УДК 004.056.55:004.384.3:004.738.5
DOI https://doi.org/10.32689/maup.it.2024.1.2

Віктор БОЙКО
кандидат технічних наук, доцент, доцент кафедри кібербезпеки,
Національний університет «Одеська юридична академія», boyko-work@ukr.net
***ORCID:** 0000-0001-5929-657X*

Микола ВАСИЛЕНКО
доктор фізико-математичних наук, доктор юридичних наук, професор,
професор кафедри кібербезпеки,
Національний університет «Одеська юридична академія», vasylenko.it@journals.maup.kiev.ua
***ORCID:** 0000-0002-8555-5712*

Валерія СЛАТВІНСЬКА
доктор філософії в галузі «Право», асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія», slatvinskaya_valeriya@ukr.net
***ORCID:** 0000-0002-6082-981X*

МОДЕЛЮВАННЯ ЖИВУЧОСТІ ТА ВІДНОВЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ В УМОВАХ ДІЇ КІБЕРЗАГРОЗ

Анотація. *У статті досліджується актуальна проблема централізації та ієрархізації інформаційно-комунікаційних мереж (ІКМ), яка призвела до розробки методів оцінки та усунення слабких місць у фізичній та функціональній інфраструктурі ІКМ. Розвиток сучасних ІКМ та послуг, що базуються на них, призвів до такого рівня складності та централізації, коли глобальні системні збої та каскадні сценарії недоступності ІКМ у майбутньому стають неодмінними.*

З'ясовано, що існуючі методи моделювання відновлення ІКС можна розділити на дві категорії: аналіз факторів відновлення та аналіз структурної і/або функціональної моделі системи. Доведено, що ІКМ мають розподілену архітектуру, але спостерігається тенденція до централізації та ієрархізації. Приділено увагу специфіці ICN як інфраструктурного об'єкта.

У роботі запропоновано когнітивно-імітаційну модель відновлення ІКМ (CSM ICN), яка базується на загальній моделі CSM CTS та використовується для комплексного прогнозування та сценарного моделювання можливих збоїв та сценаріїв недоступності ІКМ. CSM ICN використовує орієнтований граф (орграф) для моделювання компонентів ICN та зв'язків між ними. Модель може бути «мережевою» (з акцентом на зв'язки) або гібридною (з додаванням «віртуальних вузлів» для причинно-наслідкових зв'язків). Кожен вузол моделює частину ICN, її елемент або робочий компонент. Вузли мають характеристики, що включають час і характер відновлення. Модель використовує критерій Бірнбаума для оцінки впливу виходу з ладу одного елемента на інші. Відновлення вузла моделюється як змінне число кроків дискретного часу. Модель використовує три типи функцій відновлення для різних рівнів підготовленості систем і має 4 рівні оцінки. Модель може оцінювати каскадні сценарії, коли вихід з ладу одного елемента призводить до збоїв в інших частинах ICN.

Висновки. *Отже, моделювання сценаріїв відновлення й перезапуску ІКМ дозволить виявити потенційні вразливості, аналізувати каскадні сценарії недоступності ІКМ у випадку дії надзвичайних подій та природних форс-мажорів. Застосування CTS ICN сприятиме значному підвищенню живучості та стійкості експлуатації ІКМ в умовах зовнішніх атак, помилок персоналу та впливу інших надзвичайних подій та форс-мажорів.*

Ключові слова: *інформаційно-комунікаційні системи, стійкість, живучість, когнітивно-імітаційна модель, моделювання відновлення, кібератаки, інфраструктурні мережі.*

Viktor BOYKO, Nikolai VASILENKO, Valeriia SLATVINSKA. MODELING THE SURVIVABILITY AND RECOVERY OF INFORMATION AND COMMUNICATION NETWORKS IN THE FACE OF CYBER THREATS

Abstract. *The article examines the pressing issue of centralization and hierarchization in information and communication networks (ICNs), which has led to the development of methods for assessing and addressing weaknesses in the physical and functional infrastructure of ICNs. The advancement of modern ICNs and the services based on them has resulted in such complexity and centralization that global systemic failures and cascading scenarios of ICN unavailability in the future become inevitable.*

It has been established that existing methods for modeling ICN recovery can be divided into two categories: recovery factor analysis and analysis of the structural and/or functional model of the system. It is proven that ICNs have a distributed architecture, but there is a tendency towards centralization and hierarchization. Attention is paid to the specificity of ICNs as an infrastructure object.

