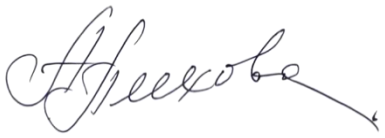
Міністерство освіти і науки України

Національний технічний університет

«Харківський політехнічний інститут»

ПЛЄХОВА ГАННА АНАТОЛІЇВНА



УДК 004.621.396.2.019.4

МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖЕВОЇ СИСТЕМИ, СТІЙКОЇ ДО ВПЛИВУ ДЕСТРУКТИВНИХ ФАКТОРІВ

Спеціальність 05.13.06 – інформаційні технології

Реферат дисертації на здобуття наукового ступеня

доктора технічних наук

Харків – 2026

Дисертацією є рукопис.
Роботу виконано на кафедрі інтелектуальних комп'ютерних систем Національного технічного університету «Харківський політехнічний інститут» та на кафедрі комп'ютерних наук і інформаційних систем Харківського національного автомобільно-дорожнього університету

Науковий консультант: доктор технічних наук, професор
Шаронова Наталія Валеріївна,
Національний технічний університет «Харківський політехнічний інститут», професор кафедри інтелектуальних комп'ютерних систем.

Опоненти:

доктор технічних наук, професор
Єрохін Андрій Леонідович,
Харківський національний університет радіоелектроніки, перший проректор;

доктор технічних наук, професор
Федорович Олег Євгенович,
Національний аерокосмічний університет «Харківський авіаційний інститут», завідувач кафедри комп'ютерних наук та інформаційних технологій, лауреат Державної премії України в галузі науки та техніки;

доктор фізико-математичних наук, професор, член-кореспондент НАН України (Інформатика),
Яковлев Сергій Всеволодович,
Заступник директора навчально-наукового Інституту комп'ютерних наук та штучного інтелекту Харківського національного університету ім. В.Н. Каразіна

Захист відбудеться «25» червня 2026 року о 14:00 годині на засіданні спеціалізованої вченої ради Д 64.050.20 в Національному технічному університеті «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Кирпичова, 2, Ректорський корпус (аудиторія 38).

З дисертацією можна ознайомитися у науково-технічній бібліотеці Національного технічного університету «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Кирпичова, 2. Посилання на захист: https://blogs.kpi.kharkov.ua/v2/vr/archives/7966

Про дату та місце захисту громадськість проінформовано «15» травня 2026 р.

Вчений секретар
спеціалізованої вченої ради Дмитро ОРЛОВСЬКИЙ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Особливий стан країни призвів до необхідності функціонування складних систем в умовах впливу негативних (агресивних) факторів зовнішнього середовища. Пошкодження об'єктів промисловості та критичної інфраструктури, які виникли за час військових дій, впливають на обороноздатність країни та погіршують соціальні умови населення. Особливо важливу роль відіграють інфокомунікаційні мережеві системи (ІМС), які забезпечують збір, передачу, розподілену обробку інформації для прийняття відповідальних рішень по управлінню економікою країни та плануванню оборонних дій.

Аналіз поняття стійкості складних систем показав, що під стійкістю складної системи розуміють здатність системи зберігати свою цілісність, структуру, функціональні властивості і стабільний стан при впливі зовнішніх і внутрішніх збурень. Існують суттєві фактори, які впливають на порушення стійкості ІМС:

- пошкодження інфраструктури ІМС;
- руйнування постачання енергії для роботи ІМС;
- порушення передачі даних;
- порушення контенту інформації, яка передається та обробляється в ІМС;
- викривлення програмного коду та втручання в систему ворожих сервісів та програм.

Проведений аналіз досліджень, за темою дисертації, показав відсутність методології, методів та моделей, які повною мірою відповідають вимогам сучасного стану країни, при створенні та модернізації ІМС, стійких до впливу деструктивних факторів зовнішнього середовища.

Тому, виникає проблемне питання щодо створення методологічних основ проєктування ІМС, яка може стійко функціонувати в умовах впливу загроз. Для вирішення цієї проблеми необхідно використовувати як вже існуючі рішення, які зарекомендували себе в мирний час, так і створювати нові, які відповідають сучасному стану країни. Необхідно сформувати системні основи методології, з використанням нових напрямків досліджень, для забезпечення розробників ІМС методологічною базою проєктування стійкої мережевої системи. Аналіз публікацій показав, що існує потреба у практичних методах розробки ІМС, які основані на сучасних методах та моделях.

Можливості використання системних методів і моделей оптимізації для потреб управління складними системами у мирний час досліджувались в працях багатьох вчених: В.М. Глушкова, О.Г. Івахненка, М.Д. Месаровича, М.З. Згуровського, М.Д. Годлевського, О.А. Павлова, Ю.П. Зайченка, Е.Г. Петрова, О.П. Алексієва, О.Є. Федоровича, Д.О. Новікова та багатьох інших. Основні наукові дослідження цих вчених пов'язані з синтезом складних систем. До них відносяться наукові праці в області системного аналізу, оптимізаційних задач та моделей імітаційного моделювання. Велика

увага приділяється розробці інформаційних технологій з використанням мережевих систем для розподіленого управління промисловими об'єктами, які базуються на концепціях: OPT, ERPII, MRPII, CSRP, DRPII, SCM. Однак мало уваги приділено самим системам управління та інфокомунікаційним мережам, які забезпечують передачу інформації для завдань оперативного управління. Також недостатньо приділено уваги методам, моделям та інформаційним технологіям розподіленого віртуального управління складними об'єктами (промисловість, критична інфраструктура, військові об'єкти, тощо) у сучасному хмарному інформаційному середовищі.

При формуванні архітектури ІМС, стійкої до впливу негативних факторів, пропонується використовувати сучасні підходи структурного синтезу, наприклад, компонентний підхід, який позитивно зарекомендував себе при розробці багаторівневих систем управління. Сучасне програмне забезпечення створюється за допомогою мультиагентного середовища, яке відкрито до включення нових агентів та сервісів. Для віртуалізації розподіленого управління, на даний час, використовуються хмарні технології (CLOUD), за рахунок яких формуються сховища даних для прийняття оперативних рішень. Дослідження по створенню інфокомунікаційних мережевих систем були проведені такими відомими вченими, як: Т.Б. Лі, К. Шенон, Д. Нейман, Л. Торвальдс, Н. Вінер, Д. Макарті, Д. Хінтон та ін. Вони показали можливості та ефективність використання таких систем в людській діяльності (управління складними системами, моніторинг зовнішнього середовища, медичні дослідження, тощо).

Все вищезазначене обумовлює актуальність науково-прикладної проблеми, яка спрямована на формування нової методології та розвитку існуючих методів та моделей, з використанням інформаційних технологій, що дозволить розробляти сучасні ІМС, стійкі до впливу деструктивних факторів зовнішнього середовища.

Зв'язок роботи з науковими програмами, планами, темами і грантами. Дисертаційна робота виконана на кафедрі комп'ютерних наук і інформаційних систем Харківського національного автомобільно-дорожнього університету та кафедрі інтелектуальних комп'ютерних систем Національного технічного університету «Харківський політехнічний інститут», відповідно до планів НДР, програм і договорів, які виконувалися на цих кафедрах. Здобувачка брала участь у впровадженні та імплементації наукових фундаментальних і прикладних результатів за темами: «Теорія інформаційного аналізу та синтезу розподілених телематичних транспортних систем» (ДР № 0113U000179); «Забезпечення конкурентоспроможності підприємств транспортної галузі України за рахунок підвищення ефективності віртуального управління процесами транспортного обслуговування» (ДР № 0116U004524); «Дослідження інноваційних підходів застосування інформаційних технологій в сфері цифровізації транспортних систем» (ДР № 0123U104192); «Комп'ютерні технології в вирішенні задач організації та управління на автомобільному транспорті» (ДР

№ 0122U201011).

Мета і завдання дослідження. Виявлено існуюче протиріччя між необхідністю здійснення розподілених управлінських дій, за допомогою інфокомунікаційної мережевої системи в умовах впливу деструктивних факторів зовнішнього середовища, та відсутністю методології, методів, моделей та інформаційних технологій, які мають забезпечити стійке функціонування мережевої системи в особливому стані країни, що дасть можливість успішного виконання завдань управління критичною інфраструктурою, промисловістю та об'єктами військового призначення.

Метою дисертаційного дослідження є створення методологічних основ, методів, моделей та інформаційної технології системного синтезу інфокомунікаційної мережі, стійкої до впливу деструктивних факторів.

Мета досягається постановкою та вирішенням комплексу наступних взаємопов'язаних задач.

1. Аналіз існуючих методів та стану вирішення проблем, які є в дослідженнях по створенню ІМС.
2. Формування методологічних основ створення ІМС, стійкої до впливу деструктивних факторів.
3. Розроблення методу та моделі архітектурного синтезу ІМС для розподіленого управління складними об'єктами та системами.
4. Моделювання превентивних заходів щодо забезпечення стійкості мережевої системи від можливих агресивних дій.
5. Створення моделі відновлення стану ІМС через вплив негативних факторів.
6. Розроблення методів стійкої маршрутизації передачі даних в мережевій системі в умовах загроз.
7. Створення прикладної інформаційної технології забезпечення стійкості ІМС.
8. Впровадження результатів наукових досліджень в практику проєктування ІМС, стійкої до впливу деструктивних факторів.

*Об'єкт дослідження***:** процес створення інфокомунікаційної мережевої системи в умовах сучасного стану країни.

*Предмет дослідження***:** методологія, методи, моделі та прикладна інформаційна технологія створення інфокомунікаційної мережевої системи, стійкої до впливу деструктивних факторів.

Методи дослідження. В основу дисертаційного дослідження покладено методи системного аналізу; багатоваріантного аналізу; теорії стійкості; методи оптимізації, зокрема багатокритеріальної оптимізації; методи штучного інтелекту; методи теорії інтелекту, зокрема метод компараторної ідентифікації; методи машинного навчання; методи та моделі маршрутизації; методи кіберзахисту.

Методи дослідження базуються на новій парадигмі щодо створення стійкої ІМС, системних концептуальних принципах синтезу, оптимізаційних методах, моделях та імітаційному моделюванні стійкості мережевої системи в умовах загроз. Прикладна інформаційна технологія створена на основі методів

інтелектуального управління та використовує віртуалізацію і хмарні (CLOUD) обчислення, мультиагентне середовище, що дозволяє створювати розподілене віртуальне управління об'єктами критичної інфраструктури, промисловими та військовими об'єктами. Це дозволяє сформувати стійке управління складними економічними системами та забезпечує підвищення обороноздатності країни.

Наукова новизна одержаних результатів. Основний науковий результат полягає в формуванні методологічних основ створення ІМС, яка відповідає сучасній парадигмі стійкості, має науково обґрунтований комплекс нових та оригінальних методів і моделей проєктування розподіленої мережевої системи управління, які лягли в основу розроблення прикладної інформаційної технології синтезу мережевої системи, стійкої до впливу деструктивних факторів.

Наукова новизна визначається наступними положеннями.

1. *Вперше* розроблені методологічні основи створення ІМС, стійкої до впливу деструктивних факторів зовнішнього середовища, які, на відміну від існуючих, засновані на аналізі та урахуванні дій агресивного характеру на ІМС, шляхом використання оригінальних та нових методів, моделей інтелектуалізації, оптимізації, імітаційного моделювання, інформаційної технології на мультиагентній платформі, що дозволило науково обґрунтувати створення та функціонування розподіленої мережевої системи в умовах особливого стану країни.

2. Вперше розроблено метод синтезу архітектури ІМС, стійкої до впливу факторів зовнішнього середовища, який, на відміну від існуючих, заснований на представленні складу системи за допомогою уніфікованих компонент (існуючих, модернізованих, інноваційних), які мають підвищені характеристики стійкості, що дозволило забезпечити підвищення загальної стійкості системи.

3. Вперше розроблено модель планування множини превентивних заходів для зменшення впливу вразливостей на ІМС, яка, на відміну від існуючих, дозволяє виявити підмножину актуальних вразливих компонент відносно планування проєкту підвищення стійкості системи.

4. Вперше розроблено метод протидії кібератакам противника, який базується на використані штучної імунної системи, що дозволяє підвищити точність і забезпечити оперативність прийняття рішень щодо нейтралізації та зменшення впливу кіберзагроз на початковому етапі розвитку кібератаки, що сприяє підвищенню стійкості ІМС від атак противника.

5. Вперше розроблено метод відновлення ІМС, який, на відміну від існуючих, ураховує різний рівень деградації окремих компонент, що дозволяє планувати дії для підвищення стійкості системи у цілому, шляхом вибору раціонального варіанту превентивних заходів при проведенні оновлення системи.

6. Отримав подальший розвиток топологічний синтез складної розподіленої ІМС, заснований на комбінаторному формуванні потрібної структури системи, зі складом різних топологій окремих мереж, що дозволило обґрунтувати загальну топологію архітектури системи, спроможної до

стійкого управління розподіленими об’єктами в умовах впливу деструктивних факторів зовнішнього середовища.

7. Отримав подальший розвиток метод вибору раціональної множини превентивних захисних заходів від атак противника на інфраструктуру ІМС, з використанням цілочисельного булевого програмування, що сприяє підвищенню її стійкості.

8. Отримав подальший розвиток метод управління станом ІМС за допомогою багатошарової нейронної мережі, який дозволяє оперативно реагувати на наявність деградації системи, а далі управляти діями щодо її покращення.

9. Отримав подальший розвиток метод пошуку раціональних маршрутів передачі даних в мережевій системі, на основі мультиагентного імітаційного моделювання, який дозволяє здійснювати пошук відносно безпечних маршрутів передачі даних в умовах впливу загроз.

10. Удосконалено метод розпізнавання стану ІМС, заснований на використанні когнітивної моделі, яка ураховує вплив негативних факторів у різних формах представлення, що сприяє забезпеченню достовірності та підвищенню точності ідентифікації стану мережевої системи.

11. Удосконалено метод управління передачею даних в мережевій системі, за рахунок подальшого розвитку алгоритму руху тварин у природі, шляхом використання машинного навчання для адаптивного управління рухом, що дозволяє оперативно реагувати на зміну умов передачі даних в ІМС.

12. Удосконалено інформаційну технологію розробки ІМС шляхом використання парадигми створення стійкої мережевої системи та методологічних засобів у вигляді комплексу методів та моделей, реалізованих за допомогою розроблених програмних компонент в мультиагентній платформи, що дозволяє створити стійку систему, в умовах впливу деструктивних факторів.

