.2, дозволяє сформулювати найважливіші властивості, притаманні процесам управління в умовах здійснення КВ: адекватність, оптимальність, оперативність, стійкість і скритність.

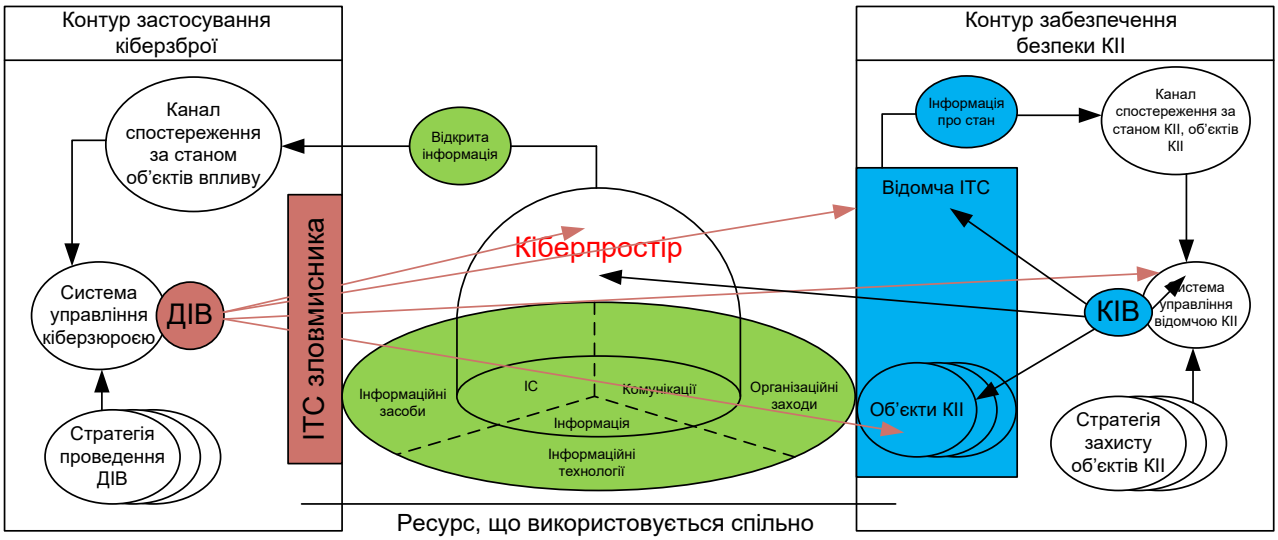

Рисунок 3.2 – Модель інформаційного протиборства в кіберпросторі

1 **Адекватність**. Адекватність управління полягає в здатності системи здійснювати перетворення інформації про стан об'єкта, отриманої від підсистеми моніторингу, в керуючий інформаційний вплив (КІВ), на основі якого об'єкт управління переходить до стану, який відповідає ситуації, що склалася. Вочевидь коректність перетворень багато в чому залежить від достовірності отриманої інформації про стан і правильності визначення цільової функції об'єкта управління. Отже, властивість адекватності значною мірою залежить від достовірності і повноти інформації, коректності операцій перетворення інформації та їх послідовності.

2 **Оптимальність**. Під оптимальністю управління розуміється вибір таких керуючих впливів, за яких точно досягається екстремальне значення деякого критерію, що характеризує якість управління. Зазвичай намагаються мінімізувати втрати в системі, що зазнає впливу, – грошові втрати або інші ресурси, що підлягають втраті. Інакше кажучи, оскільки всі допустимі траєкторії призводять до мети, і кожна з них характеризується певною витратою ресурсів (часом, додатковим навантаженням на обчислювальні ресурси тощо), то в розумінні «кращого» споживання цих ресурсів (з погляду доцільності їх споживання) існує краща траєкторія. Якщо в процесі управління система «рухається» в просторі ситуацій саме цією траєкторією,

то кажуть, що управління оптимальне.

3 **Оперативність**. Оперативність управління – це здатність системи перетворювати інформацію відповідно до часових обмежень. Інакше кажучи, оперативністю є властивість управління перетворювати інформацію відповідно до темпу зміни поточної ситуації. Залежно від виду операції, яка домінує в тому чи іншому процесі управління, розрізняють оперативність семантичного (смислового) перетворення (наприклад, вироблення рішення) та оперативність перетворення інформації (наприклад, оперативність передачі даних або виконання якихось розрахунків) тощо.

4 **Стійкість**. Стійкість управління визначається здатністю системи управління виконувати свої функції в складних обставинах, що різко змінюється, в умовах деструктивних впливів різної природи протиборчої сторони (сторін). Як правило, стійкість є інтегральною властивістю, що визначається живучістю, завадостійкістю і надійністю, під якими розуміється здатність здійснювати управління в умовах впливу всіх деструктивних видів, технічних і програмних відмов, а також помилкових дій технічного персоналу і посадових осіб, зберігаючи водночас значення всіх показників управління в установлених межах.

5 **Скритність**. Властивість процесу управління зберігати в таємниці від протиборчої сторони факт, час і місце перетворення інформації, а також її зміст і належність до керуючих об'єктів.

Деструктивні інформаційні впливи (кібератаки, кібервпливи) є збурюючим впливом. Система управління об'єктом КІІ має компенсувати ці збурення, а загалом об'єкт та система управління повинні бути стійкими до цих збурень, тобто бути кіберстійкими (cyber stability). Одним з видів стійкості є кіберстійкість об'єкта КІІ, під якою розуміється здатність системи управління об'єкта КІІ виконувати свої функції в складних, різко мінливих обставинах в умовах КВ.

Під час оцінки кіберстійкості об'єктів КІІ, як складових елементів КІІ виникає низка проблем, пов'язаних зі складністю самих об'єктів КІІ,

складністю і різнорідністю зв'язків між ними і умовами спільного із зловмисником використання ресурсів ІТКМ ЗК.

Існують різноманітні об'єкти КІІ [23, 26] і для подальшого їх розгляду доцільно провести їх декомпозицію за ознаками, що впливають на забезпечення кіберстійкості:

За структурною організацією:

Одноланкові і багатоланкові.

Одноланковий об'єкт КІІ – це самодостатній об'єкт, який володіє всією необхідною структурою для виконання цільової функції (самостійний одиничний (базовий) елемент).

Прикладом одноланкової структури можуть виступати окремі АС.

Багатоланковий об'єкт КІІ – об'єкт, який являє собою структурне послідовне об'єднання декількох одноланкових об'єктів КІІ в єдину систему в рамках виконання єдиної цільової функції.

За функціональною однорідністю:

Багатоланкові однорідні і багатоланкові неоднорідні.

Багатоланковий однорідний об'єкт КІІ – об'єкт, який являє собою структурне об'єднання декількох одноланкових об'єктів КІІ, що виконують однакову цільову функцію, в єдину систему в межах виконання єдиної цільової функції.

Прикладом багатоланкової однорідної структури є багатоінтервальна (складна) мережа передачі даних, що складається з різнотипних одноланкових систем передачі даних.

Багатоланковий різнорідний об'єкт КІІ – об'єкт, який являє собою структурне об'єднання декількох одноланкових об'єктів КІІ, що виконують різні функції, наприклад, інформаційно-телекомунікаційна мережа, інформаційні системи тощо.

Об'єкти КІІ, які використовують ІТКМ ЗК, як правило, завжди є багатоланковими. Водночас, склад окремих ланок цих ліній залежить від обраних маршрутів проходження інформації по ІТКМ ЗК, а також відомчих

інформаційно-телекомунікаційних систем.

З огляду на вищезазначене пропонується ввести деякий узагальнений показник кіберстійкості.

Узагальнений показник кіберстійкості одноланкового об'єкта КІІ має вигляд:

$$К_{ОКІІ}^{уп} = К_{ОКІІ}^{жив} * К_{ОКІІ}^{зах} * К_{ОКІІ}^{над} \quad (1)$$

де:

$\mathbf{К_{ОКІІ}^{уп}}$ – узагальнений показник кіберстійкості;

$К_{ОКІІ}^{жив}$ – **кіберживучість** об'єкта КІІ, яка трактується як здатність збереження його працездатності (виживання) в умовах виходу з ладу технічних засобів обробки інформації внаслідок КВ, тобто, по суті, – внесок кожного базового елемента одноланкового об'єкта КІІ у виконання ним цільової функції;

$\mathbf{К_{ОКІІ}^{зах}} = (1 – Р_{ЗКА})*(1 - Р_{ЦКА})$ – **кіберзахищеність** одноланкового об’єкта КІІ, що трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ із заданою якістю в умовах застосування «загальних» і цілеспрямованих КВ;

$Р_{ЗКА}$ і $Р_{ЦКА}$ – ймовірності ураження технічних засобів обробки інформації, що входять до об’єкта КІІ, загальними ($Р_{ЗКА}$) та цілеспрямованими ($Р_{ЦКА}$) КВ;

$К_{ОКІІ}^{над}$ – **кібернадійність** одноланкового об’єкта КІІ, під якою розуміється ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах виникнення різних подій (i = 1,…., N) – програмних та технічних відмов засобів об'єкта КІІ внаслідок ДІВ, де

$$К_{ОКІІ}^{над} = \prod_{i=1}^{N} K_{ОКІІНАДi} (1 - P_i) \quad (2)$$

де $Р_i$ – імовірність i-ої події (i = 1,…., N)

До об'єктів КІІ вже на етапах проєктування висуваються досить жорсткі вимоги з технічної надійності і передбачається низка спеціальних заходів щодо запобігання технічним і програмним відмовам технічних

засобів обробки інформації (наприклад, завдяки кластеризації серверів, через резервування окремих компонентів). Відповідно до цього в завданнях оцінки кіберстійкості КІІ цілком допустимо вважати ймовірність програмних та технічних відмов за умови своєчасного і якісного проведення технічного обслуговування та оновлення зневажливо малою, тобто $P_{ТН}=0$, де $P_{ТН}$ – імовірність технічного неспрацювання. У цьому разі кібернадійність одноланкового об'єкта КІІ буде визначатися як:

$$К_{ОКІІ}^{о} = К_{ОКІІ}^{жив} * К_{ОКІІ}^{зах} \quad (3)$$

Якщо вважати виходи з ладу ланок КІІ в умовах КВ незалежними подіями, кіберстійкість багатоланкового об’єкта КІІ ($К_{ОКІІстб}$) може бути знайдена із виразу:

$$К_{ОКІІстб}(N) = \prod_{i=1}^{N} К_{ОКІІоі} \quad (4)$$

де N – кількість різних шкідливих подій, зумовлених КВ;

$К_{ОКІІоі}$ – кіберстійкість i-го одноланкового об’єкта КІІ.

Кібернадійність багатоланкового об'єкта КІІ трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах виникнення програмних помилок і технічних збоїв одноланкових об'єктів КІІ, з яких складається багатоланковий.

Тобто кіберстійкість багатоланкового об'єкта КІІ має розраховуватися як спільна N-мірна функція розподілу ймовірності збереження працездатності одночасно N ланок, які складають цей багатоланковий об'єкт КІІ:

$$К_{ОКІІсб}\left(К_{ОКІІсо1,\ldots,}\, К_{ОКІІсоN}\right) = P\left\{К_{ОКІІсо1} \geq К_{ОКІІсопотр}, \ldots, К_{ОКІІсоN} \geq К_{ОКІІоспотр}\right\} \quad (5)$$

де:

$К_{ОКІІсб}(N)$ – кіберстійкість багатоланкового об’єкта КІІ;

$K_{ОКІІсо1}$ – кіберстійкість першого одноланкового об’єкта КІІ;

$K_{ОКІІсопотр}$ – потрібна кіберстійкість першого одноланкового об’єкта КІІ;

$K_{ОКІІсоN}$ – кіберстійкість N-го одноланкового об’єкта КІІ;

$K_{ОКІІоспотр}$ – потрібна кіберстійкість N-го одноланкового об’єкта КІІ.

Основою розрахунку кіберстійкості багатоланкових об'єктів КІІ є розрахунок показників кіберзахищеності і кіберживучості окремих ланок об'єкта КІІ.

Тому, необхідно розробити методику розрахунку показників кіберзахищеності і кіберживучості об'єкта КІІ, причому визначальною властивістю з погляду можливості виконання об'єктом КІІ цільової функції буде кіберживучість, а кіберзахищеність буде складовою частиною функції.

Методика оцінки кіберживучості об'єктів КІІ

Зважаючи на те, що властивості, які характеризують кіберживучість об'єкта КІІ в умовах здійснення ДІВ – Ω, починають проявлятися тільки після того, як об’єкт зазнав впливу, то міра живучості має визначатися умовною імовірністю збереження працездатності, за умови, що система отримала локальне пошкодження.

Під показником кіберживучості одноланкового об’єкта КІІ, $К_{ОКІІ\ ЖИВ}$, будемо розуміти умовну ймовірність невиходу кінцевого стану об’єкта КІІ за межі заданої області безпечних станів S^I простору безпечних станів S у разі проведення КВ S_0.

$$K_{ОКІІЖИВ} = P[(\|S - s_0\| < S^I)/\Omega]. \qquad (6)$$

З огляду на розуміння функціональної вразливості системи V_S, під якою будемо розуміти ймовірність виходу кінцевого стану системи із заданої безпечної області S^I, справедливо:

$$К_{ОКІІ\ ЖИВ} = 1 – V_S, \qquad (7)$$

а в конкретній точці часового інтервалу, що досліджується:

$$К_{ОКІІ\ ЖИВ}(t) = 1 – V_S(t). \quad (8)$$

Критерієм оцінки кіберживучості одноланкового об’єкта КІІ будемо розглядати вираз:

$$К^{пот}_{ОКІІЖИВ}(t) \geq К^{тр}_{ОКІІЖИВ}(t), \quad (9)$$

де $К^{пот}_{ОКІІЖИВ}(t)$ – поточний рівень кіберживучості одноланкового об’єкта КІІ, а $К^{тр}_{ОКІІЖИВ}(t)$ – потрібний рівень його кіберживучості в умовах здійснення КВ.

Також визначимо наступний критерій здатності об’єкта КІІ виконувати цільову функцію в умовах ДІВ W_6:

$$W_6 = \begin{cases} К^{пот}_{ОКІІЖИВ}(t) > Н1 - об'єкт\ КІІ\ повністю\ дієздатний \\ Н2 \leq К^{пот}_{ОКІІЖИВ}(t) < Н1 - об'єкт\ КІІ\ загалом\ дієздатний \\ Н3 \leq К^{пот}_{ОКІІЖИВ}(t) < Н2 - об'єкт\ КІІ\ обмежений \\ Н4 \leq К^{пот}_{ОКІІЖИВ}(t) < Н3 - об'єкт\ КІІ\ недієздатний(підлягає\ відновленню) \\ К^{пот}_{ОКІІЖИВ}(t) \leq Н4 - об'єкт\ КІІ\ недієздатний(не\ підлягає\ відновленню) \end{cases} \quad (10)$$

Де:

$Н_1$ – система повністю справна та функціонує у відповідності до проектної та експлуатаційної документації;

$Н_2$ – система в цілому справна та функціонує у відповідності до експлуатаційної документації, при цьому можливі відхилення від проектних рішень;

$Н_3$ – система вийшла з ладу, функціональні характеристики не відповідають проектній документації;

$Н_4$ – система недієздатна, функціональні характеристики не відповідають проектній та експлуатаційній документації.

Для визначення поточного показника кіберживучості

$K^{пот}_{ОКІІN ЖИВ}(t)$ введемо наступні рівні кіберживучості:

$$K_{ОКІN\ ЖИВ}(t) = \begin{cases} K^{пот}_{ОКІ\ ЖИВ}(t) - K^{тр}_{ОКІ\ ЖИВ}(t) > 0 - \textit{оптимальний рівень} \\ K^{пот}_{ОКІ\ ЖИВ}(t) - K^{тр}_{ОКІ\ ЖИВ}(t) = 0 - \textit{допустимий рівень} \\ K^{пот}_{ОКІ\ ЖИВ}(t) - K^{тр}_{ОКІ\ ЖИВ}(t) < 0 - \textit{критичний рівень} \\ K^{пот}_{ОКІ\ ЖИВ}(t) = 0 - \textit{надкритичний рівень} \end{cases} \quad (11)$$

Узагальнені результати, отримані у виразах (10) и (11), та їх візуалізація наведені на Рисунку 3.3.

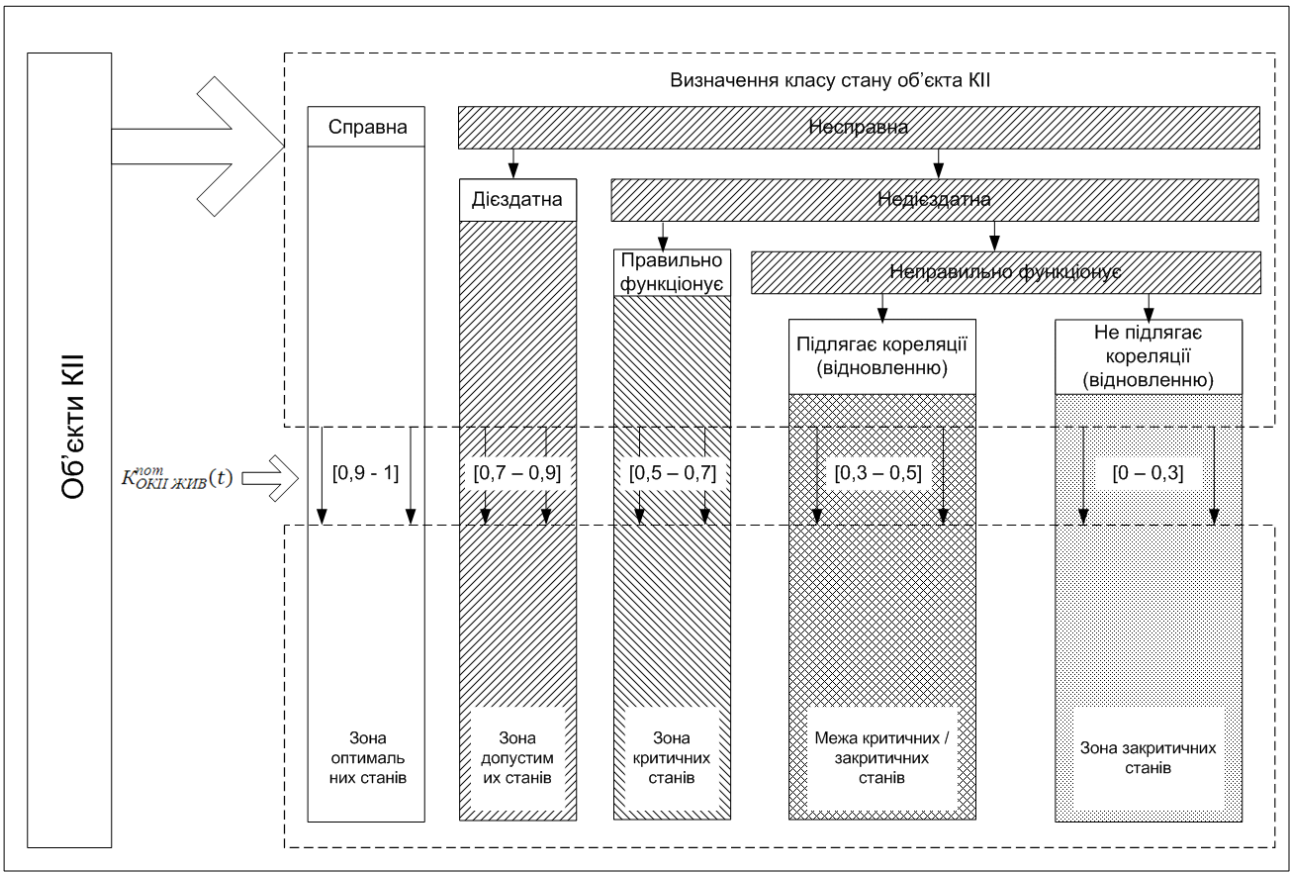

Рисунок 3.3 – Схема відповідності класу стану об'єкта КІІ рівню кіберживучості

Методика оцінки кіберстійкості охоплює такі етапи:

1. Оцінка кіберживучості кожного об'єкта КІІ окремо.

