Національний аерокосмічний університет імені М. Є. Жуковського
«Харківський авіаційний інститут»
Харківський національний університет імені В. Н. Каразіна
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ІВАНЧЕНКО ОЛЕГ ВАСИЛЬОВИЧ

УДК 629.039.58:681.518.22

ДИСЕРТАЦІЯ
«МЕТОДОЛОГІЧНІ ОСНОВИ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР»

Спеціальність 05.13.06 – інформаційні технології
(Технічні науки)

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. _____ О. В. Іванченко
підпис

Науковий консультант: Харченко Вячеслав Сергійович доктор технічних наук, професор

Харків – 2021

АНОТАЦІЯ

Іванченко О. В. Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології (Технічні науки). – Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» Міністерства освіти і науки України; Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2021.

У дисертації розкрито основні положення методології та технології спільного забезпечення готовності хмарних систем і критичних інфраструктур з урахуванням можливостей щодо оперативного моніторингу, оцінювання їхнього стану, захисту фізичних і кібернетичних активів при відмовах і атаках на вразливості. Викладено основні формальні ознаки дисертаційного дослідження, які включають існуюче протиріччя, науково-прикладну проблему, наукову новизну та практичну значущість роботи.

У першому розділі всеобічно висвітлено проблему забезпечення та оцінювання готовності хмарних систем критичних інфраструктур. Виконано аналіз можливостей застосування хмарних систем в контурі управління критичних інфраструктур (КІ). За результатами аналізу встановлено як хмарні системи можуть впливати на функційну та інформаційну безпечність КІ. У якості прикладу було розглянуто ключові фактори ненадійності критичної енергетичної інфраструктури та морської критичної інфраструктури. Додатково розглянуто тенденції розвитку концепцій, методів, інформаційних технологій оцінювання, забезпечення надійності та безпеки хмарних систем КІ. Розділ завершується вибором математичного апарату та обґрунтуванням методології наукових досліджень.

У другому розділі наведено основні положення методології оцінювання готовності та вибору характеристик хмарних систем критичних інфраструктур, яка розвиває концепцію фон Неймана побудови систем високої готовності з недостатньо надійних і безпечних компонентів. Структурно методологія складається з принципів, моделей, методів оцінювання функційної безпечності, методів забезпечення готовності, методів вибору, оцінки характеристик готовності та енергоефективності хмарних систем КІ. Значна увага в уперше розробленій методології приділяється інформаційній технології тестування регіональних хмарних систем з інтегрованими фізичними компонентами, за допомогою якої визначають час затримки інформаційних потоків даних з застосуванням віртуального ресурсу реляційних баз даних, що дозволяє здійснити оптимальний вибір інформаційного центру відповідного хмарного провайдера за критерієм мінімуму часу затримки.

Згідно запропонованої концепції негативні впливи на активи КІ представляються у вигляді зловмисних шкідливих впливів та проникнень, на реалізацію яких впливають зовнішні і внутрішні фактори природнього та штучного походження. Відомо, що різноманітні негативні події у вигляді зловмисних шкідливих проникнень, відмов, збоїв, дефектів погіршують функційну та інформаційну безпечність критичних інфраструктур. Безумовно це призводить до зниження рівня готовності, збільшує ризик негативних впливів на активи інфраструктури та сприяє виникненню аварій КІ з важкими наслідками. За результатами виконаних досліджень побудовано та вдосконалено логіко-ймовірісну модель ризику негативних впливів на активи КІ та здійснено перехід до оцінної моделі.

У третьому розділі розглянуто аналітико-стохастичні моделі готовності КІ, які отримано на основі використання апарату формалізації процесів зміни інформаційно-технічних станів інфраструктурних компонентів та врахування негативних факторів зовнішнього і внутрішнього впливу на їхню безпеку. Запропоновані моделі побудовано на основі формалізації процесів, які впливають на функційну та інформаційну безпечність критичних інфраструктур.

Відповідно до загальної концепції дослідження розроблено оцінні моделі надійності критичної енергетичної інфраструктури з системою контролю інформаційно-технічних станів. При розробці напівмарковських моделей враховано можливості щодо створення сучасної інтегрованої системи моніторингу інформаційно-технічних станів хмарних систем на основі розгортання мереж мікросервісів і віртуальних моніторів. Зазначені обставини сприяли процесу побудови вдосконалених напівмарковських моделей готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин, що дозволило за результатами моделювання виконати обгрунтування граничних величин показників готовності хмарної інфраструктури з урахуванням її відмов і атак на вразливості. Встановлено, що розширення моніторингових функцій на основі застосування сервісів та потужних інформаційно-обчислювальних ресурсів відомого хмарного провайдера AWS створює чудові умови щодо реалізації вірогідного контролю інформаційно-технічних станів критичних інфраструктур.

Розглянутий в розділі метод напівмарковського моделювання надав змогу отримати оцінки готовності критичних інфраструктур, фактично відтворюючи їхню поведінку в умовах дії різноманітних негативних факторів впливу. Результати моделювання можуть бути використані для обґрунтування граничних показників надійності та функційної безпечності компонентів критичних інфраструктур.

У четвертому розділі розглянуто метод оцінювання функційної безпечності критичної інфраструктури, який реалізовано на основі виконання удосконалених автором процедур аналітико-стохастичного моделювання та причинно-наслідкового аналізу відмов і аварій компонентних складових. Для розв’язування завдань визначення рівня функційної безпечності КІ було запропоновано аналітико-стохастичний метод побудови структурних схем безпеки. Крім того, в розділі розглянуто деякі теоретичні засади, за допомогою яких на формальному рівні описано етапи реалізації атаки на кібернетичні та хмарні активи критичної енергоінфраструктури. Для опису процесу реалізації атаки використано

формалізми на основі бінарних відношень, сформульовано та доведено теореми, за допомогою яких визначаються рівні успішності атаки на кібернетичні активи критичних інфраструктур.

Результати досліджень, які представлено в четвертому розділі підтверджують доцільність використання хмарних систем для покращення функційної безпечності КІ з урахуванням ризиків негативного впливу на активи відповідних інфраструктур. Запропонований метод апробовано на двух типах інфраструктур, а саме: критичній енергетичній інфраструктурі, морській критичній інфраструктурі. Кількісні результати моделювання підтверджують, що виграш в значеннях показника гарантоздатності компонентів контуру управління критичної енергетичної інфраструктури за умови застосування хмарних систем становить від 8,7% до 49,5%. Доведно, що варіант використання бездротових сенсорних мереж та додаткових хмарних активів як перспективних засобів для Глобальної морської системи зв’язку та забезпечення безпеки мореплавства (ГМСЗБ) морських рухомих об’єктів морської критичної інфраструктури надає можливість покращити рівень функційної й інформаційної безпечності ГМСЗБ.

У п’ятому розділі наведено основні положення методу моделювання та оцінювання готовності критичної інфраструктури, який дістав подальшого розвитку внаслідок врахування еволюційних аспектів управління КІ за інформаційно-технічним станом. Метод базується на використанні процедури аналітико-стохастичного оцінювання сервіс-орієнтованих хмарних ресурсів, які пропонується використовувати в загальному контурі управління КІ, що дозволяє підвищити точність оцінки наслідків аварій інфраструктур. Метод апробовано на компонентах критичної енергетичної інфраструктури. Кількісні результати моделювання з застосуванням пропонуємого методу підтверджують доцільність поступового переходу до управління готовністю КЕІ за інформаційно-технічним станом. Додатково в розділі розглянуто основні положення методу компаративістичного аналізу аварій критичної інфраструктури, який удосконалено автором за рахунок використання відомих операцій алгебри причинно-наслідкових комплексів, їхньому логіко-цифровому представленні та

агрегатуванні у вигляді структурно-логічних схем і аналітико-стохастичних моделей протікання аварій, що дозволяє оцінювати і формулювати рекомендації щодо зменшення ризиків негативних подій для КІ. Спільне використання методів надало можливість виконати моделювання поведінки критичної енергетичної інфраструктури, враховуючи негативні впливи на її активи, що в перспективі дозволить здійснити перехід до відповідних стратегій управління готовністю КЕІ за інформаційно-технічним станом її компонентних складових. Вважається, що наявність ефективно працюючої системи оперативного моніторингу інформаційно-технічних станів дозволить здійснювати категоризацію та паспортизацію критично важливих об’єктів за величиною ризику негативного впливу.

У шостому розділі розглянуто методи вибору, оцінки характеристик готовності та енергоефективності хмарних систем критичних інфраструктур, які удосконалено автором шляхом їхнього доповнення аналітико-стохастичними процедурами моделювання процесів зміни інформаційно-технічних станів фізичних і віртуальних машин.

При розробці методу вибору характеристик готовності хмарних систем КІ враховувалися зв’язки між активами інфраструктури та можливості щодо створення інтегрованої системи оперативного моніторингу інформаційно-технічних станів компонентних складових інфраструктур. Як результат запропоновано метод вибору, оцінки та забезпечення характеристик готовності хмарних систем КІ. У якості прикладу розглянуто процедуру встановлення ієрархії показників забезпечення готовності критичної енергетичної інфраструктури. Виконано апробацію методу при оцінці енергоефективності хмарної інфраструктури з урахуванням готовності її фізичних та віртуальних машин. У розділі наведено порівняльну характеристику результатів моделювання для двох типів серверних систем, які входять до складу відповідних хмарних інфраструктур, що надало можливість здійснити вибір найкращої конфігурації за критерієм мінімуму енергоспоживання.

У сьомому розділі розглянуто інформаційну технологію тестування

регіональних хмарних систем з інтегрованими фізичними компонентами з метою вибору інформаційного центру відповідного хмарного провайдера. Вперше створена автором інформаційна технологія реалізована у вигляді таких кроків: 1) планування експерименту щодо оцінювання часу затримки потоків даних; 2) розробка процедури тестування інформаційних центрів окремого хмарного провайдера; 3) вибір інформаційного центру окремого хмарного провайдера за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв'язку.

Для моделювання даних розроблено хмарний симулятор, за допомогою якого отримано експериментальні дані щодо часу затримки генеруємого потоку даних від штучно створеного віртуального ресурсу, що імітує функціонування хмари. Підводячи підсумки, можна відзначити, що в межах виконаного дисертаційного дослідження було систематизовано результати практичного впровадження запропонованих моделей, методів та інформаційної технології. Створена інформаційна технологія впроваджена на національних підприємствах «НВП Радій», «НВП Радікс».

Ключові слова: хмарні системи, критичні інфраструктури, аналітико-стохастичне моделювання, напівмарковські моделі, ризик негативних впливів, інформаційна технологія тестування.

ABSTRACT

Oleg V. Ivanchenko. Methodological foundations and information technology for availability assurance of cloud systems of critical infrastructures. Qualification scientific work is as a manuscript.

Thesis for a Doctoral Degree in Technical Sciences: Speciality 05.13.06 – Information Technologies (Technical Sciences). – National Aerospace University "Kharkiv Aviation Institute", Ministry of Education and Science of Ukraine; V. N. Karazin Kharkiv National University, Ministry of Education and Science of Ukraine, Kharkiv, 2021.

The dissertation reveals main provisions of the methodology and technology of joint readiness of cloud systems and critical infrastructures considering the possibilities of operational monitoring, assessment of their condition, protection of physical and cyber assets in case of failures and vulnerability attacks. The main formal features of the dissertation are presented. These features include the existing contradiction, scientific and applied problem, scientific novelty and practical significance of the work.

The first section comprehensively covers a problem of ensuring and estimation of availability level for cloud systems of the critical infrastructures. The analysis of possibilities of cloud systems' application in a management contour of the critical infrastructures (CrI) is executed. Performed analysis showed how cloud systems can affect on safety and security of CrIs. As an example, the key factors of unreliability of critical energy infrastructure and maritime critical infrastructure were considered. Additionally, the development tendencies of concepts, methods, information technologies for estimation, maintenance of reliability and safety of the cloud systems of CrIs were considered. The section ends with the choice of mathematical apparatus and justification of research methodology.

The second section presents main provisions of the methodology for assessing of availability and selection of cloud systems' characteristics of critical infrastructures, which promote the development of von Neumann's concept in order to build available

systems from insufficiently reliable and secure components. The methodology structure includes principles, models, methods for assessing functional safety, methods of ensuring availability, methods of selection, assessment of the characteristics of cloud systems energy efficiency for critical infrastructures. Considerable attention in the first time developed methodology is paid to testing information technology for regional cloud systems with integrated physical components, which determines delay time of information data flows baesd on the use a virtual resource of relational databases that allows to optimally select data center of a concrete cloud provider.

In according with the proposed concept, the negative impacts on assets of CrIs can be presented how deliberate malicious impacts and penetrations. At the same time, the implementation of deliberate malicious impacts are driven by factors of natural and piece origin. In addition, it should also be noted that there are diverse negative events such as, deliberate malicious impacts, failures and faults deteriorate information and technical states of CrIs. These negative events reduce the availability level and to increase the risk of negative influences on critical infrastructures assets and as well as to increase number of CrIs accidents with heavily consequences. Based on the getting research results logical and probability model have being built and improved, further the mathematical model is built and computed.

The third section considers analytical and stochastic availability models of CrIs, which are obtained on the basis of using the apparatus of formalization of processes considering change of infrastructure components information and technical states and taking into account negative factors of external and internal influence on their safety. The proposed models are based on the formalization of processes that affect on safety and security of the critical infrastructures.

In accordance with the general concept of the study, evaluation models for reliability of critical energy infrastructure with a control system of information and technical states have been developed. The development process of Semi-Markov models has been considered possibilities of creating a modern integrated system for monitoring of the information and technical states for cloud systems based on the deployment of microservices' networks and virtual monitors. These circumstances

contributed to the building process for advanced Semi-Markov availability models of the cloud infrastructure with an integrated monitoring system of information and technical states of physical and virtual machines. At the same time, these circumstances allowed to implement simulation process in order to perform justify limits of availability assessments for the cloud infrastructure considering its failures and attacks on infrastructures' vulnearbility. It is established that the extension of monitoring functions based on the use of services and powerful information and computing resources of the famous cloud provider AWS creates excellent conditions for the implementation of reliable control of information and technical states for the critical infrastructures.

The proposed Semi-Markov modeling method gave a possibility to get availability assessments of critical infrastructures considering their behavior, when diverse impact negative factors are at play simultaneously. These modeling results can be used in order to implement process of justify of limit reliability and safety values for components of the critical infrastructures.

The fourth section considers the method of safety assessments of critical infrastructure, which is implemented on the basis of the author's improved procedures of analytical and stochastic modeling and causal analysis of failures and accidents for critical infrastructures' components. An analytical-stochastic method of constructing structural safety schemes was proposed to solve the problems of determining the level of critical infrastructures' safety. In addition, the section discusses some theoretical principles, which formally describe the stages of the attack on cyber and cloud assets of the critical energy infrastructure. To describe the process of attack implementation, formalisms based on binary relations are used, theorems are formulated and proved, which are used to determine the levels of success of the attack on cybernetic assets of critical infrastructures.

The results of these researches presented in the fourth section confirm the feasibility of using cloud systems to improve the critical infrastructures' safety considerung risks of negative impacts on assets of the relevant infrastructures. The proposed method has been tested on two types of infrastructures, namely: critical energy

infrastructure, marintimee critical infrastructure. Numerical simulation results confirm that the gain in the values of the dependability indicator of the components for a control circuit of the critical energy infrastructure based on the use of the cloud systems is taking values from 8,7% to 49,5%. Have been prooved that the use of wireless sensor networks and additional cloud assets as promising tools for the Global Maritime Distress and Safety System (GMDSS) for objects marine critical infrastructure provides an opportunity to improve safety and security of the GMDSS.

The fifth section presents the main provisions of the method for modeling and assessing of critical infrastructures' availability, which has been further developed due to the evolutionary aspects of CrIs management considering their information and technical states. The method is based on the use of a procedure of analytical and stochastic evaluation of service-oriented cloud resources, which are proposed to be used in the general control circuit of the critical infrastructure, which allows to increase the accuracy of estimating the consequences of infrastructure accidents. The method is tested on components of critical energy infrastructure. Numerical modeling results for the proposed method confirm the feasibility of a gradual transition to critical energy infrastructure availability management considering its information and technical states. Additionally, the section considers the main provisions of the method for comparative analysis of the critical infrastructure accidents, which was improved by the author through the use of familiar operations of causal complexes algebra, their logical-digital representation and aggregation in the form of structural and logical schemes, analytical and stochastic models. This method can be used in order to evaluate and formulate recommendations for reducing the risk of negative events for the critical infrastructure. The joint use of methods made it possible to model the behavior of the critical energy infrastructure considering different negative impacts on its assets, which in the near future time will allow to implement the transition to appropriate strategies of availability management of the critical energy infrastructure considering information and technical states of its components. It is believed that the presence of an effective monitoring system of information and technical states will allow to perform categorization and certification operations of critical objects by the magnitude of the risk of negative

effects.

The sixth section considers the methods of selection, evaluation of availability assessments and energy efficiency characteristics of the cloud systems for critical infrastructures. These methods were improved by author using analytical and stochastic modeling procedures for processes of changing information and technical states for physical and virtual machines.

The development of method for selecting the characteristics of availability cloud systems of critical infrastructures was based on the use of links among infrastructure assets and the possibilities of creating an integrated system for operational monitoring of the information and technical states for critical infrastructures' components. As a result, the method for selecting, evaluating and ensuring of availability characteristics for cloud systems of the critical infrastructures is proposed. As an example, the procedure of establishing a hierarchy of the indicators for availability ensuring of the critical energy infrastructure was considered. The method was tested in assessing the energy efficiency of the cloud infrastructure considering availability of its physical and virtual machines. The section provides a comparative description of the simulation results for two types of server systems that are part of the respective cloud infrastructures, which made it possible to select the best configuration according to the criterion of minimum energy consumption.

The seventh section discusses the information technology for testing regional cloud systems with integrated physical components in order to select a data center of appropriate cloud provider. For the first time the information technology created by the author is realized in the form of the following steps: 1) planning of experiment on estimation of time of a delay of data streams; 2) development of a procedure for testing the information centers of a particular cloud provider; 3) selection of the information center of a separate cloud provider according to the criterion of the minimum delay time of the tunnel (secure) communication channel.

To simulate the data, a separate cloud simulator was developed, which was used to obtain experimental data on the delay time of the generated data stream from an artificially created virtual resource that simulates functioning of the cloud. Summing up,

it can be noted that within the dissertation research the results of practical implementation of the proposed models, methods and information technology were systematized. The created information technology is implemented at the national enterprises “NVP Radium”, “NVP Radix”.

Key words: cloud systems, critical infrastructures, analytical and stochastic modeling, Semi-Markov models, negative events’ risk, testing information technologies.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. Иванченко О. В. Модели надёжности и живучести энергетических систем. Принципы и модели управления критической энергетической инфраструктурой по техническому мегасостоянию // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : кол. монографія / Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. С. 311–336.

2. Иванченко О. В. Аналитико-стохастические модели надёжности и безопасности критических энергетических инфраструктур // Информационные технологии для критических инфраструктур : кол. монографія Севастополь : Севастопольський національний техн. ун-т, 2012. С. 89–124.

Наукові праці, в яких опубліковані основні наукові результати дисертації:

3. Иванченко О. В. Полумарковские модели мониторинга информационно-технического состояния критических инфраструктур // Радіоелектронні і комп’ютерні системи. 2012. № 7 (59). С. 219–224.

4. Іванченко О. В. Аналітико-стохастичний метод побудови структурних схем безпеки кібернетичних активів системи SCADA критичної інфраструктури // Системи та технології. 2019. № 1 (57). С. 81–106.

5. Іванченко О. В. Оцінювання рівня безпеки системи SCADA критичної інфраструктури з урахуванням доступності кібернетичних та хмарних активів // Системи та технології. 2019. № 2 (58). С. 5–32.

6. Іванченко О. В. Аналітико-стохастична модель гарантоздатності кібернетичних та хмарних активів системи SCADA критичної інфраструктури // Системи та технології. 2020. № 1 (59). С. 14–59.

7. Яцек Я. Ф., Иванченко О. В., Войтюк А. В., Степанов В. А. Комплексный подход к управлению критическими инфраструктурами по техническому мегасостоянию // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. Севастополь, 2010. Вип. 4 (4). С. 91–99 *(Особистий внесок здобувача: розроблено двохрівневі моделі управління готовністю критичних інфраструктур за технічним мегастаном)*.

8. Иванченко О. В., Харченко В. С., Одарущенко О. Н. Принципы анализа и управления безопасностью критических инфраструктур // Вісник Хмельницького національного університету. 2010. № 5 (170). С. 218–221 *(Особистий внесок здобувача: сформульовано окремі принципи аналізу безпеки критичних інфраструктур)*.

9. Мащенко Е. Н., Иванченко О. В., Смахашева Н. В. Аналитико-стохастическая модель управления техническим состоянием изделий критического применения // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 30–34 *(Особистий внесок здобувача: запропоновано концепцію управління технічним станом виробів критичного призначення)*.

10. Иванченко О. В., Харченко В. С., Бирюков Д. Ю. Полумарковская модель протекания аварии критической инфраструктуры // Радіоелектронні і комп'ютерні системи. 2013. № 5 (64). С. 45–51 *(Особистий внесок здобувача: побудовано та виконано обчислення напівмарковської моделі протікання аварії критичної енергетичної інфраструктури)*.

11. Иванченко О. В., Харченко В. С. Метод причинно-следственной декомпозиции аварий и инцидентов критических инфраструктур // Радіоелектронні і комп'ютерні системи. 2014. № 5 (69). С. 12–17 *(Особистий внесок здобувача: розроблено основні положення методу причинно-наслідкової декомпозиції та виконано аналітико-стохастичне моделювання аварії критичної енергетичної інфраструктури)*.

12. Иванченко О. В., Ловягин В. С. Техническое обслуживание компонентной составляющей критических инфраструктур // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. 2011. Вип.

1 (5). С. 253–259 *(Особистий внесок здобувача: сформульовано окремі положення концепції технічного обслуговування компонентної складової критичної інфраструктури за станом)*.

13. Иванченко О. В., Бочарова В. В., Владимирова Е. С., Фомина А. Б. Модели надёжности и безопасности критических инфраструктур // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. 2011. Вип. 4 (8). С. 109–119 *(Особистий внесок здобувача: виконано аналіз властивостей, що визначають якість застосування критичної енергетичної інфраструктури за призначенням; розроблено причинно-наслідкову модель протікання аварії критичної енергетичної інфраструктури)*.

14. Иванченко О. В., Бочарова В. В. Обоснование предельных величин показателей надёжности критических энергетических инфраструктур // Радіоелектронні і комп'ютерні системи. 2012. № 5 (57). С. 197–201*(Особистий внесок здобувача: розроблено марковську модель протікання аварії та визначено граничні величини показників надійності критичної енергетичної інфраструктури)*.

15. Иванченко О. В., Солдатенко Е. С., Владимирова Е. С. Архитектурный подход к оценке надежности программного обеспечения системы управления критической инфраструктуры // Системи обробки інформації. 2014. № 1 (117). С. 173–179 *(Особистий внесок здобувача: виконано оцінювання рівня надійності системи управління інфраструктурою з урахуванням безвідмвності програмного забезпечення критичного додатку)*.

16. Иванченко О. В., Харченко В. С. Полумарковская модель готовности облачной инфраструктуры с интегрированной системой мониторинга технического состояния // Радіоелектронні і комп'ютерні системи. 2016. № 5 (79). С. 15–19 *(Особистий внесок здобувача: побудовано та обчислено напівмарковську модель готовності хмарної інфраструктури з контролем технічного стану фізичних машин)*.

17. Иванченко О. В., Харченко В. С. Анализ стохастических методов метамоделирования и оценивания готовности облачных инфраструктур //

Радіоелектронні і комп'ютерні системи. 2016. № 6 (80). С. 6–11 *(Особистий внесок здобувача: розроблено концептуальні положення щодо побудови та обчислення метамоделі готовності хмарної інфраструктури)*.

18. Иванченко О. В., Смоктий К. В., Харченко В. С., Блындюк И. В. Стохастическая модель надежности инфраструктуры как сервиса облачных вычислений // Вісник Академії митної служби України. 2014. № 2 (52). С. 50–68 *(Особистий внесок здобувача: побудовано та обчислено напівмарковську модель готовності хмарної інфраструктури з трьома підсистемами фізичних машин)*.

19. Иванченко О. В., Буланый А. П., Прокопенко Р. А. Обобщенный критерий управления конфигурацией инфраструктуры как сервиса облачных вычислений // Вісник Академії митної служби України. 2015. № 1 (53). С. 43–55 *(Особистий внесок здобувача: розроблено таксономічну схему управління конфігурацією хмарної інфраструктури)*.

20. Иванченко О. В., Кривонос М. В., Бирюков Д. Ю. Математическая модель цифрового средства измерения с двухзвенным аналого-цифровым преобразователем последовательных приближений // Вісник СевНТУ. Серія «Інформатика, електроніка, зв'язок». 2011. Вип. 114. С. 90–94 *(Особистий внесок здобувача: побудовано математичну модель цифрового засобу вимірювання з двохланцюговим аналого-цифровим пристроєм послідовного приближення)*.

21. Гаршин А. Ю., Иванченко О. В., Мащенко Е. Н. Методика оценки уровня опасности морской критической инфраструктуры // Системи озброєння і військова техніка. 2010. № 3 (23). С. 107–109 *(Особистий внесок здобувача: запропоновано визначення морської критичної інфраструктури)*.