Практичне значення одержаних результатів для розвитку системних основ проєктування стійкої ІМС полягає у наступному: розроблені методи та моделі планування дій по створенню стійкої мережевої системи, відновлення її стану, забезпечення стійкості передачі даних, кіберзахисту від атак противника, дозволяють оптимізувати час, витрати та ураховувати ризики створення системи в умовах особливого стану країни. Комплекс методів та моделей реалізований у вигляді прикладної інформаційної технології створення стійкої до загроз ІМС. Отримані результати дозволяють підвищити ефективність управління в критичних сферах використання в умовах існуючих загроз. Основні положення дисертації доведено до практичної реалізації у вигляді: комплексу алгоритмів і програмно-апаратних рішень; захищених патентами; інструментальних засобів планування превентивних заходів щодо забезпечення стійкості ІМС. Розроблені інструментальні засоби та алгоритми утворюють прикладну інформаційну технологію, яка забезпечує стійкість мережевої системи в умовах особливого стану країни.

Результати досліджень знайшли відображення при виконанні науково-дослідних робіт, які виконувалися у Харківському національному

автомобільно-дорожньому університеті: «Розробка інтелектуальних інформаційно-керуючих технологій для дизельного двигуна у сукупності з силовою передачею: параметричний синтез системи паливоподавання», 2018р., замовник Інститут проблем машинобудування ім. А.М. Підгорного Національної академії наук України (Державний фонд фундаментальних досліджень України), (№ДР0118U007010); «Проведення випробувань програмних модулів для аналізу динаміки та міцності корпусних композитних елементів з наноармуванням», 2020р., замовник Інститут проблем машинобудування ім. А.М. Підгорного Національної академії наук України (Державне замовлення на найважливіші науково-технічні розробки), №ДР0120U102963; «Розроблення методів і засобів підвищення довговічності та енергоефективності двигунів для броньованої техніки на основі конвергенції технологій», 2020-2021рр.; у держбюджетних науково-технічних проєктах МОН України, (№ДР0119U001298), та «Розробка інтелектуальних технологій підвищення довговічності та енергоефективності мехатронних систем для броньованої техніки», 2022-2023рр. У 2024 р. укладено договір про співпрацю (підписаний 8.01.2024р.) з польським Сілезьким технологічним університетом та кафедрою комп'ютерних систем ХНАДУ про співпрацю та викладання профільних дисциплін у Сілезькій політехніці згідно з контрактом (Umowa zlecenie nr UMC/1451/2024 do wniosku nr 1437/UMC/ROZ2/2024), де здобувачка брала участь як виконавець.

Отримані практичні результати дозволили підвищити ефективність та стійкість управління автомобільними перевезеннями, розробити віртуальний розподілений скринінг медичних карт військових в умовах особливого стану країни; сформувати раціональні шляхи перевезень в умовах загроз. Результати дисертаційного дослідження впроваджені в: ПАТ АТП16364 (м. Харків), ТОВ «Експрес» (м. Харків), ТОВ «Стоматологія «МІГ», компанію «ХІМПОСТАЧАННЯ» (м. Харків), що підтверджується актами впровадження наукових результатів.

Результати наукових досліджень впроваджені у навчальний процес Харківського національного автомобільно-дорожнього університету при викладанні курсів «Комп'ютерні мережі» та «Математичне моделювання та оптимізація комп'ютерних систем»; Національного технічного університету «Харківський політехнічний інститут» на кафедрі інтелектуальних комп'ютерних систем при викладанні навчальної дисципліни «Інформаційно-ресурсне забезпечення».

Особистий внесок здобувача. Всі наукові результати дисертаційного дослідження, які подані до захисту, отримано автором самостійно. Серед них: 1) формування методологічних основ створення стійкої інфокомунікаційної мережі; 2) розробка компонентної архітектури мережевої системи, стійкої до впливу деструктивних факторів; 3) топологічний синтез структури розподіленої мережевої системи; 4) моделювання вразливостей інфокомунікаційної мережевої системи; 5) моделювання превентивних заходів щодо підвищення стійкості інфокомунікаційної мережевої системи; 6) моделювання стійкості передачі даних в мережевій системі;

7) моделювання захисту мережевої системи від кібератак; 8) метод ідентифікації стану системи на основі когнітивного моделювання; 9) моделювання управління станом інфокомунікаційної мережевої системи з метою її відновлення; 10) метод пошуку раціональних маршрутів передачі даних з використанням імітаційного моделювання; 11) метод інтелектуального управління передачею даних; 12) прикладна інформаційна технологія створення стійкої мережевої системи з використанням мультиагентного середовища.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідалися й обговорювалися на міжнародних науково-практичних конференціях: The 10th International Conference «Mechanical Technologies and Structural Materials 2021» (Split, Croatia, 2021); The XXIII International Scientific and Practical Conference «Theoretical and science bases of actual tasks» (Lisbon, Portugal, 2022); Восьма Міжнародна науково-технічна конференція «Проблеми електромагнітної сумісності перспективних безпровідних мереж зв'язку (ЕМС-2022)» (Харків, 2022); The II International Scientific and Practical Conference «General regularities and models of science development» (Zagreb, Croatia, 2023); The IV International Scientific and Practical Conference «Science and technology: problems, prospects and innovations» (Osaka, Japan, 2023); The IV International Scientific and Practical Conference «Scientific knowledge, aesthetic creativity and social practices» (Athens, Greece, 2023); The 5th International scientific and practical conference «Science and innovation of modern world» (London, 2023); The 4th International scientific and practical conference «Actual problems of modern science» (Boston, 2023); II Міжнародна науково-методична конференція «Вища освіта за новими стандартами: виклики у контексті діджиталізації та інтеграції в міжнародний освітній простір» (Харків, 2023); The 5th International scientific and practical conference «Modern research in science and education» (Chicago, 2024); The 5th International scientific and practical conference «Current challenges of science and education» (Berlin, 2024); The 4th International scientific and practical conference «Innovative development of science, technology and education» (Vancouver, 2024); The 5th International scientific and practical conference «Topical aspects of modern scientific research» (Tokyo, 2024); The 6th International scientific and practical conference «Global science: prospects and innovations» (Liverpool, 2024); Міжнародна науково-практична конференція «Енергетичні установки та альтернативні джерела енергії» (Харків, 2024); XII Міжнародна науково-практична конференція «Інформаційні управляючі системи і технології» (Одеса, 2024); The 10th International Interdisciplinary Scientific Conference «Social Development Towards Values Ethics – Technology – Society» (Wisla, Poland, 2024); Міжнародна наукова конференція «Математичне моделювання та інформаційні технології сучасності» (Харків, 2024); The 13th International conference «Mechanical Technologies and Structural Materials» (Split, Croatia, 2024); Міжнародна наукова конференція «Процеси цифровізації екосистем» (Харків, 2024); The 6th International scientific and practical conference «Scientific achievements of contemporary society» (London, 2025); The 6th International scientific and practical

conference «Current trends in scientific research development» (Boston, 2025); The 5th International scientific and practical conference «Science in the modern world: innovations and challenges» (Toronto, 2025); The 6th International scientific and practical conference «Science and technology: challenges, prospects and innovations» (Osaka, 2025); The 12th International scientific and practical conference «Modern management of organizations: concepts and digital transformations» (Varna, 2025); The 11th International Interdisciplinary Scientific Conference «Social Development Towards Values Ethics – Technology – Society» (Wisla, Poland, 2025).

Публікації. Результати дисертації опубліковані в 64 наукових працях, з них: 17 статей у наукових фахових виданнях України (7 статей входять в базу даних Scopus); 28 праць – матеріали міжнародних конференцій, 6 розділів колективних монографій, 5 патентів на корисну модель.

Структура та обсяг роботи. Дисертаційна робота складається з анотації двома мовами, вступу, семи розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи викладено на 290 сторінках, серед них 14 рисунків по тексту, 3 рисунки на окремих сторінках, 2 таблиці на 2 окремих сторінках, 8 таблиць по тексту, список використаних джерел зі 229 найменувань на 32 сторінках та 2 додатків на 24 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертаційного дослідження, наведено зв'язок роботи з науковими програмами, планами, темами. Сформульовано науково-прикладну проблему, яка вирішується, мету та завдання, об'єкт, предмет і методи дослідження. Представлено наукову новизну і практичне значення результатів. Подано інформацію щодо апробації та публікації результатів, особистого внеску автора. Представлено характеристику структури та обсяг дисертаційної роботи.

Перший розділ присвячено огляду стану наукових досліджень, постановці завдань дослідження. Здійснено огляд публікацій щодо існуючих методологій розробки інфокомунікаційних мережевих систем (ІМС). Зроблено аналіз існуючих методів, моделей та інформаційних технологій для проєктування сучасних ІМС. На основі проведеного аналізу виділено проблему створення ІМС, стійкої до впливу деструктивних факторів.

У **другому розділі** сформовані методологічні основи створення ІМС, стійкої до впливу деструктивних факторів. Методологічні основи використовують нову парадигму стійкості мережевої системи. Парадигма розкрита через такі концептуальні принципи:

- системність створення;
- архітектурна стійкість;
- інтелектуальне управління стійкістю;
- превентивні протидії;
- кібернетична безпека;

– оперативне відновлення;
– стійка маршрутизація.

Концептуальні принципи дозволили розробити методи та моделі, які сформували математичний інструментарій методології. Комплекс методів та моделей є основою для розробки прикладної інформаційної технології створення стійкої ІМС. При виборі та розробці математичного інструментарію було проведено подальший розвиток та удосконалення існуючих методів, моделей і створені нові. Використано такі методи та моделі: системний аналіз щодо проведення дій по створенню стійкої ІМС; сучасні методи оптимізації; методи експертного оцінювання, з використанням якісних і кількісних метрик; багатокритеріальна оптимізація; метод пошуку раціональних варіантів; методи та моделі штучного інтелекту для аналізу стану ІМС та управління передачею даних; імітаційне моделювання для пошуку раціональних маршрутів передачі даних у мережевій системі. Було сформоване мультиагентне середовище для програмного забезпечення розробки стійкої ІМС. На рис. 1 представлена структурна схема методології з рівнями:

– парадигма стійкої ІМС;
– концептуальні принципи створення;
– методи та моделі;
– мультиагентне середовище.

Сформовані системні основи методології синтезу стійкої ІМС є необхідними для проведення подальших проєктних дій для розробки сучасної стійкої мережевої системи. У цьому розділі представлено методи інтелектуального управління для прийняття раціональних рішень у процесах створення стійкої ІМС. Таким чином, у розділі закладені методологічні основи створення стійкої ІМС, які у подальшому розкрито в наступних розділах у вигляді створеного комплексу нових та оригінальних математичних методів, моделей та прикладної інформаційної технології.

Третій розділ присвячено створенню сучасної архітектури ІМС, яка дозволяє забезпечити стійкість функціонування системи. Моделюються та плануються заходи щодо забезпечення стійкості, які потребують часу, витрат та мають ризики виконання проєкту. Обмежені можливості, які виникли в сучасному стані країни, не дають у повній мірі забезпечити ресурсами створення стійкої ІМС, що було враховано у вигляді обмежень в розроблених методах та моделях. Запропоновано сформовану сучасну компонентну архітектуру ІМС, яка орієнтована на стійкість функціонування системи, в умовах мінливого зовнішнього середовища. Така архітектура дозволяє швидко заміняти пошкоджені або деградовані компоненти системи, та оперативно реагує на зміну умов функціонування. Виділені типи компонент (існуючі, з підвищеними характеристиками стійкості; компоненти, які суттєво модернізуються; нові, інноваційні компоненти). Склад компонент ІМС формується шляхом пошуку раціонального варіанту з множини можливих.

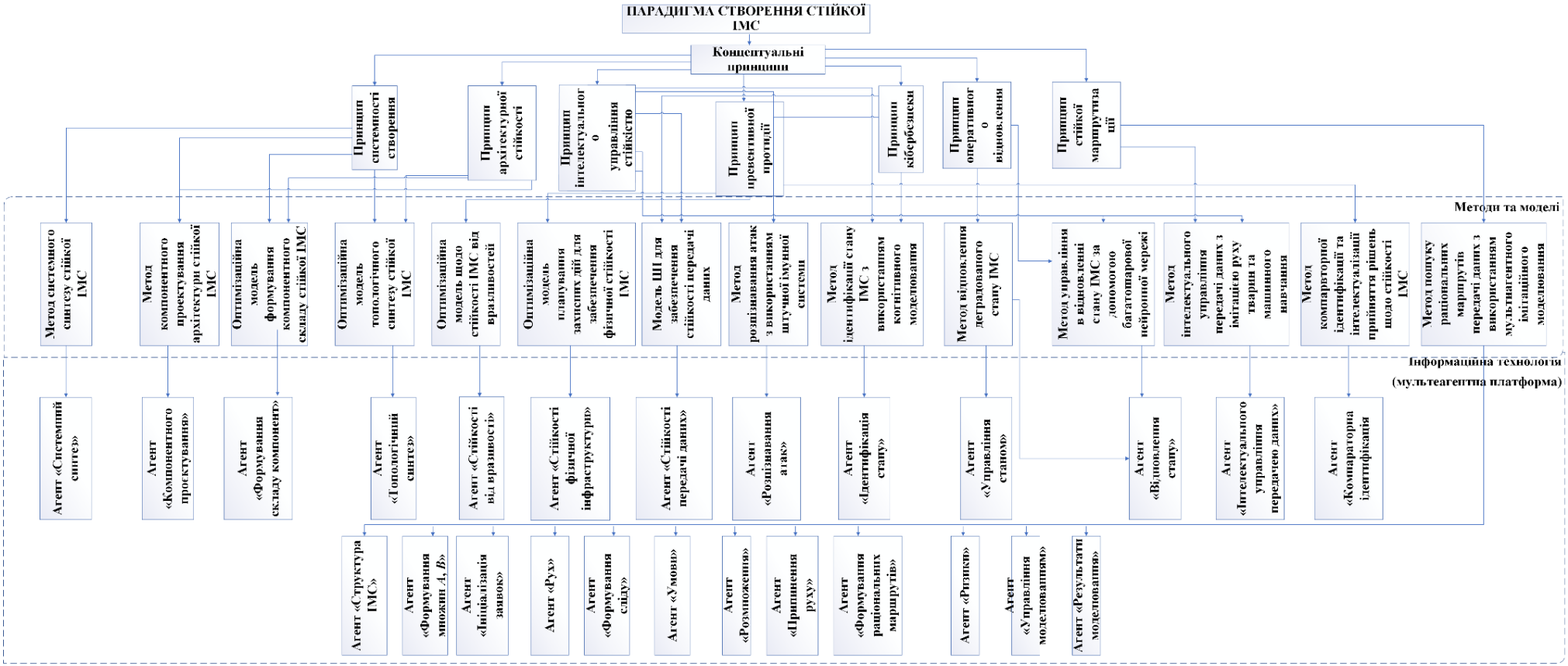


Рис. 1 – Структура методології

Запропоновано оптимізаційну модель, яка дозволяє проводити пошук раціонального варіанту, з використанням показників: стійкості ІМС (*F*); часу, потрібного для виконання проєкту для забезпечення стійкості (*T*), витрат проєкту (*W*), ризиків виконання проєкту (*R*). Проведена локальна оптимізація окремих показників. Наприклад, для мінімізації витрат проєкту необхідно:

$$\min W, \quad W = \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot W_{jk} \cdot x_{jk} \tag{1}$$

з обмеженнями:

$$\begin{aligned} F \geq F', F = \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot F_{jk} \cdot x_{jk}, \\ T \leq T', T = \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot T_{jk} \cdot x_{jk}, \\ R \leq R', R = \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot R_{jk} \cdot x_{jk}, \end{aligned} \tag{2}$$

де N – кількість альтернативних варіантів компонентного складу ІМС; n_j – кількість варіантів вибору j-ї компоненти; F_{jk}, T_{jk}, R_{jk} – оцінки показників (F, T, R) для j-ї компоненти; x_{jk} – булева змінна.