The paper proposes a cognitive-emulation model for ICN recovery (CSM ICN), which is based on the general CSM CTS model and is used for comprehensive forecasting and scenario modeling of possible failures and unavailability scenarios of ICNs. CSM ICN utilizes a directed graph (digraph) to model ICN components and their connections. The model can be "network-centric" (emphasizing connections) or hybrid (adding "virtual nodes" for cause-and-effect relationships). Each node models a part of

the ICN, its element, or working component. Nodes have characteristics that include recovery time and nature. The model uses the Burnbaum criterion to assess the impact of one element's failure on others. Node recovery is modeled as a variable number of discrete time steps. The model uses three types of recovery functions for different levels of system readiness and has 4 levels of evaluation. The model can assess cascading scenarios where the failure of one element leads to failures in other parts of the ICN.

Conclusions. *Thus, modeling recovery and restart scenarios of ICNs will help identify potential vulnerabilities, analyze cascading scenarios of ICN unavailability in case of emergencies and natural disasters. The application of CTS ICN will significantly increase the resilience and operational stability of ICNs in conditions of external attacks, personnel errors, and the impact of other emergencies and force majeure events.*

Key words: *information and communication systems, resilience, survivability, cognitive simulation model, recovery modeling, cyberattacks, infrastructure networks.*

Актуальність проблеми. Питання стійкості та живучості інформаційних систем нині набуває дедалі більшої актуальності. Більшість наявних інформаційно-комунікаційних систем (ICN) після введення в експлуатацію піддається атакам різного роду і характеру [1] і з великою ймовірністю можуть бути зламані, або виведені з ладу. У разі, якщо зламу або іншим несприятливим впливам піддаються глобальні інформаційні системи, або інформаційні системи, що обслуговують індустріальні та промислові комплекси (industrial control system – ICS) ризики і масштаби збитку багаторазово збільшуються.

Донедавна основним фокусом небезпеки були розробники промислових та інфраструктурних інформаційних систем, які, на відміну від розробників ПЗ «загального призначення», запізнюються з реакцією на нові загрози. Наприклад, під час аналізу безпеки ICS, багато фахівців схильні покладатися на т.зв. «air gap» – «повітряний отвір», що ізолює ICS від глобальних інформаційно-комунікаційних систем. Простіше кажучи – якщо керівна система не підключена до інтернету – звідти не може здійснюватися атака. При цьому один із найперших прикладів атаки – вірус Stuxnet, якраз був побудований на подоланні «повітряного отвору» [2].

Однак останнім часом почастішали збої глобальних інформаційних мереж. На думку авторів це наслідок кількох причин.

По-перше, відбувається вибуховий ріст обсягу та складності ІКТ. Forbes наводить наступні дані щодо мобільних операторів в Україні: 19 мільйонів абонентів Vodafone [3], 8,9 мільйона у Lifecell [4], 24 мільйони у Київстар [5]. За тими ж даними, Lifecell має близько 9000 базових станцій.

По-друге, спостерігається тенденція до централізації та ієрархізації ІКТ. Розвиток технологій та еволюція інформаційно-комунікаційних мереж сприяють все більшій централізації та ієрархізації наявних мереж [6]. Телефонна мережа минулого була відносно децентралізованою системою – при руйнуванні міжміських зв'язків міські телефонні мережі продовжували функціонувати у незалежному режимі, а також залишалася можливість підключень «в обхід» системи. Тепер, як показує практика, «падіння головного офісу» призводить до відключення всієї мережі на рівні країни [7], [8]. У поточному випадку відключення було здійснене вручну, щоб запобігти поширенню кібератаки [8] на ядро системи, однак, враховуючи досвід масштабних збоїв минулого, можна передбачити, що в сучасній централізованій і ієрархічній структурі ІКТ існує ймовірність повного виходу мережі з ладу внаслідок збою, атаки або іншого негативного впливу.

По-третє, досвід безперебійної роботи мобільних та інтернет-мереж призвів до того, що багато різних служб у будь-який спосіб використовують їх як частину своєї інфраструктури. Перш за все це стосується банківської сфери – банкомати, термінали поповнення, POS-термінали в більшості своєму використовують для зв'язку з банком мобільний зв'язок, і при виході з ладу мобільної мережі перестають функціонувати. Сюди також відноситься широко поширена як «просувана технологія безпеки» двофакторна аутентифікація, при якій підтвердження особи користувача відбувається за допомогою SMS-повідомлень. Згідно з джерелами Forbes у ПриватБанка під час відключення «Київстар» не працювало до третини POS-терміналів та близько 5% банкоматів. Це найбільш поширені випадки, однак глобальний збій зв'язку показав, що існують й інші вразливі системи. Зокрема, ЛКП «Львівсвітло» було змушено виконувати відключення ліній вуличного освітлення в ручному режимі [9].