Наукові праці, в яких опубліковані основні наукові результати дисертації у зарубіжних спеціалізованих виданнях:

22. Ivanchenko O., Kharchenko V., Moroz B., Kabak L. , Blindyuk I., Smoktii K. Semi-Markov Availability Model for Infrastructure as a Service Cloud Considering Energy Performance // Green IT Engineering: Social, Business and

Industrial Applications. Studies in Systems, Decision and Control. 2019. Vol. 171. P. 141–159. (***Scopus***) *(Особистий внесок здобувача: побудувано та обчислено стохастичну модель енергоефективності хмарної інфраструктури з трьома підсистемами фізичних та віртуальних машин).*

23. Ivanchenko O., Kharchenko V., Skatkov A. Management of critical infrastructures based on technical megastate // An International Journal. Information and Security. 2012. Vol. 28, no. 1. P. 37–51 *(Особистий внесок здобувача: сформульовано концепцію управління критичними інфраструктурами за технічним мегастаном).*

Наукові праці, які засвідчують апробацію матеріалів дисертації:

24. Semi-Markov availability model of an infrastructure as a service cloud with multiple pools / O. Ivanchenko, V. Kharchenko // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 12th Intern. Conf., June 21–24, Kyiv, 2016. Vol. 1614. P. 349–360 (***Scopus***) *(Особистий внесок здобувача: сформульовано принципи реконфігурування, надлишковості сервіс-орієнтованих ресурсів).*

25. Semi-Markov availability model for infrastructure as a service cloud considering hidden failures of physical machines / O. Ivanchenko, V. Kharchenko, Y. Ponochovnyi, I. Blindyuk, K. Smoktii // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 13th Intern. Conf., May 15–18, Kyiv, 2017. Vol. 1844. P. 634–644 (***Scopus***) *(Особистий внесок здобувача: сформульовано принципи оперативного моніторингу інформаційно-технічних станів хмарних систем).*

26. Availability as a cloud service for control system of critical energy infrastructure / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii, Y. Ponochovnyi // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 14th Intern. Conf., May 14–17, Kyiv, 2018. Vol. 2104. P. 571–582 (***Scopus***) *(Особистий внесок здобувача:*

сформульовано принципи побудови хмарної платформи для оцінки рівня готовності критичної енергетичної інфраструктури).

27. Risk assessment of critical energy infrastructure considering physical and cyber assets: Methodology and models / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, S. Konovalenko // 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) : Proc. of the 4th Intern. Symp., September 20 –21, Lviv, 2018. P. 225–228 (***Web of Science***) *(Особистий внесок здобувача: отримано оцінку ризику негативного впливу на фізичні та кібернетичні активи критичної енергетичної інфраструктури).*

28. Semi-Markov availability model considering deliberate malicious impacts on an Infrastructure-as-a-Service Cloud / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii // 2018 IEEE 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) : Proc. of the 14th Intern. Conf., February 20–24, Lviv–Slavske, 2018. P. 570–573 (***Web of Science***) *(Особистий внесок здобувача: побудовано та обчислено модель готовності хмарної інфраструктури з урахуванням зловмисного шкідливого впливу).*

29. Semi-Markov's models for availability assessment of an Infrastructure as a Service Cloud with multiple pools of physical and virtual machines / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) : Proc. of the 14th Intern. Conf., May 24–27, Kyiv, 2018. P. 98–102 ***(Scopus)*** *(Особистий внесок здобувача: побудовано та обчислено модель готовності хмарної інфраструктури з декількома підсистемами фізичних та віртуальних машин).*

30. Dependability Assessment for SCADA System Considering Usage of Cloud Resources / O. Ivanchenko, V. Kharchenko, E. Brezhnev, Y. Ponochovnyi, B. Moroz, L. Kabak // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT) : Proc. of the 11th Intern. Conf., May 14–18, Kyiv,

2020. P. 13–17 (***Scopus***) *(Особистий внесок здобувача: виконано оцінювання рівня гарантоздатності системи диспетчерського контролю та збору даних)*.

31. Харченко В. С., Иванченко О. В., Мащенко Е. Н. Методология FMECA: новая парадигма анализа видов и последствий отказов критических инфраструктур // Автоматизація: проблеми, ідеї, рішення : матеріали Міжнар. наук.-техн. конф., 6–10 верес. 2010 р. Севастополь, 2010. С. 142–145 Принципи аналізу та управління безпекою критичної енергетичної інфраструктури *(Особистий внесок здобувача: сформульовано принцип компліментарності побудови критичних інфраструктур)*.

32. Скатков А. В., Иванченко О. В. Цикломатическая сложность моделей компонентов критических инфраструктур // Інформаційні технології та інформаційна безпека в науці, техніці та навчанні : ІНФОТЕХ–2011 : матеріали Міжнар. наук.-практ. конф., 5–10 верес. 2011 р. Севастополь, 2011. С. 102–103 *(Особистий внесок здобувача: введено визначення цикломатичної складності для моделей функціонування компонентів критичних інфраструктур цикломатичної складності для моделей функціонування компонентів критичних інфраструктур)*.

33. Иванченко О. В., Харченко В. С. Причинно-следственная декомпозиция аварий и инцидентов критических инфраструктур // Проблемы критических ситуаций в точной механике и управлении : материалы Всерос. научн. конф. с междунар. участием, 25–27 сент. 2013 г. Саратов, 2013. С. 59–63 *(Особистий внесок здобувача: сформульовано принцип побудови причинно-наслідкового комплексу протікання аварії критичної енергетичної інфраструктури).*

34. Іванченко О. В. Методологічні основи та засоби оцінювання і моніторингу характеристик гарантоздатної хмарної інфраструктури критичних енергетичних систем // Актуальні проблеми економіки, управління та фінансів : матеріали Міжнар. наук.-практ. конф., 19 квіт. 2019 р. Дніпро, 2019. С. 329–330.

35. Іванченко О. В. Аналітико-стохастична модель готовності системи SCADA критичної інфраструктури // 20th International Scientific and Practical Conference on Perspective Directions for the Development of Science and Practice : Proc. of the 20th Intern. Conf., Athens, June 8–9, 2020, Athens, Greece. P. 166–170.

36. Іванченко О. В. Аналітико-стохастична модель зловмисного шкідливого впливу на кібернетичні активи системи SCADA критичної інфраструктури // 21st International Scientific and Practical Conference on Current Trends in the Development of Science and Practice : Proc. of the 21st Intern. and Pract. Conf., Haifa, 15–16 June, 2020, Haifa, Israel. P. 125–130.

37. Іванченко О. В. Теоретико-множинна модель кібератаки системи корпоративного управління // Математичні проблеми технічної механіки та прикладної математики : матеріали Міжнар. наук. конф., 2–5 груд. 2019 р. Дніпро : Університет митної справи та фінансів. Дніпро–Кам'янське, 2019. С. 65–66.

Наукові праці, які додатково
відображають наукові результати дисертації:

38. Иванченко О. В., Каряка А. В., Маврин С. А., Филимонов И. Л. Оценка уровня надёжности телекоммуникационных систем морских подвижных объектов для их технического обслуживания по состоянию // Радіоелектронні і комп'ютерні системи. 2008. Вип. 6 (33). С. 128–133 *(Особистий внесок здобувача: побудовано та обчислено моделі надійності морських рухомих об'єктів критичної інфраструктури для їхнього технічного обслуговування за станом)*.

39. Иванченко О. В., Паткаускас А. В., Маврин С. А., Корощенко Н. Н. Обобщённый критерий синтеза адаптивной системы технического диагностирования сложных промышленных объектов // Радіоелектронні і комп'ютерні системи. 2009. № 7 (41). С. 127–135 *(Особистий внесок здобувача: сформульовано критерій синтезу системи технічного діагностування критично важливих об'єктів)*.

40. Иванченко О. В., Харченко В. С., Смоктий К. В., Смоктий О. Д. Концепция управления готовностью критических инфраструктур на основе применения облачных информационных технологий // Системи та технології. 2016. № 1 (55). С. 5–23 *(Особистий внесок здобувача: сформульовано концепцію та розроблено критерій управління готовністю критичних інфраструктур на основі застосування хмарних систем)*.

41. Смоктий О. Д., Смоктий К. В., Иванченко О. В. Анализ механизма и последствий воздействия DDoS-атак на эталонную модель взаимодействия открытых систем OSI // Системи управління, навігації та зв’язку. 2017. № 1 (41). С. 33–37 *(Особистий внесок здобувача: виконано аналіз механізму впливу DDoS-атак на програмне забезпечення критичних інфраструктур)*.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….....……..31
ВСТУП..... 34
РОЗДІЛ 1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ТА ОЦІНЮВАННЯ ГОТОВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР.....46
1.1 Аналіз впливу хмарних систем на функційну безпечність критичних інфраструктур 46
1.1.1 Проблема впливу хмарних систем на функційну безпечність критичних інфраструктур.....46
1.1.2 Аналіз ключових факторів ненадійності критичних інфраструктур на прикладі критичної енергетичної та морської критичної інфраструктур.....50
1.1.3 Аналіз тенденцій розвитку систем моніторингу на основі застосування хмарних систем важливих для забезпечення функційної безпечності критичних інфраструктур.....57
1.2 Аналіз впливу хмарних систем на інформаційну безпеку критичної енергетичної та морської критичної інфраструктур 60
1.2.1 Аналіз інформаційної безпеки хмарних систем……...…..……61
1.2.2 Аналіз впливу хмарних систем на інформаційну безпеку критичної енергетичної інфраструктури…….……..……..65
1.2.3 Аналіз впливу хмарних систем на інформаційну безпеку морської критичної інфраструктури……..……..67
1.3 Аналіз методів оцінювання готовності, підходів з вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур……69
1.3.1 Аналіз методів оцінювання готовності хмарних систем критичних інфраструктур……70
1.3.2 Аналіз відомих підходів щодо вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур……..……...…73

1.4 Аналіз класифікаційної схеми вибору показників готовності, характеристик надійності та безпеки хмарних систем критичних інфраструктур……..76

1.5 Постановка наукової проблеми та завдань досліджень……78

1.5.1 Основні завдання в області оцінювання, забезпечення готовності, вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур…….....78

1.5.2 Вибір математичного аппарату та обгрунтування методології наукових досліджень…….……81

Висновки до розділу 1 84

РОЗДІЛ 2 РОЗРОБКА СТРУКТУРИ ТА ЕЛЕМЕНТІВ МЕТОДОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР 85

2.1 Розробка принципів оцінювання готовності та вибору характеристик надійності і безпеки хмарних систем критичних інфраструктур……..…..85

2.1.1 Аналіз концепції створення надійних та безпечних хмарних систем критичних інфраструктур з сервіс-орієнтованим розподіленням ресурсів……..…..85

2.1.2 Принцип реконфігурування та комбінованої надлишковості сервіс-орієнтованих ресурсів хмарних систем критичних інфрастрктур……..…...…… 88

2.1.3 Принцип компліментарності архітектурної побудови критичних інфраструктур……91

2.1.4 Принцип оперативного моніторингу компонентів критичної енергетичної інфраструктури на основі застосування систем синхронізованих векторних вимірювань……93

2.1.5 Принцип управління готовністю критичної енергетичної інфраструктури за інформаційно-технічним станом з застосуванням сервіс-орієнтованих хмарних ресурсів……96

2.2 Основні положення процесу оцінювання ризику негативного впливу на

активи критичних інфраструктур 98
2.2.1 Аналіз активів критичних інфраструктур……..98
2.2.2 Аналіз негативних факторів впливу на активи критичних інфраструктур……..100
2.2.3 Моделювання поведінки критичної інфраструктури з урахуванням негативних факторів впливу на її активи……101
2.2.4 Причинно-наслідковий аналіз негативного впливу на активи критичних інфраструктур……...103
2.2.5 Аналітико-стохастичне оцінювання ризику негативного впливу на активи критичних інфраструктур..……104
2.3 Логіко-ймовірнісна модель готовності критичної інфраструктури…...107
Висновки до розділу 2……..……..…….....……..109
РОЗДІЛ 3 АНАЛІТИКО-СТОХАСТИЧНІ МОДЕЛІ КРИТИЧНИХ ІНФРАСТРУКТУР…….….111
3.1 Теоретико-множинна модель інформаційно-технічних станів критичної інфраструктури……..111
3.2 Аналітико-стохастична модель надійності критичної енергетичної інфраструктури з системою моніторингу інформаційно-технічних станів..……..…112
3.2.1 Напівмарковські моделі моніторингу інформаційно-технічних станів компонентів критичної інфраструктури……...….113
3.2.2 Напівмарковська модель протікання аварії критичної енергетичної інфраструктури……...……..126
3.3 Метод напівмарковського моделювання готовності хмарної інфраструктури……..……137
3.3.1 Постановка завдання оцінювання готовності хмарної інфраструктури на основі напівмарковського моделювання...…….137
3.3.2 Етапи методу оцінювання готовності хмарної інфраструктури на основі напівмарковського моделювання……139
3.4 Напівмарковські моделі хмарної інфраструктури з інтегрованою

системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин……...140

3.4.1 Особливості архітектурної побудови хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин.……...……..140

3.4.2 Напівмарковська модель готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних машин…… 141

3.4.3 Особливості масштабованого використання віртуального ресурсу хмарної інфраструктури з декількома підсистемами фізичних машин…….148

3.4.4 Напівмарковська модель готовності хмарної інфраструктури з декількома підсистемами фізичних та віртуальних машин……..150

3.5 Напівмарковська модель готовності хмарної інфраструктури з урахуванням зловмисних шкідливих впливів……..……155

Висновки до розділу 3……....…….159

РОЗДІЛ 4 МЕТОДИ ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ КРИТИЧНИХ ІНФРАСТРУКТУР……...161

4.1 Аналітико-стохастичний метод побудови структурних схем безпеки кібернетичних активів критичних інфраструктур……..161

4.1.1 Етапи реалізації методу побудови структурних схем безпеки кібернетичних активів критичних інфраструктур…….……...161

4.1.2 Аналітико-стохастичне моделювання відмов фізичних активів критичних інфраструктур……...163

4.1.3 Аналітико-стохастичне моделювання зловмисних шкідливих впливів на кібернетичні активи критичних інфраструктур……..……164

4.2 Метод оцінювання функційної безпечності критичних інфраструктур з урахуванням ризику негативних впливів на їхні активи……...165

4.2.1 Етапи реалізації методу оцінювання функційної безпечності критичних інфраструктур з урахуванням ризику негативних впливів на

їхні активи……165
4.2.2 Аналітико-стохастична модель функційної безпечності інформаційно-керуючої системи критичної інфраструктури з урахуванням зловмисних шкідливих впливів на її кібернетичні та хмарні активи……...170
4.2.3 Аналітико-стохастична модель гарантоздатності кібернетичних та хмарних активів критичної інфраструктури.....176
4.2.4 Кількісна оцінка ризику негативного впливу на активи критичної енергетичної інфраструктури з використанням запропонованого методу.....201
4.3 Кількісна оцінка показника безпеки перспективних засобів Глобальної морської системи зв’язку та безпеки мореплавства морської критичної інфраструктури……..204
Висновки до розділу 4 214
РОЗДІЛ 5 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ 216
5.1 Метод причинно-наслідкової декомпозиції аварій критичної енергетичної інфраструктури……..……216
5.1.1 Принцип побудови причинно-наслідкового комплексу протікання аварії критичної енергетичної інфраструктури……....216
5.1.2 Структурно-логічна схема протікання аварії критичної енергетичної інфраструктури……..……219
5.1.3 Причинно-наслідкова декомпозиція аварії критичної енергетичної інфраструктури……..……..222
5.1.4 Аналітико-стохастичне моделювання протікання аварії критичної енергетичної інфраструктури…….……224
5.1.5 Логіко-цифрове представлення причинно-наслідкової декомпозиції аварії критичної енергетичної інфраструктури…….……...226
5.2 Метод компаративістичного аналізу аварій критичної енергетичної інфраструктури……...……...228

5.3 Метод управління готовністю критичної енергетичної інфраструктури за інформаційно-технічним станом 232

5.3.1 Принципи аналізу та управління безпекою критичної енергетичної інфраструктури……..…..232

5.3.2 Еволюційні аспекти управління критичною енергетичною інфраструктурою за інформаційно-технічним станом……..….236

Висновки до розділу 5……..……..……238

РОЗДІЛ 6 МЕТОДИ ВИБОРУ, ОЦІНКИ ХАРАКТЕРИСТИК ГОТОВНОСТІ ТА ЕНЕРГОЕФЕКТИВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР……..……..…. 240

6.1 Метод вибору характеристик готовності хмарних систем критичних інфраструктур……....240

6.1.1 Архітектура хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів….……. 241

6.1.2 Аналіз ієрархії властивостей хмарних систем критичних інфраструктур……..242

6.1.3 Аналіз ієрархії та вибір показників готовності хмарних систем критичних інфраструктур……..….244

6.2 Метод вибору та оцінки характеристик енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів……246

6.2.1 Процедура вибору характеристик енергоефективності хмарної іфраструктури……..246

6.2.2 Етапи оцінювання характеристик енергоефективності хмарної інфраструктури…….…… 247

6.2.3 Аналітико-стохастична модель енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів…… 249

Висновки до розділу 6……..……..……..262

РОЗДІЛ 7 ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ТЕСТУВАННЯ ХМАРНИХ СИСТЕМ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ……..…… 264

7.1 Розробка методу вибору інформаційного центру хмарного провайдера…….… 264

7.1.1 Оцінка часу затримки інформаційних даних між системою оперативного моніторингу критичної енергетичної інфраструктури та інтегрованими фізичними (віртуальними) компонентами хмарних систем……...265

7.1.2 Процедура тестування інформаційного центру хмарного провайдера……....269

7.1.3 Процедура вибору інформаційного центру хмарного провайдера за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв’язку……...272

7.2. Інформаційна технологія тестування хмарних систем критичної енергетичної інфраструктури з інтегрованими фізичними компонентами на основі використання віртуального ресурсу реляційних баз даних……..…… 276

7.3 Систематизація та аналіз результатів впровадження……..….. 281

Висновки до розділу 7.....…….282

ВИСНОВКИ..... 284

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 287

ДОДАТОК А СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ 311

ДОДАТОК Б АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ 320

ДОДАТОК В МОДЕЛЬ ГОТОВНОСТІ ХМАРНОЇ ІНФРАСТРУКТУРИ З ТРЬОМА ФІЗИЧНИМИ МАШИНАМИ……..……...……..…331

ДОДАТОК Г МОДЕЛЬ ГОТОВНОСТІ ХМАРНОЇ ІНФРАСТРУКТУРИ З ТРЬОМА ПІДСИСТЕМАМИ ФІЗИЧНИХ ТА ВІРТУАЛЬНИХ МАШИН І КОНТРОЛЕМ ІНФОРМАЦІЙНО-ТЕХНІЧНОГО СТАНУ……...332

ДОДАТОК Д АНАЛІЗ ЗЛОВМИСНИХ ШКІДЛИВИХ ВПЛИВІВ НА АКТИВИ СИСТЕМИ SCADA КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ……..325

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АЕС – Атомна електростанція;

АМПУ – Адміністрація морських портів України;

БДМ – Брандмауер;

БДСМ – Бездротові сенсорні мережі;

БПМЛ – Безпрограшний марковський ланцюг;

ВДЕ – Відновлювані джерела енергії;

ГЕС – Гідроелектростанція;

ГМСЗБ – Глобальна морська система зв’язку та забезпечення безпеки мореплавства;

ДМЛ – Дискретний марковський ланцюг;

ДНМЛ – Дискретний напівмарковський ланцюг;

ДСВ – Діаграма системних відмов;

ЗВШВ – Зловмисні шкідливі впливи;

ЗВШП – Зловмисні шкідливі проникнення;

ІБ – Інформаційна безпечність;

ІКС – Інформаційно-керуюча система;

ІТ – Інформаційні технології;

ІЦ – Інформаційний центр;

КБА – Кібернетичні активи;

КВО – Критично важливі об’єкти;

КГ – Коефіцієнт готовності;

КЕІ – Критична енергетична інфраструктура;

КІ – Критичні інфраструктури;

КС – Критичні системи;

КТС – Контроль інформаційно-технічного стану;

ЛЕП – Лінія електропередачі;

МКІ – Морська критична інфраструктура;

ММ – Марковська модель;

МР – Морський район;

МРО – Морський рухомий об’єкт;

НІСТ – Національний інститут США зі стандартизації та технологій;

НПМ – Напівмарковський процес моделювання;

НПММ – Напівмарковська модель;

НПРС – Непрацездатний стан;

ОП – Обслуговуючий персонал;

ОСКСП – Обчислювальна система з кластерною структурою побудови;

ПБ – Показник безпеки;

ПДМ – Підміна інформації;

ПЗ – Програмне забезпечення;

ПНД – Причинно-наслідкова декомпозиція;

ПНК – Причинно-наслідковий комплекс;

ПНЛ – Причинно-наслідкова ланка

ПРС – Працездатний стан;

РБД – Реляційні бази даних;

РЗІ – Розкриття інформації;

СКГ – Стаціонарний коефіцієнт готовності;

СКНГ – Стаціонарний коефіцієнт неготовності;

СМО – Системи масового обслуговування;

СМП – Стохастичні мережі Петрі;

СППР – Система підтримки прийняття рішень;

ССБ – Структурна схема безпеки;

ССВВ – Система синхронізованих векторних вимірювань;

ССН – Структурні схеми надійності;

СУ – Система управління;

СХФР – Синхрофазор;

ТММ – Теоретико-множинна модель;

ФБ – Функційна безпечність;

ФСФ – Фальсифікація інформації;

ХМА – Хмарні активи;

ХМІ – Хмарна інфраструктура;

ХМП – Хмарний провайдер;

ХМС – Хмарні системи;

ЦФ – Цільовий фішинг;

AWS – Amazon Web Services;

DDoS – Distributed Denial of Service;

FMECA – Failure Mode, Effects and Critical Analysis

GPS – Global Position System;

SCADA – Supervisory Control and Data Acquisition System;

SLA – Service Level Agreement;

VPN – Virtual Private Network

ВСТУП

Обґрунтування вибору теми дослідження. Динамічний розвиток сучасного постіндустріального суспільства суттєво залежить від надійного та безпечного функціонування критичних інфраструктур (КІ), які водночас є важливою складовою національної безпеки будь-якої країни. Кращому усвідомленню цього аспекту впливу сприяє аналіз аварій об'єктів КІ міжрегіонального та державного рівня за останні п'ятнадцять років. Для того щоб усунути ці негативні явища виконується комплекс заходів, зокрема: проведення оперативного моніторингу об'єктів КІ на основі застосування сучасних інформаційних технологій (ІТ); використання хмарних систем (ХМС) і сервісів, за допомогою яких реалізуються збір, аналіз, зберігання інформації; захист кібернетичних, фізичних активів КІ при відмовах і атаках на вразливості. На жаль, відомі факти аварійного відключення, відмов провідних хмарних провайдерів (AWS, Microsoft) і кібератак на інформаційні ресурси хмарних систем ілюструють стан неготовності і погіршення безпеки КІ. Тому проблема оцінювання та забезпечення готовності фізичних, кібернетичних, хмарних активів КІ є важливою і актуальною.

Варто зазначити, що сучасний стан досліджень в сфері оцінювання рівня безпеки КІ базується на досягненнях наукових шкіл як вітчизняних, так і закордонних вчених. Серед них слід відзначити роботи О. Г. Додонова, М. О. Ястребенецького, В. А. Заславського, В. С. Харченка та його учнів В. В. Скляра, А. В. Горбенка, Є. В. Брежнєва, О. М. Одарущенка, в яких значну увагу надано методам оцінювання рівня безпеки критичної енергетичної інфраструктури (КЕІ), аналізу інформаційної і функційної безпеки інформаційно-керуючих систем атомних електростанцій – важливої частини КЕІ, а також методам забезпечення гарантоздатності та надійності сервіс-орієнтованих систем. В роботах О. Г. Корченка, С. В. Казимірчука, Б. Б. Ахметова розглянуто

процедури оцінювання ризику розподілених систем КІ на основі використання лінгвістичної форми представлення ймовірностей негативних подій, деяких суб'єктивних оцінок та нечітко визначених оціночних параметрів. Методи адаптивного управління безпекою об'єктів КІ на основі ризик-орієнтованого підходу із застосуванням сучасних інформаційних технологій розроблено Бєгуном В. В. Методи забезпечення кібербезпеки і категоризації об'єктів КІ розроблено І. Д. Горбенком і О. В. Потієм. Дослідженню причинно-наслідкових зв'язків між негативним впливом, ефектом від нього для складних людино-машинних систем та під час аварій КЕІ присвячені роботи К. Джонса, В. А. Скопінцева. Не менш важливими є роботи Леандроса Маглараса, Мітхона Макгерджі, в яких висвітлюються результати вербального та гіпотетичного оцінювання вразливостей і загроз інформаційно-керуючих систем КІ. Низку досліджень присвячено хмарним інфраструктурам, до складу яких входять різноманітні ХМС з фізичним і віртуальним рівнем реалізації відповідних інформаційних технологій і сервісів. Відомі роботи К. Тріведі, Р. Гоша, Ф. Хана висвітлюють проблемні питання, пов'язані з моделюванням поведінки хмарної інфраструктури (ХМІ) в умовах дії негативних факторів, які знижують готовність і рівень її безпеки (наприклад, аварія ХМІ AWS в лютому 2017 р.). В цих роботах оцінка готовності ХМІ здійснювалася, враховуючи інформаційно-технічний стан як фізичних, так і віртуальних машин. Певна частина досліджень, включаючи роботи А. Бєлоглазова, Д. Сілви, присвячена питанням енергоспоживання хмарної інфраструктури. Розробленню інформаційних технологій тестування ХМС провайдерів, які застосовуються для управління бізнес-процесами присвячено дослідження М. Бакса, Р. Буя, О. В. Прохорова.

Не дивлячись на суттєві досягнення за розглянутими напрямами досліджень, в сфері оцінювання та забезпечення необхідного рівня готовності критичних інфраструктур на сьогоднішній день не розв'язано наступні завдання:

– створення методології спільного забезпечення готовності хмарних систем і критичних інфраструктур з урахуванням факторів негативного впливу;

– розроблення науково-методичного апарату оперативного моніторингу інформаційно-технічного стану хмарних систем і критичних інфраструктур;

– моделювання поведінки хмарних систем і критичних інфраструктур під час аварій, відмов та зловмисних шкідливих впливів;

– підвищення точності оцінювання рівня безпеки КЕІ на основі застосування апарату аналітико-стохастичного моделювання та зниження наслідків аварій критичної енергетичної інфраструктури;

– розроблення комплексного підходу щодо оцінки граничних величин відповідних характеристик готовності хмарних систем КІ з метою забезпечення вимог до надійності та безпеки інфраструктури;

– розроблення науково-методичного апарату вибору, обгрунтування характеристик готовності хмарних систем критичних інфраструктур та інформаційної технології тестування регіональних ХМС з інтегрованими фізичними компонентами.