Проведено багатокритеріальну оптимізацію для пошуку раціонального компонентного складу ІМС з використанням суперечливих показників (W, F, T, R). Це необхідно для забезпечення стійкості ІМС в умовах обмежених можливостей. Пронормовані показники (приведені до інтервалу зміни значень (0÷1)):

$$\hat{F} = \frac{F^* - F}{F^* - F'}, \ \hat{T} = \frac{T - T^*}{T' - T^*}, \ \hat{W} = \frac{W - W^*}{W' - W^*}, \ \hat{R} = \frac{R - R^*}{R' - R^*}, \tag{3}$$

де F^*, T^*, W^*, R^* - екстремальні значення показників, які отримані після вирішення задачі з їх оптимізації. Далі, визначено важливість показників (α_F, α_T, α_W, α_R) щодо виконання проєкту для забезпечення стійкості ІМС:

$$\alpha_F + \alpha_T + \alpha_W + \alpha_T = 1. \tag{4}$$

Сформовано комплексний показник:

$$
\begin{aligned}
Q &= \alpha_F \cdot \hat{F} + \alpha_T \cdot \hat{T} + \alpha_W \cdot \hat{W} + \alpha_R \cdot \hat{R} = \\
&= -\frac{\alpha_F}{F^* - F'} \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot F_{jk} \cdot x_{jk} + \frac{\alpha_T}{T' - T^*} \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot T_{jk} \cdot x_{jk} + \\
&+ \frac{\alpha_W}{W' - W^*} \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot W_{jk} \cdot x_{jk} + \frac{\alpha_R}{R' - R^*} \sum_{j=1}^{N} \sum_{k=1}^{3} n_j \cdot R_{jk} \cdot x_{jk} + \\
&+ \frac{\alpha_F F^*}{F^* - F'} - \frac{\alpha_T T^*}{T' - T^*} - \frac{\alpha_W W^*}{W' - W^*} - \frac{\alpha_R R^*}{R' - R^*}.
\end{aligned}
\tag{5}
$$

Необхідно знайти min Q, з виконанням обмежень:

$$
F \geq F', T \leq T', R \leq R' \tag{6}
$$

Далі, проведено топологічний синтез ІМС для формування архітектури стійкої мережевої системи. Урахована множина топологічних рішень, які можуть бути використані в окремих фрагментах мережевої системи (лінійна, кільцева, радіальна, матрична, тощо). Поставлено та вирішене завдання щодо пошуку раціонального варіанту архітектури при топологічному синтезі ІМС.

Розглянуто приклад забезпечення стійкості ІМС (F) шляхом вибору раціонального складу топології окремих мережевих систем, які входять в загальну архітектуру. Використані показники: час (T), вартість (W), ризики(R). Необхідно підвищити стійкість ІМС:

$$
\max F, F = \sum_{i=1}^{M} \sum_{e=1}^{m_i} f_{ie} \cdot x_{ie}, \tag{7}
$$

з урахуванням обмежень:

$$
\begin{aligned}
T \leq T', T &= \sum_{i=1}^{M} \sum_{e=1}^{m_i} t_{ie} \cdot x_{ie}, \\
W \leq W', W &= \sum_{i=1}^{M} \sum_{e=1}^{m_i} w_{ie} \cdot x_{ie}, \\
R \leq R', R &= \sum_{i=1}^{M} \sum_{e=1}^{m_i} r_{ie} \cdot x_{ie},
\end{aligned}
\tag{8}
$$

де $f_{ie,}\ t_{ie,} w_{ie},\ r_{ie}$ – значення показників стійкості, часу, вартості та ризиків окремих мережевих систем, які входять в загальну топологічну структуру ІМС; M – кількість окремих мережевих систем в розподіленій ІМС; m_i -кількість можливих варіантів i-ої мережі; x_{ie} – булева змінна, T', W', R' – допустимі значення показників.

У розділі увагу приділено впливу вразливостей на функціонування ІМС. Плануються превентивні заходи для мінімізації (нейтралізації) вразливостей шляхом вибору підмножини найбільших критичних вразливостей з множини можливих. Обмеженість ресурсів не дозволяє створити захист всієї множини вразливостей (S) в ІМС. Тому виникає актуальне завдання пошуку підмножини (S_e), яка задовольняє обмеженням по часу, вартості та ризикам формування захисту. Використання теорії перерахування варіантів (основні теореми Поя, де Брейна) дозволяє, шляхом відображення всіх елементів множини (S) в множину складу підмножин: S_1, S_2,…,S_N (де S_1 – підмножина з однією вразливістю, S_2 – з двома вразливостями S_N – з N вразливостями) сформувати всі варіанти можливих підмножин (S_e). Для перерахування варіантів використовуються два етапи:

1. підрахування кількості можливих варіантів створення підмножин (S_e);
2. генерування (формування) всіх варіантів підмножин (S_e).

Розглянемо приклад перерахування всіх можливих підмножин вразливостей (S_e) із загальної множини ($S=4$).

Використовуючи результати теорії перерахування, обчислимо кількість можливих варіантів підмножин (S_e) у вигляді (окремий випадок теорії перерахувань):

$$K = 2^S - 1 = 15, \tag{9}$$

За допомогою двійкового лічильника можна сформувати усі варіанти підмножин критичних вразливостей:

1. 0001	6. 0110	11. 1011
2. 0010	7. 0111	12. 1100
3. 0011	8. 1000	13. 1101
4. 0100	9. 1001	14. 1110
5. 0101	10. 1010	15. 1111,

де, наприклад, 10 варіант є підмножина з першою та третьою критичними вразливостями, а 15 варіант включає всю множину вразливостей.

З використанням цілочисельного (булевого) програмування проводиться вибір раціонального варіанту щодо планування превентивних дій для мінімізації (нейтралізації) впливу критичних вразливостей на функціонування ІМС. Тут значення булевої змінної пов’язано з вибором підмножини вразливостей (S_e) із множини всіх варіантів.

Таким чином, в даному розділі було розроблено:

- метод компонентного проєктування архітектури стійкої ІМС;
- оптимізаційна модель формування раціонального складу ІМС;
- модель топологічного синтезу структури ІМС;
- оптимізаційна модель для зменшення впливу вразливостей на

функціонування ІМС.

Четвертий розділ дисертації присвячено моделюванню протидій від атак на ІМС. Атаки призводять до: знищення критичних компонент мережевої системи; порушення передачі даних; кіберзагроз щодо сервісу управління; порушення програмного коду; спотворення інформації. Виходячи з цього, актуальним є проведення досліджень щодо створення протидій, які розглядаються та вирішуються шляхом: моделювання превентивних заходів; моделювання протидій щодо порушення передачі даних; моделювання захисту мережевої системи від кібератак.

Введено показники стійкості (*S*), часу проведення превентивних заходів (*T*), витрат на превентивні дії (*W*) та ризики проєкту (*R)*.

Для моделювання превентивних заходів використаний лексико-графічний метод упорядковування варіантів, з урахуванням як кількісних, так і якісних показників. Наприклад, для показника стійкості (*S*) була використана якісна метрика:

$$S = \begin{cases} A - \text{ висока стійкість;} \\ B - \text{ задовільна стійкість;} \\ C - \text{ низька стійкість.} \end{cases} \quad (10)$$

Упорядковані показники за їх важливістю (*S, T, R, W),* вказано на напрям зміни значень показників щодо їх покращення:

$$S\uparrow,\ T\downarrow,\ R\downarrow,\ W\downarrow. \quad (11)$$

Сформована множина можливих варіантів проведення превентивних заходів. Наприклад, (ураховані кількісні та якісні оцінки показників):

1. C, 6, R, 40 6. B, 5, O, 50 11. B, 10, O, 80
2. C, 3, R, 30 7. A, 11, R, 90 12. C, 3, R, 30
3. B, 9, R, 70 8. C, 1, O, 10 13. B, 9, O, 70
4. C, 2, O, 20 9. B, 7, O, 50 14. B, 6, O, 60
5. B, 8, O, 60 10. B, 4, O, 40 15. A, 12, G, 100

Після проведення лексикографічного упорядкування варіантів маємо:

15. A,12,G,100 9. B,7,O,50 8. C,1,O,10
7. A,11,R,90 5. B,8,O,60 4. C,2,O,20
10. B,4,O,40 3. B,9,O,70 2. C,3,O,30
6. B,5,O,50 13. B,9,O,70 12. C,3,R,30
14. B,6,O,60 11. B,10,O,80 1. C,6,R,40

Враховуючи обмеження щодо ресурсу проєкту проведення

превентивних заходів (по часу та витратам), сформована наступна множина варіантів:

10. $B,4,O,40$
6. $B,5,O,50$
8. $C,1,O,10$
4. $C,2,O,20$
2. $C,3,O,30$
12. $C,3,R,30$

Обрано варіант у голові списку, який є найкращим для використання у проєкті проведення превентивних заходів щодо забезпечення стійкості ІМС. Якщо кількість варіантів проведення превентивних заходів дуже велика, використовується метод цілочисельного (булевого) програмування.

Далі, проведено дослідження щодо ідентифікації кібератак на мережеву систему, з використанням методів ШІ. Модель створено за допомогою множини штучних імунних детекторів, представлених у вигляді часових детекторів і детекторів пам'яті, з алгоритмом їх навчання та використанням стратегії генетичної оптимізації, яка включає використання генетичних операторів (кросоверу, мутації, інверсії) та їх комбінацій, для зміни параметрів імунного детектора після його клонування.

Виявлення деструктивного впливу на ІМС здійснюється наступним чином.

1. Визначення коригувального коефіцієнту на ступінь інформованості про величину та засоби деструктивного впливу на ІМС.

2. Обчислення для кожного імунного детектора $d \in D$ значення його активації $a_d = \Psi(d,s) - threshold$. Вважається, що якщо $a_d \geq 0$, то детектор d є активованим, інакше відповідний детектор не реагує на вхідний об'єкт.

3. Мажоритарне голосування всередині кожного класу детекторів. Якщо $D_{\varsigma(C)}, \underbrace{\sum_{d \in D_{\varsigma(C)}} [a_d \geq 0]}_{A_c} > \underbrace{\sum_{d \in D_{\varsigma(C)}} [a_d < 0]}_{B_c = \# D_{\varsigma(C)} - A_c}$, то s розпізнається як «чужий» об'єкт. Якщо, $A_C<B_C$, то s розпізнається як «свій» об'єкт. В разі наявності конфліктів, тобто $A_C=B_C$, s класифікується як «чужий» об'єкт, якщо $a_{d_m^{(C)}} \geq 0$, то s класифікується як «свій» об'єкт, якщо $a_{d_m^{(C)}} < 0$, де $d_m^{(C)} \in D_M \bigcap D_{\varsigma(C)}$, $d_m^{(C)}$ – детектор пам'яті, навчений для розпізнавання «свого» об'єкту та «чужого» об'єкту з класу C.

4. Формування множини класів імунних детекторів, що активувалися $\left\{D_{\varsigma(C')}\right\}_{C' \in c}$, які розпізнають вхідний об'єкт s як «чужий» об'єкт, де

$$C^* = \left\{ C' \middle| C' \in c \wedge \left(A_{C'} > B_{C'} \vee \left(A_{C'} = B_{C'} \wedge a_{d_m^{(C')}} \geq 0 \right) \right) \right\} \subset c .$$

5. Визначення класу об'єкта *s*. Якщо $C^* = \varnothing$, то об'єкт *s* належить до класу «своїх» об'єктів. Якщо E_{c^*} $\max_{C' \in c^*} A_{C'}$ досягається в одній єдиній точці, то клас об'єкта $\arg E_{C'}$, інакше клас об'єкта *s* – це $\arg \max_{C' \in \{\arg E_{c^*}\}} \sum_{d \in D_\varsigma(C')} \times [a_d \geq 0]$.

Якщо імунний детектор розпізнав деструктивний вплив на ІМС, його термін життя збільшується. На відміну від них, детектори пам'яті мають нескінченний термін життя та не беруть участі в наповненні оновлюваного набору детекторів.

Для виявлення кожного класу деструктивного впливу $c \in C$ виділяється кілька імунних детекторів, що об'єднуються в клас детекторів $D_{\varsigma(C)}$, $\left(\bigcup_{c \in C} D_{\varsigma(C)} = D \right)$. Кожен із детекторів $d \in D$ використовує глибоке навчання.

Використання методів машинного навчання для виявлення деструктивного впливу на ІМС дозволило проаналізувати кількість невиявлених впливів. Проведено порівняння існуючих імунних систем (*M*1, *M*2, *M*3) з розробленою *M*4 (табл. 1). Результати порівняльного аналізу, що наведені в табл. 1, дозволяють зробити висновок про перевагу зазначеної моделі, у порівнянні з відомими.

Таблиця 1 – Порівняння імунних систем

Імунна модель	Незалежність від внутрішньої структури імунного детектору	Наявність клональної селекції та генетичної оптимізації	Наявність негативного відбору	Врахування типу невизначеності РЕО	Автоматичний підбір порога активації імунного детектора	Наявність механізмів навчання	Наявність детекторів пам'яті	Наявність життєвого циклу лімфоцитів	Динамічне перенавчання	Навчання детекторів на нових даних в процесі функціонування	Розподіл імунних детекторів	Підтримка мультикласового виявлення деструктивного впливу на СРЗ	Автономність імунної системи (робота без втручання оператора)	Наявність сукупності процедур обробки різнорідних даних
M_1	–	–	+	–	–	–	+	+	+	+	–	–	–	–
M_2	–	+	+	–	–	–	+	–	+	+	+	–	–	–
M_3	+	+	+	–	+	+	+	+	+	+	–	–	+	–
M_4	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Далі, у роботі розроблено метод протидії кібератакам з використанням штучної імунної системи, який складається з наступної послідовності дій.