У роботі [10], яка була опублікована ще до початку повномасштабного вторгнення, зроблено такий висновок: «В умовах впливу нових загроз стає важливим не лише управління ліквідацією безпосередніх наслідків загроз, але й боротьба за функціональну живучість з метою запобігання розпаду системи. Внаслідок нових загроз системи можуть безпосередньо виходити з ладу не лише самі системи, а й породжувати «вторинні ефекти», що впливають на суміжні системи. Для загального розпаду інформаційної системи внаслідок нових загроз часто не потрібно, щоб було виведено з ладу 100% її підсистем, а достатньо просто створити зниження працездатності одного або кількох ключових компонентів системи».

Наступні події (чорні вибухи, втрата функціональності систем через бойові дії, нещодавнє відключення мобільного зв'язку «Київстар») підтвердили актуальність викладених у статті положень.

Усе перераховане підкреслює актуальність проблеми забезпечення живучості сучасних інформаційно-комунікаційних мереж та гостро постає питання про надійність і живучість інфраструктурних систем.

Важливою складовою розв'язання проблеми живучості та стійкості ІКМ є розроблення методології комплексного прогнозування і сценарного моделювання можливих збоїв та сценаріїв каскадного виходу зі строю інформаційно-комунікаційних мереж.

Аналіз останніх досліджень і публікацій. У роботі [10] йдеться про те, що сучасні системи «розумний будинок» страждають від фрагментації та прив'язки до постачальника, що ускладнює їх використання, збільшує витрати та знижує рівень безпеки. Натомість авторами запропоноване рішення – модульна система з відкритими протоколами, натхненна глобальними інформаційними системами, що забезпечує взаємодію та незалежну розробку. У роботі [26] запропоновано методику оцінки ризиків та загроз для ICS, розроблено когнітивно-імітаційну модель ICS, запропоновані методи та моделі можуть бути використані для підвищення живучості та стійкості ICS, а також встановлено, що використання даних методів дозволить суттєво підвищити живучість та стійкість ICS. У роботі [27] розглядається питання моделювання кібернетичної складової живучості складних технічних систем. Автор пропонує підхід до моделювання, який ґрунтується на системному аналізі та імітаційному моделюванні.

Метою статті є наукове обґрунтування розробки когнітивно-імітаційної моделі (КІМ) для оцінки стійкості та живучості ІКС шляхом вирішення наступних завдань:

– огляд наявних методів моделювання відновлення інфраструктурних мереж;

– визначення специфіки ІКС як інфраструктурного об'єкта;

– обґрунтування доцільності використання когнітивно-імітаційної моделі (КІМ) для оцінки стійкості та живучості ІКС.

Виклад основного матеріалу.

Існуючі методи моделювання відновлення інфраструктурних мереж

Кількісна оцінка стійкості, надійності та живучості ІКМ є складним питанням і може розглядатися як частковий випадок більш загальної моделі руйнування та відновлення складних технічних систем.

Протягом деякого часу це питання в основному розглядалося в описовому ключі, при цьому об'єктом моделювання слугували процеси руйнування, стійкості та відновлення комунальної інфраструктури (житлового фонду, водопроводу, системи енергопостачання). При цьому як природні катастрофи і психологічні фактори розглядалися стихійні лиха – переважно землетруси. Наприклад, робота [11] описує вплив стихійних лих переважно у якісному вигляді.

Однак у роботах [12] та [13], які вважаються класичними [14], математична модель вже використовується для оцінки часу та процесів відновлення після стихійного лиха. Аналогічно, робота [15] присвячена моделюванню процесів відновлення інфраструктури після землетрусів.

У роботі [16] була запропонована парадигма, в рамках якої виділяються чотири виміри системи – технічний, організаційний, соціальний і економічний – всі з яких можна використовувати для кількісної оцінки показників стійкості різних типів фізичних і організаційних систем. Також автор виділяє живучість в умовах впливу стихійних лих та психологічних факторів, як поєднання двох аспектів – стійкості системи до впливу стихійних лих та психологічних факторів і швидкості відновлення працездатності системи. Аналогічний поділ був зроблений у роботі [17], проте там живучість системи моделювалась також з урахуванням управління системою.