Виходячи із зазначеного, насьогодні існує стійке **протиріччя**, яке полягає у невідповідності між зростаючими вимогами до ефективності функціонування, надійності, безпеки критичних інфраструктур в умовах розширеного використання хмарних сервісів, *з однієї сторони*, і рівнем розвитку методологічної бази, методів, технологій моніторингу, оцінювання готовності, вибору характеристик хмарних систем для забезпечення вимог до інфраструктур, – *з іншої*. **Наукова гіпотеза** формулюється таким чином: комплексне застосування надійних, функційно безпечних хмарних систем та сервісів як додаткових засобів комунікації, збереження інформації, аварійного відновлення і оперативного моніторингу стану критичних інфраструктур на основі аналітичного обгрунтування та використання результатів стохастичного моделювання їхньої поведінки дозволить забезпечити готовність КІ.

Таким чином, в дисертаційній роботі вирішується **науково-прикладна проблема** розроблення методології та технології спільного забезпечення готовності хмарних систем і критичних інфраструктур, оперативного моніторингу, оцінювання стану, захисту фізичних і кібернетичних активів при

відмовах і атаках на вразливості.

Мета і завдання дослідження. Метою дисертаційного дослідження є підвищення готовності хмарних систем критичних інфраструктур шляхом розроблення і використання методів, технології оцінювання і вибору відмовостійких архітектур і характеристик надійності, безпеки їхніх інтегрованих фізичних і віртуальних компонентів.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1) проаналізувати тенденції розвитку концепцій, математичного апарату, методів, інформаційних технологій оцінювання, забезпечення надійності та безпеки хмарних систем критичних інфраструктур;

2) розробити методологію (концепцію, принципи, комплекс моделей та методів) забезпечення готовності хмарних систем критичних інфраструктур;

3) розробити метод оцінювання функційної безпечності критичних інфраструктур з урахуванням негативних впливів на їхні фізичні та кібернетичні активи;

4) розробити метод причинно-наслідкової декомпозиції та компаративістики аварій критичної енергетичної інфраструктури;

5) розробити моделі готовності хмарної інфраструктури з інтегрованою системою моніторингу информаційно-технічних станів фізичних та віртуальних машин;

6) розробити метод вибору характеристик та забезпечення готовності, енергоефективності хмарних систем критичних інфраструктур;

7) розробити метод оцінки енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів;

8) розробити інформаційну технологію тестування хмарних систем критичної енергетичної інфраструктури з інтегрованими фізичними компонентами на основі застосування віртуального ресурсу реляційних баз даних.

У якості *об'єкта дослідження* розглядаються процеси оцінювання і забезпечення готовності, функційної та інформаційної безпечності хмарних

систем критичних інфраструктур.

Відповідно, *предметом дослідження* є моделі, методи та інформаційні технології моніторингу, оцінювання і вибору характеристик надійності та безпеки хмарних систем для забезпечення готовності критичних інфраструктур.

Методи дослідження. У якості теоретичної основи при виконанні досліджень використовувалися методи системного аналізу, теорії імовірностей, стохастичні методи оцінювання, включаючи методи напівмарковського моделювання. Для розв'язування блоку наукових задач щодо забезпечення готовності критичних інфраструктур при моделюванні аварій та оцінці готовності КЕІ використовувався метод аналізу безпеки складних систем на основі модифікації алгебри причинно-наслідкових комплексів, розробленої професором В. О. Твєрдохлєбовим. В процесі розв'язування науково-прикладних задач по оцінюванню функційної безпечності та ризику негативних подій для хмарних систем критичних інфраструктур використовувалися методи побудови структурних схем надійності, дерев відмов та атак.

Наукова новизна отриманих результатів.

Уперше розроблено:

– методологію оцінювання готовності та вибору характеристик хмарних систем критичних інфраструктур, яка розвиває концепцію фон Неймана побудови систем високої готовності з недостатньо надійних і безпечних компонентів та, на відміну від відомих, базується на принципах реконфігурування фізичних і кіберактивів, комбінованої надмірності сервіс-орієнтованих ресурсів (додатків), оперативного моніторингу їхніх інформаційно-технічних станів, що дозволяє забезпечити доступність інтегрованих фізичних (віртуальних) компонентів інфраструктури в умовах негативних впливів;

– інформаційна технологія тестування регіональних хмарних систем з інтегрованими фізичними компонентами, яка, на відміну від відомих, визначає час затримки інформаційних потоків даних з застосуванням віртуального ресурсу реляційних баз даних, що дозволяє здійснити оптимальний вибір інформаційного

центру відповідного хмарного провайдера за критерієм мінімуму часу затримки.

Удосконалено:

– метод компаративістичного аналізу аварій критичної інфраструктури, який, на відміну від відомих, базується на застосуванні модифікованої алгебри причинно-наслідкових комплексів, їхньому логіко-цифровому представленні та агрегатуванні у вигляді структурно-логічних схем і аналітико-стохастичних моделей протікання аварій, що дозволяє оцінювати і формулювати рекомендації щодо зменшення їх ризиків;

– напівмарковські моделі готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин, які, на відміну від відомих, враховують параметри законів розподілення часу їхнього перебування в різних режимах застосування за призначенням при використанні принципу масштабованого розгортання сервіс-орієнтованих ресурсів, що дозволяє виконати обгрунтування граничних величин показників готовності хмарної інфраструктури з урахуванням її відмов і атак на вразливості;

– метод оцінювання функційної безпечності критичної інфраструктури за рахунок використання процедур аналітико-стохастичного моделювання та причинно-наслідкового аналізу відмов і аварій, що дозволяє виконувати кількісне оцінювання ризику з урахуванням негативного впливу на фізичні та кібернетичні активи;

– метод оцінки енергоефективності хмарної інфраструктури шляхом аналітико-стохастичного оцінювання споживаної потужності за результатами напівмарковського моделювання процесів зміни рівня готовності інтегрованих фізичних та віртуальних її компонентів, що дозволяє покращити архітектурну побудову інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів;

– метод вибору характеристик хмарних систем критичної інфраструктури шляхом послідовної реалізації процедур аналітико-стохастичного

моделювання зміни готовності хмарних компонентів, оперативного моніторингу інформаційно-технічних станів та оцінювання граничних величин відповідних характеристик готовності, що дозволяє підвищити надійність і безпеку критичних інфраструктур.

Дістав подальшого розвитку:

– метод моделювання та оцінювання готовності критичної інфраструктури, який враховує еволюційні аспекти її управління за інформаційно-технічним станом, базується на аналітико-стохастичному оцінюванні сервіс-орієнтованих хмарних ресурсів, які використовуються в загальному контурі управління, що дозволяє підвищити точність оцінки наслідків аварій інфраструктур.

Особистий внесок здобувача. Основні результати дисертаційної роботи опубліковано в 41 науковій праці, серед яких дві монографії; 23 статті в наукових виданнях України (з них 19 в наукових фахових виданнях України); 2 статті в закордонних періодичних виданнях країн Європейського Союзу (з них 1 стаття внесена до наукометричної бази Scopus); 14 публікацій у матеріалах і тезах міжнародних наукових конференцій (з них 5 внесено до наукометричної бази Scopus, 2 – до наукометричної бази Web of Science).

Основні наукові результати, що належать особисто авторові одноосібно опубліковано в роботах [1–6, 34–37]. В публікаціях, які написано у співавторстві, авторові належать: [7] – двохрівневі моделі управління готовністю критичних інфраструктур за технічним мегастаном; [8] – окремі принципи аналізу безпеки критичних інфраструктур; [9] – концепція управління технічним станом виробів критичного призначення; [10] – напівмарковська модель протікання аварії критичної енергетичної інфраструктури; [11] – основні положення методу причинно-наслідкової декомпозиції та аналітико-стохастичного моделювання аварії критичної енергетичної інфраструктури; [12] – окремі положення концепції технічного обслуговування компонентної складової критичної інфраструктури за станом; [13] – аналіз властивостей, що визначають якість застосування критичної

енергетичної інфраструктури за призначенням та причинно-наслідкова модель протікання аварії критичної енергетичної інфраструктури; [14] – марковська модель протікання аварії та визначення граничних величин показників надійності критичної енергетичної інфраструктури; [15] – оцінка надійності системи управління інфраструктурою з урахуванням безвідмовності програмного забезпечення критичного додатку; [16] – напівмарковська модель готовності хмарної інфраструктури з контролем технічного стану фізичних машин; [17] – концептуальні положення щодо побудови та обчислення метамоделі готовності хмарної інфраструктури; [18] – напівмарковська модель готовності хмарної інфраструктури з трьома підсистемами фізичних машин; [19] – таксономічна схему управління конфігурацією хмарної інфраструктури; [20] – математична модель цифрового засобу вимірювання з двохланцюговим аналого-цифровим пристроєм послідовного приближення; [21] – визначення морської критичної інфраструктури; [22] – стохастична модель енергоефективності хмарної інфраструктури з трьома підсистемами фізичних та віртуальних машин; [23] – концепція управління критичними інфраструктурами за технічним мегастаном; [24] – принципи реконфігурування, надлишковості сервіс-орієнтованих ресурсів; [25] – принципи оперативного моніторингу інформаційно-технічних станів хмарних систем; [26] – принципи побудови хмарної платформи для оцінки рівня готовності критичної енергетичної інфраструктури; [27] – оцінка ризику негативного впливу на фізичні та кібернетичні активи критичної енергетичної інфраструктури; [28] – модель готовності хмарної інфраструктури з урахуванням зловмисного шкідливого впливу; [29] – модель готовності хмарної інфраструктури з декількома підсистемами фізичних та віртуальних машин; [30] – оцінювання рівня гарантоздатності системи диспетчерського контролю та збору даних; [31] – принцип компліментарності побудови критичних інфраструктур; [32] – визначення цикломатичної складності для моделей функціонування компонентів критичних інфраструктур; [33] – принцип побудови причинно-наслідкового комплексу протікання аварії критичної енергетичної інфраструктури; [38] – моделі надійності морських рухомих об’єктів критичної інфраструктури для

їхнього технічного обслуговування за станом; [39] – критерій синтезу системи технічного діагностування критично важливих об’єктів; [40] – концепція та критерій управління готовністю критичних інфраструктур на основі застосування хмарних систем; [41] – аналіз механізму впливу DDoS-атак на програмне забезпечення критичних інфраструктур.

Апробація матеріалів дисертації. Основні положення й результати дисертаційного дослідження доповідалися й обговорювалися на Всеукраїнському науково-технічному семінарі «Критичні комп’ютерні технології та системи», який проводився на кафедрі комп’ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (м. Харків, 2012, 2016, 2018, 2019 рр.).

Крім того, представлені в дисертаційній роботі наукові результати доповідалися й обговорювалися на таких конференціях та семінарах:

Міжнародних: міжнародному науковому семінарі «Theory of Reliability and Markov Modeling for Information Technologies» (Київ, 2016, 2017 рр.); XX-й міжнародній науково-практичній конференції «Perspective Directions for the Development of Science and Practice» (Афіни, Греція, 2020 р.), XXI-й міжнародній науково-практичній конференції «Current Trends in the Development of Science and Practice» (Хайфа, Ізраїль, 2020 р.); міжнародних науково-технічних конференціях «Dependable Systems, Services and Technologies» (Кіровоград, 2007, 2009, 2010 рр., Севастополь, 2011–2013 рр., Київ, 2014, 2016, 2020 рр.), «Advanced Trends in Radioelectornics, Telecommunications and Computer Engineering» (Львів-Славське, 2018 р.), «International Symposium on Wireless Systems within the International Conference on Intelligent Data Acquisition and Advanced Computing Systems» (Львів, 2019 р.), «Автоматизація: проблеми, ідеї, рішення» (Севастополь, 2009–2013 рр.), «Інформаційні технології та інформаційна безпека в науці, техніці та освіті» (Севастополь, 2009–2013 рр.).

Всеукраїнських: «Математичні проблеми технічної механіки та прикладної математики» (Дніпро-Кам’янське, 2019 р.), «Фінансово-економічна стратегія

розвитку України в умовах сучасних геополітичних викликів (економіко-управлінські правові, інформаційно-технічні, гуманітарні аспекти)» (Дніпропетровськ, 2015 р.).

Зв'язок роботи з науковими програмами, планами, темами, грантами. Робота над дисертацією проводилася на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» у 2010–2020 рр. згідно з планами науково-дослідних робіт Міністерства освіти і науки України за держбюджетними темами та програм міжнародних проєктів, саме:

– Методологічні засади та технології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур (Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» ДР №0119U100979, 2019–2021 рр.);

– Методологія сталого розвитку та інформаційні технології зеленого комп'ютингу та комунікацій (Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» ДР № 0118U003822, 2018–2020 рр.);

– Наукові основи, методи та засоби зеленого комп'ютингу та комунікацій (Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» ДР № 0115U000996, 2015–2017 рр.);

– Проєкт Європейського Союзу SAFEGUARD 158886-TEMPUS-1-2009-1-UK-TEMPUS-JPCR «National Network of Centres for Innovative Academia-Industry Cooperation on Safeware Engineering» (2010–2013 рр.);

– Проєкт Європейського Союзу TEMPUS-GREENCO (Green Computing and Communication) 530270-TEMPUS-1-2012-UK-TEMPUS-JPCR (2012–2015 рр.);

– TEMPUS-SEREIN (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains) 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR (2013–2016 рр.).

Практичне значення отриманих результатів полягає в тому, що запропоновані методи, моделі є теоретичним і науково-практичним підґрунтям

для розроблення та імплементації алгоритмів, програмних засобів, а також інформаційної технології тестування регіональних інформаційних центрів хмарного провайдера, які застосовуються в системі забезпечення готовності, функційної безпечності критичних інфраструктур. Результати дисертації впроваджено (див. додаток Б) у процесі розробки техніко-економічного обгрунтування, оцінювання ризику та функційної надійності окремих компонентів космічної програми України в Інституті технічної механіки Національної академії наук України (акт впровадження від 11.07.2020 р.); у вигляді процедур оцінювання та категоризації систем критичної енергетичної інфраструктури за рівнем ризику в публічному акціонерному товаристві «НВП «Радій» (акт впровадження від 11.09.2020 р.); при розробці нормативних документів для оцінювання рівня готовності та функційної безпечності критичної енергетичної інфраструктури, при виконанні ризик-аналізу міні платформи для розумних енергетичних мереж і тестового стенду для перевірки параметрів енергозабезпечення в публічному акціонерному товаристві «НВП «Радікс» (акт впровадження від 16.09.2020 р.); при розробленні методичних матеріалів для оцінювання та категоризації критично важливих об’єктів у Приватному акціонерному товаристві «Інститут інформаційних технологій» (акт впровадження від 16.10.2020 р.); при проєктуванні резервного контуру управління та для оцінки інфокомунікаційних каналів хмарного забезпечення компонентів критичної інфраструктури Товариства з обмеженою відповідальністю «Радіо Інформаційні Технології» (акт впровадження від 10.09.2020 р.); при проведенні лекцій та практичних занять з методів оцінювання та забезпечення готовності хмарних систем критичних інфраструктур для студентів Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (акт впровадження від 12.12.2019 р.); у вигляді науково-теоретичних положень в наукових проєктах за держзамовленням і міжнародних проєктах, які виконувалися за держзамовленням Національним аерокосмічним університетом ім. М. Є. Жуковського «Харківський авіаційний інститут» (акт впровадження від 16.12.2019 р.).

Структура та обсяг дисертації. Дисертація має анотацію, вступ, сім розділів, висновки, перелік використаних джерел, додатки; повний обсяг дисертації викладено на 336 сторінках, з яких анотація на 12 сторінках, зміст на 8 сторінках, перелік умовних позначень на 3 сторінках, основний текст на 264 сторінках, список використаних джерел зі 196 найменувань використаних джерел на 23 сторінках, додатки на 25 сторінках. Робота містить 26 таблиць, з яких 6 таблиць на 10 окремих сторінках, і 149 рисунків, з яких 3 рисунки на 3 окремих сторінках.

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ТА ОЦІНЮВАННЯ ГОТОВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР

1.1 Аналіз впливу хмарних систем на функційну безпечність критичних інфраструктур

1.1.1 Проблема впливу хмарних систем на функційну безпечність критичних інфраструктур

Одним з перспективних напрямків розвитку сучасних інформаційних технологій є хмарні обчислення та сервіси, які реалізуються на основі використання відповідних хмарних систем. За останнє десятиріччя хмарні системи досить швидко трансформувалися в діючий інформаційний галузевий стандарт, що використовується при виробництві різних видів продукції.

Потужні світового рівня IT компанії (Amazon, Microsoft, Google, IBM, Apple) застосовують хмарні системи для надання широкого спектру послуг, які охоплюють бізнес-процеси, процедури щодо зберігання та управління інформацією. Хмарні системи активно використовуються державними галузевими підрозділами, включаючи їхні інфраструктурні складові. Критичні інфраструктури не є виключенням і в тій, чи іншій мірі функціонують з застосуванням хмарних систем. Це пов’язано з переходом до цифрового формату представлення інформації, що суттєво покращує швидкодію, збільшує динамічне обчислювальне навантаження критичних інфраструктур; створює цифровий базис для реалізації програми Industry 4.0 і т.і.

Насьогодні хмарні системи активно застосовуються для управління компонентами, моніторингу робочих режимів та контролю інформаційно-технічного стану критичних інфраструктур [1]. Характеристика деяких проєктів на основі використання хмарних систем, що застосовуються для забезпечення ефективного функціонування критичних інфраструктур з урахуванням їхніх переваг та недоліків представлена в таблиці 1.1.

Таблиця 1.1

Характеристика проєктів та технологій на основі застосування ХМС для забезпечення ефективного функціонування КІ

Назва проєкту	Призначення	Переваги	Недоліки
Smart Grid [2]	Створення інтелектуальних (розумних) розподілених мереж з застосуванням ХМС	Оперативність виконання команд управління енергетичними потоками; використання ХМС дозволяє реалізувати нову парадигму управління критичною енергетичною інфраструктурою за рахунок гнучкості застосування обчислювальних ресурсів, їхньої міграції на рівні фізичних та віртуальних машин	Висока залежність від інтернет комунікацій вимагає використання великої кількості маршрутизаторів; низька фактична готовність хмарних систем (наприклад, відмова ХМС AWS в 2017 р.).
Grid Cloud [1]	Застосування ХМС AWS для управління ресурсами КЕІ в режимі реального часу	Покращення можливостей щодо динамічного управління ресурсами КЕІ; створення на основі застосування ХМС системи оперативного моніторингу інформаційно-технічних станів та параметрів компонентів КЕІ	Залежність енергетичних регуляторів від хмарного провайдера; не обгрунтовані вимоги до функційної та інформаційної безпеки ХМС
Grid Stat [3]	Створення системи динамічного моніторингу параметрів КЕІ на основі ХМС	Підключення великої кількості сенсорів; час затримки інформації не перевищує одну секунду; оперативне виявлення аномалій, включаючи зловмисні шкідливі впливи та проникнення	Низька кібербезпека, проблема синхронізації передачі даних
CloudIoT [4]	Створення мережі інтернету речей, підключеної до хмари з метою управління енергомережою КЕІ	За допомогою ХМС підтримуються ефективні та практичні рішення щодо управління компонентами КЕІ з застосуванням інтернету речей	Виклики інформаційній безпеці; перевантаження мережі великим обсягом даних; синергічність ХМС та модулів інтернету речей приводить до енерговтрат

Проаналізувавши інформацію щодо представлених проєктів, можна дійти висновку, що використання хмарних систем з метою забезпечення ефективного функціонування критичних інфраструктур має певні проблеми. Серед яких слід відзначити вплив відомих фактів відмов ХМС провідних хмарних провайдерів, що безумовно не може не викликати стурбованості у розробників та вчених, які працюють за напрямком оцінювання і забезпечення функційної безпечності критичних інфраструктур. Саме така вкрай негативна подія відбулася у лютому 2017 р., коли хмарні системи Amazon S3 були відключені та недоступні внаслідок неправильних дій обслуговуючого персоналу [5] на протязі п’яти годин у межах США, що спричинило серйозні фінансові збитки як для звичайних користувачів, так і для окремих хмарних провайдерів, наприклад Apple iCloud. Після цієї події виникли сумніви у готовності хмарних систем на рівні чотирьох дев’яток після коми. Відповідно ця обставина також суттєво знизила цінність пропозицій Amazon S3 [6]. Проте за минулий період з 2017 р. компанія Amazon засвоїла цей важливий урок і змогла виправити ситуацію, відновивши колишню репутацію лідера серед хмарних провайдерів. В значній мірі розв’язуванню проблеми сприяла направленість компанії на реалізацію одного з підходів DevOps інженіринга, згідно якого виконується фрагментація загального сервісного ресурсу. У той же час при використанні цього підходу водночас підвищується доступність відповідного ресурсу, але знижується гнучкість його управління. З зазначеного витікає, що проблема оцінки готовності хмарних систем і їх впливу на функційну безпечність критичних інфраструктур, як і раніше, не втратила своєї актуальності. Для осмислення проблеми та пошуку шляхів її розв’язування необхідно виконати аналіз побудови хмарних систем і їхніх можливостей щодо забезпечення функційної безпечності КІ.

У якості формальної підстави для проведення досліджень розглядалися Указ Президента України №27/2020 “Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242”; “Концепція створення державної системи захисту критичної інфраструктури”, яка схвалена розпорядженням Кабінету міністрів України від 6 грудня 2017 р.

№1009–р.; рішення Уряду від 18 березня 2021 р. про підтримку проєкту Закону України “Про критичну інфраструктуру та її захист”.

Згідно загальної концепції, що розроблена Національним інститутом США зі стандартизації та технологій (НІСТ) [7], хмарні обчислення реалізуються у відповідності з трирівневою класифікаційною схемою, яка представлена на рис. 1.1.

Рис. 1.1 Класифікаційна схема хмарних обчислень [7]

Відповідно до рис. 1.1 перший рівень класифікаційної схеми НІСТ враховує основні характеристики хмарних обчислень; другий рівень представляє моделі надаваємих хмарними системами послуг (сервісів); третій рівень утворений відповідними типами ХМС. Безумовно зображена класифікаційна схема хмарних обчислень не є догмою і може змінювати свою конфігурацію в залежності від необхідності використання сервіс-орієнтованих ресурсів для розв’язування конкретних завдань, включаючи застосування ХМС для забезпечення функційної безпечності критичних інфраструктур.

Найбільшу зацікавленість з точки зору зручності використання ресурсу викликає хмарна інфраструктура (рис. 1.1), оскільки за результатами виконаного аналізу саме на основі цієї моделі реалізуються найбільш відомі проєкти по управлінню критичними енергетичною та морською інфраструктурами. Тому має сенс розглянути ключові фактори ненадійності, що впливають на функційну та інформаційну безпеку цих типів КІ.

1.1.2 Аналіз ключових факторів ненадійності критичних інфраструктур на прикладі критичної енергетичної та морської критичної інфраструктур

Відомо, що на сучасному етапі розвитку суспільства проблема ненадійності критичної енергетичної інфраструктури набула глобального характеру. Про що свідчать наслідки найбільш відомих у світі аварій [8], які відбулися за останні сімнадцять років на АЕС Фукусіма–1 (Японія, 2011 р.), Саяно-Шушенській ГЕС (Росія, 2009 р.); аварії енергетичних систем США та Канади у серпні 2003 р., енергетичних систем Італії та Швейцарії, Швеції і Данії у вересні 2003 р. та інші.

Усвідомлення відомих факторів ненадійності та різноманітних загроз обумовило необхідність проведення поглибленого аналізу загальної структури існуючих активів критичних інфраструктур, до складу яких входять фізичні і кібернетичні активи (рис. 1.2).

Рис. 1.2 Загальна структура існуючих активів КІ

Необхідно відзначити, що структурно активи КЕІ побудовані аналогічно (рис. 1.3). Безумовно невирішених проблем, пов’язаних з функціоальною безпекою КЕІ, з іншими різноманітними загрозами існує велика кількість.

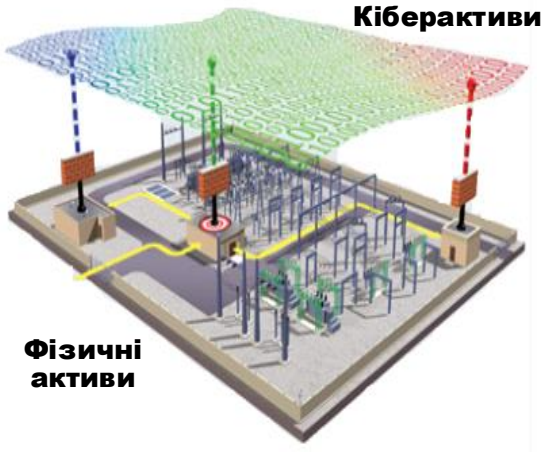


Рис. 1.3 Активи критичної енергетичної інфраструктури

За останні десять років, завдяки удосконаленню енергообладнання і державній регуляторній політиці, статистика відключень КЕІ по технічним причинам в Європі та США декілька покращилась (рис. 1.4). В той же час зростання загальних обсягів споживаємої електроенергії (рис. 1.5), ролі та масштабів задач, які вирішуються КЕІ, призвели до збільшення кількості цифрових пристроїв, інформаційних технологій, що застосовуються в системі моніторингу і контурі управління інфраструктурою.