1.1. Оцінка кіберживучості одноланкового об'єкта КІІ.

Рівень кіберзахищеності – ймовірність збереження працездатності *i*-го елемента в умовах КВ.

Оцінити коефіцієнт пов'язаності *i*-го елемента і його внесок в цільову

функцію об'єкта КІІ.

1.2. Оцінка кіберживучості багатоланкового об'єкта КІІ.

Рівень кіберзахищеності – ймовірність збереження працездатності *j*-го одноланкового об'єкта КІІ в умовах реалізації КВ.

Оцінити коефіцієнт пов'язаності *j*-го одноланкового об'єкта КІІ та його внесок у цільову функцію багатоланкового об'єкта КІІ.

2. Оцінка кіберживучості взаємодіючих об'єктів КІІ (стовпчиків об'єктів КІІ).

Рівень кіберзахищеності – ймовірність збереження працездатності *n*-го багатоланкового об'єкта КІІ в умовах реалізації КВ.

3. Оцінка кіберживучості КІІ через суму стійкості її елементів з урахуванням їх коефіцієнта пов'язаності.

Оцінка кіберживучості КІІ загалом, відповідно до поточного стану КІІ і ступеня важливості, в певний момент часу, виконання ними функцій.

Під час розробки методики оцінки стійкості об'єктів КІІ було запропоновано введення такої властивості, як кіберстійкість. Необхідність введення такої властивості викликана специфічним середовищем функціонування мережевої інфраструктури об’єктів КІІ (кіберпростір) і, як наслідок, появою нових вразливостей і загроз для об'єктів КІІ Об′єднаної енергосистеми України. Запропонована методика завдяки декомпозиції КІІ на окремі об'єкти КІІ з урахуванням коефіцієнтів зв′язаності і ступеня важливості функцій, які виконуються в цей момент, дозволяє здійснити оцінку кіберстійкості КІІ відповідно до заданого рівня. Отриманий результат, відповідно до розробленої схеми відповідності стану об'єкта КІІ рівню захищеності (Рисунок 3.3), дозволяє однозначно оцінити стан кіберзахищеності КІІ від кібератак (КВ).

Методика оцінки кіберстійкості КІІ схематично зображена на Рисунку 3.4.

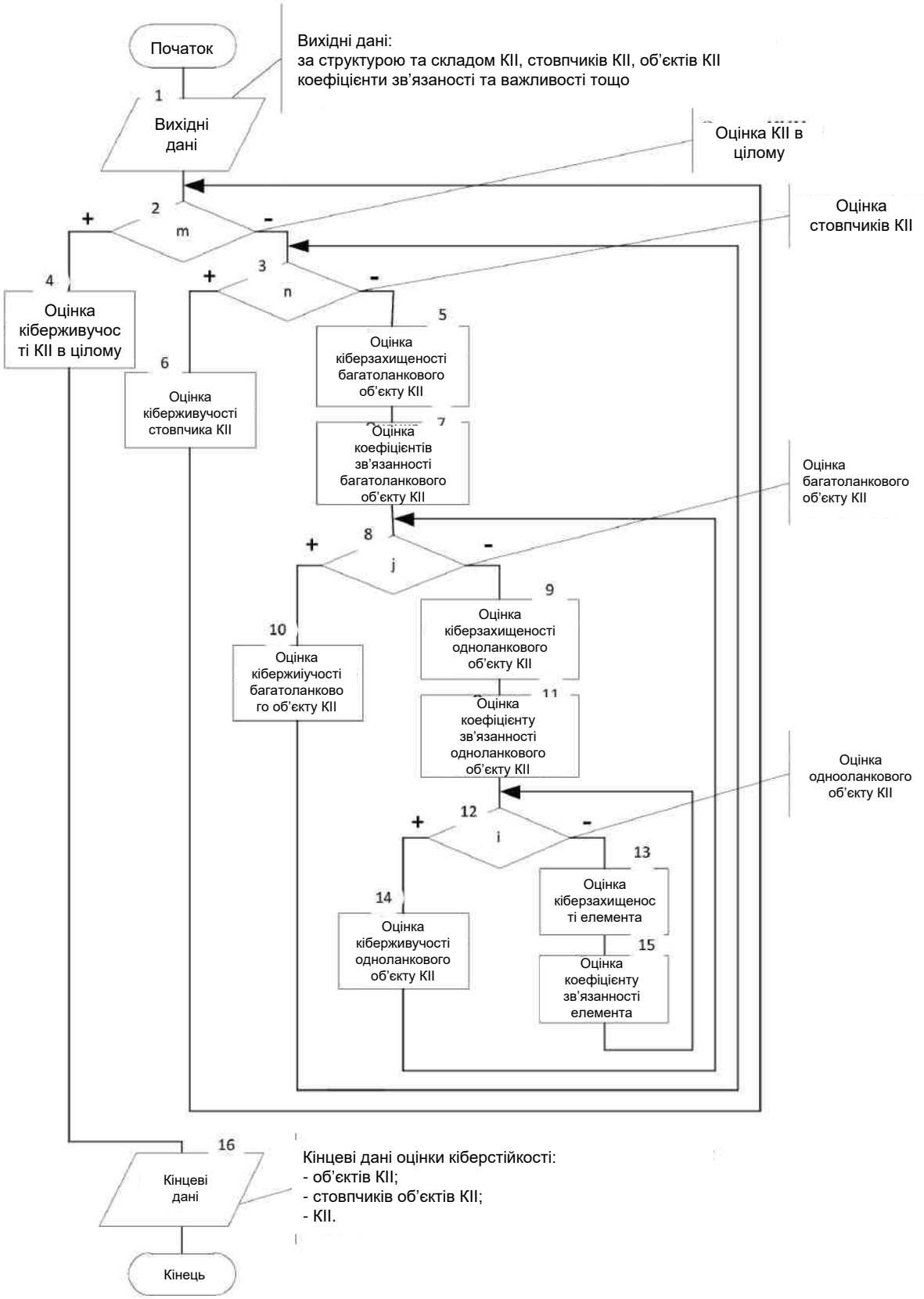

Рисунок 3.4 – Узагальнений алгоритм методики оцінки кіберстійкості КІІ

3.4. Висновки до третього розділу

1. Запропонований комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури, який за рахунок поєднання сигнатурного методу та методу виявлення аномалій, дозволяє розширити спектр виявлених кіберзагроз. Застосовуючи три рівні моніторингу та фільтрації трафіку, з'являється можливість відсікати більш широкий спектр загроз, порівняно з існуючими способами захисту від мережевих атак.

2. Розроблений метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури реалізує трирівневий механізм сканування трафіку, запобігання проникненню на рівні додатків та системного програмного забезпечення, а також шкідливому програмному забезпеченню.

3. На основі зазначеного методу розроблено багаторівневу систему виявлення підозрілих впливів на комп'ютерні системи та мережі об'єктів критичної інфраструктури.

4. Розроблено метод розрахунку узагальненого показника кіберстійкості об'єкту критичної інформаційної інфраструктури, який включає в себе показники кіберживучості, кіберзахищеності та кібернадійності однлланкових та багатоланкових об'єктів КІІ.

3. На основі запропонованих методів розроблено методику оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури, яка за рахунок використання розробленої таксономії кіберзагроз та моделі бази даних кіберзагроз дозволяє забезпечити підтримку створення систем захисту інформації комп'ютерних систем та мереж об'єктів критичної інфраструктури.

РОЗДІЛ 4
ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ КОМ'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

4.1. Розробка алгоритмів та програмного застосунку систем захисту інформації ком'ютерних систем та мереж об'єктів критичної інфраструктури

На базі запропонованої методики розроблено алгоритмічне забезпечення для реалізації відповідного програмного забезпечення і на їх основі розроблено прикладний програмний застосунок, що реалізує запропоновані у даній дисертаційній роботі методи.

На підставі багаторівневого методу розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури розробляємо алгоритм виявлення та запобігання кібервпливам на комп'ютерні системи та мережі об'єктів критичної інфраструктури. Схему алгоритму представлено на рис. 4.1.

Представлений алгоритм передбачає первинну перевірку на предмет сканування портів та визначення типів протоколів міжмережевої взаємодії. За умови відсутності таких дії ззовні мережі цикл замикається та повертається до початкового стану. У разі виявлення фактів сканування портів ззовні мережі система здійснює блокування підозрілих IP-адрес, після чого здійснює аналіз вхідного трафіку. У разі відсутності зловмисних дій система повертається до початкового стану. У разі виявлення атаки на мережеві пристрої, операційні системи, додатки чи протоколи, багаторівнева система здійснює блокування вхідного трафіку. Після чого відбувається моніторинг системних параметрів. У разі відсутності підозрілих дій система повертається до початкового стану. У разі виявлення атаки на пароль, захоплення привілей, аудиту мережі, скритих дій чи шкідливого ПЗ, система сигналізує про це адміністратору та блокує вхідний трафік від джерела

небезпеки. Після чого активуються антивірусні механізми, які здійснюють відповідні заходи (видалення/блокування/карантин) із шкідливим ПЗ.

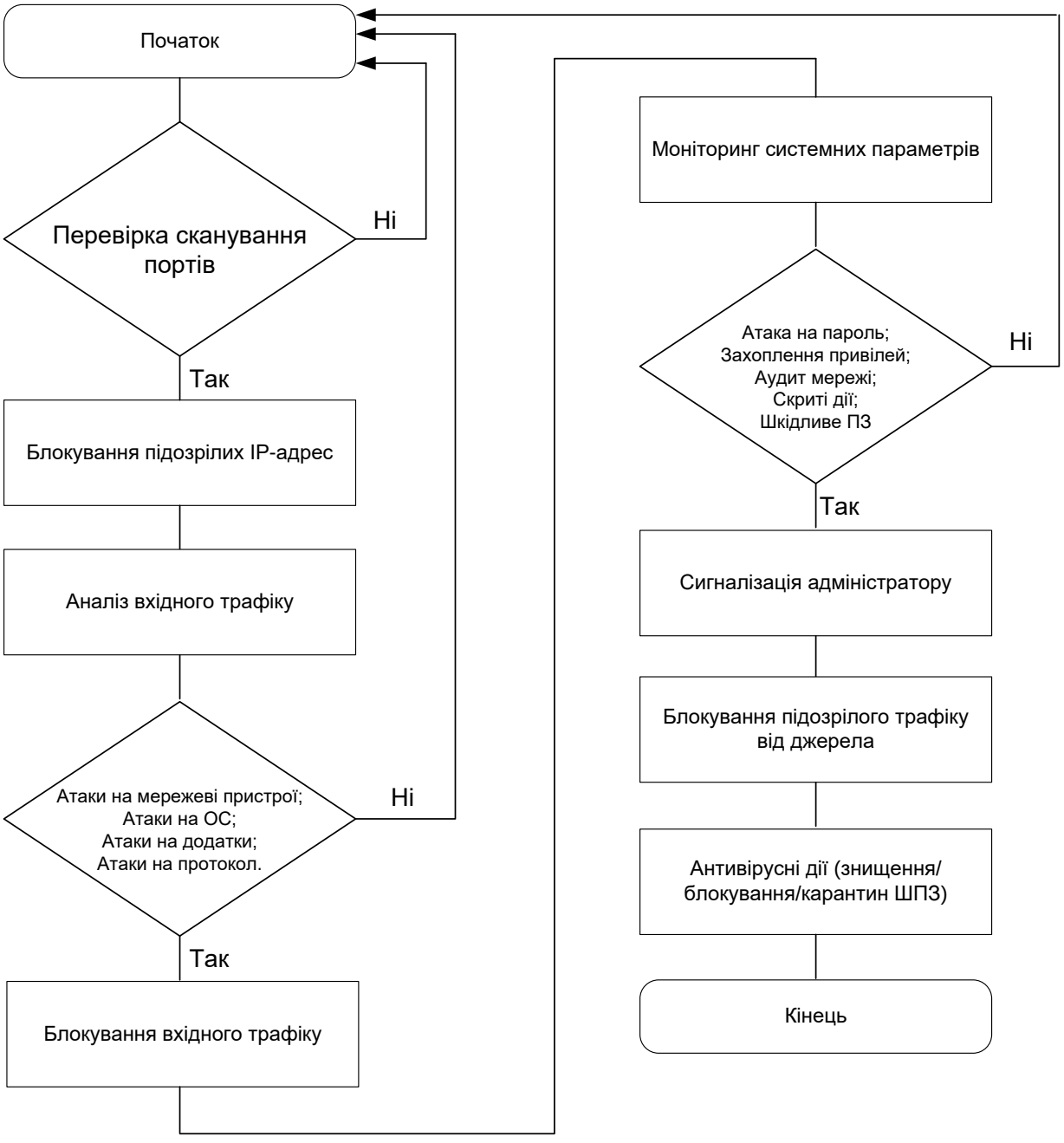

Рис. 4.1. Схема алгоритму функціонування багаторівневої системи виявлення підозрілих впливів

На підставі методики оцінки кіберстійкості КІІ розроблено відповідний алгоритм оцінки кіберстійкості об’єкту КІІ. Схему алгоритму представлено на рис. 3.4.

Представлений алгоритм передбачає введення вхідних даних, якими характеризується об’єкт КІІ, а саме клас, структура, склад, стан, коефіцієнти зв’язності та важливості об’єктів КІІ. На наступному етапі здійснюється оцінка кіберстійкості кожного об’єкта КІІ окремо. Після цього визначаються коефіцієнти зв’язності взаємодіючих об’єктів КІІ. Наступним етапом є оцінка кіберстійкості об’єкту КІІ через суму стійкості її елементів з урахуванням коефіцієнтів їх зв’язаності, включаючи оцінку кіберживучості об’єкту КІІ в динаміці при виконанні ним своїх цільових функцій.

На базі представлених алгоритмів розроблено програмний застосунок запропонованої у даній дисертаційній роботі методики.

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 Мбайт дискового простору.

Інтерфейс програмної системи оцінки кіберстійкості об’єкту КІІ, представлений на рис. 4.2.

Введення вхідних даних здійснюється в правому блоці інтерфейсного вікна програми у віконці «Додати об’єкт». Вхідними даними при цьому характеристики об’єкта КІІ, які є об’єктами обчислення, а саме показник кіберживучості, показник кіберзахищеності та показник кібернадійнсоті. Вхідні дані формуються розрахунковим методом за формулами, наведеними у п. 3.3. При цьому, ймовірність визначається у діапазоні від 0 до 1, а стани об’єкту КІІ можуть виражатися у відносних одиницях, відносно максимального значення. Натискаючи кнопку «Додати об’єкт» можливо вводити параметри необхідної кількості об’єктів КІІ. Після завершення введення вхідних даних, після натискання внизу справа інтерфейсного вікна

програми кнопки «Розрахунок», справа внизу у віконці «Результати розрахунків» з′являться результати розрахунку.

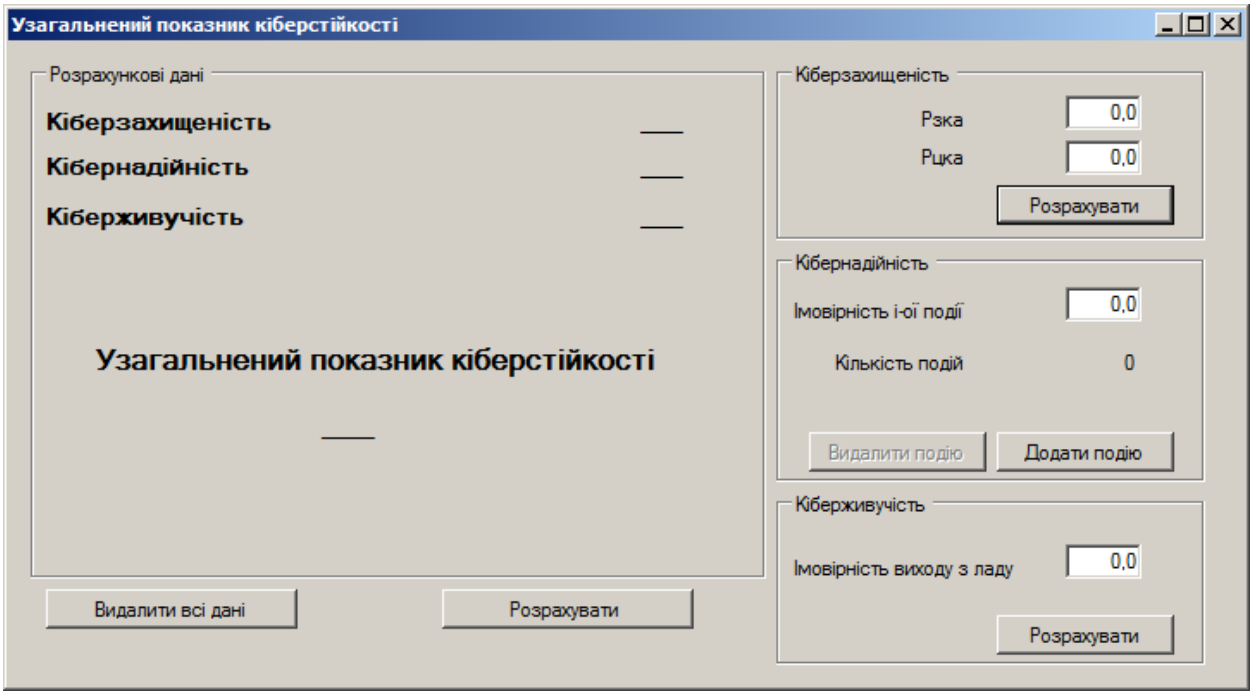

Рис. 4.2. Інтерфейс програми

Лістинг (коди) програмного застосунку приведено у додатку Б дисертаційної роботи.

4.2. Дослідження систем захисту інформації ком’ютерних систем та мереж 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 комплексних систем захисту інформації атомних електростанцій та автоматизованої інформаційної системи «Централізована база даних

перенесених номерів» ДП «Український державний центр радіочастот» [97, 98].

Далі наведено більш детальне практичне застосування програмного застосунку при створенні комплексної системи захисту інформації автоматизованої інформаційної системи «Централізована база даних перенесених номерів» ДП «Український державний центр радіочастот».