У роботі [1] вводиться досить загальна класифікація того, що можна розуміти під НВ та ПФ. Автори класифікують ці події наступним чином:

– природні небезпеки та стихійні лиха;

– атаки зловмисників, які додатково поділяються на низькочастотні – зломи та проникнення в систему, і високочастотні у вигляді кібератак (найбільш характерні – DDOS, brute-force атаки на пароль і т. д.);

– людські помилки;

– технічні збої (виходить з ладу обладнання);

– комплексні події, що містять одну, кілька або всі перелічені категорії.

У сучасний час до цього списку потрібно додати бойові дії, як результати безпосереднього та опосередкованого виведення з ладу обладнання.

У роботі [18] надано огляд поточного стану концепцій моделювання відновлення після катастроф (Conceptions for Disaster Recovery Modeling – CDRM). Автор відносить до CDRM наступні вісім концепцій:

– моделювання з обмеженими ресурсами,

– машинне навчання,

– моделювання динамічного економічного впливу,

– моделювання системної динаміки,

– агентне моделювання,

– дискретно-подійне моделювання,

– стохастичне моделювання,

– мережеве моделювання.

У роботі [1] була зроблена спроба метааналізу останніх наукових робіт у цій області та загальної категоризації наявних підходів. Основних категорій виділено дві – системні та мережеві.

Системна категорія підходів базується на урахуванні причинно-наслідкових зв'язків і моделюванні їх впливу на досліджувану систему. При цьому, як правило, всі намагаються звести до якихось числових показників, наприклад, коефіцієнтів живучості.

Мережева категорія – це уявлення системи у вигляді якої-небудь топології, використання при цьому статистичних даних про те, як ця система (або системи) себе веде в минулому та дослідження її методами математичної оптимізації.

Також у цій роботі була спроба «остаточно уточнити» поняття живучості, ризику, надійності, вразливості та стійкості.

Ще однією корисною концепцією, детально описаною в роботі, є концепція «цифрових близнюків» (DT) – цифрових подвійок, коли робота реальної інфраструктурної системи дублюється «цифровою системою», при якій кожен реальний компонент або агрегат системи має свого «цифрового подвійника» за термінологією концепції. Таким чином, утворюється віртуальна модель, яку доповнюють даними в режимі реального часу, що відображає стан реальної системи й дозволяє приймати рішення з профілактики, лікування та відновлення системи в умовах впливу НВ та ПФ.

З аналізу вищевказаного випливає, що наявні підходи до оцінки живучості, стійкості та відновлення ICN, як частинний випадок DT, можна розділити на дві основні категорії – аналіз факторів відновлення (системний підхід за термінологією) і аналіз структурної й/або функціональної моделі системи (мережевий підхід за термінологією).

Автор підкреслює, що для кожної конкретної системи не існує єдиного правильного підходу. Якщо порівняти переваги підходів, то найбільші переваги від структурної/функціональної моделі можна отримати у випадках, коли система має розвинену мережеву структуру або функціональні зв'язки. У цьому випадку модель може бути легко побудована на основі реальної схеми структури або функціональних зв'язків, що дозволяє «економити» на розкладанні системи на окремі компоненти (або агрегати, якщо мова йде про складну технічну систему).

Для багатофакторного аналізу підходять випадки, коли є достатня кількість експертів, щоб отримати експертну оцінку, і коли фактори, що впливають на стан (стійкість, живучість, відновлення) системи, визначені та класифіковані.

Специфіка ICN як інфраструктурного об'єкта

З урахуванням усього перерахованого вище, слід виділити специфіку роботи ICN, з одного боку, як інфраструктурної мережі, яка є частковим випадком інфраструктурних мереж, розглянутих вище, а з іншого – має свої власні особливості, характерні саме для ICN.

Хоча до цього часу панує досить поширене уявлення про ICN як мережі, що розподіляється та має розподілену архітектуру, як зазначалося вище, в наш час спостерігається тенденція до централізації та ієрархізації ICN. Здешевлення обладнання та збільшення обсягів зв'язку, разом із постійно зростальним попитом на обчислювальні потужності, канали зв'язку з високою пропускною здатністю та віддалений збір та обробку інформації призвели до того, що апаратна інфраструктура розвивалась непропорційно, без акценту на розподіленість та стійкість. У провайдерів та постачальників послуг склалося обманливе враження про надійність та безперебійність сервісів.

Протягом певного часового інтервалу розвитку ICN мережі справді були досить надійними та стійкими, однак зі зростанням складності та централізації систем їх надійність почала зменшуватись. У цьому розумінні цікаво спостерігати за історією глобальних вибоїв. Зазвичай вибої в ICN відбуваються постійно, однак, до нещодавнього часу, завдяки децентралізованому та розподіленому характеру ICN, їх наслідки та шкоду було місцевими, а самі вибої досить швидко усувалися або обмежувалися їх наслідки.