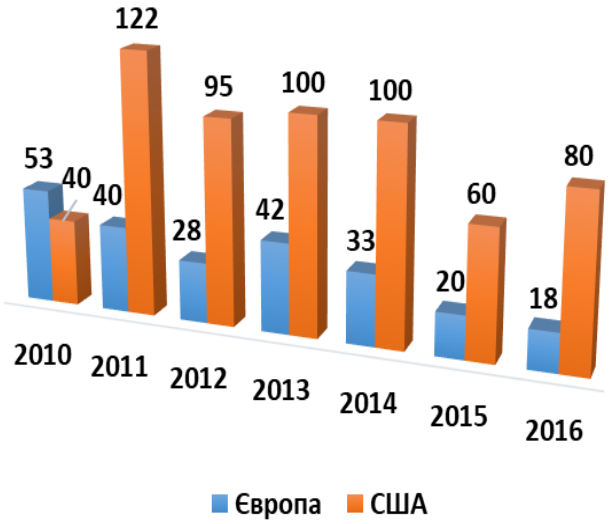


Рис. 1.4 Відключення КЕІ по технічним причинам [9]

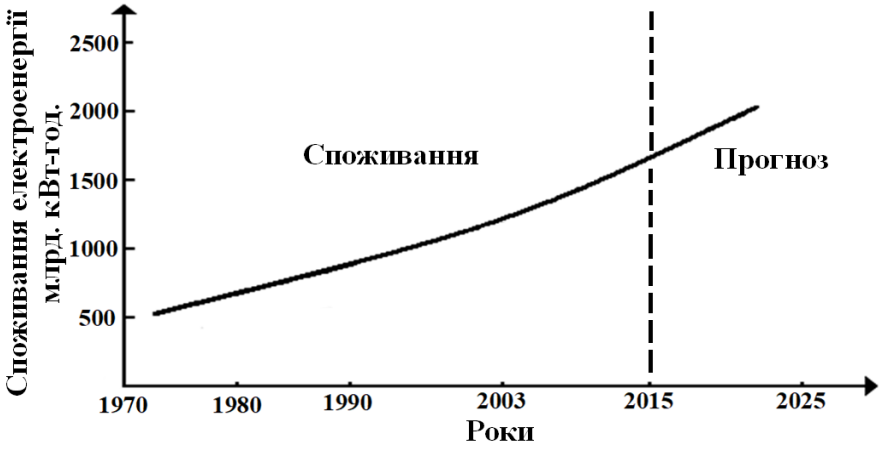


Рис. 1.5 Прогнозоване зростання споживання електроенергії

Фактично впровадження сучасних інфокомунікаційних технологій повністю дублює інформацію, яка стосується перетоків енергії в лініях електромережі КЕІ з урахуванням їхньої топології, що дозволяє здійснити перехід до цифрового формату управління інфраструктурою з використанням відповідного програмного забезпечення (ПЗ) для інформаційно-керуючих систем (ІКС) інфраструктури [10–12]. Але з використанням ПЗ для ІКС критичної енергетичної інфраструктури виникають вразливості, якими неодмінно користуються зловмисники. Продуктами їхньої цілковито руйнівної діяльності є зловмисні шкідливі впливи (ЗВШВ), що реалізуються у вигляді атак на кібернетичні активи КЕІ.

Україна як держава, що розвивається, має досить складну розгалужену енергомережу КЕІ, управління якою також здійснюється в цифровому форматі. Нажаль за останні декілька років рівень ЗВШВ на кібернетичні активи національної КЕІ суттєво виріс, про що свідчать статистичні дані, які відображено на рис. 1.6.

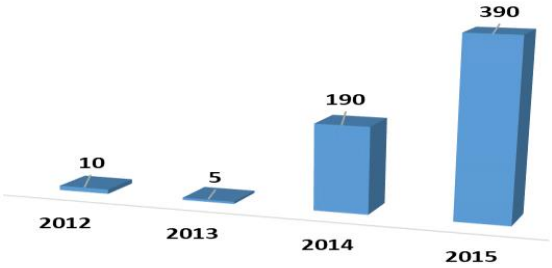


Рис. 1.6 Зростання ЗВШВ на кіберактиви КЕІ України

Відповідно до рис. 1.6 безпрецедентне зростання кількості ЗВШВ на кіберактиви КЕІ у 2015 р. пояснюється ворожою дією колективної спільноти зловмисників (КЗС). Одна з таких атак за участю КЗС відбулася у грудні 2015 р., коли було здійснено зловмисний шкідливий вплив на кібернетичні активи Тернопільської обленерго, що призвело до тяжких наслідків, а саме, відбулося повне знеструмлення області. На рис. 1.7 відображено хронологію негативних подій атаки, аналіз якої виконано в роботі [13].

Детальний аналіз ЗВШВ на кібернетичні активи національної критичної енергетичної інфраструктури виконано в роботах [14–16]. Результати аналізу свідчать, що у відповідності з міжнародним стандартом ISO/IEC 15408 за умови цілеспрямованої дії колективної спільноти зловмисників з застосуванням різноманітних сценаріїв атаки на кібернетичні активи інфраструктури при відсутності ефективних контрзаходів щодо зниження їхньої вразливості, зловмисні шкідливі впливи підвищують ризики негативних подій [17] для КЕІ. Отже, у цих умовах зловмисні шкідливі впливи стають одним з ключових факторів ненадійності, який впливає на функційну та інформаційну безпечність КЕІ та може привести до аварій інфраструктури.

Рис. 1.7 Хронологія атаки на кіберактиви Тернопільської обленерго [13]

У якості другого прикладу для аналізу факторів ненадійності пропонується розглянути морську критичну інфраструктуру (МКІ), активи якої утворюють морські рухомі об’єкти (МРО), служба маяків, доки, причали, склади, стівідори, засоби Глобальної морської системи зв’язку та забезпечення безпеки мореплавства (ГМСЗБ) (рис. 1.8). Загальне управління морськими рухомими об’єктами та іншими компонентами МКІ здійснюється Адміністрацією морських портів України (АМПУ).

Рис. 1.8 Активи морської критичної інфраструктури

З точки зору професійної направленості та впливу факторів ненадійності найбільший інтерес представляють МРО, до яких відносяться морські судна з різними класифікаційними ознаками [18]. Трьохрівнева ієрархічна структура морського рухомого об’єкту МКІ відображена на рис. 1.9.

Рис. 1.9 Ієрархічна структура морського рухомого об'єкту МКІ [19]

Відповідно до ієрархічної структури (рис. 1.9) в роботах [20–23] проведено дослідження, які дозволяють встановити найбільш вразливі системи МРО, що чутливі до впливу чинників ненадійності. Вплив зовнішніх та внутрішніх факторів ненадійності у взаємодії з загрозами та вразливостями для відповідних кібернетичних активів може призвести до аварії МРО. Структура моделі ризику морського рухомого об'єкту МКІ з урахуванням надійності відповідних систем та впливу загроз, вразливостей кібернетичним активам МРО зображена на рис. 1.10.

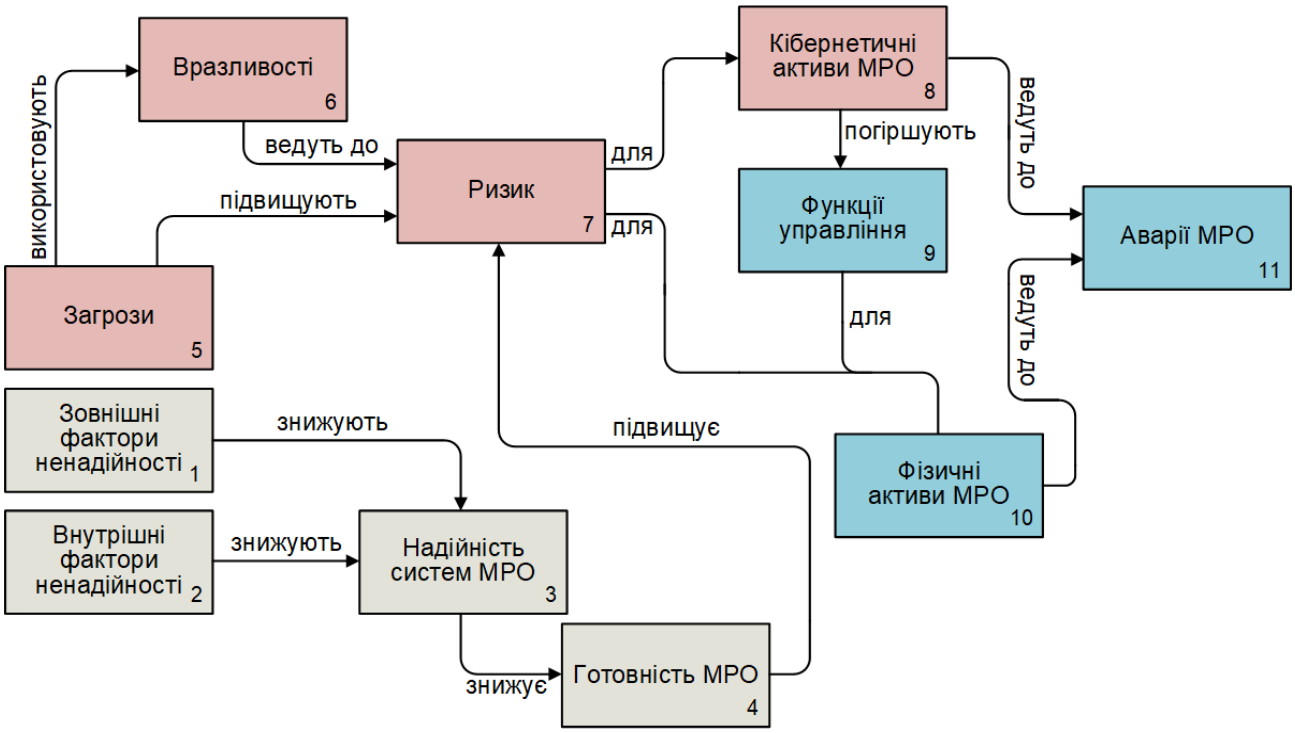


Рис. 1.10 Структура моделі ризику морського рухомого об'єкту МКІ

На рис. 1.10 блоки 5–8 відображені у відповідності до моделі інформаційної

безпеки, яка описана в роботі [17]; решта блоків 1–4, 9–11 запропонованої моделі отримані автором самостійно за результатами виконаного дисертаційного дослідження. Характеристика вразливостей систем МКІ, розглянутих в роботах [22, 23], приведена в таблиці 1.2.

Таблиця 1.2

Характеристика вразливостей систем МКІ

Системи МРО з вразливістю	Вид впливу	Наслідки	Реалізація
Глобальна навігаційна система (GNSS), Глобальна система позиціонування (GPS)	Завади, підміна сигналу	Відхилення від курсу МРО, посадка на мілину, екологічні катастрофи	В 2016 р. декілька суден США повідомляють про завади GPS. В 2017 р. 20 суден повідомляють про викривлення сигналу GPS з метою навмисної фальсифікації координат МРО
IT мережі судноходних компаній	Комп'ютерний вірус "NotPetya"	Неможливість використовувати за призначенням критично важливі системи	В 2017 р. збитки датської суднохідної компанії A.P. Moller-Maersk внаслідок кібератаки з використанням комп'ютерного вірусу "NotPetya" встановили $300 млн.

Узагальнений аналіз недоліків та вразливостей систем морських рухомих об'єктів МКІ представлено на рис. 1.11. Отримані результати свідчать, що основний внесок в ризики для морських рухомих об'єктів МКІ, які в значній мірі виникають за рахунок впливу факторів ненадійності, належить наступним бортовим системам:

1) IT мережі;

2) система диспетчерського управління та збору даних (SCADA);

3) автоматична система ідентифікації морських рухомих об'єктів;

4) інформаційна система електронного картографування;

5) антенні термінали з малою апертурою;

6) система екологічного та радіаційного моніторингу;

7) система ГМСЗБ.

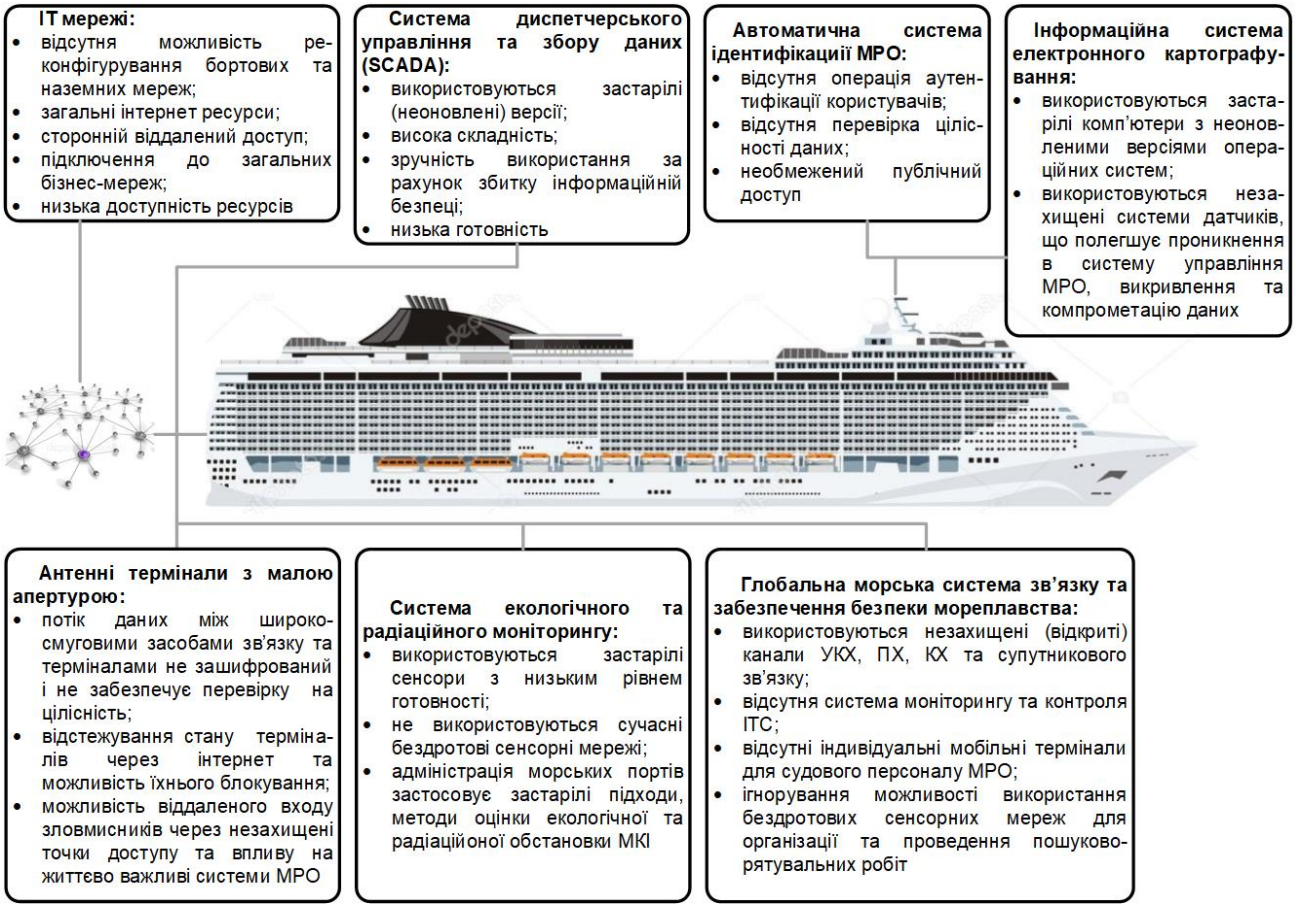


Рис. 1.11 Аналіз недоліків та вразливостей систем МРО МКІ [23]

Для усунення цих недоліків та пом'якшення виникаючих ризик-факторів для КІ пропонується застосовувати хмарні системи, які розглядаються в наступному підрозділі.

1.1.3 Аналіз розвитку систем моніторингу на основі застосування хмарних систем важливих для забезпечення функційної безпечності критичних інфраструктур

Оцінка та контроль функційної безпечності КІ базуються на застосуванні даних щодо інформаційно-технічних станів і параметрів критично важливих об'єктів, які входять до складу конкретної інфраструктури. Фактично це визначає необхідність здійснювати цілодобовий моніторинг ІТС і параметрів відповідних компонентних складових критичних інфраструктур.

Високого рівня деталізації моніторингових процесів КІ можна досягти,

використовуючи цифровий формат представлення інформації. В цьому випадку глибина та повнота контролю ІТС компонентів критичної інфраструктури тим більше, чим більше функціональних та технологічних процесів дублюється в цифровому форматі. Досягти високої щільності цифрового покриття моніторингових процесів КІ представляється можливим за рахунок застосування сервіс-орієнтованих ресурсів провідних хмарних провайдерів, а саме: Amazon, Google, Microsoft, IBM. Потужні обчислювальні ресурси та гнучкі сервіси зазначених хмарних провайдерів за умови наявності інфокомунікаційних зв'язків між інфраструктурними компонентними складовими надають можливість створити в буквальному сенсі цифровий образ будь-якої критичної інфраструктури, побудувати її досить точну системну модель [24–26].

На рис. 1.12 пояснюється загальна концепція процесу моніторингу параметрів енергетичної системи [27], яка входить до складу КЕІ.

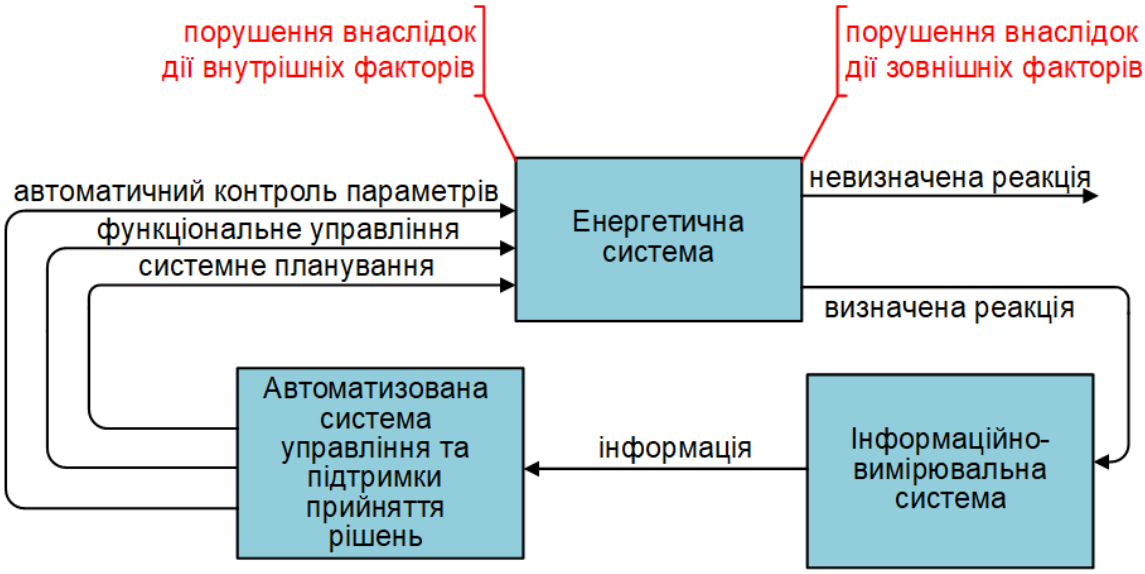


Рис. 1.12 Концепція моніторингу параметрів енергетичної системи [27]

Відповідно до рис. 1.12 порушення, які виникають внаслідок дії факторів зовнішнього та внутрішнього впливу можуть призвести до негативних подій з тяжкими наслідками (наприклад, аварії, інциденти тощо). Причиною цього до недавнього часу була невідповідність ІКС типу SCADA викликам і загрозам, що постійно виникали для національних енергетичних систем під впливом зовнішніх та внутрішніх факторів впливу, до яких можна віднести: стихійні лиха, дисбаланс

між централізованими й децентралізованими стратегіями управління перетоками енергії, високий (понад 70%) рівень зносу критично важливих об’єктів національної енергоінфраструктури, помилки обслуговуючого персоналу, кібератаки, нехтування заходами технічного обслуговування, порушення правил технічної експлуатації тощо.

За результатами аналізу також встановлено, що невпровадження сучасних систем моніторингу в минулому і насьогодні залишається одним з найсерйозніших недоліків. Тому на рубежі XX та XXI століть була розроблена і запропонована для застосування за призначенням система синхронізованих векторних вимірювань (ССВВ). Однією з переваг ССВВ у порівнянні зі SCADA [28] є можливість реалізації оперативного моніторингу параметрів компонентів інфраструктури, які впливають на функційну безпечність КІ, за рахунок збільшення як частоти, так і швидкодії виконання вимірювальних операцій на основі використання синхрофазорів, принцип функціонування яких розглянуто в [29–31]. Порівняльний аналіз можливостей ССВВ та SCADA представлено в розділі 2.

Інша проблема стосується зростання обсягів виробляємої та споживаємої суспільством електроенергії (рис. 1.5), яка водночас супроводжується різким збільшенням обсягів інформації, що представляється в цифровому форматі. В цих умовах можливості SCADA щодо реалізації операцій запису, зберігання та аналітичної обробки інформаційних потоків даних великих обсягів обмежені. Відомо, що зазначені обмеження сприяють виникненню серйозних порушень та помилок обслуговуючого персоналу, що призводять до негативних наслідків і є причиною зниження функційної безпечності КЕІ. За цих умов використання ХМС [32, 33] для вирішення проблем функційної безпечності КЕІ є цілковито обгрунтованим.

Вирішенню проблеми забезпечення функційної безпечності КІ сприяє той факт, що сучасні ХМС надають можливість отримувати, обробляти та аналізувати інформаційні потоки даних в режимі реального часу, що суттєво розширює динамічний діапазон, покращує ефективність роботи системи управління і

моніторингу КЕІ. Ці обставини сприяють всебічному висвітленню інформації щодо функціонування різноманітних компонентних складових інфраструктури, дозволяють попередити їхні відмови і решту збоїв на основі реалізації певних сервіс-орієнтованих функцій ХМС.

Найбільш складні функції відтворення та аналізу аварійних ситуацій також можуть бути реалізовані у вигляді додаткових хмарних сервісів, які мають під собою відповідне наукове підґрунтя і розробляються з використанням сучасних наукових методів. Крім того, ХМС можуть бути задіяні для інформаційного забезпечення симуляторів, що відтворюють відповідні негативні події і застосовуються для підготовки обслуговуючого персоналу КІ до дій в екстремальних ситуаціях (аварії, інциденти, критичні відмови тощо). Таким чином, ХМС можуть суттєво впливати на важливі аспекти функційної безпечності КІ та підтримувати необхідний рівень її готовності, безвідмовності та живучості.

1.2 Аналіз впливу хмарних систем на інформаційну безпеку критичної енергетичної та морської критичної інфраструктур

Не менш суттєво ХМС можуть впливати на інформаційну безпеку КІ, доповнюючи їхні фізичні (ФА) та кібернетичні активи (КБА), утворюючи таким чином хмарні активи (ХМА). Отже, існуюча структура активів критичних інфраструктур (рис. 1.2) може бути трансформована в перспективну, до складу якої входять ФА, КБА та ХМА (рис. 1.13).

Рис. 1.13 Спрощена перспективна структура активів КІ

Розглядаючи зображену на рис. 1.13 структуру КІ як базову, має сенс проаналізувати вплив хмарних систем на інформаційну безпеку критичної енергетичної та морської критичної інфраструктур. Безумовно перш ніж це зробити виконаєм аналіз інформаційної безпеки самих хмарних систем.

1.2.1 Аналіз інформаційної безпеки хмарних систем

Динамічний розвиток сучасних ХМС та їхні переваги у порівнянні з типовими комп'ютерними мережами сприяє збільшенню обсягів міграції даних підприємств, державних установ, корпоративного бізнесу в сферу хмарних обчислень. Водночас це породжує ще більші спокуси для хакерської спільноти, яка розглядає тенденції розвитку ХМС як нові можливості щодо реалізації зловмисних шкідливих впливів для отримання ще глибшого доступу до корпоративних ресурсів [34].

Як і більшість типових ІТ-впроваджень ХМС мають вразливості, завдяки яким зловмисники здійснюють кібератаки з серйозними наслідками у вигляді багатомільйонних фінансових втрат. На рис. 1.14 відображено сфери, що представляють загрозу інформаційній безпеці на технічному і юридичному рівнях організації ХМС.

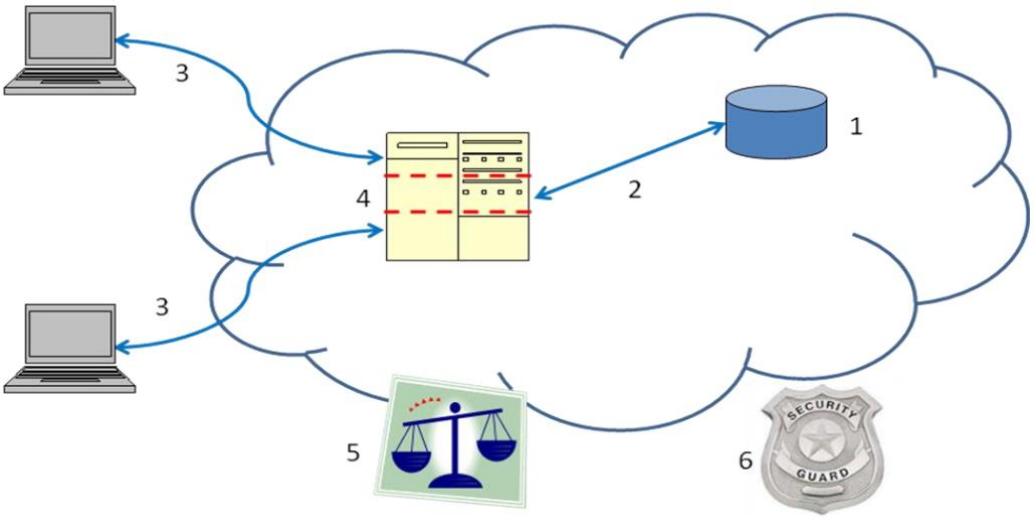


Рис. 1.14 Найбільш вразливі зони хмарних систем [35]

У відповідності до рис. 1.14 до сфер загрози інформаційній безпеці хмарних систем відносяться [35]:

1) дані, що зберігаються в базах даних, сховищах даних тощо;

2) дані, що передаються по інфокомунікаційним каналам зв’язку;

3) процес аутентифікації користувачів;

4) розподілення клієнтів та їхній віддалений доступ;

5) юридичні та нормативні питання щодо організації і застосування за призначенням ХМС;

6) оперативна відповідь на інциденти.

Актуальність цих загроз зросла під час пандемії COVID19. За даними Федерального бюро розслідувань США кількість кіберзлочинів в цей період збільшилася на 300% [36]. В 2020 році неправильно налаштоване хмарне середовище було основною причиною рекордної кількості порушень, що призвело до витоку великої кількості персональних даних користувачів та мільярдних фінансових втрат [37]. Кожну хвилину втрати від фішингових кібератак складають 17700 американських доларів [38]. Тим не менше, підстав для відмови від користування ХМС не існує саме тому, що провідні хмарні провайдери (Amazon, Microsoft, Google, IBM) використовують потужний арсенал засобів кіберзахисту пасивного та активного типу, розглядаючи це як один зі

способів забезпечення інформаційної безпеки. До них відносяться сукупність програмно-апаратних засобів, які забезпечують доступність, цілісність та конфіденціальність даних.