У ході проведення обстеження середовища функціонування автоматизованої інформаційної системи «Централізована база даних перенесених номерів» ДП «Український державний центр радіочастот» було досліджено об’єкти захисту, потенційні загрози інформації, розроблено модель порушника та модель загроз для інформації даної автоматизованої інформаційної системи.

Призначення та функції АІС

Автоматизована інформаційна система «Централізована база даних перенесених номерів» призначена для автоматизації процесів:

- перенесення абонентських номерів від оператора-донора до оператора-отримувача;
- інформаційного обміну між операторами телекомунікацій під час ППН;
- збору та обробки інформації про стан ППН, а також перенесені абонентські номери та їх номери маршрутування.

АІС ЦБД ПН забезпечує управління процесами перенесення абонентських номерів між операторами телекомунікацій, а також зберігання інформації про перенесені абонентські номери та їх номери маршрутування на основі централізованої бази даних.

Загальна структура АІС ЦБД ПН

Розглянемо загальну структуру АІС ЦБД ПН (рис. 4.3).

АІС ЦБД ПН є функціонально єдиною системою, базові складові якої утворюють інтегровану інформаційно-комунікаційну інфраструктуру для забезпечення ППН у взаємодії з ІТС операторів телекомунікацій.

Архітектура АІС ЦБД ПН включає наступні складові:

- основний центр обробки даних (ОЦОД);
- резервний центр обробки даних (РЦОД);
- робочі станції (РС).

Структурна схема АІС ЦБД ПН наведена на рисунку 4.3, на якій кількість електронних обчислювальних машин (ЕОМ) та технічних засобів телекомунікацій показана умовно.

До складу ОЦОД входять:

– сервери бази даних та додатків – 2 шт.;

– сервери резервного копіювання та тестування – 2 шт.;

– система аналізу журналів та генерування звітів обладнання мережевої безпеки;

– централізована система управління обладнанням мережевої безпеки;

– програмні засоби криптографічного захисту інформації – 2 шт.;

– технічні засоби телекомунікацій (маршрутизатори) – 2 шт.;

– обладнання мережевої безпеки – 2 шт.;

– комутатор – 2 шт.

До складу РЦОД входять:

– сервер бази даних та додатків – 1 шт.;

– програмні засоби криптографічного захисту інформації – не менш ніж 2 шт.;

– технічні засоби телекомунікацій (маршрутизатор) – 2 шт.;

– обладнання мережевої безпеки – 2 шт.;

– комутатор – 2 шт.

Робочі станції (далі – РС) АІС ЦБД ПН призначені для управління налаштуваннями програмних та апаратних засобів АІС ЦБД ПН, забезпечення доступу користувачів до інформації в базах даних АІС ЦБД ПН відповідно до наданих повноважень, роботи з інформацію, яка зберігається в ЦБД ПН.

На РС АІС ЦБД ПН використовується наступне програмне

забезпечення:

– операційні системи Microsoft Windows 8 / 8.1 / 10, комплекси захисту яких мали відповідні експертні висновки в сфері ТЗІ;

– веб-браузер, що забезпечує коректну обробку стандартних html-сторінок;

– антивірусне програмне забезпечення ESET Endpoint Protection Advanced, що має експертний висновок в сфері ТЗІ № 731 від 15.05.2017.

Деталізовані відомості щодо використання програмного забезпечення на відповідних технічних засобах АІС ЦБД ПН наводяться в формулярі АІС ЦБД ПН.

Склад технічних та програмних засобів АІС

АІС ЦБД ПН побудована на базі локальної обчислювальної мережі, яка має підключення до телекомунікаційної мережі загального користування Internet.

На серверах АІС ЦБД ПН використовується наступне програмне забезпечення:

– платформа віртуалізації – VMwarevSphere 6 Standard;

– операційні системи серверів – OracleLinux 7, CentOS 7;

– система керування базами даних OracleDatabase 12;

– прикладне програмне забезпечення «Автоматизована інформаційна система «Централізована база даних перенесених номерів».

Для розгортання серверів АІС ЦБД ПН використовуються електронно-обчислювальна машина (ЕОМ) серверного типу HP DL380 Gen9 Server. Деталізовані відомості щодо апаратного забезпечення ЕОМ, що входять до складу АІС ЦБД ПН, наведені в формулярі АІС ЦБД ПН.

Для розгортання шлюзів криптографічного захисту інформації використовується ЕОМ серверного типу HP DL360 Gen9 Server.

В ОЦОД та РЦОД використовуються маршрутизатори моделі HP MSR 3044, що мають експертний висновок за результатами державної експертизи в сфері ТЗІ № 821 від 06.03.2018, а також обладнання мережевої

безпекивиробникаFortinet моделі Fortigate 100d / 200d, яке має позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ №762 від 25.09.2017.

Живлення всіх серверів та технічних засобів телекомунікацій ОЦОД/РЦОД здійснюється від відповідних джерел безперебійного живлення (акумуляторних батарей великої ємності та/або дизель-генераторів). У разі збою електроживлення за відповідно налаштованою програмною командою джерела безперебійного живлення забезпечується автоматичне коректне завершення роботи серверів.

Для криптографічного захисту інформації, що циркулює в АІС ЦБД ПН, та між АІС ЦБД ПН та ІТС операторів телекомунікацій використовується програмний комплекс криптографічного захисту інформації "HP - Encryptor UA", що має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації № 04/03/02-5017 від 27.12.2018 (використовується в складі шлюзів криптографічного захисту).

Для захисту даних абонентів оператор телекомунікацій, який ініціює перенесення номеру, здійснює шифрування лише даних, які містяться в повідомленні оператора під час ППН, з використанням сертифіката відкритого ключа шифрування оператора, який обслуговує на даний момент номер. Для захисту інформації операторами повинні використовуватися засоби криптографічного захисту інформації, які мають позитивні експертні висновки в сфері криптографічного захисту інформації. В АІС ЦБД ПН відсутня можливість розшифрування даних абонента, що містяться в повідомленнях операторів, обмін якими здійснюється під час ППН. Інша інформація, отримана від операторів телекомунікацій, під час ППН, має оброблюватися в АІС ЦБД ПН.

Завдання генерації та управління ключовими даними, необхідними для виконання зазначених операцій, не входить до завдань прикладного програмного забезпечення АІС ЦБД ПН.

Для мережевого захисту на ОЦОД також використовуються апаратні

міжмережеві екрани (зі складу інформаційно-телекомунікаційної системи датацентра ПрАТ "ДАТАГРУП", який має у своєму складі комплексну систему захисту інформації з підтвердженою відповідністю (атестат відповідності від 13.09.2017 № 15595, дійсний до 13.09.2022)), які забезпечують виконання наступних функцій:

– фільтрація та аналіз трафіку на рівнях L3- L7 моделі OSI;

– розмежування доступу між АІС та зовнішніми мережами;

– інспекція мережевого трафіку та блокування пакетів або сесій, що є підозрілими;

– маскування топології і мережевих адрес АІС від публічного перегляду;

– контроль інформаційних потоків між АІС та Інтернет з метою виявлення спроб мережевих вторгнень та несанкціонованого доступу до мережевих ресурсів, в т.ч. атак типу “відмова в обслуговуванні”, забезпечення реєстрації, попередження та протидії таким спробам;

– виявлення комп’ютерних атак і несанкціонованої мережевої активності;

– фільтрація та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;

– завершення з’єднання з вузлом, у разі атаки;

– протоколювання (реєстрація) подій, що мають відношення до безпеки;

– інші функції, визначені політикою безпеки.

Живлення всіх серверів та комутаційного обладнання здійснюється від джерел безперебійного живлення. При відключенні електроживлення налаштоване автоматичне коректне завершення роботи серверів за відповідною програмною командою джерела безперебійного живлення.

Апаратне забезпечення серверів та робочих місць не містять штатних апаратних та апаратно-програмних засобів захисту інформації.

Деталізовані відомості щодо використаного апаратного та програмного

забезпечення наведені в паспорті-формулярі АІС.

З боку ПрАТ "ДАТАГРУП" в рамках договору надаються наступні послуги:

- надання обчислювального середовища та мережевої інфраструктури для забезпечення надійного та безперебійного функціонування системного та прикладного програмного забезпечення АІС;
- захищеність фізичного середовища з метою виключення можливості несанкціонованого доступу до серверного та мережевого обладнання;
- адміністративну технічну підтримку функціонування серверного та мережевого обладнання;
- логічну ізоляцію віртуальних серверів АІС від віртуальних серверів інших інформаційно-телекомунікаційних систем, що функціонують на цій платформі віртуалізації;
- розмежування доступу до віртуального середовища, в якому функціонують сервери АІС, з боку авторизованого адміністративного персоналу ЦОД; неможливість доступу такого персоналу до даних, що обробляються в АІС на рівні прикладного програмного забезпечення;
- локалізацію віртуальних серверів АІС в межах ізольованої інфраструктури з неможливістю перенесення віртуальних машин АІС за межі заданих фізичних ресурсів (віртуальні машини АІС використовують обчислювальні ресурси і фактично працюють в рамках однієї групи серверів віртуалізації);
- виконання резервного копіювання віртуальних машин відповідно до налаштувань власника АІС.

Можливість надання наведених вище інформаційних послуг підтверджується результатами державної експертизи в сфері технічного захисту інформації комплексної системи захисту інформації захищеного вузлу Інтернет доступу ПрАТ «ДАТАГРУП».

Структурна схема АІС ЦБД ПН наведена на рисунку 4.3.

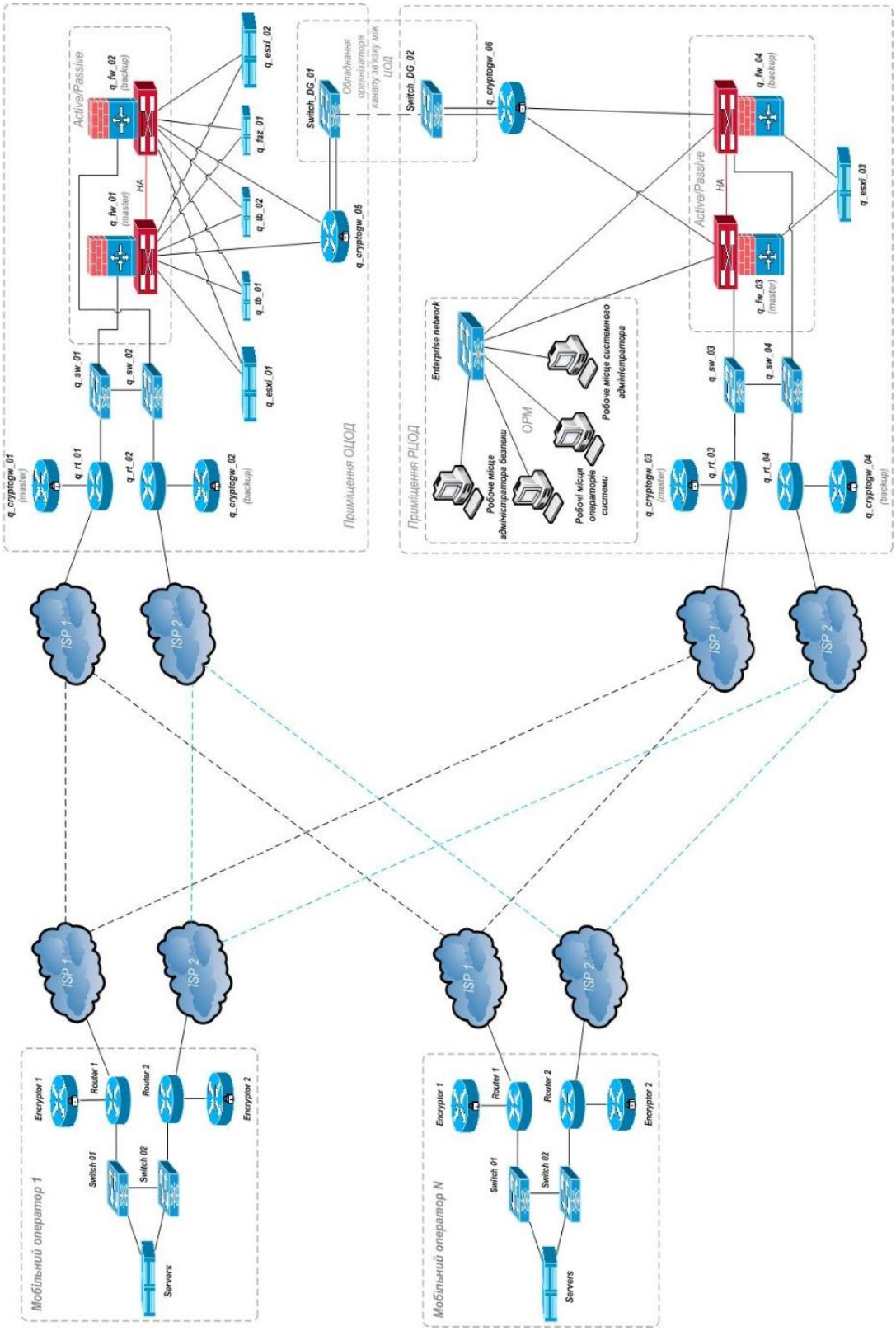

Рис. 4.3. Функціональна схема АІС ЦБД ПН

Режими функціонування

Функціонування АІС ЦБД ПН 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.

Об’єкти автоматизації

Об’єктами автоматизації АІС ЦБД ПН є процеси перенесення та повернення абонентських номерів, процеси адміністрування системи та взаємодії централізованої бази даних перенесених номерів з телекомунікаційними мережами під час надання послуги перенесення абонентського номера рухомого (мобільного) зв’язку і його подальшого обслуговування.

Алгоритми проходження процесів перенесення та повернення абонентських номерів

Процес перенесення номера

Далі наведено опис взаємодії між АІС ЦБД ПН, оператором-

отримувачем, оператором-донором та іншими операторами телекомунікацій в процесі перенесення номера. Усі повідомлення, що надсилаються до АІС ЦБД ПН мають містити цифровий підпис відправника. Якщо цифровий підпис буде відсутній повідомлення буде відхилено з відповідним статусом.

Основні етапи процесу перенесення номера:

1. Заява абонента. Абонент подає заяву новому оператору – оператору-отримувачу. Цей процес не охоплює взаємодії між абонентом і оператором, що відбуваються поза АІС ЦБД ПН.
2. Запит оператора-отримувача. Після завершення оформлення заяви оператор-отримувач в період часу T1 подає запит до АІС ЦБД ПН. При цьому фіксується дата і час оформлення заяви.

   Запит оператора-отримувача. Після отримання заяви від абонента про перенесення абонентського номера оператор-отримувач фіксує дату та час отримання заяви та протягом часу T1 з моменту реєстрації заяви надсилає до АІС ЦБД ПН повідомлення "PortingRequest" (запит ПН), яке включає відкриту інформацію про абонентський номер (номери), перенесення яких вимагається, найменування базового оператора, найменування оператора-отримувача, а також бажаний час перенесення абонентського номера (номерів), дату та час отримання заяви про перенесення абонентського номера(номерів) оператором-отримувачем. Повідомлення містить персональні дані абонента або особи, що представляє інтереси юридичної особи (прізвище, ім’я, по батькові, місце проживання, серію та номер паспорта або іншого документа, що посвідчує особу). Вони вказані у файлі XML, який шифрується та додається до запиту на перенесення. Детальний опис формату повідомлення "PortingRequest" (запит ПН), а також інших повідомлень, якими оператори обмінюються з АІС ЦБД ПН, наведено в документі “Автоматизована інформаційна система «Централізована база даних перенесених номерів». Техноробочий

проект. Специфікація SOAP/XML інтерфейсу. 3969753.79415200-8.001С2” [99]. Шифрування виконує оператор-отримувач за допомогою сертифікату відкритого ключа шифрування оператора-донора (направлене шифрування). Також оператор-отримувач з використанням свого особистого ключа здійснює підписання запиту.

3. Відповідь АІС ЦБД ПН. АІС ЦБД ПН перевіряє повідомлення "PortingRequest" (запит ПН) (детальний опис формату повідомлень наведено в документі “Автоматизована інформаційна система «Централізована база даних перенесених номерів». Техноробочий проект. Специфікація SOAP/XML інтерфейсу. 3969753.79415200-8.001С2) [99], пересилає повідомлення оператору-донору. Якщо в повідомленні "PortingRequest" (запит ПН) АІС ЦДБ ПН виявлена невідповідність критеріям перевірки, або відсутність коректного електронного цифрового підпису оператора-отримувача, то його буде відхилено, а оператору-отримувачу буде відправлено повідомлення "ProcessStatus" зі статусом «Відхилено» (відхилення ПН) (детальний опис статусів повідомлень наведено в документі “Автоматизована інформаційна система «Централізована база даних перенесених номерів». Техноробочий проект. Специфікація SOAP/XML інтерфейсу. 3969753.79415200-8.001С2”) [99].
4. Відповідь оператора-донора. Оператор-донор приймає повідомлення "PortingRequest" (запит ПН) і повинен відповісти за період часу, Т2, який встановлює і контролює АІС ЦБД ПН. Можливі три варіанти відповіді оператора-донора:
   4.1. Оператор-донор приймає повідомлення та перевіряє наведену в ньому інформацію (згідно Порядку надання послуг із перенесення абонентських номерів проводить перевірку на наявність причин для відхилення запиту), підтверджує можливість перенесення номеру, у випадку відсутності причин

для відхилення запиту, надсилаючи повідомлення "PortingAccept" (підтвердження донора).

4.2. У разі, якщо отримана в повідомленні "PortingRequest" (запит ПН) інформація не пройшла перевірку оператора-донора, оператор-донор посилає повідомлення "PortingReject" (відхилення донора), зазначивши причину відхилення запиту. Можливі причини через які оператор-донор має право відхилити запит на перенесення номеру наведено в «Порядок надання послуг із перенесення абонентських номерів».

4.3. Якщо оператор-донор не надав відповідь на запит протягом періоду часу, T2, то АІС ЦДБ ПН автоматично надсилає оператору-донору та оператору-отримувачу повідомлення "PortingAccept" (погодження донора).

5. Якщо один або декілька номерів не пройшли перевірку оператора-донора, оператор-донор вилучає цей номер(номери) з запиту (первинного повідомлення "PortingRequest" (запит ПН)) без зупинки або скасування процесу перенесення номера. Номери, що залишилися в запиті, мають бути перенесені в період часу, зазначений у запиті. АІС ЦБД ПН повинна виконати базову перевірку на відповідність структурі протоколу SOAP отриманого від оператора-донора повідомлення "DonorExclude" (вилучення ПН донором) і перенаправити це повідомлення оператору-отримувачу. В разі, якщо повідомлення оператора-донора "DonorExclude" (вилучення ПН донором) не пройшло базову перевірку, АІС ЦБД ПН відхиляє процедуру вилучення і направляє повідомлення про відхилення оператору-донору, зазначивши причину відмови на вилучення номерів.