1. *Введення вихідних даних.* На даному етапі вводяться вихідні дані інфокомунікаційної мережі.

2. *Верифікація параметрів інфокомунікаційної мережі*.

3. *Виявлення агресивних факторів в атаці противника, які впливають на інфокомунікаційну мережу*. Відбувається первинна ідентифікація атак.

4. *Ініціація штучної імунної системи.* Створюється популяція з N антитіл кандидатів.

5. *Попередній відбір антитіл.* На даному етапі здійснюється початковий відбір антитіл в кожному рої.

6. *Розподіл агентів штучної імунної системи між роями.*

7. *Клонування антитіл.* Аналізується кількість клонів, що створюються з одного батьківського антитіла.

8. *Мутація антитіл.* Антитіла елітного рою проходять самонавчальну мутацію.

9. *Машинне навчання штучної імунної системи.* Механізм навчання штучної імунної системи зв'язаний з використанням методу «рулетки» для вибору антитіл елітного рою для навчання.

10. *Пригнічення антитіл*. Запропонована штучна імунна система використовує динамічний механізм пригнічення.

11. *Оновлення рою.* Під час оновлення рою всі антитіла сортуються в порядку спадання.

12. *Оцінка необхідних обчислювальних ресурсів інтелектуальної системи підтримки прийняття рішень*.

Додатково визначається завантаженість системи. При перевищенні заданого порогу обчислювальної складності, визначається необхідна множина програмно-апаратних ресурсів. Для визначення ефективності запропонованого методу проведено моделювання його роботи для виявлення кіберзагроз, які впливають на функціонування мережевої системи.

Проведена оцінка ефективності розробленого алгоритму. Зроблено висновок, що запропонований метод гарантує підвищення точності в середньому на 16%, підвищення оперативності в середньому на 12%, що забезпечує високу збіжність отриманих результатів 95,23%.

Таким чином, у даному розділі було поставлено та вирішено актуальне завдання щодо проведення комплексу протидій атакуючим діям противника на інфокомунікаційну мережеву систему.

Створені наступні моделі та метод:

– оптимізаційна модель планування захисних дій, для забезпечення стійкості інфраструктури ІМС від атак противника в умовах обмежених можливостей;

– штучна інтелектуальна модель забезпечення стійкості передачі даних по магістралям ІМС в умовах виникнення кіберзагроз противника;

– метод, заснований на використанні штучної імунної системи для ідентифікації та розпізнання кібератак, що сприяє прийняттю раціональних управлінських рішень для їх нейтралізації.

П'ятий розділ присвячено вирішенню актуального завдання виявлення

стану інфокомунікаційної мережевої системи, яка працює в умовах впливу деструктивних факторів. Аналізуються заходи для проведення дій по відновленню деградованого стану ІМС від впливу негативних факторів зовнішнього середовища. Проведено ідентифікацію стану мережевої системи за допомогою когнітивного моделювання. Прогнозується управління зміною стану для відновлення ІМС.

До агресивних факторів, які особливо критичні для функціонування ІМС та впливають на погіршення її стану, можна віднести наступні: бойові дії противника, які спрямовані на порушення інфраструктури ІМС; кібератаки, які впливають на передачу даних та спотворення програмного забезпечення, що може порушити стабільність розподіленого управління військовими об'єктами та об'єктами подвійної інфраструктури; атаки на об'єкти енергопостачання ІМС, тощо. Розпізнавання існуючого стану, в якому знаходиться ІМС, дозволяє виявити рівень деградації системи та запланувати дії щодо її відновлення та підвищення стійкості через вплив негативних (агресивних) факторів. Виділено можливі стани ІМС, які впливають на стійкість функціонування системи: стан ІМС, яка нещодавно введена в експлуатацію; стан системи, яка деградувала у часі (фізичне старіння), і тому чутлива до впливу негативних факторів; стан пошкодженої системи від агресивних дій противника.

Суттєве відновлення ІМС потребує великих витрат та довгих строків виконання проєкту. Обмеженість ресурсів не дозволяє зробити повне відновлення ІМС. Тому, у першу чергу, необхідно проводити відновлення для тих компонент, із загальної множини, які є критичними та впливають на стан системи. Вибір необхідної підмножини компонент ІМС, які потребують відновлення, пов'язано з аналізом великої кількості можливих варіантів. Тому для вирішення цієї задачі був використаний метод цілочисельного (булевого) програмування, який показав свою ефективність при розв'язанні багатоваріантних задач для різних галузей (виробництво, економіка, екологія, тощо). При оптимізації використовується булева змінна:

$$x_{lk} = \begin{cases} 1, \textit{ якщо для } l\textit{-ї деградованої компоненти ІМС} \\ \textit{для її відновлення необхідно провести заходи,} \\ \textit{які залежать від } k\textit{-го, стану в якому вона знаходиться;} \\ 0, \textit{ в іншому випадку.} \end{cases} \quad (12)$$

Для вибору потрібного варіанту було введено показники, які оцінюють дії по відновленню стану деградованої ІМС: рівень покращення стану ІМС після проведення дій щодо її відновлення – (*P);* час необхідний для проведення заходів щодо відновлення стану деградованої ІМС – (*T);* витрати, які необхідні на проведення заходів щодо відновлення стану ІМС – (*V);* ризик виконання проєкту щодо відновлення стану деградованої ІМС – (*R).*

Сформовані можливі постановки оптимізаційної задачі щодо відновлення ІМС. Наприклад, необхідно покращувати показник (*P*) в умовах

обмежених ресурсів:

$$\max P,\ P = \sum_{l=1}^{L} \sum_{k=1}^{m_l} p_{lk} \cdot x_{lk}, \tag{13}$$

з урахуванням обмежень

$$T \le T',\ T = \sum_{l=1}^{L} \sum_{k=1}^{m_l} t_{lk} \cdot x_{lk},$$

$$V \le V',\ V = \sum_{l=1}^{L} \sum_{k=1}^{m_l} v_{lk} \cdot x_{lk}, \tag{14}$$

$$R \le R',\ R = \sum_{l=1}^{L} \sum_{k=1}^{m_l} r_{lk} \cdot x_{lk},$$

де L – кількість деградованих компонент ІМС; m_l – кількість можливих деградованих станів, в яких може знаходитися l-та компонентна ІМС; p_{lk} – рівень покращення стану l-ї деградованої компоненти ІМС, після проведення заходів щодо її відновлення, з урахуванням $к$-го стану, в якому вона знаходилась; t_{lk} – час, потрібний для проведення заходів щодо відновлення l-ї деградованої компоненти ІМС, з урахуванням її $к$-го стану; v_{lk} – витрати щодо виконання проєкту по проведенню відновлювальних дій для покращення стану l-ї компоненти, з урахуванням $к$-го стану, в якому вона знаходилась; r_{lk} – ризик виконання проєкту по відновленню стану l-ї компоненти з урахуванням $к$-го стану, в якому вона знаходилась; T', V', R' – допустимі значення показників (T, V, R). Розв’язано багатокритеріальну задачу пошуку компромісу серед значень показників (P, T, V, R).

Вирішено завдання щодо ідентифікації стану деградованої ІМС. Для ідентифікації стану ІМС був обраний та використаний сучасний метод, заснований на когнітивному моделюванні, яке дозволяє оперативно проводити оцінку стану системи з використанням як кількісних, так і якісних факторів.

На рис. 2 представлена структурна схема системи управління станом функціонування інфокомунікаційної мережі, яка поділяється на: управляючу підсистему (суб’єкт управління, S); підсистему, якою управляють (об’єкт управління, O); модель інфокомунікаційної мережі у вигляді когнітивної моделі (Y).

Розроблений метод відрізняється від відомих тим, що дозволяє проводити навчання не тільки синаптичних ваг, але й параметрів функції належності разом з архітектурою штучної нейронної мережі (ШНМ). Прогнозування стану складної ІМС може здійснюватися в наступних режимах: безпосереднє багатовимірне прогнозування стану ІМС; саморозвиток і прогнозна оцінка зміни стану складної ІМС, при якому моделювання динаміки зміни стану проводиться з поточної ситуації; розвиток і прогнозна оцінка зміни стану складної ІМС, при якому моделювання динаміки зміни стану проводиться в деякій ситуації.

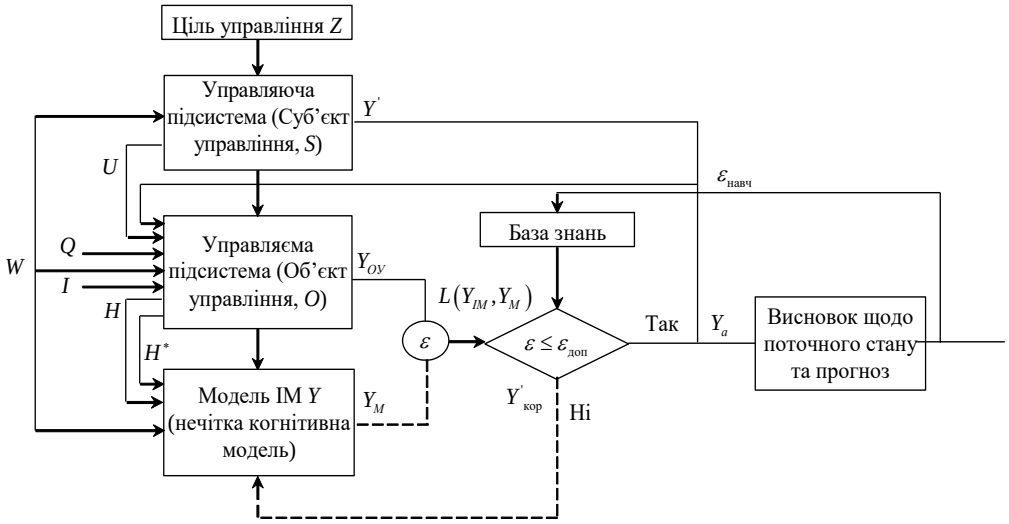


Рис. 2 – Структурна схема управління станом інфокомунікаційної мережі

Запропоновано архітектуру штучної нейронної мережі, яка є базою для оцінки стану ІМС та управління її зміною для забезпечення стійкості системи. Архітектура штучної нейронної мережі представлена у вигляді багатошарової нейро-фаззі системи, що еволюціонує та складається з п'яти послідовних шарів.

На вхідний (нульовий) шар нейро-фаззі системи надходить вектор сигналів-образів $x(k)=\left(x_1(k),\ x_2(k),\ ...,\ x_n(k)\ \right)^T$ (тут $k=1,\ 2,\ ...$ – поточний дискретний час), що підлягають обробці.

Перший прихований шар містить функції належності $\mu_{li}=\left(x_i\right),\ i=1,\ 2,\ ...,\ n;\ l=1,\ 2,\ ...,\ h$ таким чином, що для кожного входу задається h функцій належності. Перший прихований шар виконує фаззіфікацію вхідного простору. При цьому припускається, що в процесі навчання-еволюції повинні настроюватися як власне параметри цих функцій, так і їх кількість.

Другий прихований шар забезпечує агрегування рівнів належності, розрахованих у першому прихованому шарі, і складається з h блоків множення.

Третій прихований шар – це шар, що налаштовує синаптичні ваги, які підлягають визначенню в процесі контрольованого навчання.

Четвертий прихований шар утворено двома суматорами, що обчислює суми вихідних сигналів другого та третього прихованого шарів.

В п'ятому (вихідному) шарі проводиться дефаззіфікація, у результаті якої формується сигнал управління.

Таким чином, в даному розділі було розроблено методи та моделі, які дозволяють здійснювати:

– відновлення деградованої (пошкодженої) інфраструктури ІМС з використанням запропонованої оптимізаційної моделі цілочисельного (булевого) програмування для вибору необхідних заходів забезпечення стійкості в умовах обмежених ресурсів;

– ідентифікацію стану ІМС з використанням когнітивної моделі та з можливим різним представленням даних (кількісні, якісні оцінки тощо);

– управління та прогнозування стану ІМС на основі багатошарової нейронної мережі з машинним навчанням.

У **шостому розділі** представлено результати дослідження впливу негативних факторів на передачу даних в ІМС, що може привести до порушення управління в критичних галузях та при проведенні оборонних дій. Створено методи маршрутизації передачі даних в умовах загроз.

Передача даних в ІМС у мирний час дуже відрізняється в умовах військового стану країни. Актуальним є дослідження, яке проведене в даному розділі зі створення моделей для планування маршрутів передачі даних, зокрема в умовах впливу агресивних факторів зовнішнього середовища.

Існуючі методи маршрутизації, в основному, засновані на аналітичних розрахунках можливих шляхів з використанням графових моделей. До недоліків цих методів можна віднести: відсутність реального представлення часу руху у явному вигляді; неможливість одночасного (паралельного) моделювання маршрутів; не враховуються можливі відмови руху даних при виникненні збоїв та аварійних ситуацій; не враховуються ризики, які пов’язані з впливом негативних (агресивних) факторів на передачу даних; відсутність оперативного реагування на небезпечну ситуацію в мережевій системі.

З метою усунення перелічених недоліків запропоновано метод маршрутизації, який заснований на агентному подійному імітаційному моделюванні, що має такі переваги: використання фактору часу для моделювання основних подій передачі даних; заявки (пакети даних), які передаються, можуть моделюватися паралельними маршрутами в мережевій системі; існує можливість задання різних сценаріїв передачі даних; здійснюється автоматичний пошук раціональних маршрутів з урахуванням ризиків; оцінюється існуючий стан окремих компонент мережевої системи. В розробленому методі пакети даних, які рухаються в ІМС, представлені у формі заявок імітаційного моделювання. Заявки виникають при ініціалізації передачі даних між користувачами ІМС та рухаються по окремим компонентам мережевої системи. Мережева система представлена в імітаційній моделі у вигляді вузлів (комутаційні вузли) і зв’язків між ними (магістралі передачі даних). Можливе формування складних заявок (популяцій), які розмножуються (клонуються) на копії. В такому випадку складна заявка (популяція) формує нащадків у вигляді клонів. Завдяки паралельності у часі, при моделюванні руху множини заявок, створюються умови для відбору конкурентоздатних заявок (клонів), які будуть рухатися далі для формування нових маршрутів.

Сформовано послідовність основних подій в розробленому алгоритмі для пошуку раціональних маршрутів передачі даних:

1-а подія. Формується структура мережевої системи у вигляді вузлів та магістралей.

2-а подія. Ініціюється у часі формування заявок у початкових вузлах передачі даних (множина A), які будуть рухатись до кінцевих (множина B).

3-я подія. Заявки рухаються у часі до сусідніх вузлів.

4-а подія. Заявки формують слід (мітку) у тих вузлах, до яких вони прийшли.