Крім внутрішніх засобів застосовується зовнішній контур захисту, який створюється, як правило, за допомогою компаній-партнерів відповідних хмарних провайдерів. Наприклад, Amazon користується послугами та відповідними сервісами тридцяти однієї компанії, які фактично об'єднані в єдиний хаб (тобто мережевий вузол, концентратор тощо) з кібербезпеки [39]. В таблиці 1.3 приведена характеристика деяких найбільш відомих компаній-партнерів, які входять до цього хабу та співпрацюють з Amazon (AWS), забезпечуючи виконання комплексу заходів з кібербезпеки.

Таблиця 1.3

Характеристика компаній-партнерів, які входять до складу AWS хабу з кібербезпеки

Назва компанії-партнера	Характеристика засобів кіберзахисту
Barracuda [40]	Безагентний власний програмний сервіс з безпеки AWS, який контролює рівні управління та застосування даних. Сервіс автоматизує реалізацію безпеки при створенні додатків в AWS шляхом сканування власною антивірусною програмою Cloud Storage Shield інформації, яка знаходиться у сховищах даних; при появі будь-якої загрози для робочого інформаційного ресурса поміщає продукт в карантин, формує і відправляє звіти в AWS хаб з кібербезпеки
Check Point [41]	Хмарний програмний антивірусний сервіс (Check Point CloudGuard) доповнює власні засоби управління AWS, забезпечуючи підвищену безпеку для захисту клієнтських середовищ та програмного забезпечення навіть від самих складних загроз. Сервіс формує контекстну інформацію щодо безпеки, про зони доступності та динамічно оновлює політики безпеки. Клієнти можуть швидко забезпечити універсальний захист від кібератак, застосовуючи єдину консолідовану консоль
IBM Security [42]	Інтегрована система аналітики та захисту в реальному часі, яка підтримує AWS хаб з кібербезпеки і автоматизує перевірку відповідності на єдиній інформаційній панелі. Для кращого аналізу система працює в гібридному середовищі, використовуючи розподілені за пріоритетами агреговані дані про безпеку та події з декількох сервісів AWS. Система дозволяє отримати консолідовані наочні графіки та таблиці, що надає можливість аналітикам з кібербезпеки заглублятися в дані про події AWS для швидкого і точного виявлення загроз; водночас реагувати на виклики, покращуючи стан дотримання нормативних вимог

Продовження таблиці 1.3

Назва компанії-партнера	Характеристика засобів кіберзахисту
McAfee [43]	Інтеграція хмари McAfee з AWS хабом по кібербезпеці забезпечує єдину точку огляду і контролю через програмне забезпечення, платформу та інфраструктуру для захисту корпоративних даних і захисту організацій від кіберзагроз. Хмара McAfee фактично дозволяє клієнтам створювати екосистеми безпеки та управління подіями гнучким інтуїтивно зрозумілим способом
Splunk [44]	Клієнти можуть використовувати існуючу інтеграцію Splunk з хмарою Amazon для отримання даних безпосередньо з AWS хабу по кібербезпеці. За допомогою ресурсу Splunk організації можуть ставити запитання, отримувати відповіді, вживати заходи і добиватися бізнес-результатів на основі своїх даних. Організації використовують провідні на ринку рішення Splunk з машинним навчанням для моніторингу, дослідження та вжиття заходів щодо всіх форм даних бізнесу, IT, безпеки та Інтернету речей. Інтеграція Splunk з AWS хабом з кібербезпеки покликана допомогти клієнтам ще більше прискорювати процеси виявлення, розслідування і реагування на потенційні загрози в їх середовищі
Vectra [45]	Ресурс Vectra створює можливості щодо кібербезпеки, застосовуючи передовий штучний інтелект для виявлення ризиків, що створюються неавторизованими користувачами, і реагує на них. Хмарна платформа Vectra запобігає витоку даних за рахунок автоматичного виявлення і визначення ризиків безпеці, що відправляються в AWS хаб з кібербезпеки; прискорює розслідування, забезпечує упереджувану ідентифікацію ризиків і ініціювання негайного інтелектуального контролю

За характером протидії зловмисним шкідливим впливам засоби, характеристика яких представлена в табл. 1.3, відносяться до засобів кіберзахисту пасивного типу, тобто їхня дія направлена на виявлення, по можливості блокування та пом’якшення наслідків дії ЗВШВ. На відміну від них існують засоби кіберзахисту ХМС активного типу, які реалізують три модульні компоненти, а саме: попередження атаки, її виявлення та активне реагування. Принцип функціонування таких засобів кіберзахисту полягає в тому, щоб зупинити рух зловмисника в будь-якому місці гібридних та мультиагентних ХМС

[46] і сформувати відповідь у вигляді зворотнього зловмисного шкідливого впливу.

Таким чином, можна вважати, що хоча ХМС мають певні вразливості, але все ж таки рівень їхнього кіберзахисту перевищує аналогічний показник для типових компонентів кібернетичних активів, що надає можливість використовувати їх для забезпечення функційної та інформаційної безпеки критичних інфраструктур.

1.2.2 Аналіз впливу хмарних систем на інформаційну безпеку критичної енергетичної інфраструктури

Проведений аналіз [33, 47, 48] підтверджує, що за останні декілька років кількість цільових кібератак на КБА критичною енергетичною інфраструктури, які привели до аварій та відключень об’єктів інфраструктури суттєво збільшилася. Однією з найважливіших причин цих негативних подій є збільшення поверхні атак за рахунок застосування сучасних ІТ, інтелектуальних пристроїв управління та впровадження інтернету речей. Для усунення причин цих негативних подій пропонується комплекс заходів по забезпеченню інформаційної безпеки [49] та гарантоздатності національної критичної енергетичної інфраструктури, ключове місце в якому займає аварійне відновлення кібернетичних активів КЕІ з використанням резервних копій. Серед переваг використання ХМС для забезпечення інформаційної безпеки КЕІ слід також відзначити: а) можливість реалізації надлишкового принципу захисту кіберактивів інфраструктури шляхом створення адаптивних багатофункціональних брандмауерів; б) можливість здійснювати контроль за точками доступу до сховищ даних інфраструктури та надання (тунельних) каналів зв’язку.

Зазначені потреби можна задовольнити, застосувавши хмарні системи та сервіси компанії Amazon. У таблиці 1.4 відзначені наступні аспекти інформаційної безпеки та гарантоздатності [50] критичної енергетичної інфраструктури, забезпеченню яких сприяє застосування AWS: A1 – аварійне

відновлення і резервне копіювання кібернетичних активів КЕІ; А2 – узагальнення викликів, які обумовлені несправностями та змінами вимог і умов застосування за призначенням КЕІ; А3 – покращення аналізу забезпечення відмовостійкості кібернетичних активів КЕІ; А4 – багатоверсійні обчислення у контексті факторів еволюційного розвитку кібернетичних активів КЕІ.

Таблиця 1.4

Застосування AWS для забезпечення інформаційної безпеки та гарантоздатності КЕІ

Назва сервісу AWS	Призначення сервісу AWS	Аспекти забезпечення інформаційної безпеки та гарантоздатності КЕІ на основі AWS			
		А1	А2	А3	А4
Управління брандмауерами Amazon	Гнучке управління процесами фільтрації трафіку	–	–	+	–
Аналітика потокових даних Amazon Kinesis	Прийом, обробка, аналіз аномалій, розподілення та доставка інформаційних потоків даних	–	+	+	+
Хмарне сховище Amazon S3	Запис та збереження даних великих обсягів	+	–	+	+
Віртуальна приватна хмара Amazon VPC	Створює захищені приватні мережі та підмережі без відображення IP-адрес в Internet	+	+	–	–

Перспективи подальшого використання ХМС з метою забезпечення інформаційної безпеки критичної енергетичної інфраструктури пов’язані зі створенням апарату тестування вразливостей кібернетичних активів інфраструктури шляхом моделювання атак та взломів відповідного програмного

забезпечення. Отримані таким чином результати моделювання можуть бути застосовані для удосконалення системи кіберзахисту активів КЕІ.

1.2.3 Аналіз впливу хмарних систем на інформаційну безпеку морської критичної інфраструктури

Сучасні морські рухомі об’єкти МКІ поєднують в собі весь спектр досягнень науково-технічного прогресу і будуються за принципом “система-систем”. Тому значне місце в виконанні основних функцій морських рухомих об’єктів відповідно до їхньої ієрархічної структури, класифікаційних ознак [18] відводиться інфокомунікаційним технологіям, комп’ютерним системам та мережам, які мають недоліки, вразливості, відносно яких виникають ризики (рис. 1.9–1.11) і реалізуються певні загрози (рис. 1.15).

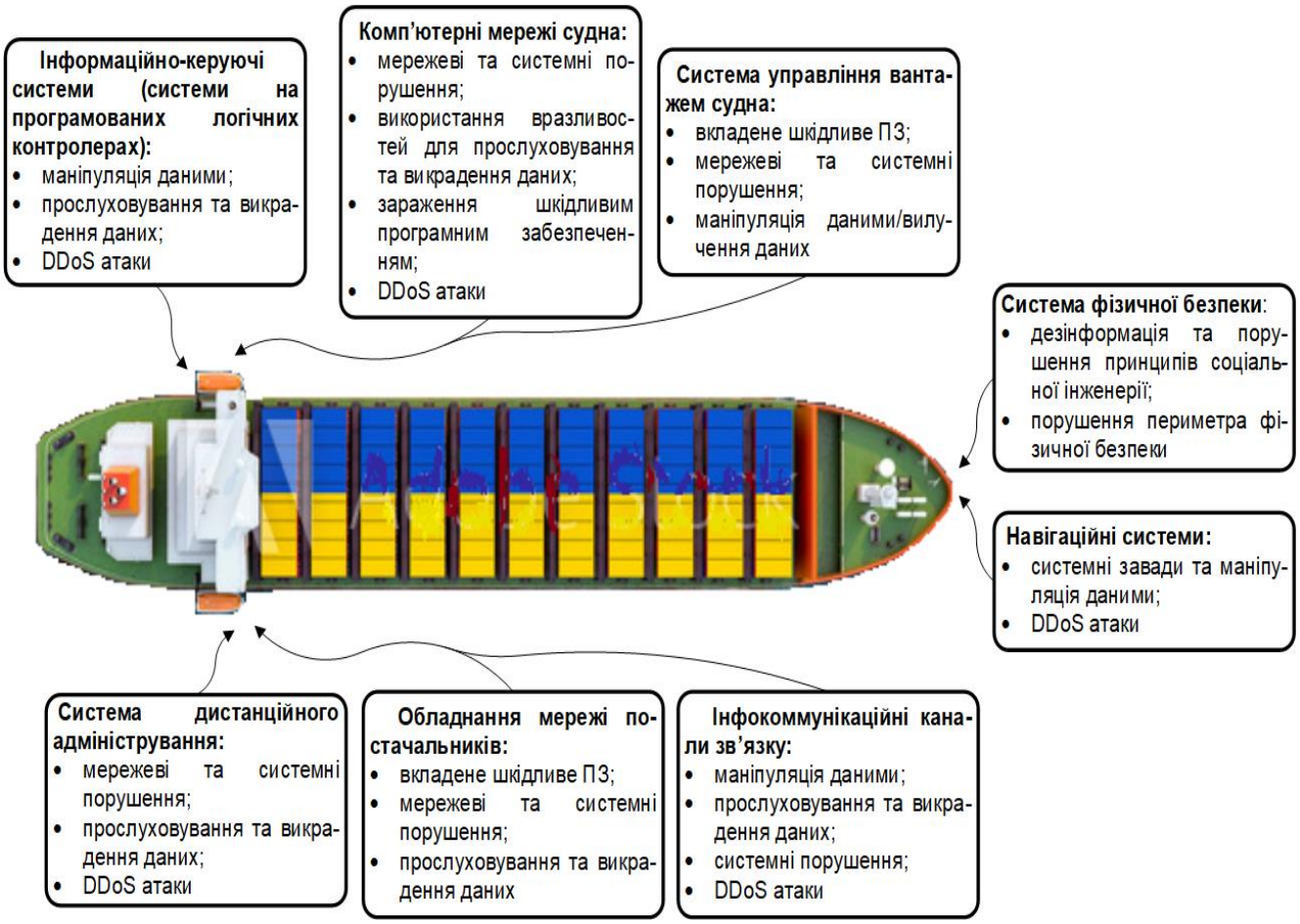


Рис. 1.15 Аналіз вразливостей для інформаційної безпеки МРО МКІ [51, 52]

Щоб запобігти та усунути зазначені недоліки необхідно виконувати вимоги стандартів з кібербезпеки IEC 62443 і ISO 27001, значне місце та роль в яких відводиться застосуванню хмарних систем. Завдяки використанню ХМС можна реалізувати наступні переваги, а саме:

1) створити електронний периметр кібербезпеки, що дозволить контролювати вхідний та вихідний інформаційні трафіки;

2) покращити виконання процедур діагностування та прогнозування інформаційно-технічних станів різних систем морських рухомих об’єктів;

3) проводити аналіз аномалій, які зазвичай передують процесам порушення кіберзахисту систем з відповідним програмно-апаратним забезпеченням;

4) отримувати різноманітну аналітичну інформацію, яка безпосередньо впливає на інформаційну безпеку морських рухомих об’єктів інфраструктури;

5) підвищити ефективність застосування за призначенням ГМСЗБ за рахунок підключення до інформаційних центрів відповідних хмарних провайдерів, що надасть можливість обробляти значно більший обсяг інформації, яка поступає від перспективних засобів колективного та індивідуального користування, що значно покращить оперативність проведення пошуково-рятувальної операції під час лиха морського рухомого об’єкту.

Розглянуті заходи планується проводити в рамках єдиної концепції забезпечення кібербезпеки морських рухомих об’єктів МКІ. Основні принципи запропонованої концепції [53] доцільно реалізовувати під час побудови та розробки дизайну конкретного судна.

1.3 Аналіз методів оцінювання готовності, підходів з вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур

Для відтворення повної картини розглянемо тенденції розвитку концепцій, методів, ІТ оцінювання, забезпечення надійності та безпеки хмарних систем КІ, які в наочній формі відображено на рис. 1.16.

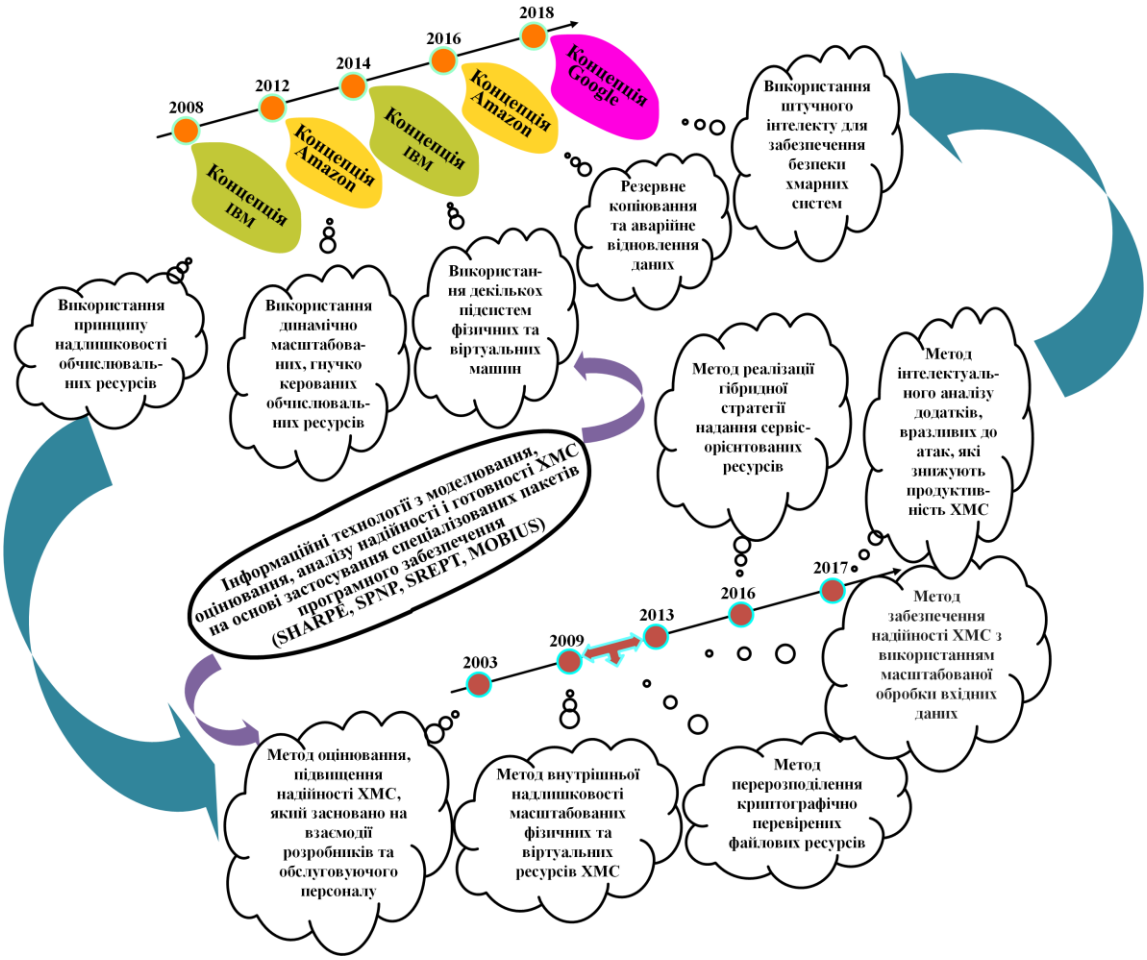


Рис. 1.16 Концепції, методи, ІТ оцінювання, забезпечення надійності та безпеки ХМС КІ [54–58]

Фактично на рис. 1 зображено динаміку розвитку підходів провідних хмарних провайдерів (IBM, Amazon, Google) в період з 2008 по 2018 роки щодо вирішення проблем масштабованого, гнучкого управління обчислювальними сервіс-орієнтованими ресурсами, аварійного їхнього відновлювання та копіювання на основі застосування відомих методів оцінювання готовності, принципів надлишковості використання ХМС, інтелектуального аналізу додатків, вразливих до атак і т.і.

За певний час зазначені методи трансформувалися у відповідні інформаційні технології, які були реалізовані за допомогою пакетів програмного забезпечення та об’єктно-орієнтованого моделювання (SHARPE, SPNP, SREPT,

Möbius). Подальший детальний аналіз ієрархії властивостей дозволив здійснити вибір показників готовності, надійності та безпеки ХМС КІ.

1.3.1 Аналіз методів оцінювання готовності хмарних систем критичних інфраструктур

Відповідно до класифікаційної схеми (рис. 1.1) оцінювання готовності хмарних систем КІ з урахуванням особливостей їхньої побудови та поведінки може бути виконано з використанням різноманітних стохастичних методів [59], архітектура яких зображена на рис. 1.17.

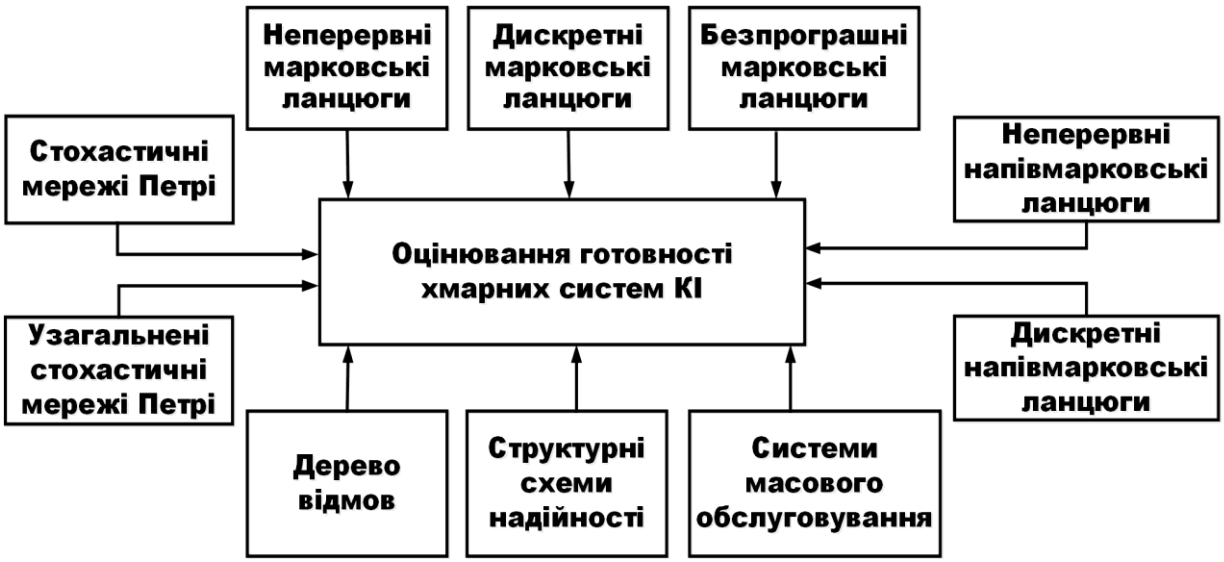


Рис. 1.17 Архітектура стохастичних методів оцінювання готовності ХМС КІ

Узагальнені дані оцінки можливостей використання зазначених методів (рис. 1.17) для моделювання поведінки та визначення характеристик готовності хмарних систем критичних інфраструктур, представлено в табл. 1.5. Зокрема, стохастичні мережі Петрі (СМП) можуть бути використані для моделювання та оцінки можливостей забезпечення гнучкості управління хмарними системами. У разі спостереження марковського альтернируючого процесу відмов та відновлень для оцінки показників готовності хмарних систем критичних інфраструктур доцільно використовувати узагальнені стохастичні мережі Петрі [60]. Цей же

апарат можна використовувати для оцінки показників гнучкості управління хмарною інфраструктурою, яка будується на основі ХМС. Не менш ефективно можна використовувати класичні методи побудови дерева відмов і структурних схем надійності (ССН) [61] для вирішення завдань забезпечення готовності хмарних систем. Для оцінки метрик якості послуг (QoS), надаваємих хмарними системами, може бути використаний апарат побудови і моделювання як неперервних (НМЛ) [62], дискретних (ДМЛ) [63] та безпрограшних марковських ланцюгів (БПМЛ) [61], так і систем масового обслуговування (СМО) [64].

Слід зазначити, що у разі відсутності інформації про можливі інформаційно-технічні стани компонентів хмарних систем, коли відомі тільки їхні вхідні та вихідні параметри пропонується використовувати метод оцінки відповідних характеристик гарантоздатності з застосуванням прихованих марковських ланцюгів [65]. В окремих випадках оцінювання характеристик гарантоздатних ХМС КІ може здійснюватися із застосуванням немарковського апарата моделювання. Це стосується ситуацій, коли не спостерігається марковська властивість, скажімо, перевищено період виконання сезонного технічного обслуговування та діагностики технологічного обладнання хмарних активів; коли протягом декількох років не проводиться оновлення програмного забезпечення кіберактивів КІ; внаслідок помилок обслуговуючого персоналу виникають непередбачені тривалі простої обладнання фізичних активів КІ тощо. В цих умовах пропонується застосовувати методи моделювання напівмарковських процесів, а саме напівмарковських ланцюгів. Наприклад, якщо виконуються різні види сервісного обслуговування, відновлення працездатності, контролю ІТС компонентів ХМС КІ, то з’являються додаткові інтервали часу, тривалість яких є детермінованою або випадковою величиною з відомим стохастичним розподіленням. У випадку детермінованої величини для моделювання застосовується метод побудови дискретних напівмарковських ланцюгів (ДНМЛ); у випадку стохастично розподілених інтервалів часу застосовується метод побудови неперервних напівмарковських ланцюгів (ННМЛ).

Таблиця 1.5

Стохастичні методи оцінювання готовності хмарних систем критичних інфраструктур

№	Моделі, які застосовуються для реалізації відповідного методу	Можливість використання для оцінки характеристик готовності хмарних систем критичних інфраструктур				
		доступність	продуктивність	енерго-витрати	гнучкість	масштабованість
1.	СМП	-	-	-	+	-
2.	Узагальнені СМП	+	-	-	+	-
3.	НМЛ	+	+	+	+	+
4.	ДМЛ	+	+	+	+	+
5.	БПМЛ	+	+	+	+	+
6.	ННМЛ	+	+	+	+	+
7.	ДНМЛ	+	+	+	+	+
8.	СМО	+	+	-	+	-
9.	ССН	+	-	-	-	+
10.	Дерево відмов	+	-	-	+	-

Розглянуті методи певною мірою є універсальними і можуть бути використані для отримання оптимальних архітектурних рішень у відповідності з встановленими критеріями готовності для хмарних систем критичних інфраструктур.

1.3.2 Аналіз відомих підходів щодо вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур

Найбільш відомий підхід щодо вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур розроблено на основі використання інформації про мінімально припустимий час простою за рік. Ця вимога, як правило, зазначається у вигляді конкретного пункту договору про надаваємі хмарними системами послуги (SLA) [33]. Виходячи з часу простою, розраховуються інші показники надійності. Наприклад, в [66] проведено дослідження і встановлено як інтенсивність відмов віртуальних машин впливає на готовність серверних систем, що входять до складу ХМС.

В той же час в роботі [67] відображено підхід, який надає можливість проаналізувати та оцінити надійність обчислювального кластеру в залежності від доступності його ресурсу та часу відновлення працездатності. Отримано також основні співвідношення для визначення показників надійності обчислювальної системи з кластерною структурою побудови (ОСКСП), яка може служити прототипом ХМС (табл. 1.6). Згідно з [68] час простою в хвилинах за рік обчислюється за формулою

$$T_{пр} = (1 - A) \times 8760 \times 60. \qquad (1.1)$$

Хмарні провайдери обирають різні підходи щодо вибору характеристик надійності, інколи проголошуючи їх декларативно без належного обгрунтування. Так, хмарний провайдер AWS робить ставку на забезпечення показника надійності $R(t) = 99 \cdot 10^{-11}$ для сховища даних Amazon S3, за допомогою якого зберігаються мільйони додатків в інтересах компаній зі всього світу [69]. Тим не менш, навіть така висока надійність хмарного сховища не гарантує забезпечення необхідного рівня функціональної безпечності сервісів AWS і не виключає випадки аварій з серйозними наслідками, що можна довести на наступному прикладі. Відомо, що у лютому 2017 року сховище даних Amazon S3 було відключено в наслідок помилки обслуговуючого персоналу майже на шість годин [5, 6]. Для цього випадку відповідно до формули (1.1) стаціонарний коефіцієнт

готовності складає A = 0,9993, що свідчить про невідповідність хмарних систем AWS необхідному рівню готовності КІ.