6. Якщо абонент відмовився від перенесення одного або декількох номерів (блоку, або групи), оператор-отримувач вилучає номер (номери) з процесу перенесення, надіславши повідомлення

«RecipientExclude», в якому вказуються номер (номери), що виключаються з процесу перенесення. Номери, що залишилися в запиті, мають бути перенесені в період часу, зазначений в запиті. АІС ЦБД ПН повинна виконати базову перевірку на відповідність структурі протоколу SOAP отриманого від оператора-отримувача повідомлення "RecipientExclude" (вилучення ПН отримувачем) і перенаправити це повідомлення оператору-донору. В разі, якщо повідомлення оператора-донора " RecipientExclude " (вилучення ПН отримувачем) не пройшло базову перевірку, АІС ЦБД ПН відхиляє процедуру вилучення і направляє повідомлення про відхилення оператору-отримувачу, зазначивши причину відмови на вилучення номерів

7. Можливість скасування. Абонент має право скасувати замовлення на перенесення номера доки не укладений договір з оператором-отримувачем. У разі скасування перенесення номера абонентом, оператор-отримувач надсилає повідомлення “Cancel” про скасування перенесення до АІС ЦБД ПН. АІС ЦБД ПН пересилає повідомлення “Cancel” оператору-донору і запит на перенесення номера "PortingRequest" (запит ПН) скасовується.
8. Укладання договору. Коли оператор-донор підтверджує можливість перенесення номера, оператор-отримувач повідомляє про це абонента і пропонує укласти договір. Можливі 2 варіанти:
   8.1. Абонент протягом періоду часу Т3, звертається до оператора-отримувача, підписує договір і отримує SIM-картку. В цьому разі, оператор-отримувач посилає повідомлення підтвердження "PortingConfirm" (контракт ПН) до АІС ЦБД ПН. АІС ЦБД ПН направляє "PortingConfirm" оператору-донору. АІС ЦБД ПН також направляє повідомлення “ProcessStatus” оператору-отримувачу та оператору-донору, що означає готовність номеру до перенесення.

8.2. Якщо абонент не прийшов за ідентифікаційною телекомунікаційною карткою і/або не уклав договір в період часу, встановленого таймером Т3 , запит про перенесення номера "PortingRequest" (запит ПН) скасовується, АІС ЦБД ПН надсилає повідомлення “Cancel” оператору-отримувачу та оператору-донору

9. Активація. В час DueDate протягом часу Т4, оператор-отримувач повинен активувати номер абонента в своїй мережі і повідомити про це АІС ЦБД ПН, надіславши до АІС ЦБД ПН повідомлення “Activated”.
10. Повідомлення про деактивацію. Після надходження до АІС ЦДБ ПН повідомлення від оператора-отримувача “Activated” надсилає оператору-донору повідомлення “Deactivate”, запит на деактивацію абонентського номера в мережі оператора-донора.
11. Деактивація. Оператор-донор протягом часу Т5, зобов'язаний деактивувати абонентський номер у своїй мережі і надіслати в АІС ЦБД ПН повідомлення “Deactivated”. Після отримання відповіді оператора-донора про деактивацію абонентського номера, АІС ЦДБ ПН висилає всім операторам повідомлення “Broadcast”, запит на зміну маршрутування на цей абонентський номер.
12. Завершення. Оператори після отримання від АІС ЦДБ ПН запиту на зміну маршрутування, повинні оновити дані у власних системах, змінити маршрутизацію й проінформувати АІС ЦБД ПН про завершення робіт, надіславши повідомлення підтвердження “АСК” у час Т6.

Процес повернення номера

Далі наведено опис взаємодії між АІС ЦБД ПН, оператором-отримувачем, базовим-оператором та іншими операторами телекомунікацій в процесі повернення номера.

Основні етапи процесу повернення номера:

1. Базовий оператор за заявою абонента або за власною ініціативою ініціює припинення надання послуг за номером (Contract break).

2. Базовий оператор у час T7 надсилає в АІС ЦБД ПН повідомлення "Terminate" (повернення номера) про відключення перенесеного номера.

3. Відповідь АІС ЦБД ПН. АІС ЦБД ПН підтверджує повідомлення "Terminate" (повернення номера), вилучає номер зі списку перенесених номерів, включає до списку повернених номерів та надсилає повідомлення Broadcast (повернення підтверджено) оператору-донору та усім іншим операторам.

Характеристика інформації, що циркулює в АІС ЦБД ПН

Розглянемо характеристики інформації, що обробляється в АІС ЦБД ПН. Узагальнені відомості про інформацію, що обробляється та зберігається в АІС ЦБД ПН, наведені в табл. 4.1.

Таблиця 4.1

№ з/п	Вид інформації	Стисла характеристика інформації	Обмеження доступу до інформації	Вигляд даних
1	Програмне забезпечення АІС ЦБД ПН	Операційні системи, прикладне програмне забезпечення, антивірусне програмне забезпечення	Відкрита	У вигляді файлів
2	Журнали реєстрації подій	Журнали реєстрації подій, що ведуться апаратними та програмними засобами АІС ЦБД ПН	Конфіденційна (технологічна)	У вигляді файлів та об’єктів бази даних
3	Файли конфігурації програмного та апаратного забезпечення	Файли конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи АІС ЦБД ПН	Конфіденційна (технологічна)	У вигляді файлів
4	Інформація, що зберігається в базі даних АІС ЦБД ПН			
4.1	Блок зашифрованих даних в заявці на перенесення номеру	Блок зашифрованих даних в заявці на перенесення номеру, що призначений для передачі даних абонентів від одного оператора іншому без можливості їх розшифрування в АІС ЦБД ПН	Відкрита	У складі xml-файлів спеціалізованого формату в зашифрованому вигляді

№ з/п	Вид інформації	Стисла характеристика інформації	Обмеження доступу до інформації	Вигляд даних
4.2	Дані перенесених абонентських номерів	Відомості про перенесені абонентські номери абонентів операторів телекомунікацій	Відкрита	У вигляді об’єктів бази даних
5	Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	Відкрита	У вигляді файлів

Узагальнені відомості щодо забезпечення властивостей (конфіденційності, цілісності, доступності та спостережності) інформації, що обробляється в АІС, наведені в табл. 4.2.

Таблиця 4.2

Вид інформації (згідно з таблицею 4.1)	Відомості щодо забезпечення властивостей інформації			
	конфіденційність	цілісність	доступність	спостережність
Програмне забезпечення ЕОМ	-	+	+	+
Журнали реєстрації подій	+	+	+	+
Файли конфігурації програмного та апаратного забезпечення	+	+	+	+
Інформація, що зберігається в базах даних	+	+	+	+
Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	+	+	+	+

Найвищий ступінь обмеження доступу до інформації, що може зберігатися та обробляться в АІС ЦБД ПН – конфіденційна.

Забезпечення захисту даних абонентів відповідних операторів телекомунікацій здійснюється операторами телекомунікації при оформленні заявки на перенесення номеру. В АІС ЦБД ПН дані абонентів циркулюють

виключно в зашифрованому вигляді без можливості їх розшифрування відповідно до вимог ТЗ на проектування, розроблення та впровадження Автоматизованої інформаційної системи "Централізована база даних перенесених номерів".

Об’єктами захисту є дані, сукупність даних логічної структури (файл, база даних) АІС ЦБД ПН, в яких знаходиться інформація, що підлягає захисту, а також програмне забезпечення, що реалізує технології оброблення такої інформації, для виконання АІС ЦБД ПН своїх функцій.

Об’єкти захисту поділені відповідно до функціонального призначення, місця розміщення та виду представлення в АІС ЦБД ПН наведені в таблиці 4.3.

Таблиця 4.3 – Поділ об’єктів захисту

Об’єкт захисту	**Умовне позначення**	**Вигляд представлення**
Операційні системи, прикладне та спеціалізоване програмне забезпечення АРМ та серверів АІС ЦБД ПН	{SOFT}	У вигляді файлів
Журнали реєстрації подій системного програмного забезпечення АІС ЦБД ПН в електронній формі	{SOFT-LOG}	У вигляді файлів
Журнали реєстрації подій прикладного програмного забезпечення АІС ЦБД ПН в електронній формі	{DB-LOG}	У вигляді об’єктів бази даних
Дані про план нумерації	{PLAN}	У вигляді файлів та об’єктів бази даних
Дані про перенесені номери (повний список перенесених номерів, інкрементальний список перенесених номерів, список повернених номерів)	{NUM}	
Блок зашифрованих даних в заявці на перенесення номеру	{REQ-PERS}	У складі xml-файлів спеціалізованого формату
Відкриті технологічні дані, що містяться в заявках на перенесення номера	{REQ-DATA}	
Статистична інформація про виконання ППН	{STAT}	
Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	{DB-BACKUP}	У вигляді файлів
Конфігураційні та системні об’єкти складових елементів АІС ЦБД ПН, що визначають параметри конфігурації, функціонування та правила розмежування доступу	{SOFT-CFG}	У вигляді файлів
Конфігураційні та системні об’єкти прикладного програмного забезпечення АІС ЦБД ПН	{DB-CFG}	У вигляді файлів та об’єктів баз даних
Конфігураційні та системні об’єкти складових елементів АІС ЦБД ПН, що визначають правила	{SEC-CFG}	У вигляді файлів

Об’єкт захисту	Умовне позначення	Вигляд представлення
розмежування доступу		

Обробка та зберігання інформації в АІС ЦБД ПН здійснюється у встановленому порядку з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 [100], та ТЗ на проектування, розроблення та впровадження Автоматизованої інформаційної системи "Централізована база даних перенесених номерів".

Характеристики користувачів

Розглянемо вимоги до ролей користувачів АІС ЦБД ПН. За рівнем повноважень щодо доступу до інформації та характером робіт, що виконуються у процесі забезпечення функціонування АІС ЦБД ПН, особи, які мають доступ до її ресурсів, поділяються на такі категорії:

1) *системний адміністратор* – користувач, який здійснює управління системними налаштуваннями апаратних та програмних засобів АІС ЦБД ПН;

2) *адміністратор безпеки* – користувач, який здійснює управління комплексом засобів захисту від несанкціонованого доступу (зокрема обліковими записами користувачів всіх категорій АІС ЦБД ПН (прикладному та системному програмному забезпеченні), налаштуваннями обладнання мережевої безпеки АІС ЦБД ПН, управління засобами мережевої безпеки, антивірусного програмного забезпечення та засобів криптографічного захисту);

3) *користувач УДЦР* – співробітник ДП "Український державний центр радіочастот", який забезпечує підтримку інформаційного обміну між операторами телекомунікацій при виконанні ППН, обробку інформації, яка зберігається в ЦБД ПН;

4) *користувач оператора телекомунікацій* – співробітник оператора телекомунікацій, який забезпечує виконання технологічних процедур, пов’язаних із реалізацією ППН;

5) *користувач інформаційних послуг АІС ЦБД ПН* – співробітник державного органу або суб'єкта господарювання, який використовує дані про перенесені абонентські номери у власних технологічних процесах;

6) *постачальники та розробники* апаратних засобів та прикладного програмного забезпечення АІС ЦБД ПН, що забезпечують їх технічну підтримку, а в разі необхідності їх модернізацію.

Усі користувачі АІС ЦБД ПН, в залежності від категорії, повинні мативідповідну підготовку щодо експлуатації апаратних та програмних засобів АІС ЦБД ПН для забезпеченнявиконання своїх службових та функціональних обов'язків.

Забороняється суміщення ролей адміністраторів АІС ЦБД ПН та користувачів АІС ЦБД ПН.

Розподіл обов'язків адміністраторів АІС ЦБД ПН повинен здійснюватися на основі функціональних задач, які виконують адміністратори. В АІС ЦБД ПН встановлено наступні ролі адміністраторів:

1) системний адміністратор, що здійснює адміністрування апаратних та програмних засобів АІС ЦБД ПН;

2) адміністратор безпеки, що здійснює управління обліковими записами користувачів та їх правами доступу до інформаційних об'єктів АІС ЦБД ПН, налаштування обладнання мережевої безпеки АІС ЦБД ПН.

З технічної точки зору виконання задач з адміністрування АІС ЦБД ПН умовно поділяється на:

1) адміністрування віртуальної інфраструктури;

2) адміністрування прикладного програмного забезпечення (зокрема QuadonTM);

3) адміністрування мережі передачі даних (активного мережевого обладнання);

4) адміністрування баз даних;

5) адміністрування робочих станцій користувачів УДЦР, що входять до складу АІС ЦБД ПН.

Адміністрування відбувається з АРМ адміністраторів, що розміщено в межах контрольованої зони.

Враховуючи наведений поділ **системний адміністратор по відношенню до кожної складової виконує наступні функції:**

1) *адміністрування віртуальної інфраструктури* – встановлення та налаштування операційних систем та прикладного програмного забезпечення (далі – ПЗ) (зокрема VMware vSphere), що забезпечує функціонування віртуальної інфраструктури АІС ЦБД ПН. Підтримка його функціонування та безперебійної роботи.

2) *адміністрування прикладного програмного забезпечення* – первинне встановлення та налаштування прикладного забезпечення. Підтримка його функціонування та безперебійної роботи.

Примітка: враховуючи технічну неможливість розподілу обов'язків адміністраторів у ПЗ QuadonTM, після встановлення зазначеного програмного забезпечення, системний адміністратор передає логін та пароль доступу адміністратору безпеки, який, в свою чергу, зобов'язаних змінити первинний пароль. При необхідності проведення технічних робіт адміністратор безпеки надає тимчасовий доступ системному адміністратору під особистим контролем.

3) *адміністрування мережі передачі даних* – налаштування та підтримка функціонування активного мережевого обладнання (зокрема маршрутизаторів, комутаторів, обладнання мережевої безпеки та ін.)

4) *адміністрування баз даних* – встановлення та налаштування ПЗ системи керування базами даних (зокрема Oracle Database). Підтримка його функціонування та безперебійної роботи.

5) *адміністрування робочих станцій користувачів* – встановлення операційної системи та прикладного програмного забезпечення (в т.ч. антивірусного) робочих станцій користувачів. Підтримка їх функціонування та безперебійної роботи.

Примітка: перелік програмного забезпечення робочих станцій

зазначається у формулярах та не повинен містити неліцензійного ПЗ, а також ПЗ, наявність якого не обумовлено службовою необхідністю.

Також на системного адміністратора покладаються обов'язки щодо оновлення програмного забезпечення (окрім антивірусного). Порядок оновлення програмних та технічних засобів визначений в окремому документі «Автоматизована інформаційна система "Централізована база даних перенесених номерів" Комплексна система захисту інформації. Порядок модернізації та оновлення компонентів АІС ЦБД ПН». У разі, якщо оновлення програмних засобів впливає на функції безпеки, в обов'язковому порядку залучається адміністратор безпеки та здійснює контроль за процесом оновлення.

Адміністратор безпеки по відношенню до кожної складової виконує наступні функції:

1) *адміністрування віртуальної інфраструктури* – налаштування політик безпеки віртуальних операційних систем та прикладного ПЗ (зокрема VMware vSphere), що забезпечує функціонування віртуальної інфраструктури АІС ЦБД ПН. Налаштування розподілу обов'язків та прав доступу облікових записів користувачів (адміністраторів).

2) *адміністрування прикладного програмного забезпечення* – налаштування повноважень облікових записів користувачів ПЗ QuadonTM згідно прийнятої політики безпеки. Підтримка функціонування та безперебійної роботи ПЗ QuadonTM. Контроль доступу користувачів та здійснення аналізу системних журналів.

3) *адміністрування мережі передачі даних* – розробка політик безпеки активного мережевого обладнання, здійснення контролю функціонування обладнання мережевої безпеки. Управління засобами криптографічного захисту (зокрема програмного комплексу криптографічного захисту інформації "HP - Encryptor UA") та забезпечення їх функціонування (в т.ч. генерація сертифікатів та контроль актуальності бази відкликаних сертифікатів).

4) *адміністрування баз даних*– налаштування розподілу обов'язків та прав доступу облікових записів користувачів (адміністраторів) ПЗ системи керування базами даних (зокрема Oracle Database). Контроль доступу користувачів та здійснення аналізу системних журналів.

5) *адміністрування робочих станцій користувачів* – налаштування політик безпеки операційної системи та прикладного програмного забезпечення (в т.ч. антивірусного) робочих станцій користувачів. Підтримка актуальності (оновлення) антивірусних баз згідно вимог чинних керівних документів. Розмежування та контроль доступу облікових записів користувачів та здійснення аналізу системних журналів операційної системи.

Системний адміністратор – рівень адміністрування апаратного та програмного забезпечення ЕОМ АІС ЦБД ПН штатними засобами відповідних операційних систем.

Адміністратор безпеки – управління обліковими записами (профілями) користувачів (груп користувачів) АІС ЦБД ПН, перегляд журналів реєстрації подій та отримання статистики функціонування АІС ЦБД ПН.

Атрибути доступу користувачів використовуються для ідентифікації та автентифікації. Атрибути доступу об'єкту користувача використовуються для розмежування доступу до об'єктів захисту АІС ЦБД ПН.

Атрибути доступу об'єктів захисту використовуються КЗЗ для розмежування доступу до них.

Усі дії, які прямо чи опосередковано можуть вплинути на захищеність інформації (зміни дозволів на доступ до файлів та папок, очищення журналів ОС, зміни налаштувань BIOS Setup тощо), системний адміністратор має узгоджувати з адміністратором безпеки.

За рівнем повноважень щодо доступу до технічних та програмних засобів, інформації, що циркулює та накопичується в АІС ЦБД ПН, характером та змістом робіт, які виконуються в процесі функціонування, суб'єкти доступу поділяються на групи, наведені в таблиці 4.4.

Таблиця 4.4 – Суб'єкти доступу до ресурсів АІС ЦБД ПН

Суб'єкт доступу	**Умовне позначення**
Системний адміністратор	[А_СА]
Адміністратор безпеки	[А_АБ]
Користувач УДЦР	[О_У]
Користувач оператора телекомунікацій	[О_Т]
Користувачів інформаційних послуг АІС ЦБД ПН	[О_К]
Розробники програмного забезпечення та постачальники апаратного забезпечення АІС ЦБД ПН	[К_РП]

Загрози інформації

З огляду на сферу можливої дії, а також причини виникнення, загрози інформації АІС ЦБД ПН 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 АІС ЦБД ПН.

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) [67, 68] 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).

При аналізі загроз, які існують для АІС ЦБД ПН, основне припущення

робиться з врахуванням того, що користувач, який має повний адміністративний доступ до компонентів системи і фізичний доступ до комутаційного та серверного обладнання, не розглядається в якості потенційного порушника. Технічні заходи, описані в цьому ТЗ, що спрямовані на захист від зловмисних дій користувачів з адміністративними правами, розглядаються як додаткові. В якості основних заходів для захисту від загроз розглядаються організаційні заходи (кадрова політика, взаємний контроль адміністраторів при виконанні важливих технологічних операцій).

Якісна оцінка імовірності реалізації загроз та умовні втрати внаслідок їх реалізації зроблена за чотирирівневою шкалою (низький, середній, високий, дуже високий), визначений сукупний рівень загрози.

При цьому при розроблення КСЗІ брались до уваги тільки загрози з середнім та високим ефективним рівнем.