5-а подія. Якщо заявка прийшла у вузол, який вже має слід від минулої заявки, то вона знищується, оскільки немає сенсу продовжувати її рух далі, через більший час подальшого просування в мережевій системі (заявка не конкурентоспроможна).

6-а подія. Якщо заявка прийшла в сусідній вузол, який не має сліду (він не помічений) від іншої заявки, то вона формує популяцію з множини клонів (копій заявки), які будуть рухатися далі до сусідніх вузлів.

Далі події 3, 4, 5, 6 повторюються.

…

7-а подія. Якщо заявка дійшла до кінцевого вузла передачі даних (множина *B*), то її рух припиняється.

8-а подія. Формуються маршрути передачі даних у вигляді послідовності помічених вузлів, починаючи від кінцевих вузлів (множина *B*) та закінчуючи початковими вузлами (множина *A*).

Показано, що послідовність дій в розробленому алгоритмі формує, у часі, найбільш короткий маршрут (T_{min}) передачі даних в мережевій системі.

Розроблено алгоритм моделювання найкоротшого маршруту з урахуванням впливу ризиків загроз (атак) на мережеву систему, що є актуальним в умовах особливого стану країни. Розроблено мультиагентну модель для пошуку раціональних маршрутів передачі даних в ІМС, з урахуванням впливу негативних (агресивних) факторів зовнішнього середовища. Сформовано множину агентів для моделювання основних подій: «Структура ІМС», «Формування множин *A*, *B*», «Ініціалізація заявок», «Рух», «Формування сліду», «Умови», «Клонування», «Припинення руху», «Формування раціональних маршрутів».

Для пошуку раціональних маршрутів передачі даних в умовах впливу ризиків негативних (агресивних) факторів, використовується агент: «Ризики». Формується множина можливих ризиків для всіх компонент. За допомогою агента «Управління моделюванням» проводиться інтерактивне моделювання процесу маршрутизації. Агент «Результати моделювання» видає основні результати моделювання: маршрути, які сформовано для передачі даних в мережевій системі; час, потрібний для передачі; маршрути передачі даних в умовах впливу негативних (агресивних) факторів, з урахуванням ризиків, тощо.

На рис. 3 представлено структурну схему мультиагентної імітаційної моделі.

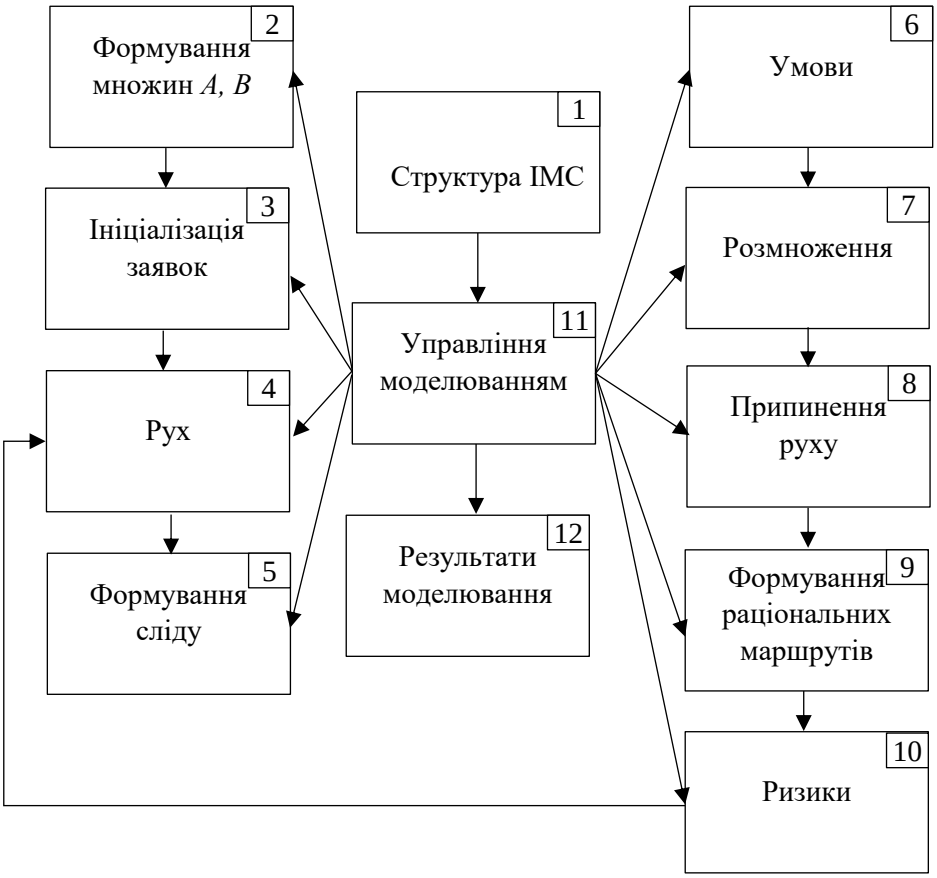


Рис. 3 – Структурна схема мультиагентної імітаційної моделі

Швидка динаміка змін зовнішнього середовища, з поширенням множини факторів деструктивного характеру, які впливають на передачу даних в мережевій системі, спричинили необхідність створення інтелектуального управління процесом передачі даних. Запропоновано метод, який заснований на імітації руху тварин у природі. В алгоритмі цього методу використане машинне навчання, яке дозволяє оперативно адаптуватися до змін умов зовнішнього середовища при управлінні передачею даних.

Таким чином, у даному розділі проведено дослідження, яке дозволяє:

– формувати раціональні маршрути передачі даних в умовах впливу деструктивних факторів на основі використання імітаційного мультиагентного моделювання;

– управляти передачею даних та адаптуватися до можливих змін зовнішнього середовища, з використанням когнітивного моделювання.

У **сьомому розділі** представлено прикладну інформаційну технологію створення стійкої інфокомунікаційної мережевої системи (ПІТСІМС), яка функціонує в умовах впливу деструктивних факторів зовнішнього середовища. Основою для розробки ПІТСІМС є науково обґрунтована методологія (див. розділ 2), яка заснована на новій парадигмі синтезу стійкої ІМС, має концептуальні принципи створення розподіленої мережевої системи. Розроблені оригінальні нові методи та створені моделі, які детально представлені у попередніх розділах дисертаційного дослідження.

При створені ПІТСІМС проведені дослідження за напрямками:

створення архітектури системи; проєктування складових у вигляді програмних компонент; формування мультиагентної платформи для розробки програмного забезпечення; створення інтерфейсу користувачів системи; проведення експериментальних досліджень з аналізу ефективності розробленої системи.

Виявлені маловивчені в існуючих дослідженнях проблеми, які ураховані при створенні ІМС, стійкої до впливу негативних факторів: формування архітектури розподіленої ІМС, яка може функціонувати у період особливого стану країни; аналіз впливу деструктивних факторів зовнішнього середовища на інфраструктуру ІМС та її управління; віртуалізація розподіленого управління в ІМС; використання сучасного мультиагентного середовища для управління та моніторингу ІМС; використання хмарного середовища (CLOUD) для створення розподіленої мережевої системи, стійкої до впливу деструктивних факторів. Ураховані складності створення ієрархічної ІМС, та визначені такі рівні: система; підсистема; програмні компоненти; мультиагентне середовище; користувачі системи.

Архітектура системи відображає множину управлінських дій та функціональних завдань щодо забезпечення стійкості ІМС: система (ПІТСІМС); підсистеми (ССМС, ФАСМС, ІУСМС, ПЗСМС, ВСМС, КМС, СММС); програмні компоненти (ССМС, КПМС, ОСМС, СТМС, ВМС, ЗФСМС, СПДМС, РАМС, ІСМС, ВСМС, УВМС, ПБММС, УПДМС, ПРМС); агенти: «Системний синтез», «Компонентне проєктування», «Формування складу компонент», «Топологічний синтез», «Стійкість від вразливості», «Стійкість фізичної інфраструктури», «Стійкість передачі даних», «Розпізнавання атак», «Ідентифікація стану», «Управління станом», «Відновлення стану», «Інтелектуальне управління передачею даних», «Компараторна ідентифікація», «Структура ІМС», «Формування множин A, B», «Ініціалізація заявок», «Рух», «Формування сліду», «Умови», «Клонування», «Припинення руху», «Формування раціональних маршрутів», «Ризики», «Управління моделюванням», «Результати моделювання»; «Користувачі підсистем».

На рис. 4 представлена архітектура ПТІСІМС.

Тут використані такі позначення в описі архітектури: «Синтез стійкої мережевої системи» (ССМС); «Формування архітектури стійкої мережевої системи» (ФАСМС); «Інтелектуальне управління стійкістю мережевої системи» (ІУСМС); «Превентивні заходи стійкості мережевої системи» (ПЗСМС); «Відновлення стану мережевої системи» (ВСМС); «Кібербезпека мережевої системи» (КМС); «Стійка маршрутизація мережевої системи» (СММС).

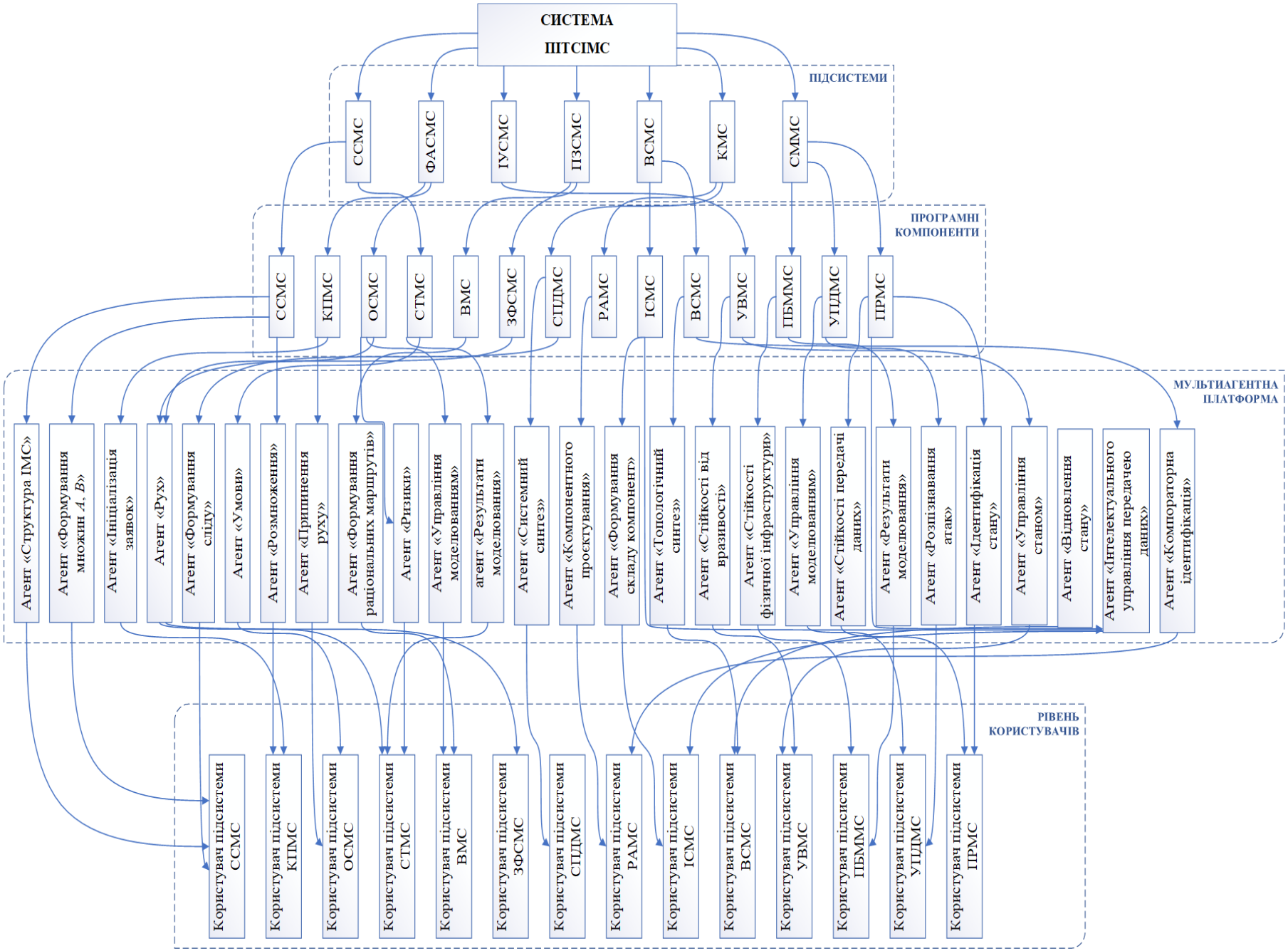


Рис. 4 – Архітектура ПІТСІМС

На рівні програмних компонент ПСМС було створено: «синтез стійкої мережевої системи» (КСМС); «компонентне проєктування мережевої системи» (КПМС); «оптимальний склад мережевої системи» (ОСМС); «синтез топології мережевої системи» (СТМС); «вразливості мережевої системи» (ВМС); «захист фізичної структури мережевої системи» (ЗФСМС); «стійкість передачі даних мережевої системи» (СПДМС); «розпізнавання атак в мережевій системі» (РАМС); «ідентифікація стану мережевої системи» (ІСМС); «відновлення стану мережевої системи» (ВСМС); «управління відновленням мережевої системи» (УВМС); «пошук безпечних маршрутів мережевої системи» (ПБММС); «управління передачею даних в мережевій системі» (УПДМС); «прийняття рішень в мережевій системі» (ПРМС); «синтез стійкої мережевої системи» (ССМС). Для формування мультиагентної платформи було створено мультиагентне середовище з множиною агентів.

Для демонстрації ефективності методології та прикладної інформаційної технології створення стійкої ІМС розглянуто приклад розробки розподіленого управління перевезеннями, в умовах впливу агресивних факторів на мережеву систему та її компоненти, що дозволило забезпечити стійке управління формуванням відносно безпечних маршрутів для військових та цивільного населення.

Створена розподілена система віртуального скринінгу для військової медицини, із застосуванням мережевої системи. Інформаційний скринінг являє собою процес розподіленої семантичної обробки слабоструктурованих, неповних, неоднозначних даних з метою проведення аналізу ознак і виявлення закономірностей та невідповідностей. Запропоновано використання методу компараторної ідентифікації (МКІ) для вирішення задачі інформаційного скринінгу медичної документації військових. МКІ є основним методом теорії інтелекту та дозволяє створити сукупність моделей передачі та розподіленої обробки даних з використанням стійкої інформаційної мережі (рис. 5).