Один із перших глобальних випадків відмови стався із Skype [19] – система була недоступною протягом двох днів, а саму відмову, за поясненням корпорації, викликав аномально великий обсяг перезапусків після того, як користувачі завантажили оновлення безпеки Windows. Представник корпорації пояснив це так: «Велика кількість перезавантажень позначила на мережеві ресурси Skype. Це призвело до потоку запитів на вхід до системи, що в поєднанні з нестачею ресурсів піринговой мережі викликало ланцюгову реакцію, яка мала критичні наслідки» [20]. Важливо зазначити – відмова не була викликана усвідомленою атакою хакерів або відмовами в критично важливій інфраструктурі (наприклад, перебоями з електропостачанням) – це був наслідок складної взаємодії кількох підсистем єдиної системи. При цьому відновлення функціональності сервісу зайняло тривалий час.

Наступна глобальна відмова сталася 21 вересня 2015 року [21] і тривала понад 15 годин, і знову не була результатом кібератаки або стихійних лих. У блозі корпорації з'явилось наступне пояснення [22]: «Ми випустили зміну конфігурації, яка була більшою, ніж зазвичай, і яку деякі версії Skype не змогли правильно обробити, що призвело до відключення користувачів від мережі. Коли ці користувачі

намагалися знову під'єднатися, виникала велика кількість трафіку, і деякі з вас не могли користуватися безкоштовними послугами Skype, такими як обмін повідомленнями, присутність та керування списком контактів. Інші взагалі не могли увійти в Skype або вийти з нього, а також здійснювати дзвінки на стаціонарні або мобільні телефони».

Слід відзначити, що власники глобальних систем чим далі, тим менш охоче розкривають причини та подробиці відмов, що сталися.

Наступним значним випадком відмов були відмови Facebook – у 2019 [23] та 2021 роках [24]. При цьому відмова призводила до відключення не лише Facebook, але й суміжних проектів – Instagram, WatsApp і т.д. Подібні відмови у більшості сучасних глобальних сервісів сталися протягом останніх кількох років, і кожний раз відмова якої-небудь платформи послужила причиною відмови інших сервісів.

Найбільш помітною була відмова в роботі Amazon[25]. Оскільки сервіс AWS є хостингом для інших сервісів, то відмова в роботі Amazon призвела до відмови в роботі мережі доставлення контенту CDN, крім того, відключилися такі сайти, як Stack Overflow, GitHub, gov.uk, Hulu, HBO Max, Quora, PayPal, Vimeo і Shopify.

Перелічені вище сервіси виходили з ладу в основному через внутрішні помилки – в кожному випадку за повідомленнями їх представників та пресслужб. Однак, варто нагадати, що існують прецеденти цілеспрямованих атак на інфраструктуру. Найбільш відомий – епідемія вірусів WannaCry і Petya. Відомими прикладами подібних відмов є вірус Triton, який був націлений на атаку «останнього рубіжу оборони» – виведення з ладу приладових систем безпеки (SIS) Schneider Triconex, а також епідемії WannaCry, Petya та пов'язані з ними відмови в українській енергосистемі у 2015 році.

Отже, можна стверджувати, що сучасні ІКС та сервіси, що ґрунтуються на них, досягли такого рівня складності та централізації, що подібні збої є неминучими у майбутньому, а їх масштаб буде зростати. У зв'язку з цим набуває максимальної актуальності розробка систем та методів, які дозволяють оцінювати ймовірність збою, визначати слабкі та уразливі місця в фізичній та функціональній інфраструктурі ІКС.

При цьому складність й ієрархізація ІКС дозволяють розглядати їх як частковий випадок складних технічних систем (СТС) та використовувати для аналізу та моделювання їх поведінки когнітивно-імітаційну модель СТС (КІМ СТС), адаптовану під специфіку та особливості роботи ІКС – КІМ ІКС.

Для оцінки можливостей відновлення ІКС після впливу НВ та ПФ суттєво підвищити точність моделі можна було б використовуючи обидва підходи, описані у [1], у поєднаній, гібридній моделі, яка базувалася б на концепції когнітивно-імітаційної моделі складної технічної системи (cognitive-simulation models of complex technical systems CSM CTS), описаній у [17], а також у загальній структурі КІМ, викладеній у [26].