Деталізовані відомості щодо моделі загроз інформації в АІС ЦБД ПН та моделі порушника наведені в окремому документі «Автоматизована інформаційна система «Централізована база даних перенесених номерів». Комплексна система захисту інформації. Модель загроз для інформації та модель порушника безпеки інформації» [101].

Оскільки неможливо одержати достатньо об’єктивні дані про імовірність реалізації більшості з загроз імовірність реалізації загроз визначено експертним методом та, для окремих загроз, що є типовими для АС класу "3", емпіричним шляхом з врахуванням досвіду експлуатації подібних систем.

Загрози конфіденційності інформації

Порушення конфіденційності інформації, що обробляється та зберігається в АІС ЦБД ПН

Розглядаються наступні шляхи порушення конфіденційності інформації, що обробляється та зберігається в АІС ЦБД ПН (відкрита та конфіденційна інформація, перелічена в таблиці 4.1).

К.1.1 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок несанкціонованого фізичного доступу до обладнання.

Імовірність реалізації: середня

Втрати внаслідок реалізації: високі

Ефективний рівень: високий

К.1.2 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, під час її обробки внаслідок навмисного підключення до обладнання, помилок при налаштуванні технічних засобів телекомунікацій або апаратних збоїв.

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

К.1.3 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок навмисного підключення до каналів зв’язку чи обладнання з наступним використанням для несанкціонованого доступу відомих вразливостей програмно-технічних засобів АІС ЦБД ПН.

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

К.1.4 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок навмисного підключення до каналів зв’язку чи обладнання з наступним використанням для несанкціонованого доступу перехоплених атрибутів доступу авторизованих користувачів.

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

К.1.5 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок фізичного доступу до носіїв інформації (змінних носіїв, носіїв, що вийшли з ладу, носіїв, що підлягають утилізації).

Імовірність реалізації: середня

Втрати внаслідок реалізації: високі

Ефективний рівень: високий

Порушення конфіденційності технологічної інформації

К.2.1 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) сторонніми особами внаслідок необережного поводження авторизованих користувачів з атрибутами доступу (розглядається в якості частини реалізації атак **К.1.1**, **К.1.4**, спрямованих на порушення конфіденційності інформації).

Імовірність реалізації: середня

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

К.2.2 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) зі сторони авторизованих користувачів системи внаслідок необережного поводження з ними (як мета такого порушення розглядається ескалація прав доступу до ресурсів АІС ЦБД ПН та виконання несанкціонованих дій від імені іншого користувача, розглядається в якості частини атак **Ц.1.3**, **Ц.2.1**, **Ц.2.2**, спрямованих на порушення цілісності інформації).

Імовірність реалізації: висока

Втрати внаслідок реалізації: середні

Ефективний рівень: високий

К.2.3 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів системи) зі сторони авторизованих користувачів системи з застосуванням відомих вразливостей програмно-

технічних засобів АІС ЦБД ПН (розглядається в якості частини атак **Ц.1.3**, **Ц.2.1**, **Ц.2.2**, спрямованих на порушення цілісності інформації).

Імовірність реалізації: висока

Втрати внаслідок реалізації: середні

Ефективний рівень: високий

К.2.4 Отримання несанкціонованого доступу сторонніх осіб до технологічної інформації (атрибути доступу, конфігураційні налаштування), що зберігається та обробляється в АІС ЦБД ПН, внаслідок фізичного доступу до носіїв інформації (змінних носіїв, носіїв, що вийшли з ладу, носіїв, що підлягають утилізації).

Імовірність реалізації: середня

Втрати внаслідок реалізації: низькі

Ефективний рівень: середній

Загрози цілісності інформації

Загрози цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН

Ц.1.1 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок апаратного або програмного збою.

Імовірність реалізації: середня

Втрати внаслідок реалізації: дуже високі

Ефективний рівень: високий

Ц.1.2 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, сторонніми особами внаслідок отримання фізичного доступу до обладнання (навмисне чи внаслідок необережного поводження з обладнанням, що забезпечують його функціонування).

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

Ц.1.3 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок навмисних дій авторизованого користувача будь-якого рівня в межах його повноважень.

Імовірність реалізації: середня

Втрати внаслідок реалізації: дуже високий

Ефективний рівень: високий

Ц.1.4 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок ненавмисних (помилкових) дій авторизованого користувача будь-якого рівня.

Імовірність реалізації: середня

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Ц.1.5 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок ураження шкідливим ПЗ.

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Загрози цілісності технологічної інформації

Ц.2.1 Порушення цілісності технологічної інформації (журнали реєстрації подій) сторонніми особами або авторизованими користувачами з застосуванням відомих вразливостей програмно-технічних засобів АІС ЦБД ПН або перехоплених атрибутів доступу користувачів АІС ЦБД ПН з адміністративними правами (як мета реалізації даної загрози розглядається приховування несанкціонованих дій в системі в рамках реалізації інших загроз, спрямованих на порушення цілісності або конфіденційності інформації).

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

Ц.2.2 Порушення цілісності технологічної інформації (конфігураційні файли, виконувані файли програмного забезпечення) сторонніми особами або авторизованими користувачами з застосуванням відомих вразливостей програмно-технічних засобів АІС ЦБД ПН або перехоплених атрибутів доступу користувачів АІС ЦБД ПН з адміністративними правами (як мета реалізації даної загрози розглядається створення умов для подальшого несанкціонованого доступу до інших компонент системи в рамках реалізації загроз **К.1.1** – **К.1.4**, **Ц.2.1** (для сторонніх осіб), **Ц.1.3** (для авторизованих користувачів)).

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Ц.2.3 Порушення цілісності технологічної інформації (конфігураційні файли, виконувані файли програмного забезпечення) внаслідок ураження системи шкідливим ПЗ.

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Загрози доступності інформації

Загрози доступності інформації, що зберігається в АІС ЦБД ПН

Д.1.1 Втрата доступності інформації, що зберігається в АІС ЦБД ПН, внаслідок виходу з ладу комутаційного або серверного обладнання, або елементів, що їх забезпечують (найбільш імовірним вважається вихід з ладу системи електроживлення).

Імовірність реалізації: висока

Втрати внаслідок реалізації: низькі

Ефективний рівень: середній

Д.1.2 Втрата доступності інформації, що зберігається в АІС ЦБД ПН, внаслідок ураження системи шкідливим ПЗ (перевантаження каналів зв’язку інтенсивним трафіком, що генерується вірусами типа "хробак", при

розповсюдженні, вичерпання дискового простору або процесорного часу на уражених деякими типами шкідливого програмного забезпечення серверах, що призводить до неможливості обробки запитів та виникненні відмов в обслуговуванні).

Імовірність реалізації: середня

Втрати внаслідок реалізації: низькі

Ефективний рівень: середній

Розробимо модель порушника АІС ЦБД ПН.

За локалізацією джерела, загрози поділяються на внутрішні та зовнішні. До зовнішніх відносяться загрози, джерело яких знаходиться поза межами АІС ЦБД ПН. Внутрішні загрози реалізуються в межах контрольованої зони, в приміщеннях, де розташовані засоби обробки та збереження інформації АІС ЦБД ПН. Відповідно до цього розрізняються два види порушників: зовнішній та внутрішній.

1. Зовнішній порушник (ЗП) – це порушник, що діє із зовнішнього, відносно АІС ЦБД ПН, 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 АІС ЦБД ПН).

Категорії осіб, які можуть бути зовнішніми порушниками:

- сторонні особи, що знаходяться за межами контрольованої території АІС ЦБД ПН;

- відвідувачі;

- представники організацій, що взаємодіють з питань обслуговування АІС ЦБД ПН та підтримки його функціональності.

2. Внутрішній порушник (ВП) – це порушник, що діє зсередини АІС ЦБД ПН. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки АІС ЦБД ПН. 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 АІС ЦБД ПН (Тр 1);

- користувачі АІС ЦБД ПН;

- адміністратор безпеки;

- системний адміністратор АІС ЦБД ПН;

- представники організацій, що взаємодіють з питань технічного забезпечення;

- фахівці організацій, що підтримуються АІС ЦБД ПН.

Модель загальних загроз АІС ЦБД ПН приведена у Додатку В. На підставі отриманих даних проведемо аналіз ризиків АІС ЦБД ПН.

У табл. 4.5 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» [102]. Розрахунок ефективного рівня загроз здійснюється за формулами, наведеними у тому ж документі.

Таблиця 4.5

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 АІС ЦБД ПН								
ПВ1	Персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти АІС ЦБД ПН, технічні засоби (інженери, техніки) (Тр1)	2	1	1,3	3	1, 2	1, 2	4–6	2,06
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 АІС ЦБД ПН (Ad2)	4	1	1	4	3	4	5, 6	3.33
ПВ5	Фахівці організацій, що підтримуються АІС ЦБД ПН (Ad3)	4	1, 3	1, 3	4	2-5	4	1-6	3.37
	Зовнішні по відношенню до АІС ЦБД ПН								
ПЗ1	Сторонні особи, що знаходяться за межами контрольованої території вузлів АІС ЦБД ПН	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	2	1, 3	1	1	1	1, 2	2, 3	1.67

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 АІС ЦБД ПН								
ПВ1	Персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти АІС ЦБД ПН, технічні засоби (інженери, техніки) (Тр1)	2	1	1,3	3	1, 2	1, 2	4–6	2,06
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 АІС ЦБД ПН (Ad2)	4	1	1	4	3	4	5, 6	3.33
ПВ5	Фахівці організацій, що підтримуються АІС ЦБД ПН (Ad3)	4	1, 3	1, 3	4	2-5	4	1-6	3.37
	забезпечення (енерго-, водо-, теп-лопостачання і т.і.)								
ПЗ4	Представники орга-нізацій, що	3	1, 3	1-3	3–6	1 – 5	1,4	3-6	2.82

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 АІС ЦБД ПН								
ПВ1	Персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти АІС ЦБД ПН, технічні засоби (інженери, техніки) (Тр1)	2	1	1,3	3	1, 2	1, 2	4–6	2,06
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 АІС ЦБД ПН (Ad2)	4	1	1	4	3	4	5, 6	3.33
ПВ5	Фахівці організацій, що підтримуються АІС ЦБД ПН (Ad3)	4	1, 3	1, 3	4	2-5	4	1-6	3.37
	взаємо-діють з питань об-слуговування АІС ЦБД ПН та під-тримки його функ-ціональності								

В таблиці 4.6 представлені імовірності реалізації, величина збитків та значення ризику для загальних та цілеспрямованих ДІВ на АІС ЦБД ПН.

Таблиця 4.6 – Загальні та цілеспрямовані ДІВ

Ідентифікатор загрози	Назва загрози	Ймовірність реалізації загрози (p)	Величина збитків (h)	Ймовірність виходу з ладу
1	2	3	5	6
Загальні ДІВ				
3.1.1	Пожежа	0.1	6.62	0.9
3.1.2	Руйнування	0.02	6.62	0.8
3.1.3	Затоплення	0.03	6.62	0.8
3.1.4	Забруднення	0.05	6.62	0.33
3.1.5	Перегрів	0.3	6.62	0.55
3.1.6	Вологість	0.2	6.62	0.32
3.1.7	Електромагнітні випромінювання	0.05	6.62	0.33
3.1.8	Поламки, відмови та збої апаратури	0.3	6.62	0.99
3.1.9	Нестача ресурсів	0.5	6.62	0.19
3.1.10	Випадкове пошкодження обладнання	0.3	6.62	0,82
3.1.11	Відсутність фізичного з’єднання	0.1	8	0,82
3.1.12	Помилки та непрацездатність активного мережевого обладнання	0.2	11.29	0,34
3.1.13	Непрацездатність мережевих застосувань	0.2	7,30	0,8
3.1.14	Помилка, збій та відмова прикладного ПЗ	0.3	8,09	0,2
3.1.15	Несумісність версій ПЗ	0.1	6,50	0,21
3.1.16	Помилка, збій та відмова системного ПЗ	0.3	7,97	0,77
3.1.17	Помилка користувача	0.2	10,10	0,1
3.1.18	Ненавмисне пошкодження БД	0.1	7	0,24
Цілеспрямовані ДІВ				
3.2.1	Навмисне пошкодження або крадіжка обладнання	0.2	8.86	0,73
3.2.2	Розголошення даних про мережу	0.2	3.73	0,13
3.2.3	Перехоплення (сніферінг) пакетів	0.1	3.73	0,04
3.2.4	Підміна отримувача (спуфінг пакетів)	0.1	6.62	0,85
3.2.5	Відмова в обслуговуванні (DoS)	0.2	3.32	0,96
3.2.6	Дзеркалювання трафіку	0.05	6.88	0,56
3.2.7	Створення альтернативних	0.5	4,5	0,67

	несанкціонованих точок доступу до мережі			
3.2.8	Виконання недокументованих функцій	0.05	5,83	0,99
3.2.9	Розповсюдження вірусів та хробаків	0.5	8,86	0,64
3.2.10	Перехоплення ТІЗ	0.2	3,87	0,82
3.2.11	Підміна або дезорганізація	0.05	6,5	0,84
3.2.12	Злам	0.02	4,42	0,18
3.2.13	Пошкодження файлів ОС	0.2	6,25	0,87
3.2.14	Збирання «сміття»	0.02	2,63	0.13
3.2.15	Втручання в роботу ОС з мережі	0.2	6,47	0,71
3.2.16	Відмова від авторства	0,2	7	0,18
3.2.17	Розголошення даних	0,3	10,10	0,75

Використовуючи запропоноване програмне забезпечення здійснено розрахунок кіберзахищеності АІС ЦБД ПН, яка трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ із заданою якістю в умовах застосування «загальних» і цілеспрямованих ДІВ: $\mathbf{К_{ОКІІ}^{зах}} = (1 - Р_{ЗКА})*(1 - Р_{ЦКА})$.

Вводячи у відповідні поля «Рзка» (ймовірність реалізації загальних кібератак) та «Рцка» (ймовірність реалізації цілеспрямованих кібератак) із стовпчика 3 таблиці 4.6, та натискаючи після цього кнопку «Розрахувати» отримуємо показник кіберзахищеності об’єкта КІІ (АІС ЦБД ПН).

На рисунку 4.4 показаний результат розрахунку кіберзахищеності об’єкту КІІ при виникненні пожежі (загальний ДІВ) та навмисного пошкодження або крадіжки обладнання (цілеспрямований ДІВ).

Використовуючи запропоноване програмне забезпечення здійснено розрахунок кібернадійності АІС ЦБД ПН, яка трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах періодичного виникнення події (i = 1,…., N) – програмних та технічних відмов засобів об'єкта КІІ внаслідок ДІВ, де

$К_{ОКІІ}^{над} = \prod_{i=1}^{N} К_{ОКІІНАДi} (1 - P_i)$.

Вводячи значення ймовірності реалізації певної події у поле «Імовірність і-ої події» та додаючи кількість таких подій шляхом натискання

кнопки «Додати подію» отримуємо показник кібернадійності об’єкта КІІ (АІС ЦБД ПН).

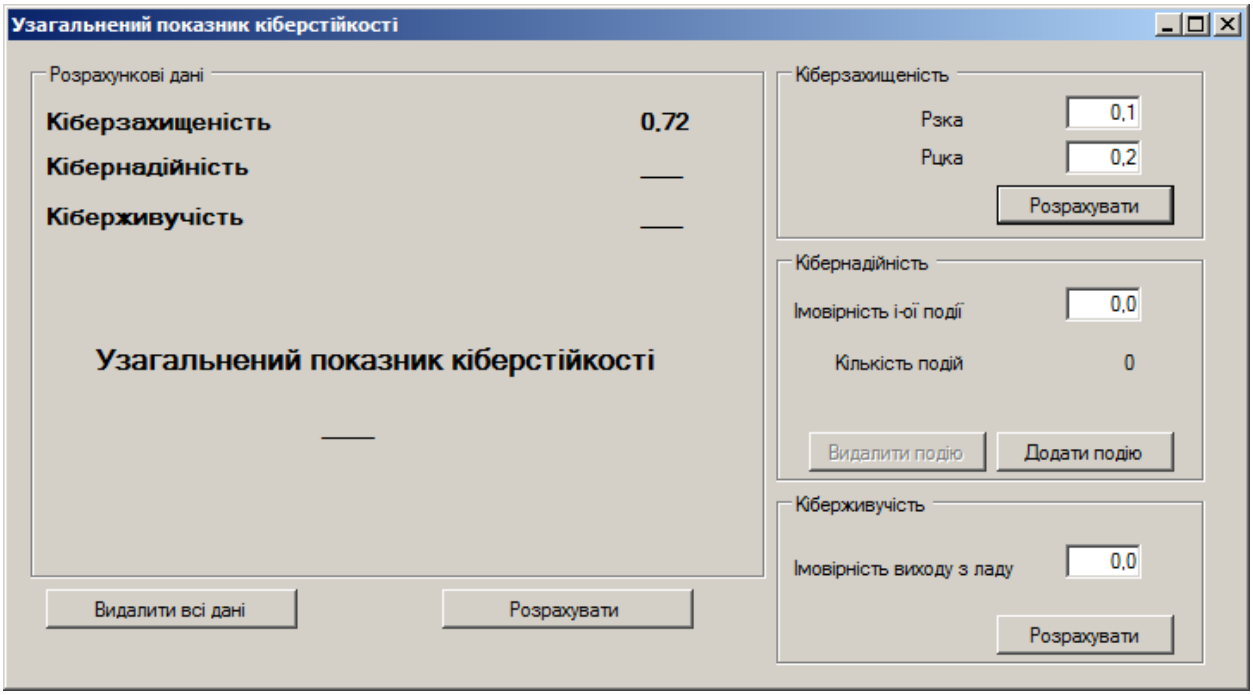

Рисунок 4.4 – Розрахунок кіберзахищеності

На рисунку 4.5 показаний результат розрахунку кібернадійності об’єкту КІІ при здійсненні п’яти спроб спуфінгу (підміна отримувача).