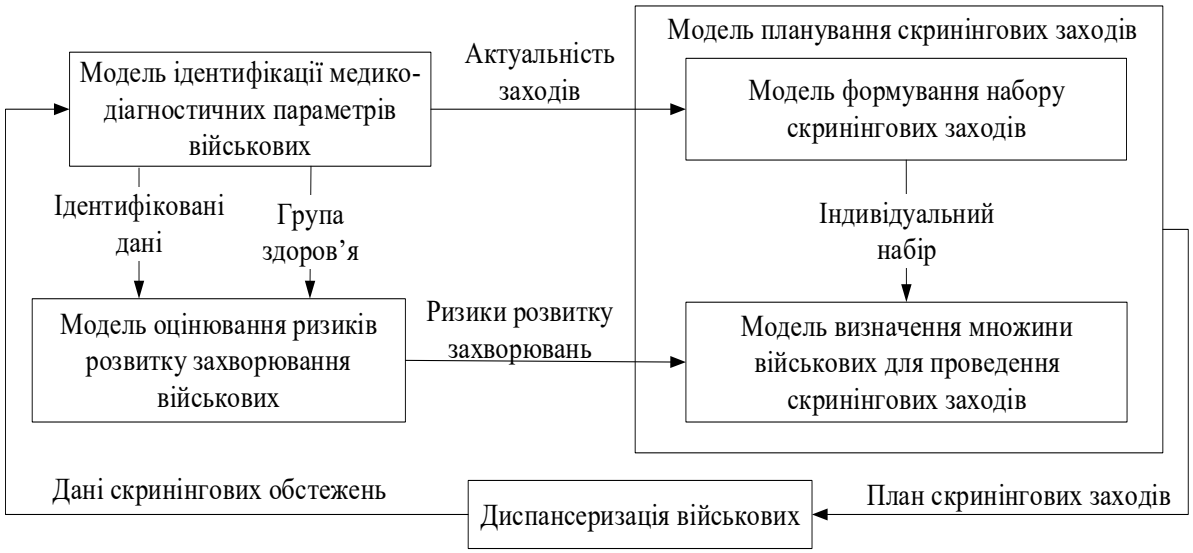


Рис. 5 – Структура розподіленого інформаційного скринінгу медичної документації військових з використанням стійкої інформаційної мережі

Таким чином, у даному розділі представлено розроблену прикладну інформаційну технологію створення стійкої ІМС, яка заснована на науково обґрунтованій методології синтезу стійкої ІМС. Сформована ієрархічна архітектура ПІТСІМС. Програмне забезпечення ПІТСІМС було розроблено у вигляді мультиагентного представлення множини функціональних задач та управління стійкої ІМС, що забезпечує можливість її ефективного використання, в умовах особливого стану країни. Мережева система функціонує в умовах загроз, реагує на зміну обставин функціонування і є відкритою для нових завдань.

ВИСНОВКИ

В дисертаційній роботі вирішено актуальне науково-прикладне завдання формування методологічних основ створення інфокомунікаційної мережевої системи (ІМС), стійкої до впливу деструктивних факторів зовнішнього середовища. Сформовано нову парадигму стійкої ІМС, яка має концептуальні принципи синтезу (системне створення, архітектурний синтез, інтелектуалізація управління стійкістю, превентивна протидія, кібербезпека, оперативне відновлення, стійка маршрутизація). На основі запропонованої методології розроблені методи, моделі та прикладна інформаційна технологія створення стійкої ІМС. Проведення дисертаційного дослідження призвело до вирішення актуальних задач, які мають наступні науково обґрунтовані результати.

1. Проаналізовано проблеми стійкості ІМС у мирний час та в умовах особливого стану країни. Проведено аналіз існуючих методів, моделей та інформаційних технологій, які використовуються для створення та функціонування ІМС у теперішній час.
2. Створено методологічні основи синтезу розподіленої ІМС, стійкої до впливу факторів зовнішнього середовища.
3. Розроблено метод та моделі архітектурного синтезу стійкої ІМС для формування компонентного складу та топології структури розподіленої системи.
4. Розроблено моделі планування превентивних заходів для забезпечення стійкості ІМС, з урахуванням її вразливості.
5. Розроблено моделі проведення заходів по відновленню ІМС, з урахуванням можливих пошкоджень критичних компонент.
6. Розроблено моделі ідентифікації та інтелектуального управління станом ІМС, для адаптування к динамічним змінам зовнішнього середовища.
7. Створено метод та моделі для забезпечення маршрутизації передачі даних, в умовах впливу негативних (агресивних) факторів.
8. Науково обґрунтовано та створено прикладну інформаційну технологію забезпечення стійкості ІМС з використанням мультиагентної платформи та хмарного середовища.
9. Результати дисертаційного дослідження впроваджені в практику створення мережевих систем, які використовуються для розподіленого

управління об’єктами критичної інфраструктури та виробництва. Впровадження показало ефективність запропонованої методології та прикладної інформаційної технології в умовах особливого стану країни.

Достовірність результатів підтверджується:

– використанням комплексу методів і моделей, який інтегрує теоретичні і прикладні методи дослідження, зокрема методи системного аналізу, теорії стійкості складних систем, моделі оптимізації, моделі штучного інтелекту та машинного навчання, що дозволило адекватно описати процес створення стійкої інфокомунікаційної мережі в умовах впливу деструктивних факторів зовнішнього середовища;

– коректною постановкою задач та обґрунтованістю припущень, зроблених при створенні моделей і методів, а також значень вхідних параметрів для моделювання, виходячи з досвіду функціонування ІМС в умовах особливого стану країни;

– зведенням отриманих математичних залежностей до раніше відомих, при застосуванні граничних значень параметрів, які не були раніше враховані;

– практичним впровадженням і позитивним досвідом використання отриманих результатів;

– збігом результатів розрахунку показників стійкості, які отримані з використанням перевірених аналітичних виразів, з результатами, отриманими з практики використання ІМС в особливому стані країни.

Подальші дослідження доцільно спрямувати за напрямками:

– розроблення методологічних основ, моделей та прикладної інформаційної технології прогнозування, планування та управління створенням ІМС подвійного призначення в загострених умовах експлуатації;

– розроблення моделей та засобів для дослідження дії агресивних кібератак на функціонування ІМС та формування заходів кіберзахисту;

– розроблення методів прогнозування появи ризиків пошкодження інфраструктури мережевої системи для забезпечення підвищення її стійкості в агресивному зовнішньому середовищі.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових виданнях, включених до Переліку фахових видань України:

1. Застосування моделей і критеріїв семантичної еквівалентності даних для підвищення ефективності функціонування економічних систем / Плєхова Г. А., Алісейко О. В., Кочуєва З. А. // Автомобіль і електроніка. Сучасні технології. – 2021. – № 19. – С. 41 – 46.

Здобувачкою запропоновано визначення моделей і критеріїв семантичної еквівалентності даних в економічних системах.

2. Плєхова Г. А., Костікова М. В. Інформаційна безпека з урахуванням нової загрози. *Вісник Харківського національного автомобільно-дорожнього університету*. 2022. № 98. С. 7–12.

Здобувачкою запропоновано класифікацію методів інформаційної безпеки.

3. Левтеров А. І., Плєхова Г. А., Костікова М. В., Бережна Н. Г., Окунь А. О. Дослідження методів безпечної маршрутизації у програмно-конфігурованих мережах // А. І. Левтеров, Г. А. Плєхова, М. В. Костікова, Н. Г. Бережна, А. О. Окунь / Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології : зб. наук. пр. / Нац. техн. ун-т «Харків. політехн. ін-т». – Харків : НТУ «ХПІ», 2023. – № 1 (9) 2023. С. 10–18.

Здобувачці належить визначення та обробка даних безпечної маршрутизації у програмно-конфігурованих мережах.

4. Левтеров А. І., Плєхова Г. А., Костікова М. В., Очеретенко С. В. Аналіз вразливостей площини даних SDN і функціональних можливостей засобів маршрутизації щодо протидії можливим атакам // А. І. Левтеров, Г. А. Плєхова, М. В. Костікова, С. В. Очеретенко / Системи управління, навігації та зв'язку, 2023, № 3 (73), С. 123–127. DOI: https://doi.org/10.26906/SUNZ.2023.3.123.

Здобувачкою запропоновано загальну постановку задачі аналізу вразливостей площини даних SDN в особливому стані країни.

5. Єременко О. С., Плєхова Г. А. Дослідження моделей безпечної маршрутизації на основі базових метрик уразливостей у мережах SND. Електронне наукове фахове видання-журнал «Проблеми телекомунікацій». 2022. № 2. С. 34-50.

Здобувачці належить метод дослідження моделей безпечної маршрутизації на основі базових метрик уразливостей.

6. Плєхова Г. А., Костікова М. В., Петренко С. О., Яценко О. О. Модель інформаційно-комунікаційної системи // Б. С. Карпішен, С. М. Неронов, Г. А. Плєхова, М. В. Костікова, С. О. Петренко, О. О. Яценко / Біоніка інтелекту, 2023, № 1 (99), С. 78 – 82. DOI: 10.30837/bi.2023.1(99).11.

Здобувачкою запропоновано метод побудови моделі інформаційно-комунікаційної системи.

7. Неронов С. М., Плєхова Г. А., Очеретенко С. В. Синергія автомобільного трансферу та утримання автомобільних доріг // С. М. Неронов, Г. А. Плєхова, С. В. Очеретенко / Системи управління, навігації та зв'язку, 2024, № 3 (77), С. 16 – 19. DOI: 10.26906/SUNZ.2024.3.016.

Здобувачкою запропоновано методику оцінювання синергії автомобільного трансферу та утримання автомобільних доріг в умовах воєнного стану.

8. Плєхова Г. А., Неронов С. М., Костікова М. В., Кашкевич С. О. Удосконалення моделі безпечної маршрутизації в програмно-конфігурованих мережах // Г. А. Плєхова, С. М. Неронов, М. В. Костікова, С. О. Кашкевич / Біоніка інтелекту, 2024, № 1 (100), С. 50 – 57. DOI: 10.30837/bi.2024.1(100).07.

Здобувачкою розроблено загальний підхід до удосконалення моделі безпечної маршрутизації в програмно-конфігурованих мережах.

9. Плєхова Г. А., Костікова М. В., Неронов С. М., Багмут Р. Б.,

Яценко О. О. Пристрій утворення маршрутів передачі інформації в радіомережах спеціального призначення із можливістю самоорганізації // Г. А. Плєхова, М. В. Костікова, С. М. Неронов, Р. Б. Багмут, О. О. Яценко / Біоніка інтелекту, 2024, № 2 (101), С. 30 – 33. DOI: 10.30837/bi.2024.2(101).04.

Здобувачці належить розробка принципів самоорганізації для впровадження пристрою утворення маршрутів передачі інформації в радіомережах спеціального призначення.

10. Левтеров А. І., Плєхова Г. А., Костікова М. В., Окунь А. О. Система контролю політики кібербезпеки з елементами штучного інтелекту корпоративної мережі зв'язку // А. І. Левтеров, Г. А. Плєхова , М. В. Костікова, А. О. Окунь / Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, 2025, № 1 (13), С. 10 – 16. DOI: 10.20998/2079-0023.2025.01.02.

Здобувачці належить загальна постановка задачі розробки системи контролю політики кібербезпеки з елементами штучного інтелекту корпоративної мережі зв'язку.

11. Шаронова Н. В., Плєхова Г. А., Неронов С. М., Костікова М. В., Плєхов Д. О. Спосіб інтеграції різнорідних даних в системі геопросторового аналізу // Н. В. Шаронова, Г. А. Плєхова, С. М. Неронов, М. В. Костікова, Д. О. Плєхов / Біоніка інтелекту, 2025, № 1 (102), С. 70 – 74. DOI: 10.30837/bi.2025.1(102).09.

Здобувачкою запропоновано загальний підхід до створення способу інтеграції різнорідних даних в системі геопросторового аналізу даних.

12. Плєхова Г. А. Математична модель оцінки рівня захищеності функціонування інфокомунікаціних мереж // Г. А. Плєхова / Наука і техніка сьогодні, 2025, № 9 (50), С. 1437 – 1449.

13. Плєхова Г. А. Формування складу інфокомунікаціонної мережевої системи з використанням компонентного підходу // Г. А. Плєхова / Наука і техніка сьогодні, 2025, № 10 (51), С. 1886 – 1898. URL: http://perspectives.pp.ua/index.php/nts/issue/view/410/513.

14. Плєхова Г. А. Побудова системи ознак для бази знань на основі формальної алгебро-логічної моделі складної системи // Г. А. Плєхова / Наука і техніка сьогодні, 2025, № 11 (52), С. 2590 – 2596. URL: https://perspectives.pp.ua/index.php/nts/issue/view/421/524.

15. Плєхова Г. А. Застосування алгебро-логічного моделювання в умовах інтелектуалізації прийняття рішень неповного визначення інформації // Г. А. Плєхова / Біоніка інтелекту, 2025, № 2 (103), С. 102 – 107. DOI: 10.30837/bi.2025.2(103).13. URL: http://bionics.nure.ua/issue/view/20095/13641.

16. Плєхова Г. А. Моделювання превентивних заходів щодо захисту фізичної інфраструктури інфокомунікаційної мережевої системи від атакуючих дій противника // Г. А. Плєхова / Наука і техніка сьогодні, 2025, № 13 (54), С. 2443 – 2455.

17. Плєхова Г. А. Метод інтелектуального управління маршрутизацією передачі даних в мережевій системі // Г. А. Плєхова / Наука і техніка сьогодні, 2026, № 1 (55), С. 2468 – 2478.

Статті у наукових виданнях України та інших держав, в тому числі проіндексовані у Scopus:

18. Volkov V., Gritsuk I, Volkova T., Berezhnaja N., Pliekhova G., Bulgakov M., Marmut I., Volska O. System Approach to Forecasting Standards of Vehicles' Braking Efficiency. SAE Technikal Paper 2021-01-5083, 2021, DOI: 10.4271/2021-01-5083(Scopus).

Внесок здобувачки полягає у розробці адаптації методу прогнозування та визначенні критеріїв оцінювання точності.

19. Levterov A., Pliekhova H., Kostikova M., Okun A. Geometric modelling of tracks and flows // A. Levterov, H. Pliekhova, M. Kostikova, A. Okun / U. P. B. Scientific Bulletin, Series A: Applied Mathematics and Physics, Vol. 85, Iss. 3, 2023. Pp. 87–92(Scopus).

Внесок здобувачки полягає у формалізації задачі геометричного моделювання траєкторій і потоків та визначенні основних припущень і метрик оцінювання.

20. Owaid, S. R., Zhuravskyi, Y., Lytvynenko, O., Veretnov, A., Sokolovskyi, D., Plekhova, G., Hrinkov, V., Pluhina, T., Neronov, S., Dovbenko, O. (2024). Development of a method of increasing the efficiency of decision-making in organizational and technical systems. Eastern-European Journal of Enterprise Technologies, 1 (4 (127)), 14–22. DOI: 10.15587/1729-4061.2024.298568(Scopus).