CSM відновлення стійкості ICN

Розглянемо принципи CSM CTS у застосуванні до ICN. Основою такої моделі [26] є орієнтований граф (орграф). Вузли орграфа моделюють компоненти системи ICN, спрямовані ребра (дуги) – зв'язки між компонентами. Залежно від рівня моделювання, така модель з різною точністю і достовірністю відображає взаємодію складових системи, при цьому дуги можуть розглядатися у різних функціональних ролях. Такий підхід дозволяє гнучко перебудовувати CSM CTS згідно з вимогами моделювання.

Якщо в орграфі CSM CTS зв'язки між елементами розглядаються як зв'язок її компонентів за ресурсом, відповідному категоріям стійкості системи («енергія» – «інформація» – «речовина»), то модель має структурно-функціональний акцент («мережевий» за термінологією [1]). Модель допускає використання спеціальних вузлів («віртуальні вузли» за визначенням авторів), які моделюють причинно-наслідкові зв'язки та відносини між компонентами [27] – додавання таких вузлів дозволяє доповнити модель елементами багатофакторного аналізу і отримати гібридну CSM ICN, що використовує «мережеву модель» відновлення ICN, розширену за допомогою віртуальних вузлів, які моделюють причинно-наслідкові зв'язки та залежності від зовнішніх факторів.

Кожен з вузлів системи в рамках моделі відновлення може представляти частину ICN, її елемент або окремий робочий компонент робочої підсистеми. При цьому цей вузол в рамках моделі має характеристики, що включають час і характер відновлення елемента. Запропонована методика оцінки часу відновлення використовує безрозмірні невимірні оцінки «важливості», «уразливості» елемента з погляду загальної задачі мінімізації часу відновлення системи в цілому. Така оцінка ґрунтується на критерії Бірнбаума [28], що визначає частку елементів, на які впливає виходження з ладу розглянутого елемента – чим більше ця частка, тим більше кількість елементів буде заторкнута виходом з ладу даного елемента.

Якщо в моделі використовується дискретний час, то відновлення вузла моделюється як змінне за певним законом число кроків, за які вузол змінює свою функціональність. Окрім зміни функціональності, в моделі передбачено моделювання процесу перезапуску, яке також задається у вигляді послідовності й числа кроків дискретного часу, витрачених на виходження вузла на повне функціонування після його відновлення. Якщо в моделі використовується не дискретний, а неперервний час, то як схеми відновлення вузла може бути прийнята класифікація, наведена у [29], в якій відновлення різних за рівнем підготовленості систем відповідає різним функціям.

$$f_{rec}(t) = ae^{-b\frac{t-t_{0E}}{T_{Я}}} \quad (1)$$

$$f_{rec}(t) = a\left(\frac{t-t_{0E}}{T_{Я}}\right) + b \quad (2)$$

$$f_{rec}(t) = \frac{a}{2}\left(1 + cos\left(\pi b\frac{t-t_{0E}}{T_{Я}}\right)\right) \quad (3)$$

де:

$f_{rec}(t)$ – функція відновлення, що виражає готовність системи до відновлення;

a, b – є постійними значеннями, які обчислюються з використанням кривої, що відповідає доступним даним;

t_{0E} – момент часу, коли відбувається екстремальна подія;

$T_{Я}$ – час відновлення, необхідний для повернення до стану, що передував катастрофі, оцінюваний починаючи з t0E.

При цьому (1) – експоненційна залежність – добре підготовлена система, (2) – лінійна залежність – середньо підготовлена система, (3) – тригонометрична залежність – не дуже добре підготовлена система.

Розподіл за рівнями CSM ICN відповідає розподілу за рівнями у базовій моделі CSM CTS [26] і ґрунтується на розподілі оцінок за різними рівнями.

На загальному рівні оцінюється лише топологія і структура системи в цілому – без врахування реальних характеристик її елементів. Така оцінка є заздалегідь зайвою і моделює «найгірший сценарій» розвитку подій, встановлюючи «потолок» у системній оцінці ролі та важливості елемента.

На рівні оцінки критичності вводиться поняття критичності – елементам на основі експертної оцінки може бути присвоєно значення, що визначає важливість і критичність даного елемента для загальної тривалості відновлення ICN. Залежно від зміни критичності елементів з'являється можливість отримати оцінку тривалості відновлення не за загальною, а за реальною системою – з урахуванням ролі і важливості кожного з її елементів.

На рівні оцінки витрат часу на відновлення враховується не лише положення і роль елемента в системі, а й його власні характеристики відновлення та залежність від ступеня працездатності та часу відновлення інших вузлів системи. Кінцевою інтегральною оцінкою внеску елемента в оперативність відновлення системи є математичне очікування часу відновлення для даного об'єкта.