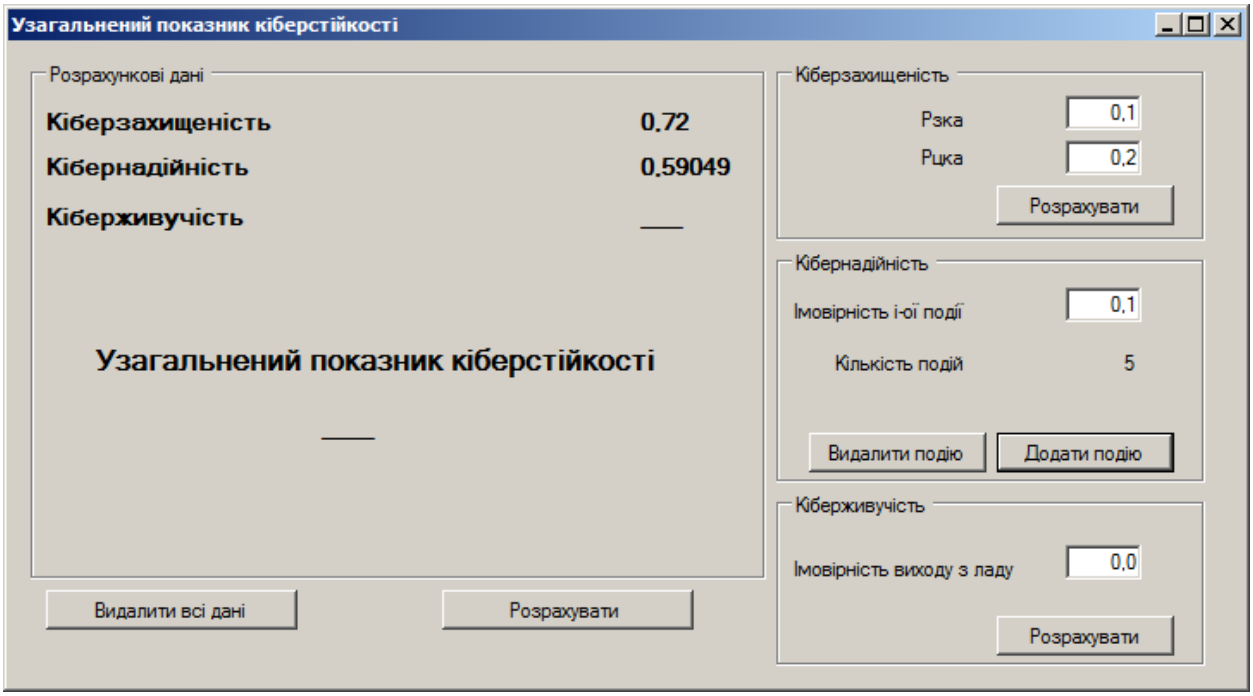

Рисунок 4.5 – Розрахунок кіберзахищеності

Використовуючи запропоноване програмне забезпечення здійснено розрахунок кіберживучості АІС ЦБД ПН, яка трактується як ймовірність невиходу кінцевого стану системи із заданої безпечної області S (невиходу з ладу). Тобто

$К_{окіп\ жив} = 1 – V_S$,

де V_S – ймовірність виходу кінцевого стану системи із заданої безпечної області S (виходу з ладу).

Вводячи значення ймовірності виходу кінцевого стану системи із заданої безпечної області у поле «Імовірність виходу з ладу» та натискаючи кнопку «Розрахувати» отримуємо показник кіберживучості об’єкта КІІ (АІС ЦБД ПН) при здійсненні певного ДІВ.

На рисунку 4.6 показаний результат розрахунку кіберживучості об’єкту КІІ при здійсненні пошкодження файлів ОС.

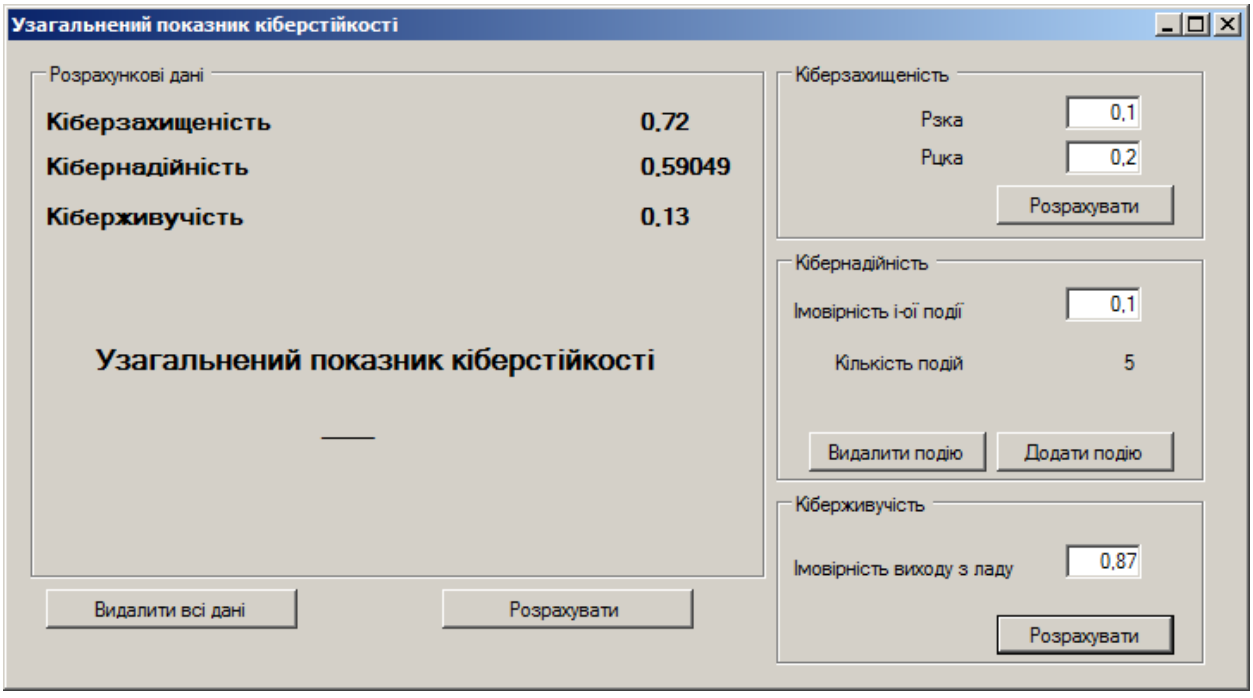

Рисунок 4.6 – Розрахунок кіберзаживучості

З огляду на те, що узагальнений показник кіберстійкості трактується як добуток показників кіберживучості, кібернадійності та кіберзахищеності, його було обчислено за допомогою програмного застосунку. Після

натискання кнопки «Розрахувати» у полі «Узагальнений показник кіберстійкості» з′являється результат (рис. 4.7).

Зовнішній вигляд вікна програми з результатами обчислень приведений на рисунку 4.7.

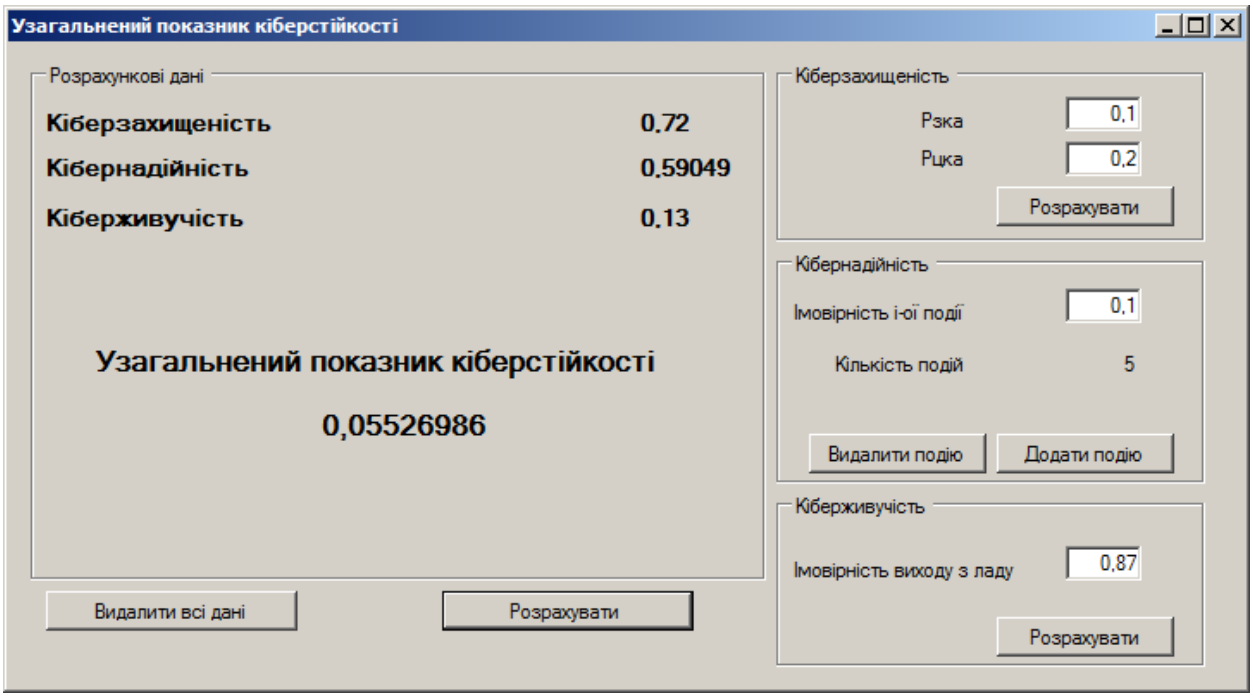

Рисунок 4.7 – Розрахунок узагальненого показника кіберстійкості

В результаті роботи програмного засобу здійснено розрахунок значення узагальненого показника кіберстійкості, як добутку показників кіберживучості, кібернадійності та кіберзахищеності.

Отримані результати підтверджують функціонування системи оцінювання кіберстійкості комп’ютерних мереж та систем об’єктів критичної інфраструктури та її успішне практичне застосування.

4.3. Висновки до четвертого розділу

1. Розроблено алгоритмічне забезпечення та програмний застосунок захисту інформації, яка циркулює в комп’ютерних мережах та системах об’єктів критичної інфраструктури, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість з використанням

розробленої методики. Зазначений програмний застосунок використано при побудові комплексних систем захисту інформації інформаційних систем об’єктів критичної інфраструктури.

2. Отримані результати підтверджують ефективність розробленого методу та методики, орієнтованої на захист інформації в комп’ютерних мережах та системах об’єктів критичної інфраструктури.

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 технологій кібербезпеки та захисту інформації (акт від 11.03.2021р.), Державного підприємства «Український державний центр радіочастот» (відгук від 10.10.2019р. №80/14.2-55/847/13063), Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (акт від 12.01.2021р.), ПрАТ «Фарлеп-Інвест» (відгук від 09.07.2018р. №65/04-10), ТОВ "ІНТЕСИС" (відгук від 01.10.2019р. №011019/01).

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну задачу, пов’язану з підвищенням рівня захисту інформації від кібервпливів в комп’ютерних мережах та системах об’єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації.

При вирішенні цієї задачі отримані такі основні результати:

1. Проаналізовано сучасні методи та засоби захисту інформації в

комп’ютерних мережах та системах. Встановлено, що дослідженню проблем, пов’язаних із процесом захисту інформації від кібервпливів в комп’ютерних системах та мережах об’єктів критичної інфраструктури, 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. Розроблено таксономію кіберзагроз інформаційній безпеці комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів системи, властивостей порушника та визначеної структури загрози дозволяє розробити модель загроз та модель порушника інформації в комп’ютерних мережах та системах об’єктів критичної інформаційної інфраструктури.

3. Складено матрицю залежності інформаційних об’єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз.

4. Розроблено модель бази даних кіберзагроз інформаційним об’єктам захисту комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії, параметрів властивостей інформації, що підлягає захисту, дозволяє розробити базу даних кіберзагроз інформаційній безпеці комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури.

5. Розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп’ютерних мереж та систем об’єктів критичної інформаційної інфраструктури, який за рахунок поєднання сигнатурного методу та методу виявлення аномалій, дозволяє розширити спектр виявлених кіберзагроз.

6. Розроблено методику оцінювання кіберстійкості комп’ютерних

систем та мереж об’єктів критичної інформаційної інфраструктури, яка за рахунок використання розробленої таксономії кіберзагроз та моделі бази даних кіберзагроз дозволяє забезпечити підтримку створення систем захисту інформації комп’ютерних систем та мереж об’єктів критичної інформаційної інфраструктури.

7. Розроблено структурну модель багаторівневої системи виявлення кібервпливів на ком’ютерні мережі та системи об’єктів критичної інфраструктури на основі запропонованого комбінованого методу розпізнавання кіберзагроз, що дозволяє здійснювати атоматизоване розпізнавання кіберзагроз та здійснювати захист від них.

8. Розроблено алгоритмічне забезпечення та програмний застосунок захисту інформації, яка циркулює в комп’ютерних мережах та системах об’єктів критичної інфраструктури, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість з використанням розробленої методики. Зазначений програмний застосунок використано при побудові комплексних систем захисту інформації інформаційних систем об’єктів критичної інфраструктури.

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), Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації (акт від 11.03.2021р.), Державного підприємства «Український державний центр радіочастот» (відгук від 10.10.2019р. №80/14.2-55/847/13063), Інституту

проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (акт від 12.01.2021р.), ПрАТ «Фарлеп-Інвест» (відгук від 09.07.2018р. №65/04-10), ТОВ "ІНТЕСИС" (відгук від 01.10.2019р. №011019/01).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. М. Комаров, С. Гончар, «Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури», *Національна академія наук України. Інститут проблем моделювання в енергетиці. Моделювання та інформаційні технології. Збірник наукових праць. Випуск 81, С. 12-19, 2017.*
2. 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.*
3. М. Комаров, С. Гончар, «Аналіз та дослідження загроз для захищеного вузлу Інтернет доступу», *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 29 (68). № 4, 2018. С. 165 - 168.*
4. 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.*
5. М. Комаров, «Підсистема управління доступом системи управління базами даних ORACLE DATABASE 12C ENTERPRISE EDITION», *Моделювання та інформаційні технології, №84, С. 87-96, 2018.*
6. 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.*
7. М. Комаров, «Загальні характеристики підприємства електроенергетики і елементи їх вразливості технологічного походження», *Електронне моделювання. Том 41. 1. С. 93 – 104 2019.*

8. М. Комаров, «Огляд кібератак на об’єкти критичної інфраструктури», *Національна академія наук України. Інститут проблем моделювання в енергетиці. Електронне моделювання. Т 41 № 6, 2019, С. 91 – 106.*

9. M. Komarov, A. Davydiuk, A. Onyskova, V. Tkachenko, S. Honchar “Critical Infrastructure Facilities and Analysis of Existing Approaches” *Studies in Systems, Decision and Control in Energy I. vol. 346, p. 189-205.*

10. М. Комаров «Особливості оцінки рівня гарантій Г-3 коректності реалізації функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу», *Безпека інформації в інформаційно-телекомунікаційних системах: Міжнар. наук.-практ. конф., 2015, Київ, 2015, С. 52-53.*

11. М. Комаров, С. Гончар, Г. Леоненко, «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.*

12. М. Комаров, С. Гончар, «Практичні аспекти побудови комплексної системи захисту інформації», *Кібербезпека енергетики: Наук.-практ. конф., 2018, м. Одеса.*

13. М. Комаров, С. Гончар, «Застосування систем управління інформаційною безпекою на об’єктах критичної інфраструктури», *Інформаційна безпека України: Наук.-практ. конф. 2018, м. Київ.*

14. 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.*

15. В. Ткаченко, М. Комаров, «Основні підходи оцінювання ризиків інформаційної безпеки», *Комп’ютерні системи та мережні технології: конф., Київ, 2019.*

16. М. Комаров, С. Гончар «Методика оцінки кіберстійкості об’єктів критичної інфраструктури», *Безпека соціально-економічних процесів в кіберпросторі: Всеук. наук.-практ. конф., 2019, Київ, 2019, С. 49-50.*

17. М. Комаров, «Аналіз шкідливого програмного забезпечення, як кіберзброї, та методи протидії кібератакам», *Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн: конф., Житомир, 2019, С. 235 – 238.*
18. М.Ю. Комаров, А.В. Оніськова, С.Ф. Гончар, В.В. Ткаченко, С.М. Сергєєв «Розробка бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури», *Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: XXXVIII наук-техн. конф. молодих вчених, Київ, 2020, С. 30 – 32.*
19. В.В. Ткаченко, М.Ю. Комаров, С.М. Сергєєв «Основні підходи до оцінки кібербезпеки SMART GRID систем» *Європейський університет, Національний авіаційний університет: Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна наук-практ. конф., Київ 2020, С. 99 – 104.*
20. М. Комаров, С. Гончар, А. Ониськова «Дослідження актуальних проблем забезпечення кібербезпеки Об'єднаної енергосистеми України в рамках впровадження концепції інтелектуальних мереж», *Матеріали Другої науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», Київ, 2020, С. 11.*
21. 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.
22. Мохор В.В., Гончар С.Ф., Комаров М.Ю., Чьочь В.В. База даних «Кіберзагрози об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України». *Свідоцтво про реєстрацію авторського права на твір № 95314 від 14.01.2020.*
23. Закон України «Про основні засади забезпечення кібербезпеки України».

24. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», введене в дію Указом Президента України від 15 березня 2016 року № 96.
25. 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.
26. Постанова Кабінету Міністрів України від 23.08.2016 № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».
27. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».
28. Постанова Кабінету Міністрів України від 9 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»
29. Постанова Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури».
30. Постанова Кабінету Міністрів України від 11 листопада 2020 року №1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом».
31. Стратегія національної безпеки України від 26 травня 2015 року № 287/2015.
32. Доктрина інформаційної безпеки України від 25 лютого 2017 року №47/2017.
33. Наказ Адміністрації Держспецзв'язку від 15 січня 2021 року № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури».

34. *С.Ф. Гончар* Визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами / Гончар С.Ф. // Захист інформації. – 2015. – Том 17, № 3. – С. 225-230.
35. *С.Ф. Гончар* Анализ угроз и уязвимостей индустриальных автоматизированных систем управления / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. - №2(26). – С. 9-14.
36. *С.Ф. Гончар* Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / Гончар С.Ф. // Захист інформації. – 2014. – Том 16, № 1. – С. 40-46.
37. *С.Ф. Гончар* Загальна модель загроз безпеці інформації АСУ ТП / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. - №1(29). – С. 78-82.
38. *С.Ф. Гончар* Модель імовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки / Гончар С.Ф. // Наукоємні технології. – 2015. – № 3(27). – С. 250-253.
39. *С.Ф. Гончар* Алгоритм визначення актуальних загроз безпеці інформації на об’єктах критичної інфраструктури / Гончар С.Ф., Юдін О.Ю., Леоненко Г.П. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. - №2(32). – С. 40-48.
40. *Гончар С.Ф., Леоненко Г.П., Юдін О.Ю.* Ймовірність реалізації загроз інформаційній безпеці АС критичної інфраструктури через можливі деструктивні дії персоналу : Матеріали Всеукраїнської наукової конференції «Математичне моделювання та математична фізика», Кременчук, 2015. – С. 29-30.
41. *Гончар С.Ф.* Імовірнісний аналіз кіберзагроз інформаційних об’єктів енергетики : The international research and practical conference: «The

development of technical sciences: problems and solutions», Brno, The Czech Republic, 2018. – С. 6-7.

42. *Гончар С.Ф.* Кіберзагрози використання сучасних інформаційних технологій в енергетиці : Матеріали науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», Київ, 2019. – С. 10.

43. *Ткаченко В.В., Ониськова А.В., Гончар С.Ф.*, та ін. Аналіз загроз системи захисту інформації в SMART GRID системах на базі методів SREP і CORAS : Збірник тез XXXVII науково-технічної конференції молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України, Київ, 2020. – С. 55-56.

44. *С.Ф. Гончар* Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Монографія. – К.: «Альфа Реклама», 2019. – 176 с.

45. *Honchar S.* Analytical geometry approach for information security risk analyses / V. Mokhor, S. Honchar, V. Bezshtanko, H. Kravtsov, I. Kotsiuba, O. Kruk, O. Makarevych, Y. Maksymenko, V. Tsurkan. // Information Technology and Security, January-June, Vol. 3, Iss.1(4), 2015. – P. 60-67.