Таблиця 1.6

Показники надійності обчислювальної системи з кластерною структурою побудови [67]

Ймовірність безвідмовної роботи	Функція готовності	Стаціонарний коефіцієнт готовності	Ймовірність успішного розв'язування задачі ОСКСП за час τ
$R(t) = e^{-\lambda t}$	$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$	$A = \frac{\mu}{\lambda+\mu}$	$R_{ОСКСП}(t,\tau) = A(t) e^{-\lambda\tau}$

Інший підхід до вибору показників надійності ХМС демонструє компанія Microsoft, реалізуючи концепцію забезпечення відмовостійкості через віртуалізацію на основі створення гіперконвергентної інфраструктури. Такий підхід дозволяє декларувати в SLA високий рівень готовності, який відповідає значенню стаціонарного коефіцієнта готовності A = 0,9995. Нажаль, відомі факти простою хмарного ресурсу (наприклад, в період з 2013 по 2017 роки загальний час простою хмарної платформи Microsoft змінювався від дванадцяти до двох годин) свідчать, що навіть такий високий рівень готовності не гарантує належну функціональну безпечність ХМС. Аналогічна ситуація спостерігалася у хмарного провайдера Google. Наприклад, в липні 2017 року внаслідок дефекту ПЗ інтерфейсу програмних додатків понад три години не було доступу до хмарного сховища Google.

З точки зору відповідності вимогам функційної безпечності ХМС КІ відносяться до відмовостійких систем з четвертим рівнем готовності, тобто їхній стаціонарний коефіцієнт готовності (КГ) повинен приймати значення не менше 0,9999 [70]. В табл. 1.7 представлено результати порівняльного аналізу рівня

функційної безпечності ХМС провідних хмарних провайдерів за період з 2013 по 2017 роки з урахуванням часу простою та оцінки стаціонарного КГ, обчисленого з використанням співвідношення (1).

Таблиця 1.7

Порівняльний аналіз рівня функційної безпечності ХМС провідних хмарних провайдерів за період з 2013 по 2017 роки

Назва компанії	Час простою, год./рік				
	Кількісна оцінка стаціонарного КГ				
	2013	2014	2015	2016	2017
Amazon	1	–	4	–	≈6
	0,9998	0,9999	0,9995	0,9999	0,9993
Google	–	0,83	4,7	–	3,2
	0,9999	0,9999	0,9994	0,9999	0,9996
Microsoft	12	–	2	–	4
	0,9986	0,9999	0,9997	0,9999	0,9995

В табл. 1.7 у якості вхідних даних для обчислення застосовувалися матеріали доповіді професора К. Тріведі на науковій конференції RAMS 2020 (27–30 січня 2020 р., США).

За результатами проведених досліджень можна зробити висновок, що питання, які стосуються наукового обгрунтування, вибору показників готовності, характеристик надійності та безпеки хмарних систем критичних інфраструктур, як і раніше, є важливими і актуальними. У цьому сенсі слід виконати певну роботу з метою отримати необхідний інструментарій, використання якого власне дозволить оцінювати спільний рівень готовності та безпеки хмарних систем критичних інфраструктур.

1.4 Аналіз класифікаційної схеми вибору показників готовності, характеристик надійності та безпеки хмарних систем критичних інфраструктур

Зважаючи на актуальність проблеми забезпечення готовності, надійності та безпеки ХМС КІ, виникає питання як отримати відповідні оцінки при їхньому спільному застосуванні за призначенням. З цієї точку зору цікавою є критична енергетична інфраструктура, стосовно до якої може бути використано базовий інструментарій оцінювання. На рис. 1.18 зображено спрощену структурну схему активів КЕІ, відповідно до якої доцільно виконати вибір зазначених показників та характеристик.

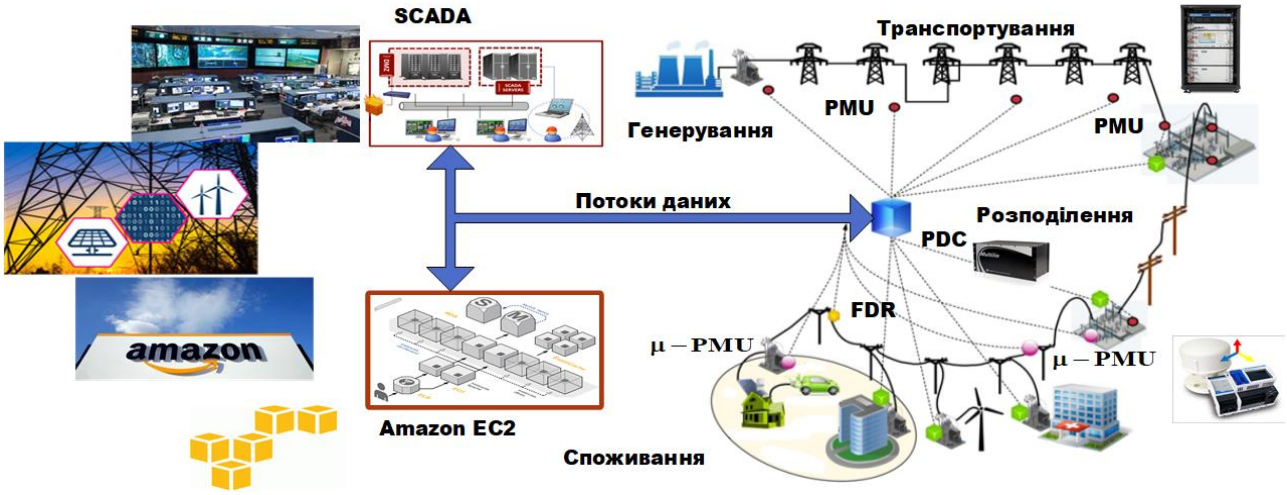


Рис. 1.18 Спрощена структурна схема активів КЕІ [71]

Згідно з рис. 1.18 критична енергетична інфраструктура працює в чотирьох основних режимах. Загальне управління здійснюється інформаційно-керуючою системою інфраструктури, важливою складовою частиною якої є система SCADA. Оперативний моніторинг інформаційно-технічних станів компонентів КЕІ здійснюється за допомогою модулів системи синхронізованих векторних вимірювань [71], а саме: спеціалізованих звичайних (PMU) та мікро-вимірювачів (μ-PMU) фази, концентраторів інформації (PDC), реєстраторів порушень частоти (FDR) і т.і. Для розширенння пропускної спроможності SCADA та у разі

необхідності здійснення аварійного відновлювання її інформаційних ресурсів пропонується застосовувати додаткові хмарні системи і сервіси AWS (наприклад, Amazon S3, Amazon Kinesis, Amazon Lamda) [69].

Всі зазначені системи та ресурси надають можливість посилити готовність, покращити характеристики надійності та безпеки КЕІ. В цілому запропонований підхід можна розширити та використовувати для інших критичних інфраструктур у вигляді певної процедури, класифікаційна схема реалізації якої зображена на рис. 1.19.

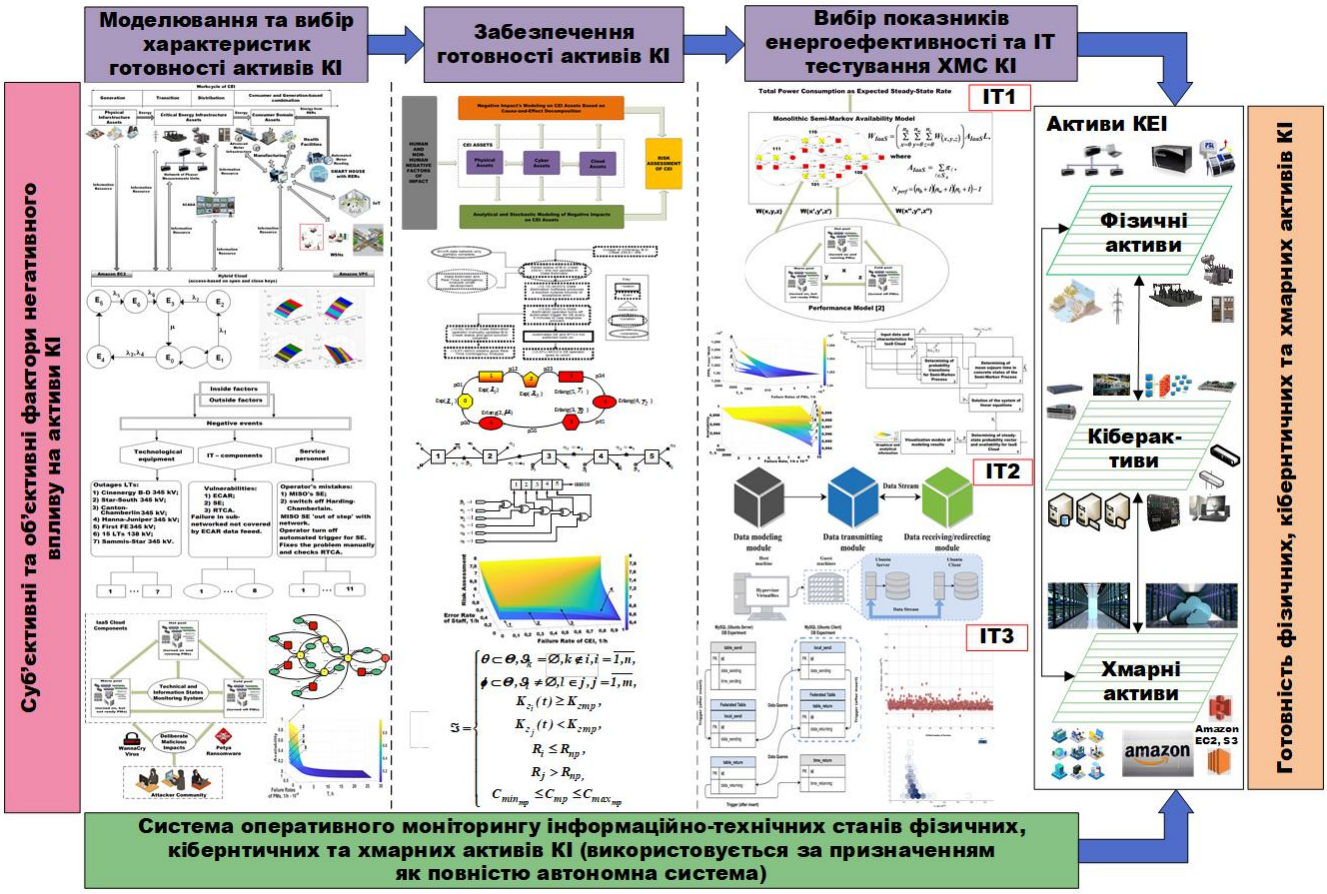


Рис. 1.19 Класифікаційна схема реалізації процедури вибору показників готовності, характеристик надійності та безпеки ХМС КІ

Згідно з приведеною класифікаційною схемою (рис. 1.19) запропонована процедура враховує суб’єктивні та об’єктивні фактори негативного впливу на активи КІ, включає комплекс заходів, сукупність методів, моделей та відповідну інформаційну технологію. Процедура реалізується в три етапи, в ході виконання

яких виконується аналітико-стохастичне моделювання поведінки, вибір характеристик готовності критичних інфраструктур; розробляються відповідні методи забезпечення готовності критичних інфраструктур; здійснюється вибір показників енергоефективності та розробляється інформаційна технологія тестування хмарних систем критичних інфраструктур.

1.5 Постановка наукової проблеми та завдань досліджень

1.5.1 Основні завдання в області оцінювання, забезпечення готовності, вибору характеристик надійності та безпеки хмарних систем критичних інфраструктур

Використовуючи результати попереднього аналізу і розроблену класифікаційну схему, виконаємо постановку наукової проблеми та розглянемо завдання досліджень. Фактично у дисертаційній роботі вирішується науково-прикладна проблема розробки методологічних основ та відповідної інформаційної технології, використання яких дозволить суттєво зменшити протиріччя, що існує насьогодні між багатофакторними вимогами до критичних інфраструктур за умови розширеного використання хмарних систем і рівнем розвитку методології оцінювання готовності, вибору характеристик ХМС для забезпечення вимог до КІ.

У формалізованому вигляді постановка задачі може бути записана так:

– до складу будь-якої КІ входять критичні системи (об’єкти), взаємозалежність та взаємозв’язок між якими описуються нотаціями виду

$$\forall\ \mathrm{CrS}_{\ell} \in \mathrm{CrI},\ \mathrm{CrI} = \bigcup_{\ell=1}^{L} \left\{ \mathrm{CrS}_{\ell} \right\} \text{ та } \mathrm{S}_{\mathrm{CrS}}^{j} \in \mathrm{S}_{\mathrm{CrI}},\ \mathrm{S}_{\mathrm{CrI}} = \bigcup_{j=1}^{J} \left\{ \mathrm{S}_{\mathrm{CrS}}^{j} \right\} \exists$$

$$\exists\ \mathrm{TM} = \left\{ \mathrm{CrIS}, \mathrm{CrSS}, \mathrm{CrIF}, \mathrm{CrIR}, \mathrm{CrSF}, \mathrm{CrSR} \right\}, \tag{1.2}$$

де $\mathrm{CrIS} = \left\{ \mathrm{CrIS}_{i} \right\}_{i=1}^{N}$ – множина основних ІТС, в яких КІ виконує функції за призначенням; $\mathrm{CrSS} = \left\{ \mathrm{CrSS}_{j} \right\}_{j=1}^{M}$ – підмножина ІТС КС, які впливають на

виконання КІ функцій за призначенням, $CrSS \subset CrIS$; $CrIF = \left\{ CrIF_p \right\}_{p=1}^{Q}$ – множина ІТС відмов, несправностей КІ; $CrIR = \left\{ CrIR_d \right\}_{d=1}^{U}$ – множина ІТС, в яких реалізується процес відновлення КІ; $CrSWV = \left\{ CrSWV_g \right\}_{g=1}^{H}$, $CrSWP = \left\{ CrSWP_z \right\}_{z=1}^{V}$ – множина станів вразливостей програмного забезпечення та множина станів пом'якшення дії вразливостей ПЗ КІ.

Тоді відображення $\Omega 1 : CrIF \Rightarrow CrIR$ ототожнюється з підмножиною

$$H = \left\{ (x, y) \middle| x \in CrIF \wedge y \in CrIR \wedge \Omega 1(x) = y \right\}. \quad (1.3)$$

Аналогічно відображення $\Omega 2 : CrSWV \Rightarrow CrSWP$ ототожнюється з підмножиною

$$N = \left\{ (w, z) \middle| w \in CrSWV \wedge z \in CrSWP \wedge \Omega 2(w) = z \right\}. \quad (1.4)$$

Співвідношення (1.2)–(1.4) та відповідні нотації розглядаються як теоретико-множинна модель (ТММ) КІ.

– критичні інфраструктури можуть також представлятися у вигляді сукупності фізичних, кібернетичних та хмарних активів, процес застосування яких за призначенням описується множиною інформаційно-технічних станів $M_{CI} = \left\{ M_{FF}^{PhA}, M_{DMI}^{CbrA}, M_{DMI}^{CldA}, M_{SS}^{CI} \right\}$. Теоретико-множинна модель ІТС критичної інфраструктури за умови існування відображень $\Omega(x_i)$, $\Omega(w_j)$ записується у вигляді

$$H_{PhA}^{CI} = \left\{ (x_1, y_1) \middle| x_1 \in M_{FF}^{PhA} \wedge y_1 \in M_{SS}^{CI} \wedge \Omega(x_1) = y_1 \right\}, \quad (1.5)$$

$$H_{CbrA}^{CI} = \left\{ (x_2, y_2) \middle| x_2 \in M_{DMI}^{CbrA} \wedge y_2 \in M_{SS}^{CI} \wedge \Omega(x_2) = y_2 \right\}, \quad (1.6)$$

$$H_{CldA}^{CI} = \left\{ (x_3, y_3) \middle| x_3 \in M_{DMI}^{CldA} \wedge y_3 \in M_{SS}^{CI} \wedge \Omega(x_3) = y_3 \right\}, \quad (1.7)$$

$$N_{CbrA}^{PhA} = \left\{ (w_1, z_1) \middle| w_1 \in M_{DMI}^{CbrA} \wedge z_1 \in M_{FF}^{PhA} \wedge \Omega(w_1) = z_1 \right\}, \quad (1.8)$$

де M_{FF}^{PhA} – множина відмов та дефектів ФА КІ; M_{DMI}^{CbrA} – множина ЗВШВ на кібернетичні активи КІ; M_{DMI}^{CldA} – множина ЗВШВ на хмарні активи КІ; M_{SS}^{CI} –

множина ІТС фізичних, кібернетичних та хмарних активів, які впливають на функційну та інформаційну безпечність КІ.

– необхідно для конкретної критичної інфраструктури, яка задається у вигляді кортежу

$$CI = \left\{ \left\{ M^{PhA} \right\}, \left\{ M^{CbrA} \right\}, \left\{ x^{PhA} \right\}, \left\{ x^{CbrA} \right\}, F_{CI} \right\}, \tag{1.9}$$

$$M^{PhA} = \bigcup_{i=1}^{n} M_i^{PhA},\ M^{CbrA} = \bigcup_{j=1}^{m} M_j^{CbrA},\ x^{PhA} = \bigcup_{s=1}^{k} x_s^{PhA},\ x^{CbrA} = \bigcup_{\ell=1}^{d} x_\ell^{CbrA}, \tag{1.10}$$

шляхом застосування систем синхронізованих векторних вимірювань та ХМС, робота яких описується граматиками виду $L = \left\langle S_{L_i}, Q_{L_{ij}}(t), G_L, \Theta_L, R_{L_r} \right\rangle$, забезпечити необхідний рівень готовності КІ у відповідності з критерієм

$$\Im = \begin{cases} K_{\Gamma_{CI}}(T) \geq K_{\Gamma_0}; \\ R_{CI} = \lim\limits_{L_{ПНД_{CI}} \xrightarrow[ITS]{} \min} \left\{ \left(1 - K_{\Gamma_{CI}}\right) L_{ПНД_{CI}} \right\}; \\ \Delta t \longrightarrow \min; \\ C_{\min_0} \leq C_0 \leq C_{\max_0}. \end{cases} \tag{1.11}$$

Отже, використовуючи представлену ТММ та співвідношення (1.5–1.11), необхідно розв’язати задачу забезпечення необхідного рівня готовності КІ. Для розв’язування пропонується враховувати еволюційні аспекти розвитку КІ, а також етапи аналітико-стохастичного оцінювання готовності сервіс-орієнтованих хмарних ресурсів, які використовуються в загальному контурі управління інфраструктурами, за умови мінімізації ризиків будь-яких негативних впливів.

Відповідно до мети дисертаційного дослідження необхідно вирішити такі завдання:

1) проаналізувати тенденції розвитку концепцій, математичного апарату, методів, інформаційних технологій оцінювання, забезпечення надійності та безпеки хмарних систем критичних інфраструктур;

2) розробити методологію (концепцію, принципи, комплекс моделей та методів) забезпечення готовності хмарних систем критичних інфраструктур;

3) розробити метод оцінювання функційної безпечності критичних

інфраструктур з урахуванням негативних впливів на їхні фізичні та кібернетичні активи;

4) розробити метод причинно-наслідкової декомпозиції та компаративістики аварій критичної енергетичної інфраструктури;

5) розробити моделі готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин;

6) розробити метод вибору характеристик та забезпечення готовності, енергоефективності хмарних систем критичних інфраструктур;

7) розробити метод оцінки енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів;

8) розробити інформаційну технологію тестування хмарних систем критичної енергетичної інфраструктури з інтегрованими фізичними компонентами на основі застосування віртуального ресурсу реляційних баз даних.

1.5.2 Вибір математичного апарату та обгрунтування методології наукових досліджень

Методологія наукових досліджень відповідно до формальних ознак пропонуємої дисертаційної роботи базується на єдиній концепції, для послідовної реалізації якої необхідно:

1) сформулювати основні принципи оцінювання готовності та вибору характеристик надійності і безпеки хмарних систем критичних ынфраструктур;

2) сформулювати основні положення процесу оцінювання ризику негативного впливу на активи критичних інфраструктур;

3) розробити оцінні аналітико-стохастичні моделі готовності та ризику активів критичних інфраструктур;

4) розробити методи оцінювання функційної безпечності критичних інфраструктур;

5) розробити методи забезпечення готовності критичної енергетичної інфраструктури;

6) отримати кількісні оцінки ризику та функційної безпечності критичних інфраструктур;

7) розробити методи вибору, оцінки характеристик готовності та енергоефективності хмарних систем критичних інфраструктур;

8) отримати кількісні оцінки аналітико-стохастичного моделювання енергоефективності хмарної інфраструктури;

9) розробити процедуру тестування інформаційних центрів хмарного провайдера;

10) створити інформаційну технологію тестування хмарних систем критичної енергетичної інфраструктури з інтегрованими фізичними компонентами на основі застосування віртуального ресурсу реляційних баз даних.

Виходячи з основних положень запропонованої методології, доцільно здійснити вибір відповідного математичного апарату, застосування якого дозволить розв’язати задачі дисертаційного дослідження. В табл. 1.8 наведено інформацію щодо відповідності математичного апарату, який планується застосовувати для розв’язування конкретних наукових завдань дисертаційного дослідження.

Таблиця 1.8

Відповідність математичного апарату науковим завданням дисертаційного дослідження

№ п.п.	Наукові завдання	Математичний апарат, який застосовується для розв’язування наукового завдання
1.	Аналіз тенденцій розвитку концепцій, математичного апарату, методів, інформаційних технологій оцінювання, забезпечення надійності та безпеки хмарних систем критичних інфраструктур	Методи системного аналізу, теорії надійності, методи аналізу функціональної та інформаційної безпечності складних систем

Продовження таблиці 1.8

2.	Розробка методології (концепції, принципів, комплекса моделей та методів) забезпечення готовності хмарних систем критичних інфраструктур	Методи системного аналізу, методи теорії імовірностей, метод аналізу безпеки складних систем на основі модифікації алгебри причинно-наслідкових комплексів
3.	Розробка методу оцінювання функційної безпечності критичних інфраструктур з урахуванням негативних впливів на їхні фізичні та кібернетичні активи	Методи побудови структурних схем надійності та аналізу дерев відмов, метод напівмарковського моделювання
4.	Розробка методу причинно-наслідкової декомпозиції та компаративістики аварій критичної енергетичної інфраструктури	Методи логічного аналізу, методи алгебри причинно-наслідкових комплексів
5.	Розробка моделі готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин	Методи теорії імовірностей, стохастичні методи оцінювання, метод напівмарковського моделювання
6.	Розробка методу вибору характеристик та забезпечення готовності, енергоефективності хмарних систем критичних інфраструктур	Методи системного та логічного аналізу
7.	Розробка методу оцінки енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів	Методи теорії імовірностей, стохастичні методи оцінювання, метод напівмарковського моделювання
8.	Розробка інформаційної технології тестування хмарних систем критичної енергетичної інфраструктури з інтегрованими фізичними компонентами на основі застосування віртуального ресурсу реляційних баз даних	Методи імітаційного моделювання, технології розробки програмного забезпечення

Послідовне виконання завдань, які зазначено в таблиці 1.8, є запорукою успішного виконання загального завдання, що відповідає всім формальним ознакам наведеного дисертаційного дослідження.

Висновки до розділу 1

1. Виконано аналіз проблеми впливу хмарних систем на функційну безпечність критичних інфраструктур. Найбільшу зацікавленість з точки зору зручності використання обчислювального ресурсу викликає хмарна інфраструктура.

2. Проведено аналіз ключових факторів ненадійності критичних інфраструктур на прикладі критичної енергетичної інфраструктури та морської критичної інфраструктури. Для усунення цих недоліків та пом’якшення виникаючих ризик-факторів для критичних інфраструктур пропонується застосовувати хмарні системи.

3. Розглянуто та проаналізовано тенденції розвитку концепцій, методів, інформаційних технологій оцінювання, забезпечення надійності та безпеки хмарних систем критичних інфраструктур.

4. Розроблено класифікаційну схему реалізації процедури вибору показників готовності, характеристик надійності та безпеки хмарних систем критичних інфраструктур.

5. Сформульовано наукову проблему та основні завдання в області оцінювання, забезпечення готовності, вибору характеристик надійності й безпеки хмарних систем критичних інфраструктур. Виконано математичну постановку задачі дисертаційного дослідження.

6. Здійснено вибір відповідного математичного апарату, застосування якого дозволить розв’язати задачі дисертаційного дослідження. Наведено інформацію щодо відповідності математичного апарату, який планується застосовувати для розв’язування конкретних наукових завдань.

Основні положення цього розділу викладені у публікаціях автора [8, 20, 32, 33, 59].

РОЗДІЛ 2
РОЗРОБКА СТРУКТУРИ ТА ЕЛЕМЕНТІВ МЕТОДОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР

2.1 Розробка принципів оцінювання готовності та вибору характеристик надійності і безпеки хмарних систем критичних інфраструктур

Насьогодні в сфері застосування критичних інфраструктур набули широкого розповсюдження різні моделі застосування хмарних систем. Переваги ХМС у порівнянні з типовими комп'ютерними системами очевидні. Поряд з тим використання ХМС як важливого елемента контуру управління критичними інфраструктурами породжує певні загрози для функціональної та інформаційної безпеки КІ. Крім того, аспекти надійності та безпеки ХМС як і раніше залишаються слабкою ланкою й потребують подальших досліджень.

Тому важливими і актуальними залишаються питання, пов'язані з розробкою принципів оцінювання готовності та вибору характеристик надійності, безпеки ХМС критичних інфраструктур.