На реальному рівні моделюється вплив несприятливих факторів на систему, максимально точно відображуючи реальність, що дає можливість оцінити можливі наслідки для швидкості відновлення при виході з ладу тих чи інших елементів ICN і сценарії розвитку негативних наслідків, включаючи каскадні сценарії – коли вихід однієї системи призводить до перерозподілу навантаження на залишені системи і призводить до послідовних збоїв по всьому простору ICN [30].

Висновки. Наразі спостерігається тенденція до централізації та ієрархізації ICN, що призвело до непропорційного розвитку інфраструктури ICN без акценту на розподіленість та стійкість. Сучасні ICN та сервіси, що ґрунтуються на них, досягли такого рівня складності та централізації, що у майбутньому необхідні глобальні системні збої та каскадні сценарії виходу ICN з ладу. Це підтверджує аналіз прецедентів, наведений у роботі. У зв'язку з цим набуває максимальної актуальності розробка систем та методів, які дозволяють оцінювати ймовірність збою, визначати слабкі та вразливі місця в фізичній та функціональній інфраструктурі ICN.

У роботі пропонується когнітивно-імітаційна модель відновлення ICN (CSM ICN), заснована на загальній моделі CSM CTS, в якій поєднуються мережевий та загальний підходи до оцінки часу та сценаріїв відновлення працездатності ICN методами комплексного прогнозування та сценарного моделювання можливих збоїв та каскадних сценаріїв виходу ICN з ладу.

Моделювання сценаріїв відновлення працездатності та перезапуску ICN дозволить виявити можливі вразливості в ICN, проаналізувати каскадні сценарії виходу ICN з ладу в умовах дії НВ та ПФ, що в свою чергу дозволить усунути ці вразливості шляхом прийняття заходів організаційного та технічного характеру (дублювання критично вразливих вузлів, усунення вузьких місць, використання гнучких алгоритмів перерозподілу навантаження тощо). Таким чином, використання CTS ICN дозволить суттєво підвищити живучість та стійкість експлуатації ICS в умовах дії зовнішніх атак, помилок персоналу та впливу інших НВ та ПФ.

Список використаних джерел:

1. Балашова Л., Галкін А., Мельник Т., Шевчук С. Найбільший збій за останні роки: оператор Kyivstar із 24 млн абонентів не працює. Імовірна причина – кібератака. Що відомо. URL: https://forbes.ua/innovations/naybilshiy-zbiy-za-ostanni-roki-operator-kiivstar-iz-24-mlnabonentiv-ne-pratsyue-imovirna-prichina-kiberataka-shcho-vidomo-12122023-17826.

2. Бойко В. Д. Моделювання кібернетичної складової живучості складних технічних систем / Матеріали Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2014), 23–25 вересня 2014 року. Одеса, 2014. С. 239–241.

3. Бойко В. Д. Оцінка живучості та стійкості компонентів інформаційних систем за допомогою когнітивно-імітаційного моделювання / Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття (до 25-річчя Національного університету «Одеська юридична академія» та 175– річчя Одеської школи права) / ed. by Ківалов С. В. Одеса: Видавничий дім «Гельветика», 2022. С. 746–749.

4. Інформація про Kyivstar – Forbes Ukraine. URL: https://forbes.ua/profile/kiivstar-244

5. Інформація про Lifecell – Forbes Ukraine. URL: https://forbes.ua/profile/lifecell-574

6. Інформація про Vodafone. Forbes Ukraine. URL: https://forbes.ua/profile/vodafone-251

7. Масштабний збій у роботі Київстар – з якими проблемами стикнулись у регіонах – УНІАН. URL: https://www.unian.ua/incidents/masshtabniy-zbiy-u-roboti-kijivstar-z-yakimiproblemami-stiknulis-u-regionah-12481575.html

8. Некряч О. Ієрархічні системи управління конвергентними мережами // Зв'язок. – Міністерство зв'язку України, 2015. – Is. 5. P. 11–13.

9. Через несправність мобільного оператора Київстар відключення вуличного освітлення відбуваються в ручному режимі – Львівська міська рада. URL: https://cityadm.lviv.ua/news/city/housing-and-utilities/299531-cherez-nespravnistiu-mobilnoho-operatorakyivstar-vidkliuchennia-vulychnoho-osvitlennia-vidbuvaiutsia-v-ruchnomu-rezhymi

10. AP Agency by. Skype blackout due to surge of reboots. 2007. URL: https://www.latimes.com/archives/la-xpm-2007-aug-21-fi-skype21-story.html.