46. *С.Ф. Гончар* Идея построения алгебры рисков на основе теории комплексных чисел / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2018. – Т.40. – №4. – С. 107-111.

47. *С.Ф. Гончар* Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури / Мохор В.В., Гончар С.Ф., Дибач О.М. // ДНТЦ ЯРБ. 2019. №2(82) – С.57-61.

48. *В.В. Мохор* Дослідження правомірності подання ризиків векторами у евклідовому просторі / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2019. – Т.41. – №4. – С. 73-84.

49. *С.Ф. Гончар* Методологія оцінки ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури / Гончар С.Ф. // Вчені

записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2019. – Т.30(69). Ч.1. – №4. – С. 40-44.

50. *С.Ф. Гончар* Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури / Мохор В.В., Гончар С.Ф. // Електронне моделювання. – 2019. – Т.41. – № 6. – С. 65-76.

51. *С.Ф. Гончар* Метод оцінювання ризиків кібербезпеки інформаційних систем SMART GRID / Гончар С.Ф. // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2020. – Т.31(70). Ч.1. – №3. – С. 97-101.

52. *Гончар С.Ф.* Підхід до аналізу ризику на основі теорії комплексних чисел : Збірник тез доповідей XII Міжнародної науково-технічної конференції «Комп’ютерні системи та мережні технології», Київ, 2019. – С. 35-36.

53. *Гончар С.Ф.* Методологія оцінки ризику кібербезпеки інформаційних систем : Збірник тез XXXVII науково-технічної конференції молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України, Київ, 2019. – С. 71.

54. *Гончар С.Ф.* Методологія оцінки суми ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури : Матеріали V Всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації», Одеса, 2019. – С. 26-28.

55. *Гончар С.Ф.* Моделі та метод оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури : Матеріали VI Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», Закарпатська обл., туристичний комплекс «Едельвейс» ПВНЗ «Європейський університет», 2020р. – С. 27-32.

56. *Honchar S.F., Onyskova A.V.* Relevance of the subjective component in cybersecurity risk assessment: Papers of participants of the International Multidisciplinary Scientific and Practical Conference

«Theoretical and empirical scientific research: concept and trends», held in Oxford, July 24, 2020. pp. 22-23.

57. *V. Mokhor, S. Honchar, A. Onyskova*. Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects. Papers of participants of the 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, (PIC S&T`2020), on the basis of Kharkiv National University of Radio and Electronics, 6 - 9 October, 2020. http://picst.org/files/program_picst20.pdf.

58. *Гончар С.Ф.* Дослідження суб'єктивної складової ризику кібербезпеки об'єктів критичної інфраструктури : Матеріали VII міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», Київ, 2021. – С. 28-30.

59. *Гончар С.Ф., Мохор В.В., Бакалінський О.О.* Апаратно-програмний комплекс розрахунку сумарного ризику : пат. 135456 Україна : МПК G06Q 90/00, G06F 17/00. № u201903831; заявл. 15.04.2019; опубл. 25.06.2019, Бюл. № 12.

60. *Гончар С.Ф., Мохор В.В., Бакалінський О.О.* Апаратно-програмний комплекс розрахунку комплексного ризику : пат. 136792 Україна : МПК G06Q 90/00, G06F 17/00. № u201906995; заявл. 24.06.2019; опубл. 27.08.2019, Бюл. № 12.

61. *Гончар С.Ф., Мохор В.В., Бакалінський О.О.* Апаратно-програмний комплекс візуалізації ризиків : пат. 136949 Україна : МПК G06Q 90/00, G06F 17/00. № u201908431; заявл. 17.07.2019; опубл. 10.09.2019, Бюл. № 12.

62. *Гончар С.Ф., Мохор В.В., Бакалінський О.О.* Апаратно-програмний комплекс оцінки та аналізу ризику : пат. 136947 Україна : МПК G06Q 90/00, G06F 17/00. № u201908305; заявл. 16.07.2019; опубл. 10.09.2019, Бюл. № 12.

63. *Peter G. Neumann* Computer-Related Risks. ACM Press / Addison Wesley, 1995.

64. *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
65. *Гончар С.Ф., Комаров М.Ю.* Спосіб виявлення кібератак на інформаційно-телекомунікаційні системи : Матеріали Всеукраїнської науково-практичної Інтернет-конференції „Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку", Черкаси, 2019. – С. 64-66
66. *Сергєєв С.М., Ониськова А.В., Гончар С.Ф.*, та ін. Аналіз основних технологій виявлення вторгнень для забезпечення кібербезпеки автоматизованих систем класу 3 : Збірник тез XXXVII науково-технічної конференції молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України, Київ, 2020. – С. 108-113
67. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»
68. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»
69. *John D. Howard, Thomas A. Longstaff* A common language for computer security incidents. Sandia Report. Sandia National Laboratories. 1998.
70. The IEEE standard dictionary of electrical and electronics terms. Sixth edition. John Radatz. editor. Institute of Electrical and Electronics Engineers. New York, 1996.
71. *Attanasio C. R., Markstein P. W., Phillips R. J.* Penetrating an operating system: a study of VM/370 integrity. IBM System Journal, 15(1), 1976. P. 102–116.
72. *Giri Vijayaraghavan, Cem Kaner* Bug Taxonomies. STAR EAST 2003, Orlando, FL, May-2003.
73. *James P. Anderson* Computer security threat monitoring and surveillance. Technical Report Contract 79F296400, Washington, April 1980.

74. *Peter Neumann, Donald Parker* A summary of computer misuse techniques, In 12th National Computer Security Conference, 1989.
75. *Simon Hansman* A taxonomy of network and computer attacks methodologies. University of Canterbury. New Zealand, November 2003.
76. *Jeffrey Undercoffer, John Pinkston* Modeling computer attacks: a target-centric ontology for intrusion detection. University of Maryland Baltimore Country.
77. *Медведовский И. Д., Семьянов П. В., Платонов В. В.* Атака через Internet. М., 1997.
78. *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
79. *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
80. *Гончар С.Ф., Ониськова А.В.* Актуальність забезпечення кібербезпеки сучасних електроенергетичних об'єктів з використанням інтелектуальних мереж Smart Grid : Збірник тез XXXVII науково-технічної конференції молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України, Київ, 2019. – С. 72
81. *Гончар С.Ф., Мохор В.В., Бакалінський О.О.* Апаратно-програмний комплекс визначення проектних характеристик системи управління інформаційною безпекою : пат. 138045 Україна : МПК G06F 21/00, G06F 17/00, G06Q 90/00. № u201909221; заявл. 09.08.2019; опубл. 11.11.2019, Бюл. № 21
82. *Д.Л. Осипов* Технологии проектирования баз данных. – М.: «ДМК Пресс», 2019. – 498 с.

83.*В. Ф. Шаньгин* Информационная безопасность и защита информации. – М.: «ДМК Пресс», 2017. – 702 с.

84.*К. А. Монаппа* Анализ вредоносных программ. – М.: «ДМК Пресс», 2019. – 452 с.

85.*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

86.*Гончар С.Ф.* Підходи до оцінки небезпеки атак в інформаційних системах об'єктів критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. - №2(30). – С. 47-52.

87. *Гончар С.Ф.* Наслідки можливих кібератак на об'єкти критичної інфраструктури. / Леоненко Г.П. // Information Technology and Security, January-June, Vol. 4, Iss.1(6), 2016. – P. 108-113.

88.*Гончар С.Ф.* Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури. / Леоненко Г.П. // Information Technology and Security, July-December, Vol. 4, Iss.2(7), 2016. – P. 262-268.

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

90.*В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа* Інформаційна та кібербезпека: соціотехнічний аспект; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К.: ДУТ, 2015.— 288 с.

91.*В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко* Безопасность информационных систем. Учебное пособие. – М.: «Флинта», 2015.

92. *Чио К., Фримэн Д.* Машинное обучение и безопасность. Пер. с анг. А.В. Снастина. М.: ДМК Пресс, 2020. 388 с.

93.*Гончар С.Ф.* Дослідження проблеми кіберживучості Об'єднаної енергосистеми України / Герасимов Р.П., Ткаченко В.В. // Електронне моделювання. – 2019. – Т.41. – №1. – С.43-53

94.*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.

95.*Климовський А.А.* Таксономия кибератак и ее применение к задаче формирования сценариев их проведения / Труды ИСА РАН. – 2006. Т. 27. – с. 74 – 107.

96.*Гончар С.Ф.* Аналіз впливу на екологію стану кібербезпеки об'єктів критичної інфраструктури / Гончар С.Ф. // Екологічні науки. – 2018. № 2(21). – С. 65-68.

97.Автоматизована інформаційна система «Централізована база даних перенесених номерів». Техноробочий проект. Пояснювальна записка. 3969753.79415200-8.001П2.

98.Автоматизована інформаційна система «Централізована база даних перенесених номерів». Техноробочий проект. Загальний опис АІС ЦБД ПН. 3969753.79415200-8.001ПД.

99.Автоматизована інформаційна система «Централізована база даних перенесених номерів». Техноробочий проект. Специфікація SOAP/XML інтерфейсу. 3969753.79415200-8.001С2.

100. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

101. Централізована база даних перенесених номерів». Комплексна система захисту інформації. Модель загроз для інформації та модель порушника безпеки інформації.

102. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технологій. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій.

Додаток А

Список публікацій здобувача за темою дисертації

1. М. Комаров, С. Гончар, «Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури», *Національна академія наук України. Інститут проблем моделювання в енергетиці. Моделювання та інформаційні технології. Збірник наукових праць. Випуск 81, С. 12-19, 2017.*
2. 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.*
3. М. Комаров, С. Гончар, «Аналіз та дослідження загроз для захищеного вузлу Інтернет доступу», *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 29 (68). № 4, 2018. С. 165 - 168.*
4. 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.*
5. М. Комаров, «Підсистема управління доступом системи управління базами даних ORACLE DATABASE 12C ENTERPRISE EDITION», *Моделювання та інформаційні технології, №84, С. 87-96, 2018.*
6. 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.*
7. М. Комаров, «Загальні характеристики підприємства електроенергетики і елементи їх вразливості технологічного походження», *Електронне моделювання. Том 41. 1. С. 93 – 104 2019.*
8. М. Комаров, «Огляд кібератак на об’єкти критичної інфраструктури», *Національна академія наук України. Інститут проблем моделювання в енергетиці. Електронне моделювання. Т 41 № 6, 2019, С. 91 – 106.*
9. M. Komarov, A. Davydiuk, A. Onyskova, V. Tkachenko, S. Honchar “Critical Infrastructure Facilities and Analysis of Existing Approaches” *Studies in Systems, Decision and Control in Energy I. vol. 346, p. 189-205.*
10. М. Комаров «Особливості оцінки рівня гарантій Г-3 коректності реалізації функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу», *Безпека інформації в інформаційно-телекомунікаційних системах: Міжнар. наук.-практ. конф., 2015, Київ, 2015, С. 52-53.*
11. М. Комаров, С. Гончар, Г. Леоненко, «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.*

12. М. Комаров, С. Гончар, «Практичні аспекти побудови комплексної системи захисту інформації», *Кібербезпека енергетики: Наук.-практ. конф., 2018, м. Одеса.*
13. М. Комаров, С. Гончар, «Застосування систем управління інформаційною безпекою на об'єктах критичної інфраструктури», *Інформаційна безпека України: Наук.-практ. конф. 2018, м. Київ.*
14. 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.*
15. В. Ткаченко, М. Комаров, «Основні підходи оцінювання ризиків інформаційної безпеки», *Комп'ютерні системи та мережні технології: конф., Київ, 2019.*
16. 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.*
17. М. Комаров, «Аналіз шкідливого програмного забезпечення, як кіберзброї, та методи протидії кібератакам», *Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн: конф., Житомир, 2019, С. 235 – 238.*
18. М.Ю. Комаров, А.В. Оніськова, С.Ф. Гончар, В.В. Ткаченко, С.М. Сергєєв «Розробка бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури», *Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: XXXVIII наук-техн. конф. молодих вчених, Київ, 2020, С. 30 – 32.*
19. В.В. Ткаченко, М.Ю. Комаров, С.М. Сергєєв «Основні підходи до оцінки кібербезпеки SMART GRID систем» *Європейський університет, Національний авіаційний університет: Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна наук-практ. конф., Київ 2020, С. 99 – 104.*
20. М. Комаров, С. Гончар, А. Ониськова «Дослідження актуальних проблем забезпечення кібербезпеки Об'єднаної енергосистеми України в рамках впровадження концепції інтелектуальних мереж», *Матеріали Другої науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», Київ, 2020, С. 11.*
21. 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.
22. Мохор В.В., Гончар С.Ф., Комаров М.Ю., Чьочь В.В. База даних «Кіберзагрози об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України». *Свідоцтво про реєстрацію авторського права на твір № 95314 від 14.01.2020.*

Додаток Б

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

УПМЕ вх. 111
22.03.2019р

"ЗАТВЕРДЖУЮ"
В.о. начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації
к.в.н.

Володимир КОЗАК

"11" 03 2021 року

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційної роботи
«Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури»
Комарова Максима Юрійовича
на здобуття наукового ступеню кандидата технічних наук
за спеціальністю 05.13.05 – «Комп'ютерні системи та компоненти»

Комісія у складі:

голови комісії – заступника начальника Інституту – начальника науково-дослідного центру ДержНДІ технологій кібербезпеки к.т.н. полковника Юдіна О.Ю.,

членів комісії – начальника центру технічного захисту інформації ДержНДІ технологій кібербезпеки підполковника Сущенка В.А., начальника науково-дослідного відділу науково-дослідного центру ДержНДІ технологій кібербезпеки к.т.н. доцента полковника Держспецзв'язку Липського О.А. з'ясувала, що в Державному науково-дослідному інституті технологій кібербезпеки та захисту інформації впровадженні розроблені Комаровим М.Ю. такі наукові результати:

- таксономія кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури, яка за рахунок використання ієрархічної структури відносин з деревовидним розкриттям категорій дозволила описати багатоетапні атаки, які на сьогоднішній день отримали дуже широку розповсюдженість;
- модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії та параметрів властивостей інформації, що підлягає захисту, дозволила розробити базу даних кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури.

Ефект від впровадження набутих наукових результатів полягає в тому, що вони дозволили розробити адекватні рекомендації, методи та засоби щодо захисту інформації на об'єктах критичної інфраструктури.

Результати, отримані Комаровим М.Ю. при написанні дисертаційної роботи, використані при створенні комплексних систем захисту інформації у Національній телекомунікаційній мережі, побудові об'єктів інформаційної діяльності на рухомих та стаціонарних об'єктах спеціального зв'язку, в тому числі об'єктів інформаційної діяльності в дипломатичних установах України за кордоном.

Голова комісії
к.т.н.
полковник Олексій ЮДІН

Члени комісії:
підполковник Віталій СУЩЕНКО

к.т.н., доцент
полковник Олександр ЛИПСЬКИЙ

НАЦІОНАЛЬНА КОМІСІЯ, ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ
РЕГУЛЮВАННЯ У СФЕРІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

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

«__» _____ 2021 р.

АКТ ВПРОВАДЖЕННЯ

результатів дисертаційної роботи

«Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури»

Комарова Максима Юрійовича

на здобуття наукового ступеню кандидата технічних наук

за спеціальністю 05.13.05 – «Комп'ютерні системи та компоненти»

Комісія у складі голови комісії заступника директора Інституту, доктора технічних наук Чемериса Олександра Анатолійовича та членів комісії у складі: наукового співробітника Герасимова Ростислава Павловича та провідного наукового співробітника, доктора технічних наук Гончара Сергія Феодосійовича встановила, що програмна реалізація засобів захисту інформації від кіберзагроз в комп'ютерних системах та мережах об'єктів критичної інфраструктури, що є результатом досліджень Комарова М.Ю., реалізована в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Розроблено алгоритмічне забезпечення на основі запропонованого комбінованого методу розпізнавання кіберзагроз для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизоване розпізнавання кіберзагроз та здійснювати захист від них, а також алгоритмічне забезпечення на основі запропонованої методики оцінювання кіберстійкості для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність кіберзахищеність та кіберстійкість. На основі запропонованих алгоритмів розроблені програмні застосунки, що використовують запропонований метод та методику для захисту інформації в комп'ютерних мережах та системах обєктів критичної інформаційної інфраструктури.

Таким чином, результати, отримані Комаровим М.Ю. при написанні дисертаційної роботи, дозволили використовувати засоби захисту інформації від кіберзагроз в комп'ютерних системах та мережах об'єктів критичної інфраструктури при побудові комплексних систем захисту інформації і систем управління інформаційною безпекою.

Вказані результати було використано в ході виконання науково-дослідних робіт «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів», шифр «ВПЛИВ», № держреєстрації 0118U005320, а також «Розроблення методів забезпечення кібернетичної безпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж», шифр «Інтеленерго», № держреєстрації 0119U101856.