2.1.1 Аналіз концепції створення надійних та безпечних хмарних систем критичних інфраструктур з сервіс-орієнтованим розподіленням ресурсів

Як було попередньо зазначено, існуюче протиріччя в сфері застосування КІ може бути усунуто шляхом використання ХМС з сервіс-орієнтованим розподіленням ресурсів. У той же час ХМС теж потребують проведення додаткових заходів по забезпеченню необхідного рівня надійності та безпеки. Вочевидь, методологія, основні положення якої було викладено в першому

розділі, повинна враховувати ці особливості і аспекти спільного функціонування критичних інфраструктур та ХМС.

На рис. 2.1 зображено структуру методології забезпечення готовності хмарних систем критичних інфраструктур.

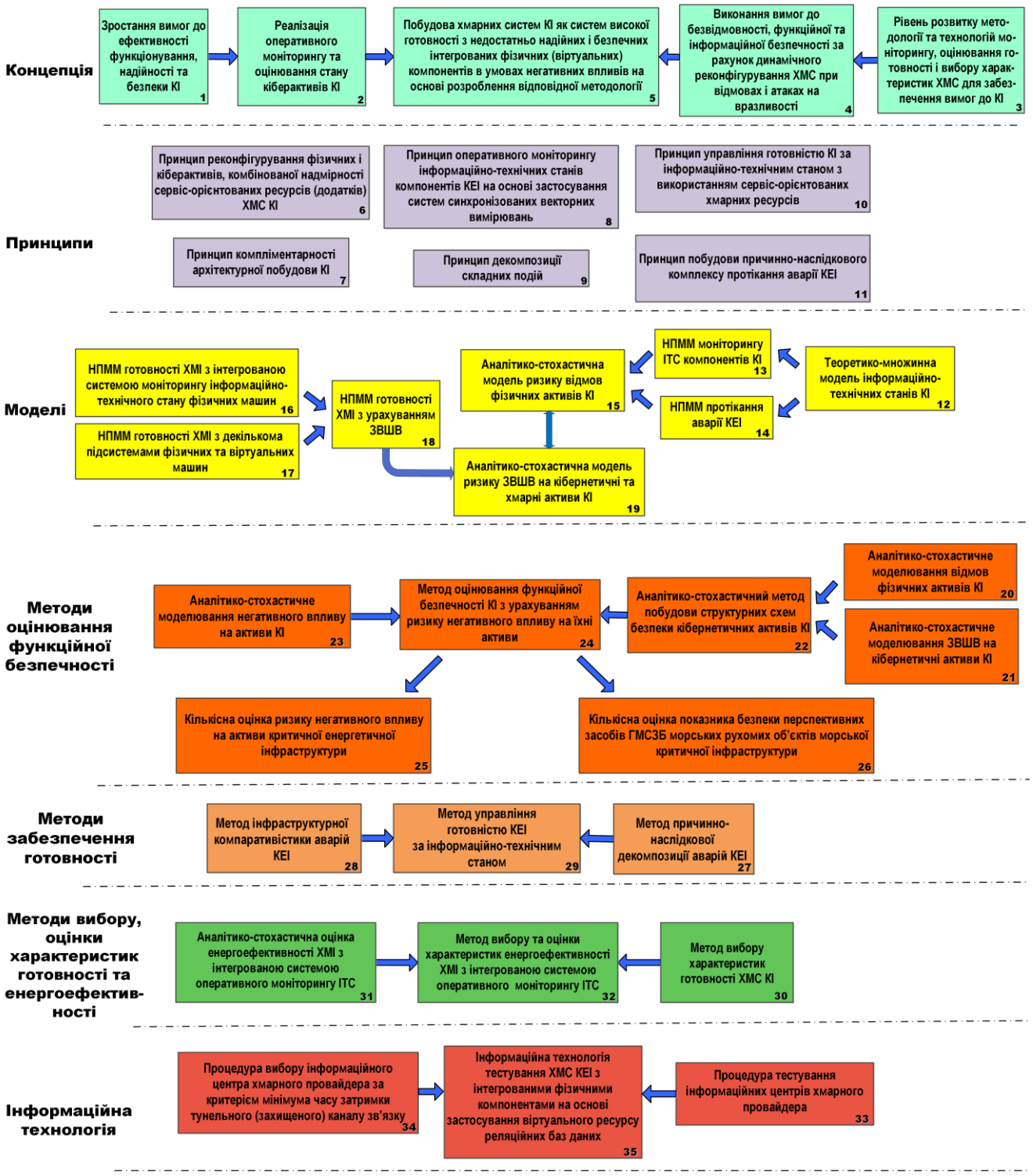


Рис. 2.1 Структура методології забезпечення готовності ХМС КІ

Відповідно до рис. 2.1 надана методологія базується на розвитку парадигми фон Неймана [72].

Основу запропонованої методології складає концепція, яка враховує нюанси створення надійних та безпечних хмарних систем з сервіс-орієнтованим розподіленням ресурсів. Сутність концепції полягає в побудові хмарних систем критичних інфраструктур як систем високої готовності з недостатньо надійних і безпечних інтегрованих фізичних (віртуальних) компонентів в умовах негативних впливів та атак на вразливості. Концепція (рис. 2.2) реалізується у вигляді сукупності принципів, моделей, методів та відповідної інформаційної технології.

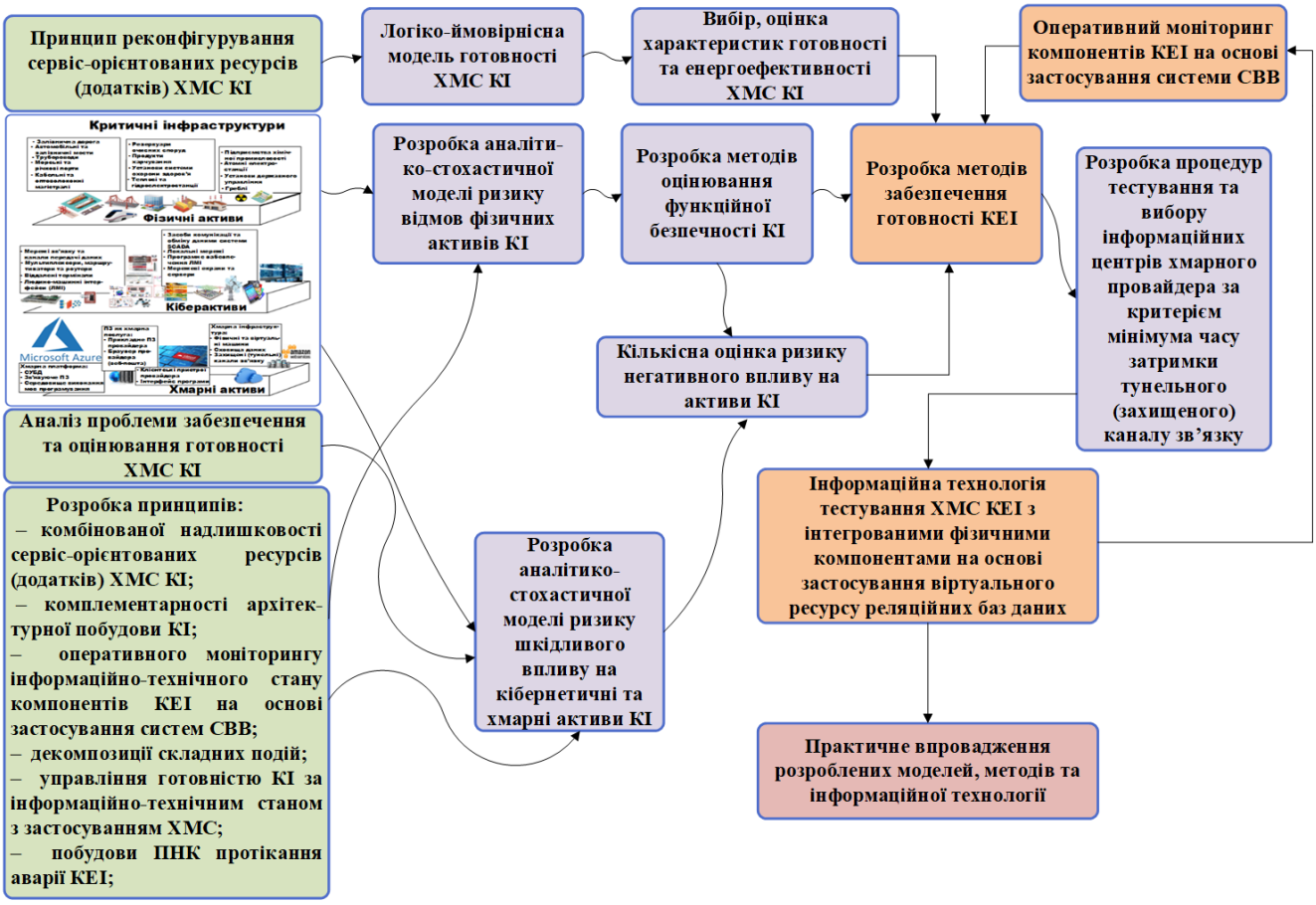


Рис. 2.2 Концепція забезпечення готовності ХМС КІ

Відповідно до рис. 2.2 загальна концепція базується на положеннях, які враховують структурну побудову активів КІ і в якості прикладу реалізується на основі застоування за призначенням компонентів критичної енергетичної

інфраструктури. Комплексна реалізація сформульованих принципів надає можливість побудувати зазначений модельний ряд (рис. 2.1) і перейти до розробки сукупності методів оцінювання функційної безпечності, забезпечення готовності, вибору характеристик енергоефективності хмарних систем КІ і т. і. Послідовне виконання цих методів, доповнене процедурою тестування та вибору інформаційних центрів конкретного хмарного провайдера за критерієм мінімума часу затримки тунельного (захищеного) каналу зв'язку, надає можливість створити відповідну інформаційну технологію. В свою чергу спільне застосування пропонуємої ІТ та систем синхронізованих векторних вимірювань дзоволяє проводити оперативний моніторинг компонентів критичної енергетичної інфраструктури і покращує точність розробляємих методів забезпечення готовності КЕІ.

Розглянемо декілька принципів, які складають основу запропонованої методології (рис. 2.1).

2.1.2 Принцип реконфігурування та комбінованої надлишковості сервіс-орієнтованих ресурсів хмарних систем критичних інфраструктур

Для забезпечення готовності хмарних систем критичних інфраструктур в дисертаційній роботі пропонується застосовувати принцип реконфігурування та комбінованої надлишковості сервіс-орієнтованих ресурсів ХМС КІ, який на відміну від відомих, дозволяє виконувати перерозподілення фізичних та віртуальних машин хмарних систем критичних інфраструктур за кількісною ознакою, здатністю до ресурсної міграції, використовуючи результати оперативного моніторингу їхніх інформаційно-технічних станів, враховуючи негативні впливи, що визначаються факторами ненадійності і атаками на вразливості.

Згідно з [73–76] реконфігурування ХМС здійснюється для трьох підсистем фізичних машин (ФМ), які функціонують як сервісна модель хмарної інфраструктури [77]. Реконфігурування здійснюється у межах визначених

підсистем ФМ, що працюють в трьох режимах: гарячому, теплому та холодному. Надана модель в кортежній формі записується у вигляді

$$\text{IaaS Cloud} = \left\{ \left\{ M^{Hot} \right\}, \left\{ M^{Warm} \right\}, \left\{ M^{Cold} \right\}, \left\{ x^{Hot} \right\}, \left\{ x^{Warm} \right\}, \left\{ x^{Cold} \right\}, F^{CI}_{\text{IaaS Cloud}} \right\}, \quad (2.1)$$

де $M^{Hot} = \bigcup_{i=1}^{n} M^{Hot}_{PM_i}$ – множина ФМ гарячої підсистеми ХМІ; $M^{Warm} = \bigcup_{j=1}^{n} M^{Warm}_{PM_j}$ – множина ФМ теплої підсистеми ХМІ; $M^{Cold} = \bigcup_{r=1}^{n} M^{Cold}_{PM_r}$ – множина ФМ холодної підсистеми ХМІ; $x^{Hot} = \bigcup_{i=1}^{m} x^{Hot}_{PM_i}$ – множина зв'язків ФМ гарячої підсистеми з фізичними машинами інших підсистем ХМІ; $x^{Warm} = \bigcup_{j=1}^{d} x^{Warm}_{PM_j}$ – множина зв'язків ФМ теплої підсистеми з фізичними машинами інших підсистем ХМІ; $x^{Cold} = \bigcup_{r=1}^{g} x^{Cold}_{PM_r}$ – множина зв'язків ФМ холодної підсистеми з фізичними машинами інших підсистем ХМІ; $F^{CI}_{\text{IaaS Cloud}}$ – функція (нова властивість) хмарної інфраструктури у складі КІ; $U = M^{Hot} \cup M^{Warm} \cup M^{Cold}$ – множина всіх ФМ.

Запропонована до розгляду модель працює таким чином, що виконання функцій застосування за призначенням хмарною інфраструктурою здійснюється тільки шляхом використання множини фізичних машин M^{Hot} за умови $M^{Hot} \neq \varnothing$, тобто $m\left(M^{Hot}\right) \geq 1$. Вважається, що в початковий момент часу, коли немає необхідності в виконанні реконфігурування компонентних складових інфраструктури, загальна кількість включених ФМ визначається як

$$m\left(M^{Hot} \cup M^{Warm}\right) = m\left(U\right) - m\left(M^{Hot} \cup M^{Warm}\right)'.$$

При здійсненні реконфігурування кількість задіяних ФМ обчислюється так:

$$m\left(M^{Hot} \cap M^{Warm}\right) = m\left(M^{Hot}\right) + m\left(M^{Warm}\right) - m\left(M^{Hot} \cup M^{Warm}\right).$$

Виходячи з загальної концепції побудови ХМС (рис. 1.1), віртуальні машини (ВМ) розвертаються на ресурсній і схемотехнічній базі ФМ. Реконфігурування ВМ здійснюється аналогічно як і для фізичних машин інфраструктури. На рис. 2.3 зображена схема реконфігурування ФМ та ВМ представленої хмарної інфраструктури, віртуальна частина якої реалізується з застосуванням відповідних апаратного забезпечення, операційних систем (ОС), програмних додатків (ПД) та монітора віртуальних машин [78, 79].

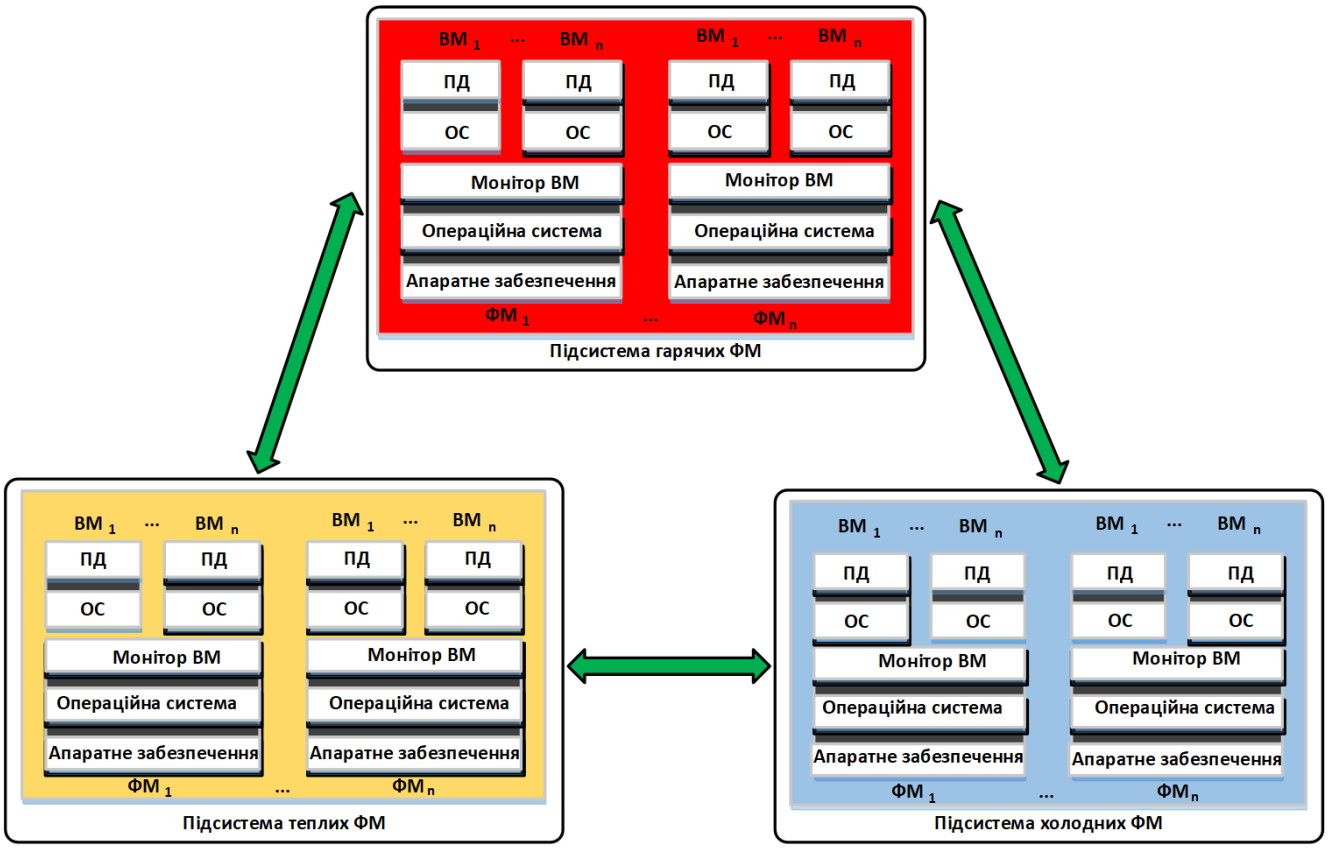


Рис. 2.3 Схема реконфігурування ФМ та ВМ хмарної інфраструктури [78,79]

Згідно з рис. 2.3 реконфігурування фізичних та віртуальних машин здійснюється за даними моніторингу їхнього інформаційно-технічного стану. Принципи побудови ХМІ з інтегрованою системою моніторингу ІТС фізичних та віртуальних машин викладено в третьому розділі роботи. Процедура реконфігурування здійснюється відповідно до наступної системи вимог і обмежень:

$$\Im = \begin{cases} K_{\Gamma}\left(\tau_M, \lambda_F, \gamma_M, \Lambda_{DMI}\right) \geq K_{\Gamma_0}; \\ n_{PM} \geq 1;\ n_{VM} \geq 1; \\ C_{min_0} \leq C_0 \leq C_{max_0}; \end{cases} \tag{2.2}$$

де K_{Γ_0} – гранично припустиме значення стаціонарного коефіцієнта готовності ХМС КІ; Т – загальний час застосування ХМС КІ за призначенням; $\tau_M \in [0, T]$ – тривалість оперативного моніторингу ІТС; λ_F – інтенсивність відмов ФМ та ВМ; γ_M – інтенсивність міграції ФМ та ВМ; Λ_{DMI} – інтенсивність зловмисних шкідливих впливів; n_{PM} – кількість ФМ; n_{VM} – кількість ВМ; $C_0 \in \left[C_{min_0}; C_{max_0}\right]$ – граничні витрати необхідні на підтримання необхідного рівня готовності ХМС КІ.

В системі вимог і обмежень (2.2) враховується можливість здійснення ресурсної міграції фізичних та віртуальних машин з інтенсивністю $\gamma_M = \gamma_{ФМ} + \gamma_{ВМ}$, де $\gamma_{ФМ}$, $\gamma_{ВМ}$ – інтенсивність міграції ФМ і ВМ, відповідно. Ресурсна міграція ФМ та ВМ здійснюється у відповідності з загальними принципами інформаційного забезпечення хмарних обчислень, викладеними в [77, 79].

2.1.3 Принцип компліментарності архітектурної побудови критичних інфраструктур

Критичні інфраструктури (system of systems) представляють собою структурні утворення штучного походження, які функціонують синергічно при вирішенні завдань використання за призначенням або при виробництві життєво необхідних суспільству товарів, послуг (електро- і водопостачання, охорона здоров’я, телекомунікації, залізничний транспорт та ін.) і впливають на національну безпеку держави. Негативні наслідки реалізації існуючих небезпек і загроз для критичних інфраструктур, як правило, проявляються у вигляді каскадного ефекту.

Для запобігання каскадному ефекту та негативним явищам, пов’язаним з ним, а також для забезпечення готовності критичних інфраструктур пропонується застосовувати принцип компліментарності архітектурної побудови, який, на

відміну від відомих, передбачає дотримання вимог масованого паралелізму архітектурної побудови КІ [80]. Зокрема, можуть висуватися вимоги забезпечення ефективного функціонування КІ при пріоритеті інфраструктурної надійності та безпеки.

Необхідною умовою масованого паралелізму є прояв властивості компліментарності Уотсона–Кріка [81]. Це означає, що в термінах генної інженерії за основу приймається компліментарна побудова молекули ДНК (дезоксирибонуклеінової кислоти), коли зв'язування відбувається шляхом взаємного тяжіння компонентів, а саме: компонента А завжди зв'язується тільки з компонентою Т, а компонента Г – з компонентою Ц. Тоді, архітектура будь-якої критичної інфраструктури може бути побудована у відповідності з наступними припущеннями: А – це об'єкт управління, наприклад, КІ (або окремий її критично важливий об'єкт); Т – система забезпечення безпеки та готовності КІ (або окремого її КВО); Г – система підтримки прийняття рішень для КІ (або окремого її КВО); Ц – система управління КІ (або окремого її КВО).

Властивість компліментарності Уотсона–Кріка при утворенні подвійних ланцюжків ДНК зображена на рис. 2.4, а його парадигма досить детально розглянута в [82].

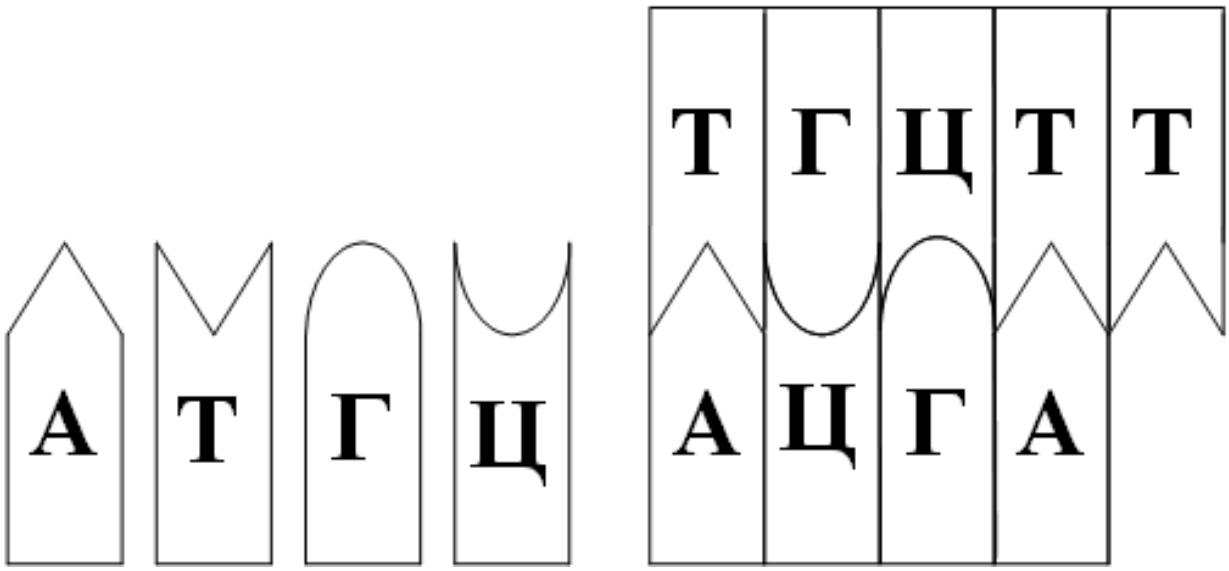


Рис. 2.4 Компліментарність Уотсона–Кріка [82]

Отже, дотримуючись принципу масованого паралелізму, можна побудувати

критичні інфраструктури, характерною особливістю яких буде відповідність властивості компліментарності Уотсона–Кріка. Тільки після цього має сенс висувати жорсткі вимоги щодо забезпечення готовності, функційної та інформаційної безпечності як критичних інфраструктур в цілому, так і окремих КВО, які входять до складу КІ.

2.1.4 Принцип оперативного моніторингу компонентів критичної енергетичної інфраструктури на основі застосування систем синхронізованих векторних вимірювань

Відповідно до принципу компліментарності (рис. 2.4) архітектурної побудови до складу будь-якої критичної інфраструктури повинна входити система забезпечення безпеки та готовності, яка функціонує з використанням даних оперативного моніторингу компонентів КІ. Розглянемо яким чином здійснюється оперативний моніторинг компонентів КЕІ.

Оперативний моніторинг компонентів КЕІ здійснюється за допомогою системи синхронізованих векторних вимірювань (рис. 1.18). Головними елементами системи ССВВ є спеціалізовані звичайні та мікро-вимірювачі фази, які називаються синхрофазорами (СХФР) [83, 84]. Поєднані в мережу СХФР надають можливість з високою точністю та швидкодією вимірювати напругу, струм, частоту, фазу та інші параметри сигналів, які поступають з вихідних пристроїв КЕІ. Фактично за допомогою вимірювальних модулів СХФР в цифровому форматі з високою швидкістю оновлення даних (не менше 50 раз/сек) виконується моніторинг інформаційно-технічних станів та параметрів компонентів критичної енергетичної інфраструктури; здійснюється управління нормальними та аварійними режимами експлуатації енергосистем КЕІ [85]. Структурна схема вимірювального модуля СХФР представлена на рис. 2.5.

Принцип функціонування СХФР заснований на вимірюванні різниці фаз між синхронізованими вимірами напруги (струму) в точках передачі і прийому енергії, що надає можливість створювати повний параметричний профіль КЕІ. Загальна синхронізація пристроїв СХФР здійснюється за допомогою системи

GPS. Використання ССВВ надає можливість за лічені секунди фіксувати негативні явища та оперативно реагувати на них з точки зору мінімізації наслідків, що покращує функціональну безпечність КЕІ. Наприклад, відомий досвід свідчить, що за допомогою модулів СХФР було визначено місце короткого замикання на відстані 550 км саме тому, що мікро-синхрофазор зафіксував зміну напруги на 0,002 % [86].