Внесок здобувачки полягає у розробці математичної моделі та алгоритмічної процедури узгодження рішень з урахуванням обмежень ресурсів і невизначеності.

21. Sova, O., Dmytriiev, I., Kuchuk, N., Yefymenko, O., Lytvynenko, N., Plekhova, G., Shatrov, A., Chemerys, Ye., Dovbenko, O., Stoichev, M. (2024). Development of a method for managing technical systems using a bio-inspired algorithm. Eastern-European Journal of Enterprise Technologies, 3 (4 (129)), 35–43. DOI:10.15587/1729-4061.2024.304471(Scopus).

Здобувачкою розроблено метод керування технічною системою на основі біоінспірованого алгоритму, реалізувала його програмно.

22. Mahdi, Q. A., Shyshatskyi, A., Voznytsia, A., Plekhova, G., Shostak, S., Tulenko, I., Semko, R., Zheliezniak, D., Momit, A., Sova, M. (2025). Development of a method for increasing the efficiency of processing different types of data in organizational and technical systems. Eastern-European Journal of Enterprise Technologies, 2 (4 (134)), 23–31. DOI: 10.15587/1729-4061.2025.325102 (Scopus).

Здобувачкою розроблено метод адаптивної обробки різнотипних даних.

23. Owaid, S. R., Miahkykh, H., Odarushchenko, E., Kashkevich, S., Shyshatskyi, A., Plekhova, G., Hrymud, A., Petruk, S., Shaposhnikova, O., Stryhun, V. (2025). Development of a method for detecting cyber attacks on information systems based on artificial intelligence technologies. Eastern-European Journal of Enterprise Technologies, 3 (9 (135)), 33–39. DOI: 10.15587/1729-4061.2025.329258 (Scopus).

Здобувачкою розроблено AI-метод виявлення кібератак, підготовлено дані та ознаки, реалізовано прототип.

24. Pliekhova, G., Neronov, S., Volkova, T., Ptytsia, N., Kuzhel, V. (2025). Consideration of the CVSS Base Metrics in Building a Mathematical Routing Model Concerning Route Vulnerabilities for Engineering Systems. In: Pavlenko, D., Tryshyn, P., Honchar, N., Kozlova, O. (eds) Smart Innovations in Energy and Mechanical Systems. SIEMS 2025. Lecture Notes in Networks and Systems, 16 July 2025, vol. 1480, pp. 205–218. Springer, Cham. DOI: 10.1007/978-3-031-95191-6_20 (Scopus).

Здобувачкою інтегровано CVSS Base Metrics у математичну модель маршрутизації, розроблено алгоритм оцінювання вразливості маршруту.

Розділи у колективних монографіях:

25. Theoretical Foundations in Economics and Management: collective monograph / Toporkova O., Lytovchenk O.,Pliekhova G., Levterov A., Suhanova N. – etc. – International Science Group. – Boston : Primedia eLaunch, 2022. 872 p. vailable at : DOI – 10.46299/ISG.2022.MONO.ECON.2 (Scopus)..

Здобувачкою сформульовано теоретико-методичні положення щодо аналізу складних систем , наведено практичні рекомендації.

26. Pliekhova Ganna A., Kostikova Maryna V. Удосконалення математичної моделі безпечної маршрутизації з врахуванням базових метрик критичності вразливостей. World trends in the use of interactive technologies in education. International collective monograph. Intellebence Transportation System And Smart City Institute (ITSSCI). Lima, Peru, 2023. Pp. 418–432.

Здобувачкою інтегровано базові метрики CVSS у вдосконалену математичну модель безпечної маршрутизації.

27. Костікова М. В., Неронов С. М., Плєхова Г. А. Інформаційні системи, моделі даних та їх використання. Modern aspects of science. International collective monograph. International Economic Institute s.r.o.. Czech Republic: International Economic Institute s.r.o., 2024. Vol. 41. Pp. 275 – 298(Scopus).

Здобувачкою виконано розробку та обґрунтування моделі даних і сценаріїв її використання в інформаційній системі, а також узагальнено результати у вигляді рекомендацій.

28. Кашкевич С. О., Дмитрієва О. І., Єфименко О. В., Плєхова Г. А., Шишацький А. В. Методи оцінки стану складних динамічних об’єктів з використанням біоінспірованих алгоритмів. Modern aspects of science. International collective monograph. International Economic Institute s.r.o.. Czech Republic: International Economic Institute s.r.o., 2024. Vol. 44. Pp. 138 – 177 (Scopus).

Здобувачкою розроблено біоінспірований метод оптимізаційної оцінки стану складних динамічних об’єктів і експериментально підтверджено його ефективність порівняно з класичними оцінювачами.

29. Кашкевич С. О., Дмитрієва О. І., Плєхова Г. А., Протас Н. М., Неронов С. М., Шишацький А. В. Науково-методичний підхід з підвищення оперативності обробки різнотипних даних з використанням метаевристичних

алгоритмів. Modern aspects of science. International collective monograph. International Economic Institute s.r.o.. Czech Republic: International Economic Institute s.r.o., 2024. Vol. 46. Pp. 510 – 543(Scopus).

Здобувачкою розроблено науково-методичний підхід і метаевристичний алгоритм для прискорення обробки різнотипних даних та експериментально підтверджено зниження затримок і кількості порушень SLA.

30. Плєхова Г. А., Шкнай О. В., Протас Н. М., Налапко О. Л., Возниця А. С., Шишацький А. В. Інтелектуальні методи оцінки стану ієрархічних систем. Modern aspects of science. International collective monograph. International Economic Institute s.r.o.. Czech Republic: International Economic Institute s.r.o., 2025. Vol. 53. Pp. 407 – 447 (Scopus).

Здобувачкою розроблено інтелектуальний метод багаторівневої оцінки стану ієрархічної системи та експериментально підтверджено його ефективність і стійкість до неповних даних.

Опубліковані праці апробаційного характеру:

31. Kostykova M., Kozachok L., Levterov A., Plekhova A., Shevchenko V., Okun A. A heuristic method for an approximate solution of the knapsack problem. Mechanical Technologies and Structural Materials 2021. Proceedings of the 10th International Conference (Split, Croatia, 2021). FESB, Ruđera Boškovića 32, Split, 2021. – Pp. 63–66. – ISSN 1847-7917(Scopus).

Здобувачці належить аналіз евристичних методів розв'язання задач.

32. Kostykova M., Kozachok L., Levterov A., Plekhova A., Shevchenko V., Okun A. The use of the heuristic method for solving the knapsack problem. 2021 IEEE 2nd KhPI Week on Advanced Technology (KhPI Week): conference proceedings (Kharkiv, Ukraine, 2021). Kharkiv, 2021. P. 177–180. DOI: 10.1109/KhPIWeek53812.2021.9570025(Scopus).

Внесок здобувачки полягає у формалізації постановки задачі рюкзака та виборі критеріїв оцінювання якості розв'язків.

33. Плєхова Г. А., Костікова М. В. Актуальні проблеми інформаційної безпеки. Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті: матеріали Всеукраїнської науково-практичної Internet-конференції (м. Харків, 2022). Харків, 2022. С. 68–73.

Здобувачкою розроблено та апробовано концептуально-методичний підхід до використання моделей IT у науці, техніці, кібербезпеці та освіті, узагальнено результати у вигляді практичних рекомендацій.

34. Pliekhova G. A., Kostikova M. V. (2023). Peculiarities of the structure and properties of materials for sound absorption of eavesdropping devices in cyber security. Proceedings of the II International Scientific and Practical Conference : General regularities and models of science development. Zagreb, Croatia, 09–10 January. Pp. 61–62.

Здобувачкою досліджено структурні параметри матеріалів, оцінено їхню ефективність для використання в процесах передачі інформації.

35. Плєхова Г. А, Костікова М. В., Птиця Н. В. (2023). Аналіз стандартів побудови програмно-конфігурованих мереж. Proceedings of the IV International Scientific and Practical Conference: Science and technology: problems, prospects and innovations. CPN Publishing Group, Osaka, Japan, 18–20 January. Pp. 187–194.

Здобувачкою систематизовано та порівняно стандарти побудови SDN, проаналізовано їхню сумісність і безпекові вимоги та сформовано практичні рекомендації щодо впровадження.

36. Плєхова Г. А., Костікова М. В. (2023). Кібербезпека підключених автомобілів. Proceedings of the IV International Scientific and Practical Conference : Scientific knowledge, aesthetic creativity and social practices. Athens, Greece, Pp. 32–36.

Здобувачкою виконано моделювання загроз для підключених автомобілів, оцінено ризики ключових векторів атак і запропоновано комплекс архітектурних та алгоритмічних заходів захисту.

37. Левтеров А. І., Плєхова Г. А., Костікова М. В. Кібербезпека та автомобільний транспорт. Science and innovation of modern world: Proceedings of the 5th International scientific and practical conference (London, 2023). Cognum Publishing House. London, United Kingdom. 2023. Pp. 171–178.

Здобувачкою виконано аналіз загроз кібербезпеці автомобільного транспорту, оцінено ризики та запропоновано комплекс технічних і організаційних контрзаходів.

38. Левтеров А. І., Плєхова Г. А., Костікова М. В. Захист інформації в кіберпросторі. Actual problems of modern science: Proceedings of the 4th International scientific and practical conference (Boston, 2023). International Science Group. Boston. 2023. Pp. 460–464.

Здобувачкою виконано моделювання загроз, оцінювання ризиків і обґрунтовано комплекс заходів захисту інформації в кіберпросторі з практичними рекомендаціями щодо впровадження.

39. Костікова М. В., Неронов С. М., Плєхова Г. А. Синергетичний ефект використання дорожнього порталу WEB-рішень клієнт-серверної технології та мультиагентних систем віртуального управління перевізними процесами. Current challenges of science and education: Proceedings of the 5th International scientific and practical conference (Berlin, 2024). MDPC Publishing. Berlin, Germany. 2024. Pp. 180 – 185.

Здобувачкою розроблено інтегровану архітектуру WEB-порталу та мультиагентної системи, запропоновано критерії оцінки синергії.

40. Костікова М. В., Неронов С. М., Плєхова Г. А. Математичні підходи до обґрунтування складових елементів систем менеджменту інформаційної безпеки. Topical aspects of modern scientific research: Proceedings of the 5th International scientific and practical conference (Tokyo, 2024). CPN Publishing Group. Tokyo, Japan. 2024. Pp. 218 – 227.

Здобувачкою розроблено математичний підхід до обґрунтування вибору елементів СМІБ на основі кількісної оцінки ризику та багатокритеріальної оптимізації.

41. Vysotska, V., Smelyakov, K., Sharonova, N., Derenskyi, M., Pliekhova, G., Repikhov, V. Information System for Monitoring and Planning Maintenance of Offshore Wind Farms. CEUR Workshop Proceedings, 2024, 3668, 63 – 82. (Scopus).

Здобувачкою розроблено архітектуру та ключові алгоритми інформаційної системи для моніторингу стану й планування ТОіР.

42. Cherednichenko, O., Sharonova, N., Pliekhova, G., Babkova, N. Intelligent Methods of Secure Routing in Software-Defined Networks. CEUR Workshop Proceedings, 2024, 3664, 342 – 351 (Scopus).

Здобувачкою розроблено ризик-орієнтований інтелектуальний метод безпечної маршрутизації для SDN, реалізовано прототип.

43. Pliekhova G., Neronov S., Kostikova M., Kozachok L. Software-configured network architecture vulnerabilities. Energy Systems and Alternative Energy Sources 2024 (ESAES – 2024): AIP Conference Proceedings (Kharkiv 2024). AIP Publishing. Vol. 3238, Iss. 1, 5 June 2025. Pp. 050001-1 – 050001-6. DOI: 10.1063/5.0248882 (Scopus).

Здобувачкою виконано класифікацію вразливостей архітектури software-configured (SDN) мереж, оцінено їхню критичність і запропоновано комплекс контрзаходів.

44. Levterov A., Pliekhova H., Kostikova M., Okun A. Engine crankshaft position sensor. Mechanical Technologies and Structural Materials: Proceedings of the 13th International conference (Split, 2024). Publisher: Croatian society for mechanical technologies. Split, Croatia. 2024. Pp. 263 – 272 (Scopus).

Здобувачкою розроблено модель і алгоритми обробки сигналу датчика та обґрунтовано критерії його діагностики на основі експериментальних даних.

45. Плєхова Г. А., Костікова М. В., Козачок Л. М. Проблематика побудови програмно-конфігурованих мереж. Енергетичні установки та альтернативні джерела енергії: збірник тез доповідей міжнародної науково-практичної конференції (м. Харків, 2024). Харків: ФОП Бровін О. В., 2024. С. 168 – 172.

Здобувачкою систематизовано типові структури та топологію програмно-конфігурованих мереж.

46. Neronov S., Pliekhova G., Kostikova M. Use of distributed computer systems for hardware and software virtualization. Інформаційні управляючі системи і технології (ІУСТ-ОДЕСА-2024): матеріали XII Міжнародної науково-практичної конференції (м. Одеса, 2024). Одеса: Видавничий дім «Гельветика», 2024. С. 185 – 188.

Здобувачкою розроблено архітектурно-методичний підхід до використання розподілених систем для віртуалізації апаратних і програмних ресурсів.

47. Pliekhova G., Neronov S., Bogatov O. Logistics models of critical situations; their use during warfare. Social Development Towards Values Ethics – Technology – Society: Proceedings of the 10th International Interdisciplinary Scientific Conference (Wisla, Poland, Silesian University of Technology, 24.09.2024 – 26.09.2024). Pp. 90 – 91.

Здобувачкою розроблено ризик-орієнтовану логістичну модель для критичних ситуацій у воєнний час, реалізовано алгоритм динамічного перепланування.

48. Neronov S. M., Pliekhova G. A., Kostikova M. V. Virtualization in distributed systems. Математичне моделювання та інформаційні технології сучасності: матеріали міжнародної наукової конференції (Харків, 2024). ХНАДУ. Харків, 2024. С. 238 – 239.

Здобувачкою розроблено й апробовано математичну модель та IT-інструментарій для використання в інформаційно комунікаційних системах.

49. Сова О. Я., Плєхова Г. А., Неронов С. М. Методика обробки різнотипних даних в інтелектуальних системах управління мережевою та серверною архітектурою інтернету бойових речей. Наукові підсумки 2024 року: збірка наукових тез XIII наукової конференції (Харків, 2024). ПП «ТЕХНОЛОГІЧНИЙ ЦЕНТР», Харків. Х.: ПП «ТЕХНОЛОГІЧНИЙ ЦЕНТР», 2024. С. 48.