11. Arak V. The Microsoft Connection Clarified. 2007. URL: https://web.archive.org/web/20080220105941/http://heartbeat.skype.com/2007/08/ the_microsoft_connection_explained.html.

12. Barrett C., Beckman R., Channakeshava K., Huang F., Kumar V. S. A., Marathe A., Marathe M. V., Pei G. Cascading failures in multiple infrastructures: From transportation to communication network / 2010 5th International Conference on Critical Infrastructure (CRIS). – IEEE, 2010

13. Barzashka I. Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme // The RUSI Journal. – Taylor & Francis, 2013. – Vol. 158, no. 2. P. 48–56.

14. Bi W., MacAskill K., Schooling J. Old wine in new bottles? Understanding infrastructure resilience: Foundations, assessment, and limitations // Transportation Research Part D: Transport and Environment. – Elsevier BV, 2023. – Vol. 120. P. 103–793.

15. Boyko V., Rudnichenko N., Kramskoy S., Hrechukha Y., Shibaeva N. Concept Implementation of Decision Support Software for the Risk Management of Complex Technical System // Advances in Intelligent Systems and Computing: Selected Papers from the International Conference on Computer Science and Information Technologies, CSIT 2016, September 6-10 Lviv, Ukraine» / ed. by Shakhovska N. – Cham: Springer International Publishing, 2017. P. 255–269.

16. Boyko V., Vasilenko M., Slatvinska V. Survivability and sustainability of smart city information system components // Municipal economy of cities. – O.M. Beketov National University of Urban Economy in Kharkiv, 2021. – Vol. 6, no. 166. P. 20–27.

17. Bruneau M., Chang S. E., Eguchi R. T., Lee G. C., O'Rourke T. D., Reinhorn A. M., Shinozuka M., Tierney K., Wallace W. A., Winterfeldt D. von. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities // Earthquake Spectra. – SAGE Publications, 2003. – Vol. 19, no. 4. P. 733–752.

18. Cimellaro G. P., Reinhorn A. M., Bruneau M. Framework for analytical quantification of disaster resilience // Engineering Structures. – Elsevier BV, 2010. – Vol. 32, no. 11. P. 3639– 3649.

19. Dent S. Amazon, Reddit, Twitter and Twitch Impacted by Huge Network Outage. URL: https://www.engadget.com/amazon-reddit-twitter-twitch-fastly-outage-131112143.html.

20. Harihara J. Skype Outage: An Update, and an Apology. 2015. URL: https://web.archive.org/web/20151204065003/http://heartbeat.skype.com/2015/09/ skype_outage_an_update_and_an.html.

21. Isaac M., Conger K. Facebook, Instagram and WhatsApp Suffer Outages. 2019. URL: https://www.nytimes.com/2019/03/14/technology/facebook-whatsapp-outage.html.

22. Isaac M., Frenkel S. Facebook and Instagram Are Down for Many Users. URL: https://www.nytimes.com/2021/10/04/technology/facebook-down.html.

23. Isumi M., Nomura N., Shibuya T. Simulation of Post-Earthquake Restoration of Lifeline Systems // International journal of mass emergencies and disasters. 1985. – Vol. 3, no. 1. P. 87–105.

24. Kates R. W. Assessing the Assessors: The Art and Ideology of Risk Assessment // Ambio. 1977. – Vol. VI, no. 5. P. 247–252.

25. Kates R. W. Dealing With Disaster // Science Year. 1976. P. 166–179.

26. Kates R. W., Pijawka D. From Rubble to Monument: The Pace of Reconstruction // Reconstruction Following Disaster / ed. by Haas J. E., Kates R. W., Bowden M. J. – Cambridge, MA: MIT Press, 1977. P. 1–23.

27. Miles S. B., Burton H. V., Kang H. Community of Practice for Modeling Disaster Recovery // Natural Hazards Review. – American Society of Civil Engineers (ASCE), 2019. – Vol. 20, no. 1.

28. Rausand M., Høyland A. System Reliability Theory: Models, Statistical Methods, and Applications, Second Edition / 2nd ed. – Wiley-Interscience, 2003.

29. Scott M. Skype Service Disrupted for Some Users Worldwide. 2015. URL: https://www.nytimes.com/2015/09/22/technology/skype-service-disrupted-for-some-usersworldwide.html.

30. Sobhaninia S., Buckman S. T. Revisiting and adapting the Kates-Pijawka disaster recovery model: A reconfigured emphasis on anticipation, equity, and resilience // International Journal of Disaster Risk Reduction. – Elsevier BV, 2022. – Vol. 69. P. 102–738.