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:
науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України Р.П. Герасимов

пров. наук. співробіт. ІПМЕ ім. Г.Є. Пухова НАН України
д.т.н., ст.досл. С.Ф. Гончар

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

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 95314

База даних "Кіберзагрози об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України"

(вид, назва службового твору)

Автор(и) **Мохор Володимир Володимирович, Гончар Сергій Феодосійович, Комаров Максим Юрійович, Чьочь Вікторія Володимирівна**

(повне ім'я, псевдонім (за наявності))

Авторські майнові права належать **Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, вул. Ген. Наумова, 15, м. Київ, 03164**

(повне ім'я фізичної та/або повне офіційне найменування юридичної особи, адреса)

Дата реєстрації 14.01.2020

Заступник Міністра розвитку економіки, торгівлі та сільського господарства України Д. О. Романович

Лістинги (коди) програмних засобів

```
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 Max_Proga
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        //

        //
        float Kgiv = 0;
        //
        float Kzah = 0;
        float Rzka = 0;
        float Rcka = 0;
        //
        float Knad = 1;
        float KnadTemp = 1;
        int KilkPodiy=0;
        //
        private void button1_Click(object sender, EventArgs e)
        {

            try {
                if (Convert.ToSingle(textBox1.Text) > 1)

                    MessageBox.Show("Рзка не може бути більше 1");
                else
                    if (Convert.ToSingle(textBox2.Text) > 1)

                    MessageBox.Show("Рцка не може бути більше 1");

                else
                {
                    Rzka = Convert.ToSingle(textBox1.Text);
                    Rcka = Convert.ToSingle(textBox2.Text);
                    Kzah = (1 - Rzka) * (1 - Rcka);
                    label10.Text = Convert.ToString(Kzah);
```

```
                }
            }
            catch
            {
                MessageBox.Show("Помилка вводу даних");
            }

        }

        private void button3_Click(object sender, EventArgs e)
        {
            try {
                if (Convert.ToSingle(textBox3.Text) > 1)

                    MessageBox.Show("Імовірність і-ої події не може бути
більше 1");
                else
                {
                    KilkPodiy = KilkPodiy + 1;
                    KnadTemp = Knad;
                    Knad = Knad * (1 -
Convert.ToSingle(textBox3.Text));
                    label11.Text = Convert.ToString(Knad);
                    label5.Text = Convert.ToString(KilkPodiy);
                    button2.Enabled = true;
                }
            }
            catch
            {
                MessageBox.Show("Помилка вводу даних");
            }

        }

        private void button2_Click(object sender, EventArgs e)
        {
            KilkPodiy = KilkPodiy - 1;
            label5.Text = Convert.ToString(KilkPodiy);
            Knad = KnadTemp;
            label11.Text = Convert.ToString(Knad);
            button2.Enabled = false;
        }

        private void Form1_Load(object sender, EventArgs e)
        {
            label10.Text = "___";
            label11.Text = "___";
            label12.Text = "___";
            label13.Text = "___";
        }

        private void button5_Click(object sender, EventArgs e)
```

```
        {
            //
            Kgiv = 0;
            Kzah = 0;
            Rzka = 0;
            Rcka = 0;
            Knad = 1;
            KnadTemp = 1;
           //
            KilkPodiy = 0;
            textBox1.Text = "0,0";
            textBox2.Text = "0,0";
            textBox3.Text = "0,0";
            label5.Text = "0";
            label10.Text = "___";
            label11.Text = "___";
            label12.Text = "___";
            label13.Text = "___";

        }

        private void button6_Click(object sender, EventArgs e)
        {
            try {
                if (Convert.ToSingle(textBox4.Text) > 1)

                   MessageBox.Show("Імовірність виходу з ладу не може бути
більше 1");
                else
                {
                    Kgiv = 1 - Convert.ToSingle(textBox4.Text);
                    label12.Text = Convert.ToString(Kgiv);

                }
            }
            catch
            {
                MessageBox.Show("Помилка вводу даних");
            }

        }

        private void button4_Click(object sender, EventArgs e)
        {


            if ((label10.Text == "___") || (label11.Text == "___") ||
(label12.Text == "___"))
            {
                MessageBox.Show("Розрахуйте всі необхідні параметри");
            }
            else
```

```
            label13.Text =
Convert.ToString(Convert.ToSingle(label10.Text) *
Convert.ToSingle(label11.Text) * Convert.ToSingle(label12.Text));
        }
    }
}
namespace Max_Proga
{
    partial class Form1
    {
        /// <summary>
        /// Обязательная переменная конструктора.
        /// </summary>
        private System.ComponentModel.IContainer components = null;

        /// <summary>
        /// Освободить все используемые ресурсы.
        /// </summary>
        /// <param name="disposing">истинно, если управляемый ресурс должен
быть удален; иначе ложно.</param>
        protected override void Dispose(bool disposing)
        {
            if (disposing && (components != null))
            {
                components.Dispose();
            }
            base.Dispose(disposing);
        }

        #region Код, автоматически созданный конструктором форм Windows

        /// <summary>
        /// Требуемый метод для поддержки конструктора — не изменяйте
        /// содержимое этого метода с помощью редактора кода.
        /// </summary>
        private void InitializeComponent()
        {
            this.groupBox1 = new System.Windows.Forms.GroupBox();
            this.label2 = new System.Windows.Forms.Label();
            this.label1 = new System.Windows.Forms.Label();
            this.textBox2 = new System.Windows.Forms.TextBox();
            this.textBox1 = new System.Windows.Forms.TextBox();
            this.button1 = new System.Windows.Forms.Button();
            this.groupBox2 = new System.Windows.Forms.GroupBox();
            this.label5 = new System.Windows.Forms.Label();
            this.textBox3 = new System.Windows.Forms.TextBox();
            this.label4 = new System.Windows.Forms.Label();
            this.label3 = new System.Windows.Forms.Label();
            this.button3 = new System.Windows.Forms.Button();
            this.button2 = new System.Windows.Forms.Button();
            this.groupBox3 = new System.Windows.Forms.GroupBox();
```

```
            this.button6 = new System.Windows.Forms.Button();
            this.textBox4 = new System.Windows.Forms.TextBox();
            this.label14 = new System.Windows.Forms.Label();
            this.groupBox4 = new System.Windows.Forms.GroupBox();
            this.label13 = new System.Windows.Forms.Label();
            this.label12 = new System.Windows.Forms.Label();
            this.label11 = new System.Windows.Forms.Label();
            this.label10 = new System.Windows.Forms.Label();
            this.label9 = new System.Windows.Forms.Label();
            this.label8 = new System.Windows.Forms.Label();
            this.label7 = new System.Windows.Forms.Label();
            this.label6 = new System.Windows.Forms.Label();
            this.button4 = new System.Windows.Forms.Button();
            this.button5 = new System.Windows.Forms.Button();
            this.groupBox1.SuspendLayout();
            this.groupBox2.SuspendLayout();
            this.groupBox3.SuspendLayout();
            this.groupBox4.SuspendLayout();
            this.SuspendLayout();
            //
            // groupBox1
            //
            this.groupBox1.Controls.Add(this.label2);
            this.groupBox1.Controls.Add(this.label1);
            this.groupBox1.Controls.Add(this.textBox2);
            this.groupBox1.Controls.Add(this.textBox1);
            this.groupBox1.Controls.Add(this.button1);
            this.groupBox1.Location = new System.Drawing.Point(446,
12);
            this.groupBox1.Name = "groupBox1";
            this.groupBox1.Size = new System.Drawing.Size(249, 103);
            this.groupBox1.TabIndex = 0;
            this.groupBox1.TabStop = false;
            this.groupBox1.Text = "Кіберзахищеність";
            //
            // label2
            //
            this.label2.AutoSize = true;
            this.label2.Location = new System.Drawing.Point(81, 48);
            this.label2.Name = "label2";
            this.label2.Size = new System.Drawing.Size(32, 13);
            this.label2.TabIndex = 4;
            this.label2.Text = "Рцка";
            //
            // label1
            //
            this.label1.AutoSize = true;
            this.label1.Location = new System.Drawing.Point(81, 26);
            this.label1.Name = "label1";
            this.label1.Size = new System.Drawing.Size(32, 13);
            this.label1.TabIndex = 3;
            this.label1.Text = "Рзка";
```

```
            //
            // textBox2
            //
            this.textBox2.Location = new System.Drawing.Point(168,
45);
            this.textBox2.Name = "textBox2";
            this.textBox2.Size = new System.Drawing.Size(44, 20);
            this.textBox2.TabIndex = 2;
            this.textBox2.Text = "0,0";
            this.textBox2.TextAlign =
System.Windows.Forms.HorizontalAlignment.Right;
            //
            // textBox1
            //
            this.textBox1.Location = new System.Drawing.Point(168,
19);
            this.textBox1.Name = "textBox1";
            this.textBox1.Size = new System.Drawing.Size(44, 20);
            this.textBox1.TabIndex = 1;
            this.textBox1.Text = "0,0";
            this.textBox1.TextAlign =
System.Windows.Forms.HorizontalAlignment.Right;
            //
            // button1
            //
            this.button1.Location = new System.Drawing.Point(128, 71);
            this.button1.Name = "button1";
            this.button1.Size = new System.Drawing.Size(103, 23);
            this.button1.TabIndex = 0;
            this.button1.Text = "Розрахувати";
            this.button1.UseVisualStyleBackColor = true;
            this.button1.Click += new
System.EventHandler(this.button1_Click);
            //
            // groupBox2
            //
            this.groupBox2.Controls.Add(this.label5);
            this.groupBox2.Controls.Add(this.textBox3);
            this.groupBox2.Controls.Add(this.label4);
            this.groupBox2.Controls.Add(this.label3);
            this.groupBox2.Controls.Add(this.button3);
            this.groupBox2.Controls.Add(this.button2);
            this.groupBox2.Location = new System.Drawing.Point(446,
121);
            this.groupBox2.Name = "groupBox2";
            this.groupBox2.Size = new System.Drawing.Size(249, 134);
            this.groupBox2.TabIndex = 1;
            this.groupBox2.TabStop = false;
            this.groupBox2.Text = "Кібернадійність";
            //
            // label5
            //
```

```
            this.label5.AutoSize = true;
            this.label5.Location = new System.Drawing.Point(199, 58);
            this.label5.Name = "label5";
            this.label5.Size = new System.Drawing.Size(13, 13);
            this.label5.TabIndex = 5;
            this.label5.Text = "0";
            //
            // textBox3
            //
            this.textBox3.Location = new System.Drawing.Point(168,
21);
            this.textBox3.Name = "textBox3";
            this.textBox3.Size = new System.Drawing.Size(44, 20);
            this.textBox3.TabIndex = 4;
            this.textBox3.Text = "0,0";
            this.textBox3.TextAlign =
System.Windows.Forms.HorizontalAlignment.Right;
            //
            // label4
            //
            this.label4.AutoSize = true;
            this.label4.Location = new System.Drawing.Point(31, 58);
            this.label4.Name = "label4";
            this.label4.Size = new System.Drawing.Size(82, 13);
            this.label4.TabIndex = 3;
            this.label4.Text = "Кількість подій";
            //
            // label3
            //
            this.label3.AutoSize = true;
            this.label3.Location = new System.Drawing.Point(7, 28);
            this.label3.Name = "label3";
            this.label3.Size = new System.Drawing.Size(106, 13);
            this.label3.TabIndex = 2;
            this.label3.Text = "Імовірність і-ої події";
            //
            // button3
            //
            this.button3.Location = new System.Drawing.Point(128,
105);
            this.button3.Name = "button3";
            this.button3.Size = new System.Drawing.Size(103, 23);
            this.button3.TabIndex = 1;
            this.button3.Text = "Додати подію";
            this.button3.UseVisualStyleBackColor = true;
            this.button3.Click += new
System.EventHandler(this.button3_Click);
            //
            // button2
            //
            this.button2.Enabled = false;
            this.button2.Location = new System.Drawing.Point(19, 105);
```

```
            this.button2.Name = "button2";
            this.button2.Size = new System.Drawing.Size(103, 23);
            this.button2.TabIndex = 0;
            this.button2.Text = "Видалити подію";
            this.button2.UseVisualStyleBackColor = true;
            this.button2.Click += new
System.EventHandler(this.button2_Click);
            //
            // groupBox3
            //
            this.groupBox3.Controls.Add(this.button6);
            this.groupBox3.Controls.Add(this.textBox4);
            this.groupBox3.Controls.Add(this.label14);
            this.groupBox3.Location = new System.Drawing.Point(446,
261);
            this.groupBox3.Name = "groupBox3";
            this.groupBox3.Size = new System.Drawing.Size(249, 100);
            this.groupBox3.TabIndex = 2;
            this.groupBox3.TabStop = false;
            this.groupBox3.Text = "Кіберживучість";
            //
            // button6
            //
            this.button6.Location = new System.Drawing.Point(128, 71);
            this.button6.Name = "button6";
            this.button6.Size = new System.Drawing.Size(103, 23);
            this.button6.TabIndex = 2;
            this.button6.Text = "Розрахувати";
            this.button6.UseVisualStyleBackColor = true;
            this.button6.Click += new
System.EventHandler(this.button6_Click);
            //
            // textBox4
            //
            this.textBox4.Location = new System.Drawing.Point(168,
30);
            this.textBox4.Name = "textBox4";
            this.textBox4.Size = new System.Drawing.Size(44, 20);
            this.textBox4.TabIndex = 1;
            this.textBox4.Text = "0,0";
            this.textBox4.TextAlign =
System.Windows.Forms.HorizontalAlignment.Right;
            //
            // label14
            //
            this.label14.AutoSize = true;
            this.label14.Location = new System.Drawing.Point(7, 37);
            this.label14.Name = "label14";
            this.label14.Size = new System.Drawing.Size(135, 13);
            this.label14.TabIndex = 0;
            this.label14.Text = "Імовірність виходу з ладу";
            //
```

```
            // groupBox4
            //
            this.groupBox4.Controls.Add(this.label13);
            this.groupBox4.Controls.Add(this.label12);
            this.groupBox4.Controls.Add(this.label11);
            this.groupBox4.Controls.Add(this.label10);
            this.groupBox4.Controls.Add(this.label9);
            this.groupBox4.Controls.Add(this.label8);
            this.groupBox4.Controls.Add(this.label7);
            this.groupBox4.Controls.Add(this.label6);
            this.groupBox4.Location = new System.Drawing.Point(13,
12);
            this.groupBox4.Name = "groupBox4";
            this.groupBox4.Size = new System.Drawing.Size(427, 299);
            this.groupBox4.TabIndex = 3;
            this.groupBox4.TabStop = false;
            this.groupBox4.Text = "Розрахункові дані";
            //
            // label13
            //
            this.label13.AutoSize = true;
            this.label13.Font = new System.Drawing.Font("Microsoft
Sans Serif", 12F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label13.Location = new System.Drawing.Point(165,
199);
            this.label13.Name = "label13";
            this.label13.Size = new System.Drawing.Size(67, 20);
            this.label13.TabIndex = 7;
            this.label13.Text = "label13";
            //
            // label12
            //
            this.label12.AutoSize = true;
            this.label12.Font = new System.Drawing.Font("Microsoft
Sans Serif", 9.75F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label12.Location = new System.Drawing.Point(351, 81);
            this.label12.Name = "label12";
            this.label12.Size = new System.Drawing.Size(59, 16);
            this.label12.TabIndex = 6;
            this.label12.Text = "label12";
            //
            // label11
            //
            this.label11.AutoSize = true;
            this.label11.Font = new System.Drawing.Font("Microsoft
Sans Serif", 9.75F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label11.Location = new System.Drawing.Point(351, 52);
            this.label11.Name = "label11";
            this.label11.Size = new System.Drawing.Size(59, 16);
```

```
            this.label11.TabIndex = 5;
            this.label11.Text = "label11";
            //
            // label10
            //
            this.label10.AutoSize = true;
            this.label10.Font = new System.Drawing.Font("Microsoft
Sans Serif", 9.75F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label10.Location = new System.Drawing.Point(351, 26);
            this.label10.Name = "label10";
            this.label10.Size = new System.Drawing.Size(59, 16);
            this.label10.TabIndex = 4;
            this.label10.Text = "label10";
            //
            // label9
            //
            this.label9.AutoSize = true;
            this.label9.Font = new System.Drawing.Font("Microsoft Sans
Serif", 12F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label9.Location = new System.Drawing.Point(34, 162);
            this.label9.Name = "label9";
            this.label9.Size = new System.Drawing.Size(333, 20);
            this.label9.TabIndex = 3;
            this.label9.Text = "Узагальнений показник кіберстійкості";
            //
            // label8
            //
            this.label8.AutoSize = true;
            this.label8.Font = new System.Drawing.Font("Microsoft Sans
Serif", 9.75F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label8.Location = new System.Drawing.Point(6, 52);
            this.label8.Name = "label8";
            this.label8.Size = new System.Drawing.Size(129, 16);
            this.label8.TabIndex = 2;
            this.label8.Text = "Кібернадійність ";
            //
            // label7
            //
            this.label7.AutoSize = true;
            this.label7.Font = new System.Drawing.Font("Microsoft Sans
Serif", 9.75F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label7.Location = new System.Drawing.Point(6, 81);
            this.label7.Name = "label7";
            this.label7.Size = new System.Drawing.Size(126, 16);
            this.label7.TabIndex = 1;
            this.label7.Text = "Кіберживучість ";
            //
            // label6
```

```
            //
            this.label6.AutoSize = true;
            this.label6.Font = new System.Drawing.Font("Microsoft Sans
Serif", 9.75F, System.Drawing.FontStyle.Bold,
System.Drawing.GraphicsUnit.Point, ((byte)(204)));
            this.label6.Location = new System.Drawing.Point(6, 26);
            this.label6.Name = "label6";
            this.label6.Size = new System.Drawing.Size(142, 16);
            this.label6.TabIndex = 0;
            this.label6.Text = "Кіберзахищеність ";
            //
            // button4
            //
            this.button4.Location = new System.Drawing.Point(252,
317);
            this.button4.Name = "button4";
            this.button4.Size = new System.Drawing.Size(146, 23);
            this.button4.TabIndex = 4;
            this.button4.Text = "Розрахувати ";
            this.button4.UseVisualStyleBackColor = true;
            this.button4.Click += new
System.EventHandler(this.button4_Click);
            //
            // button5
            //
            this.button5.Location = new System.Drawing.Point(22, 317);
            this.button5.Name = "button5";
            this.button5.Size = new System.Drawing.Size(146, 23);
            this.button5.TabIndex = 5;
            this.button5.Text = "Видалити всі дані";
            this.button5.UseVisualStyleBackColor = true;
            this.button5.Click += new
System.EventHandler(this.button5_Click);
            //
            // Form1
            //
            this.AutoScaleDimensions = new System.Drawing.SizeF(6F,
13F);
            this.AutoScaleMode =
System.Windows.Forms.AutoScaleMode.Font;
            this.ClientSize = new System.Drawing.Size(718, 373);
            this.Controls.Add(this.button5);
            this.Controls.Add(this.button4);
            this.Controls.Add(this.groupBox4);
            this.Controls.Add(this.groupBox3);
            this.Controls.Add(this.groupBox2);
            this.Controls.Add(this.groupBox1);
            this.FormBorderStyle =
System.Windows.Forms.FormBorderStyle.FixedDialog;
            this.Name = "Form1";
            this.Text = "Узагальнений показник кіберстійкості";
            this.Load += new System.EventHandler(this.Form1_Load);
```

```
            this.groupBox1.ResumeLayout(false);
            this.groupBox1.PerformLayout();
            this.groupBox2.ResumeLayout(false);
            this.groupBox2.PerformLayout();
            this.groupBox3.ResumeLayout(false);
            this.groupBox3.PerformLayout();
            this.groupBox4.ResumeLayout(false);
            this.groupBox4.PerformLayout();
            this.ResumeLayout(false);

        }

        #endregion

        private System.Windows.Forms.GroupBox groupBox1;
        private System.Windows.Forms.Button button1;
        private System.Windows.Forms.Label label2;
        private System.Windows.Forms.Label label1;
        private System.Windows.Forms.TextBox textBox2;
        private System.Windows.Forms.TextBox textBox1;
        private System.Windows.Forms.GroupBox groupBox2;
        private System.Windows.Forms.GroupBox groupBox3;
        private System.Windows.Forms.Label label5;
        private System.Windows.Forms.TextBox textBox3;
        private System.Windows.Forms.Label label4;
        private System.Windows.Forms.Label label3;
        private System.Windows.Forms.Button button3;
        private System.Windows.Forms.Button button2;
        private System.Windows.Forms.GroupBox groupBox4;
        private System.Windows.Forms.Label label13;
        private System.Windows.Forms.Label label12;
        private System.Windows.Forms.Label label11;
        private System.Windows.Forms.Label label10;
        private System.Windows.Forms.Label label9;
        private System.Windows.Forms.Label label8;
        private System.Windows.Forms.Label label7;
        private System.Windows.Forms.Label label6;
        private System.Windows.Forms.Button button4;
        private System.Windows.Forms.Button button5;
        private System.Windows.Forms.Button button6;
        private System.Windows.Forms.TextBox textBox4;
        private System.Windows.Forms.Label label14;
    }
}
```