Здобувачкою запропоновано основні кроки обробки різнотипних даних.

50. Плєхова Г. А., Неронов С. М., Костікова М. В. Покращення моделі безпечної маршрутизації в програмно-конфігурованих мережах. Процеси цифровізації екосистем: матеріали міжнародної наукової конференції (Харків, 2024). ХНАДУ. Харків, 2024. С. 126 – 145.

Здобувачкою розроблено модель, метод для забезпечення безпечної маршрутизації в умовах впливу загроз.

51. Плєхова Г. А., Шубін І. Ю., Костікова М. В., Неронов С. М. Методика використання мультиагентної технології в дистанційному навчанні. Інформаційні технології в освітньому процесі ЗВО: матеріали всеукраїнської науково-методичної конференції (Харків, 2024). ХНАДУ. Харків, 2024. С. 70 – 74.

Здобувачкою обґрунтовано доцільність використання мультиагентної технології в дистанційному навчанні.

52. Шаронова Н. В., Неронов С. М., Костікова М. В., Плєхова Г. А. Процеси прийняття рішень з віртуальної логістики. Scientific achievements of contemporary society: Proceedings of the 6th International scientific and practical conference (London, 2025). Cognum Publishing House. London, United Kingdom. 2025. Pp. 287 – 292.

Здобувачкою розроблено модель і алгоритм підтримки прийняття рішень у віртуальній логістиці

53. Sharonova N. V., Neronov S. M., Kostikova M. V., Pliekhova G. A. Virtualization of software and hardware. Current trends in scientific research development: Proceedings of the 6th International scientific and practical conference (Boston, 2025). BoScience Publisher. Boston, USA. 2025. Pp. 166 – 169.

Здобувачкою систематизовано технології віртуалізації, запропоновано критерії та методику оцінювання для сучасних складних систем.

54. Плєхова Г. А., Лоцкіна Я. Г., Неронов С. М., Костікова М. В. Аналіз сучасного стану проблеми прийняття рішень у надзвичайних ситуаціях. Science in the modern world: innovations and challenges: Proceedings of the 5th International scientific and practical conference (Toronto, 2025). Perfect Publishing. Toronto, Canada. 2025. Pp. 155 – 162.

Здобувачкою виконано системний огляд і порівняльний аналіз сучасних методів прийняття рішень з ліквідації надзвичайних ситуацій.

55. Плєхова Г. А., Лоцкіна Я. Г., Неронов С. М., Костікова М. В. Методологія та інструментальні засоби створення інтелектуальних систем підтримки прийняття рішень у застосуванні до задач попередження та ліквідації надзвичайних ситуацій техногенного характеру. Science and technology: challenges, prospects and innovations: Proceedings of the 6th International scientific and practical conference (Osaka, 2025). CPN Publishing Group. Osaka, Japan. 2025. Pp. 172 – 180.

Здобувачкою розроблено методологію та інструментальний підхід з проведення попередження техногенних надзвичайних ситуацій.

56. Плєхова Г. А., Мягких Г. Г., Шишацький А. В. Аналіз основних типів кібератак в інфокомунікаційних інтелектуальних мережах. Modern management of organizations: concepts and digital transformations: Proceedings of the 12th International scientific and practical conference (Varna, 2025). International Science Group. Varna, Bulgaria. 2025. Pp. 181 – 190.

Здобувачкою систематизовано типи кібератак на інтелектуальні інфокомунікаційні мережі.

57. Vysotska V., Smelyakov K., Chupryna A., Kochkina A., Pliekhova G., Naumov A. Improving model explainability in dynamic facial expression recognition for hybrid intellectual systems / Proceedings of the Computational Linguistics Workshop (CLW-CoLInS 2025) at the 9th International Conference on Computational Linguistics and Intelligent Systems (CoLInS 2025) - Kharkiv, Ukraine, May 15-16, 2025. (SCOPUS) DOI 10.31110/COLINS/2025-1/009(Scopus).

Здобувачкою розроблено метод формування просторово-часових пояснень для моделей розпізнавання динамічних виразів обличчя та доведено підвищення інтерпретованості без критичної втрати точності.

58. Pliekhova G., Kostikova M., Gurko O., Pliekhov D. Method for creating a device for processing various heterogeneous data in decision support systems. Social Development Towards Values Ethics – Technology – Society: Book of summaries with the program of the 11th International Interdisciplinary Scientific Conference (Wisla, Poland, 2025). Silesian University of Technology, Gliwice. 2025. Pp. 106 – 107.

Здобувачкою розроблено метод, який забезпечує потокову обробку даних в інформаційних ситемах.

59. Volkov V., Shubin I., Pliekhova G., Kopytkov D., Volkova T. Decomposition of conjunctive formulas in the algebra of finite predicates for modeling logical structures of transport networks. Транспорт, екологія, сталий розвиток. ЕКОВАРНА 2025: збірник доповідей, XXXI науково – технічна конференція (Варна, 2025). ТУ-Варна. 2025. Pp. 128 – 144.

Здобувачці належить ідея застосування алгебри скінченних предикатів для моделювання логічних структур транспортних мереж.

Патенти на корисну модель:

60. Патент на корисну модель № 158804 Україна, МПК H04B 1/56 (2006.01), H04B 1/58 (2006.01), H04B 3/60 (2006.01). Пристрій утворення маршрутів передачі інформації в радіомережах спеціального призначення із можливістю самоорганізації / Кашкевич С. О., Шишацький А. В., Неронов С. М., Плєхова Г. А., Єфименко О. В., Плугина Т. В., Ільге І. Г.; власники: Харківський національний автомобільно-дорожній університет, Плєхова Г. А. – Номер заявки u 2024 04315; дата подання заявки 03.09.2024; публікація відомостей 19.03.2025, Бюл. «Промислова власність», № 12. Том 1. С. 4.29.

Здобувачкою запропоновано підхід до самоорганізованого формування та перебудови маршрутів передавання інформації у радіомережах при зміні топології та умов зв'язку.

61. Патент на корисну модель № 160507 Україна, МПК H04B 1/54 (2006.01), H04B 1/56 (2006.01), H04B 1/58 (2006.01), H04B 3/60 (2006.01). Пристрій обробки різнотипних даних в системах підтримки прийняття рішень з елементами штучного інтелекту / Кашкевич С. О., Шишацький А. В., Неронов С. М., Плєхова Г. А., Єфименко О. В., Плєхов Д. О., Багмут Р. Б., Гурко О. Г., Возниця А. С., Яценко О. О., Кочина А. А., Любий Є. В., Асаєнко Ю. С., Шаронова Н. В.; власники: Харківський національний автомобільно-дорожній університет. – Номер заявки u 2025 01406; дата подання заявки 31.03.2025; публікація відомостей 10.09.2025, Бюл. № 37.

Здобувачкою розроблено рішення щодо інтелектуальної обробки різнотипних даних, зокрема їх узгодження, попереднього аналізу та підготовки для модулів штучного інтелекту.

62. Патент на корисну модель № 160744 Україна, МПК H04B 1/54 (2006.01), H04B 1/56 (2006.01), H04B 1/58 (2006.01), H04B 3/60 (2006.01). Спосіб вибору робочих частот для безпілотних літальних апаратів в складній електромагнітній обстановці / Кашкевич С. О., Шишацький А. В., Неронов С. М., Плєхова Г. А., Єфименко О. В., Гурко О. Г., Кононихін О. С., Дмитрієва О. І., Шаронова Н. В.; власники: Харківський національний автомобільно-дорожній університет. – Номер заявки u 2024 05280; дата подання заявки 06.11.2024; публікація відомостей 08.10.2025, Бюл. № 41.

Здобувачкою запропоновано спосіб адаптивного вибору робочих частот з урахуванням рівня завад.

63. Патент на корисну модель № 160872 Україна, МПК H04B 1/54

(2006.01), H04B 1/56 (2006.01), H04B 1/58 (2006.01), H04B 3/60 (2006.01). Пристрій обробки різнотипних даних в системах підтримки прийняття рішень / Кашкевич С. О., Шишацький А. В., Неронов С. М., Плєхова Г. А., Єфименко О. В., Плєхов Д. О., Багмут Р. Б., Гурко О. Г., Возниця А. С., Пронін С. В.; власники: Харківський національний автомобільно-дорожній університет. – Номер заявки u 2025 01382; дата подання заявки 31.03.2025; публікація відомостей 15.10.2025, Бюл. № 42.

Здобувачкою розроблено принцип обробки даних для підвищення оперативності та обґрунтованості формування керуючих рішень.

64. Патент на корисну модель № 161339 Україна, МПК H04B 1/54 (2006.01), H04B 1/56 (2006.01), H04B 1/58 (2006.01), H04B 3/60 (2006.01). Пристрій для обробки різнотипних гетерогенних даних в системах підтримки прийняття рішень / Кашкевич С. О., Шишацький А. В., Неронов С. М., Плєхова Г. А., Єфименко О. В., Плєхов Д. О., Багмут Р. Б., Гурко О. Г., Возниця А. С., Пронін С. В.; власники: Харківський національний автомобільно-дорожній університет. – Номер заявки u 2025 01384; дата подання заявки 31.03.2025; публікація відомостей 26.11.2025, Бюл. № 48.

Здобувачкою запропоновано підхід до обробки даних різної структури та походження з їх подальшим приведенням до узгодженого вигляду.

АНОТАЦІЯ

Плехова Г.А. Методологічні основи створення інфокомунікаційної мережевої системи, стійкої до впливу деструктивних факторів. – на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології. – Національний технічний університет «Харківський політехнічний інститут», Харків, 2026.

У дисертаційній роботі запропонована та вирішена важлива науково-прикладна проблема створення інфокомунікаційної мережевої системи, стійкої до впливу деструктивних факторів, шляхом формування методології, методів, моделей, які лягли в основу прикладної інформаційної технології розробки мережевої системи, яка функціонує в умовах мінливого зовнішнього середовища та загроз.

Виконано огляд та аналіз існуючих підходів до створення інфокомунікаційних мережевих систем (ІМС). З урахуванням новизни проблеми сформовано мету та сформульовані завдання дослідження. Висунута нова парадигма створення стійкої ІМС, яка спирається на сформовані концептуальні принципи та науково обґрунтований комплекс методів та моделей. Створено метод синтезу мережевої системи, який дозволяє вибрати оптимальний склад системи з використанням типових, а також нових (інноваційних) компонент. Проведено топологічний синтез архітектури розподіленої мережевої системи. Створені моделі аналізу для виявлення критичних вразливостей інфраструктури мережевої системи для планування дій щодо їх мінімізації та нейтралізації. Вирішено актуальне

завдання, з використанням лексикографічного упорядкування варіантів та цілочисельного (булевого) програмування, для планування превентивних дій для відновлення стану мережевої системи в умовах її деградації та пошкодження від впливу агресивних факторів. Проведена багатокритеріальна оптимізація витрат, часу та ризику проєкту відновлення мережевої системи. Створена інтелектуальна модель для адаптації ІМС до змін зовнішнього середовища, шляхом управління її станом. Розроблено модель маршрутизації передачі даних, яка використовує мультиагентне імітаційне моделювання та ураховує ризики впливу деструктивних факторів. Створена модель управління передачею даних з використанням багатошарової нейронної мережі та машинного навчання, яка дозволяє оперативно реагувати та адаптуватися до зміни умов зовнішнього середовища.

У результаті проведених наукових досліджень створена прикладна інформаційна технологія управління розробкою та функціонуванням інфокомунікаційної мережевої системи, стійкої до впливу деструктивних факторів, яка використовує мультиагентне середовище та хмарні (CLOUD) технології.

Результати досліджень по створенню стійкої інфокомунікаційної системи впроваджено в управління вантажоперевезеннями, що забезпечує ефективність виконання плану перевезень в умовах впливу загроз, а також в розробку системи віртуального розподіленого скринінгу медичної документації військових та у навчальний процес кафедри інтелектуальних комп'ютерних систем НТУ «ХПІ» та кафедри комп'ютерних наук і інформаційних систем ХНАДУ.

Ключові слова: стійкість системи, інфокомунікаційна мережева система, концептуальні принципи стійкості, вразливості інфраструктури, архітектурний синтез, відновлення системи, обмеженість ресурсів, вплив загроз, оптимізація, імітаційне та агентне моделювання, прикладна інформаційна технологія, компараторна ідентифікація.

ABSTRACT

Plekhova G.A. Methodological foundations of creating an infocommunication network system resistant to the influence of destructive factors. – on the rights of the manuscript.

Dissertation for the degree of Doctor of Technical Sciences in the specialty 05.13.06 – Information Technologies (12 – Information Technologies). – National Technical University "Kharkiv Polytechnic Institute", Kharkiv, 2026.

The dissertation proposes and solves an important scientifically applied problem of creating an infocommunication network system resistant to the influence of destructive factors, by forming a methodology, methods, models, which formed the basis of applied information technology for developing a network system that functions in a changing external environment.

A review and analysis of existing approaches to creating infocommunication network systems is carried out. Taking into account the novelty of the problem, the goal and objectives of the study are formulated. A new paradigm for creating a

sustainable INS has been put forward, which is based on the established conceptual principles and a scientifically substantiated set of methods and models. A method for synthesizing a network system has been created, which allows choosing the optimal composition of the system using typical, as well as new (innovative) components. A topological synthesis of the architecture of a distributed network system has been carried out. Analysis models have been created to identify critical vulnerabilities of the network system infrastructure for planning actions to minimize and neutralize them. A topical task has been solved, using lexicographic ordering of options and integer (Boolean) programming, for planning preventive actions to restore the state of the network system in conditions of its degradation and damage from the influence of aggressive factors. Multi-criteria optimization of costs, time and risk of the network system restoration project has been carried out. An intelligent model has been created for adapting the INS to changes in the external environment by managing its state. A data transmission routing model has been developed, which uses agent simulation modeling and takes into account the risks of the influence of destructive factors. A management model has been created using a multilayer neural network and machine learning, which allows for rapid response and adaptation to changes in environmental conditions.

As a result of the conducted scientific research, an applied information technology for managing the development and operation of an infocommunication network system that is resistant to the influence of destructive factors, which uses a multi-agent environment and cloud (CLOUD) technologies, has been created.

The results of research on the creation of a stable infocommunication system have been implemented in freight transportation management, which ensures the effectiveness of the transportation plan under the influence of threats, as well as in the development of a system for virtual distributed medical screening of military medical documentation and in the educational process of the Department of Computer Science and Information Systems of the Kharkiv National Automobile and Road University.

Keywords: resilient system, infocommunication network system, conceptual principles of resilience, infrastructure vulnerability, architectural synthesis, system recovery, resource constraints, threat impact, optimization, simulation and agent modeling, applied information technology, comparator identification.