Рис. 2.5 Структурна схема вимірювального модуля СХФР [83, 84]

Насьогодні модулі синхрофазорів застосовуються для вимірювання фазового зсуву високовольтних ліній електропередачі (ЛЕП), величина якого впливає на виконання операцій по управлінню перетоками електроенергії та надає можливість операторам інформаційно-керуючих систем КЕІ контролювати перехідні процеси. Отримуючі від модулів синхрофазорів дані про зміну фазового кута між “стоком і витоком”, системний регулятор має можливість своєчасно реагувати на негативні явища, що відбуваються в мережі.

У якості прикладу на рис. 2.6 показано на скільки збільшився фазовий кут між двома лініями електропередачі Клівленд та Мічиган протягом 14 серпня 2003 року, в період, коли сталася найбільша аварія об’єднаної енергосистеми США і Канади [87]. Відповідно до рис. 2.6 саме фазовий зсув між цими ЛЕП відображає

ситуацію, коли відбулося аварійне відключення лінії Клівленд, що призвело до каскадного відключення електромережі. За наявності модулів системи синхронізованих векторних вимірювань, основу яких складають відповідні лінійки синхрофазорів, цю аварійну ситуацію можна було б попередити та усунути.

Зокрема, відповідно до рис. 2.6 чутливість та швидкодія СХФР на протязі майже хвилини дозволяли відслідкувати появу фазового зсуву між ЛЕП Клівленд та Мічіган 14 серпня 2003 р. Але як видно з рис. 2.6 цього не сталося. В значній мірі цьому сприяли відсутність системи ССВВ, а також помилки операторів, які не зреагували на суттєву зміну фази, що призвело до виникнення каскадного ефекту.

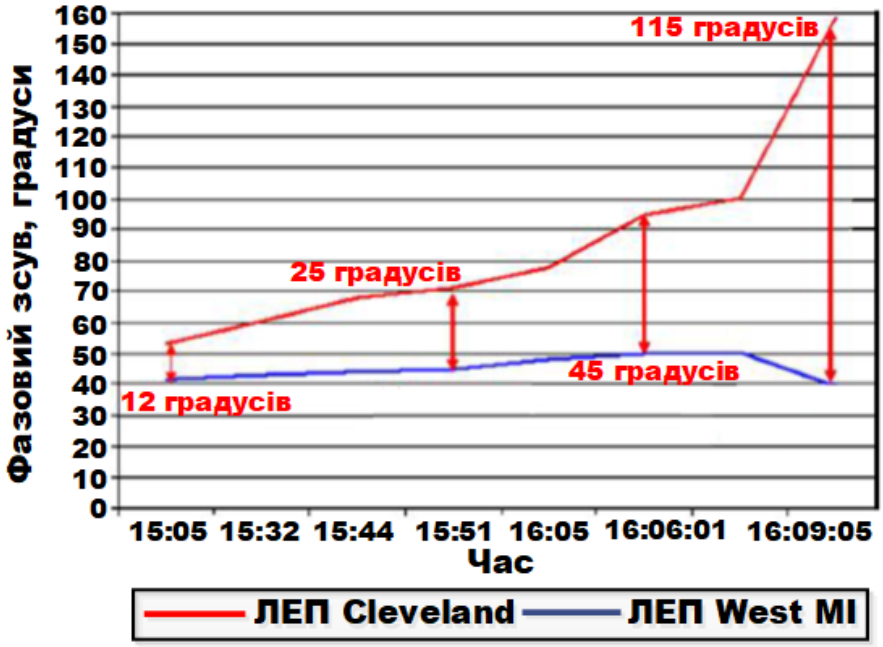


Рис. 2.6 Фазовий зсув між ЛЕП Клівленд та Мічіган 14 серпня 2003 р. [88]

Аналогічний підхід може бути використано для аналізу аномалій та встановлення місця проникнення ЗВШВ в контур управління КЕІ, що безумовно покращить рівень інформаційної безпечності інфраструктури. У той же час збільшення кількості модулів ССВВ дозволить підвищити якість, інформативність системи оперативного моніторингу інформаційно-технічних станів компонентів

КЕІ, що в подальшому буде сприяти вирішенню проблеми оцінювання та забезпечення готовності інфраструктури в цілому.

2.1.5 Принцип управління готовністю критичною енергетичною інфраструктурою за інформаційно-технічним станом з застосуванням сервіс-орієнтованих хмарних ресурсів

Принцип управління готовністю КЕІ за інформаційно-технічним станом, на відміну від відомих, дозволяє забезпечити ефективне застосування інфраструктури за призначенням, розглядаючи її як «систему систем» (system of systems) з синергічним виконанням функцій по перетворенню та доставці електроенергії до користувача за допомогою сервіс-орієнтованих хмарних ресурсів. Реалізація зазначеного принципу базується на комплексному застосуванні системи ССВВ та відповідних хмарних технологій для покращення надійності та функціональної безпечності КЕІ.

Успішне розв’язування запропонованої задачі можливе за рахунок спільного використання модулів ССВВ, за допомогою яких утворюється система оперативного моніторингу ІТС компонентів КЕІ [89], та сервіс-орієнтованих хмарних ресурсів AWS [90]. Фактично, використовуючи результати оперативного моніторингу ІТС компонентів КЕІ на основі застосування системи синхронізованих векторних вимірювань, обслуговуючий персонал має можливість оцінювати та контролювати рівень готовності компонентів інфраструктури. В залежності від отриманих результатів визначаються виконавчі функції щодо забезпечення необхідного рівня готовності критичної енергетичної інфраструктури (наприклад, визначення стратегій технічного обслуговування та ремонту, режимів навантаження енергобладнання і т.і.). Після чого формуються відповідні керуючі впливи. Детально ці аспекти розглянуто в розділі 5 дисертаційної роботи.

Використання безпечних масштабованих сервіс-орієнтованих обчислювальних хмарних ресурсів Amazon EC2 [91] дозволить заощадити значну частину коштів на утримання кіберактивів КЕІ і розширити обсяг завдань, що

вирішуються з використанням інформаційного ресурсу. Серед завдань, які належить вирішити, використовуючи AWS, найбільш актуальними є:

1) створення інформаційно-обчислювального ресурсу на основі моделі віртуальної приватної хмари, яка в подальшому розгортається в віртуальну мережу (VPN) [92];

2) організація збору даних та транспортної інфраструктури VPN, архівація, фільтрація, пакетна обробка, зберігання, оновлення і візуалізація даних в хмарній інфраструктурі Amazon EC2, які поступають від модулів ССВВ;

3) реалізація комплексу заходів щодо забезпечення інформаційної безпеки хмарної інфраструктури Amazon EC2 з використанням засобів кіберзахисту (таблиця 1.3).

На рис. 2.7 зображена схема функціонування критичної енергетичної інфраструктури з застосуванням сервіс-орієнтованих хмарних ресурсів AWS.

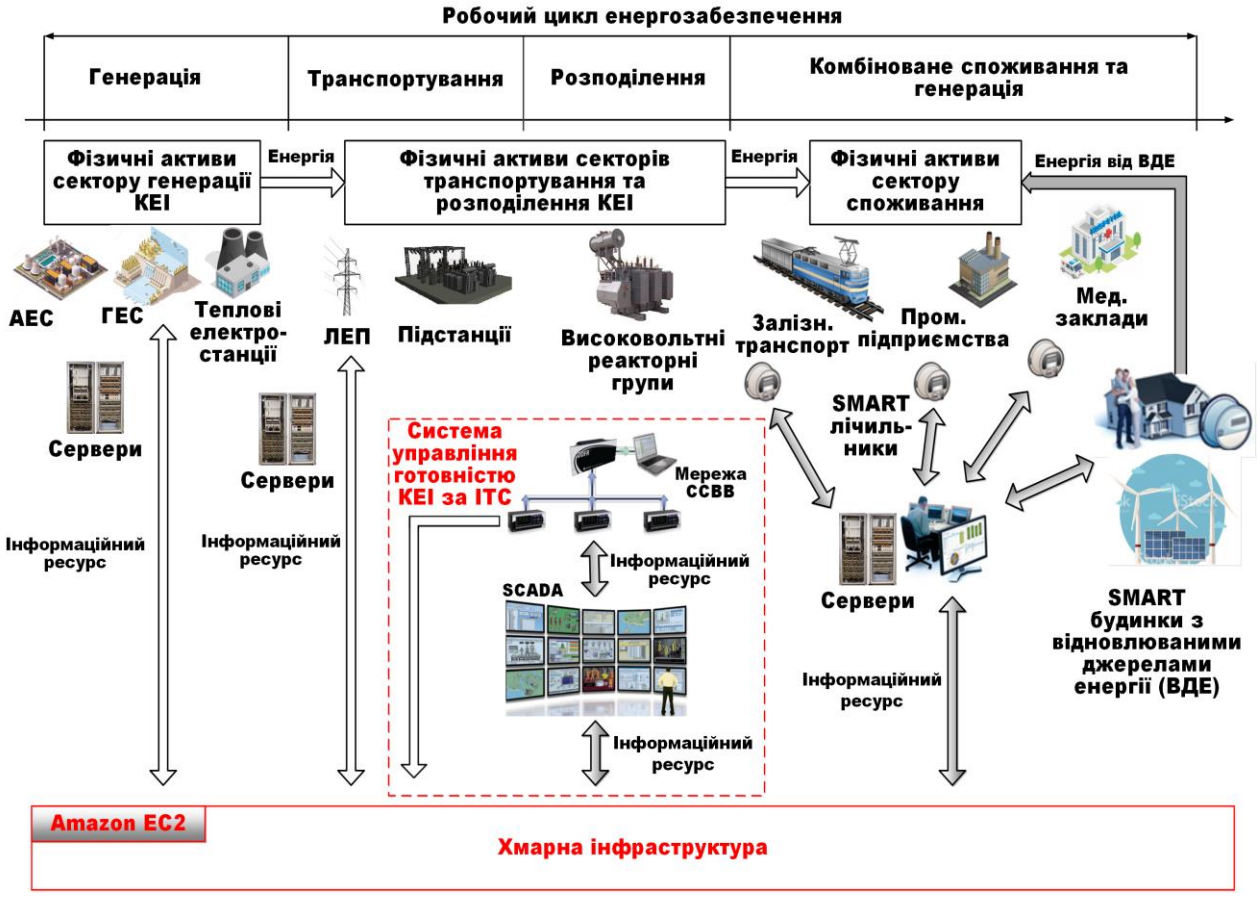


Рис. 2.7 Схема функціонування КЕІ з застосуванням сервіс-орієнтованих хмарних ресурсів AWS [93]

Вочевидь з використанням сервіс-орієнтованих хмарних ресурсів AWS істотно розширюються можливості щодо інформаційного забезпечення процесів по визначенню та контролю ІТС компонентів КЕІ за рахунок значного збільшення обсягів даних, які поступають від модулів системи синхронізованих векторних вимірювань. Водночас це дозволяє зменшити час реагування та збільшує повноту проведення операцій по управлінню готовністю КЕІ за інформаційно-технічним станом.

2.2 Основні положення процесу оцінювання ризику негативного впливу на активи критичних інфраструктур

Перш ніж оцінити ризик негативного впливу на критичні інфраструктури необхідно виконати аналіз активів КІ. Однак, цей аналіз буде неповним якщо не виконати моделювання поведінки критичних інфраструктур з урахуванням негативних факторів впливу на їхні активи.

Відповідно до запропонованої методології (рис. 2.1) та концепції забезпечення готовності харних систем КІ (рис. 2.2) в ході виконання першого етапу процедури оцінювання встановлюються причинно-наслідкові зв’язки між негативними факторами впливу на компоненти, з яких складаються активи критичних інфраструктур. Далі, застосовуючи отриманий причинно-наслідковий комплекс, виконується аналітико-стохастичне моделювання та оцінювання ризику негативного впливу на активи критичних інфраструктур.

2.2.1 Аналіз активів критичних інфраструктур

Загальна структура активів критичних інфраструктур в наочному вигляді зображена на рис. 1.13. Проаналізуємо з яких компонентів в перспективі повинні складатися фізичні, кібернетичні та хмарні активи, щоб забезпечити необхідні ефективність застосування за призначенням, функціональну та інформаційну безпечність КІ згідно з принципом компліментарності їхньої архітектурної побудови.

На рис. 1.2 представлена спрощена структура активів критичних інфраструктур, яка існує насьогодні. Відповідно до рис. 1.2 фізичні активи КІ складаються з критично важливих об’єктів (КВО), які споживають ключові ресурси, що виробляються інфраструктурами [93]. Фактично фізичні активи представлені певною кількістю КВО, які виконують відповідні критичні функції інфраструктури.

Кібернетичні активи КІ (рис. 1.2) представлені такими засобами та додатками:

1) мережі зв’язку та канали передачі даних в цифровому форматі;

2) мультиплексори, маршрутизатори та роутери;

3) віддалені термінали;

4) людино-машинні інтерфейси (ЛМІ);

5) засоби комунікації та обміну даними системи SCADA;

6) локальні мережі;

7) програмне забезпечення ЛМІ;

8) мережеві екрани, сервери і т.і.

До складу хмарних активів (рис. 1.13) критичних інфраструктур можуть входити ХМС, за допомогою яких надаються відповідні сервіс-орієнтовані ресурси. Як було зазначено, спираючись на відомий досвід застосування [91], перевага надається хмарній інфраструктурі AWS, на основі використання якої можуть надаватися різноманітні ресурси (табл. 1.4), а саме: хмарне сховище Amazon S3 [93], обчислювальна хмара Amazon EC2 [94], аналітика потокових даних Amazon Kinesis [95] і т.і.

Крім розв’язування задач, пов’язаних з управлінням КІ в різноманітних умовах їхнього використання за призначенням, хмарні активи можуть застосовуватися для аварійного відновлювання та резервного копіювання інформаційних ресурсів критичних інфраструктур. Економічна доцільність використання ХМА пов’язана також з можливістю трансформування кібернтичних активів в хмару. Аналіз застосування ХМІ AWS для забезпечення

гарантоздатності системи управління критичної інфраструктури, виконаний за результатами аналітико-стохастичного моделювання, розглянуто в розділі 4.

2.2.2 Аналіз негативних факторів впливу на активи критичних інфраструктур

Негативні фактори впливу на активи критичних інфраструктур можна розділити на три групи, а саме:

1) зовнішні та внутрішні фактори негативного впливу на фізичні активи критичних інфраструктур;

2) зловмисні шкідливі впливи на кібернетичні активи критичних інфраструктур;

3) зловмисні шкідливі впливи на хмарні активи критичних інфраструктур.

До першої групи відносяться фактори негативного впливу, які пов’язані з дефектами, збоями в функціонуванні, раптовими і прихованими відмовами компонентних складових, які представляють ФА КІ. Ці негативні явища призводять до дисбалансу в управлінні КІ, що може бути причиною каскадних відмов, які протікають в формі неконтролюємих відключень більшості інфраструктурних компонентів. Внаслідок чого порушуються складні комплементарні зв’язки [8] між різними інфраструктурними утворюваннями, які можуть надавати руйнівний вплив на навколишнє середовище, на економіку держави та створюють серйозну загрозу життю, здоров’ю людей, – споживачів продукції, послуг, які виробляються та надаються КІ. Крім того, зазначені негативні явища можуть сприяти виникненню безпечних відмов, які можуть привести до аварій та катастроф. Безпосередньо про це свідчать наслідки аварій КЕІ, які розглянуто в підрозділі 1.1.2 запропонованої дисертаційної роботи.

Друга група негативних факторів впливу пов’язана з дією різноманітних ЗВШВ на кібернетичні активи критичних інфраструктур та враховує вразливості й загрози, які виникають для відповідних компонентних складових КБА. Як правило, ЗВШВ реалізуються зловмисниками за схемою: цільовий фішинг–оцінка вразливостей–взлом системи кіберзахисту–проникнення в систему (в

контур управління системою)–викривлення інформації з метою компрометації системи. Відомий досвід зловмисних шкідливих впливів на кібернетичні активи КІ (підрозділи 1.1–1.3) свідчить, що абсолютно безпечних систем, приладів, додатків відповідного ПЗ не існує; їхня компрометація – це лише справа часу. Тим не менше, покращити стан інформаційної безпеки критичних інфраструктур можуть хмарні системи, об’єднані в відповідні ХМА КІ. Використання ХМА розширює функціональність, пропускну спроможність компонентів як фізичних, так і кібернетичних активів КІ; посилює арбітражні функції аналізу ЗВШВ; надає можливості по оперативному усуненню наслідків ЗВШВ за рахунок реалізації функцій аварійного відновлювання.

Третя група негативних факторів впливу утворюється ЗВШВ на хмарні активи критичних інфраструктур. Дія ЗВШВ цього типу проявляється аналогічно дії попередньої групи. Порівняльний аналіз рівня функційної безпечності ХМС провідних хмарних провайдерів з урахуванням негативних факторів впливу представлено в таблиці 1.7.

2.2.3 Моделювання поведінки критичної інфраструктури з урахуванням негативних факторів впливу на її активи

Для оцінювання ризику КІ необхідно попередньо виконати моделювання їхньої поведінки, враховуючи негативні події, які впливають на функційну та інформаційну безпечність інфраструктурних активів. Базуючись на результатах аналізу методів оцінювання готовності хмарних систем та негативних факторів впливу на активи КІ, який виконано в підрозділах 1.3.1 та 2.2.2, запропонована відповідна узагальнена схема (рис. 2.8) моделювання поведінки окремо взятої критичної інфраструктури.

Відповідно до рис. 2.8 моделювання поведінки КІ відбувається в декілька етапів як з урахуванням, так і без урахування ІТС інфраструктурних компонентів. На першому етапі записується кортежна модель КІ, яка представляє собою узагальнений формалізований опис активів інфраструктури. На другому етапі

будується логіко-ймовірнісна модель поведінки КІ з урахуванням негативних подій, які можуть відбуватися по відношенню до активів інфраструктури. Далі, застосовуючи причинно-наслідковий аналіз, будуються структурно-логічні схеми цих негативних подій. Крім того, можуть бути побудовані структурні схеми надійності та дерева відмов, які дають чітке уявлення про перебіг й послідовність негативних подій.

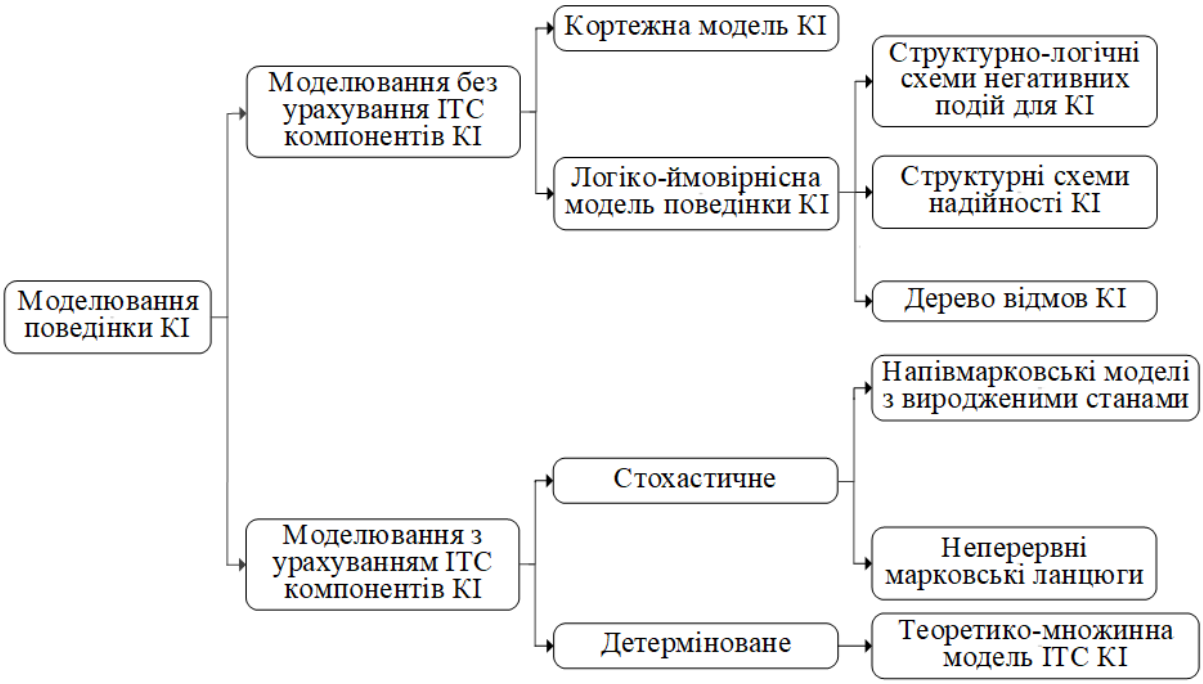


Рис. 2.8 Схема моделювання поведінки критичної інфраструктури з урахуванням негативного впливу на її активи

В ході виконання третього етапу будуються марковські або напівмарковські моделі в залежності від припущень, які враховують (або не враховують) предісторію відбуття подій, особливості та режими застосування компонентів критичних інфраструктур за призначенням. Результати стохастичного моделювання застосовуються для аналізу готовності КІ з урахуванням негативних факторів впливу на активи інфраструктури. На четвертому етапі будується теоретико-множинна модель ынформаційно-технічних станів критичної інфраструктури, яка застосовується як базова для виконання оцінного моделювання поведінки та визначення рівня готовності КІ.

При певних умовах послідовність реалізації етапів може змінюватися, що

використовується для розробки нових методів моделювання поведінки критичних інфраструктур з урахуванням негативних факторів впливу на їхні активи.

2.2.4 Причинно-наслідковий аналіз негативного впливу на активи критичних інфраструктур

Важливе місце в загальній процедурі оцінювання ризику КІ займає причинно-наслідковий аналіз негативного впливу на інфраструктурні активи. Відомі дослідження за цим напрямком представлено у вигляді деякої базової структури, за допомогою якої відображаються причинно-наслідкові зв'язки між негативними подіями, що через загрози впливають на вразливості критичних інфраструктур. Під дією цих загроз виникає негативний ефект у вигляді відмов, збоїв, каскадних відключень відповідних компонентів, тощо. Примітною в цьому сенсі є критична енергетична інфраструктура, яка на стику століть була найбільш вразливою до негативних впливів, що виливалися в каскадні відмови з важкими фінансово-економічними втратами та людськими жертвами. Наприклад, в роботах [96, 97] зображено модель типу "краватка-метелик", за допомогою якої структуризуються та візуалізуються причини і наслідки негативних подій для КЕІ (рис. 2.9). При побудові моделі (рис. 2.9) було враховано бар'єри (Б) на шляху реалізації розглянутих негативних подій.

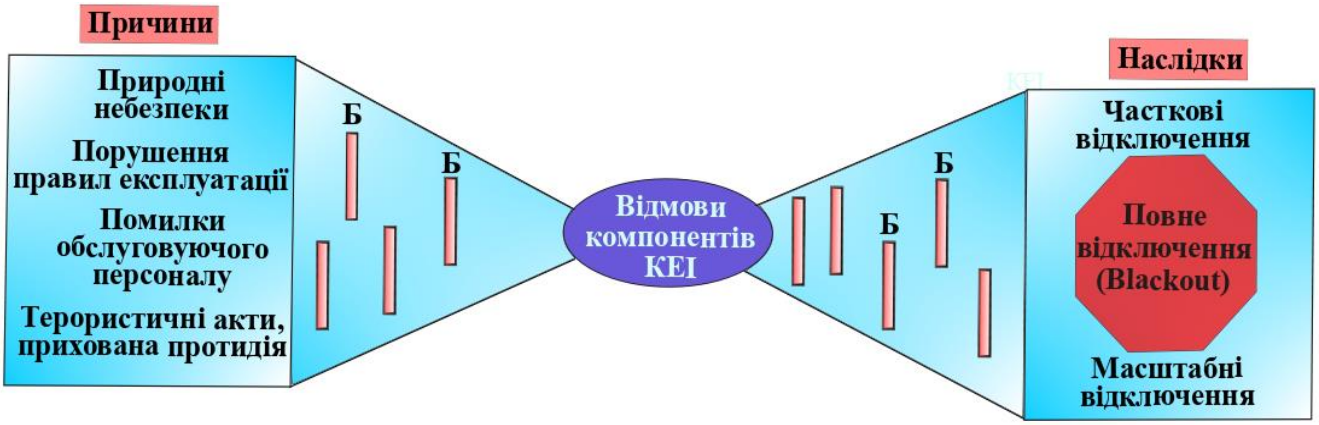


Рис. 2.9 Модель причинно-наслідкового аналізу відмов КЕІ [96]

Модель, яка зображена на рис. 2.9, є однією зі складових частин методології

аналізу вразливостей критичної енергетичної інфраструктури і застосовувалась в процесі ідентифікації наслідків негативних подій для активів КЕІ [96]. Ще один підхід на основі причинно-наслідкового аналізу реалізовано на рівні міжнародного стандарту IEC 61882, який використовується в дослідженнях по оцінці рівня небезпеки та працездатності критично важливих об’єктів нафтогазової промисловості [98].

В запропонованій дисертаційній роботі причинно-наслідковий аналіз застосовується як інструментарій, за допомогою якого виконується упорядкування негативних подій для КІ за місцем, часом, послідовністю їх виникнення. За результатами виконаного аналізу будується систематизована формалізована структура, яка використовується для побудови відповідних аналітико-стохастичних моделей і оцінки ризику негативних впливів на активи критичних інфраструктур.

2.2.5 Аналітико-стохастичне оцінювання ризику негативного впливу на активи критичних інфраструктур

Значна частина відомих методів оцінювання ризику критичних інфраструктур базується на визначенні якісних характеристик КІ у вигляді відповідних метрик, які отримують за допомогою використання цільових технологій. Одним з розповсюджених та найвідоміших є метод аналізу видів, наслідків та критичності відмов (FMECA) [99]. Сутність методу FMECA полягає у визначенні критичності виявлених відмов, для яких відомі ймовірність виникнення, причини та тяжкість їхніх наслідків [100]. Серед безумовних переваг суттєвим недоліком методу FMECA є складність визначення ризику КІ через відсутність гнучкої процедури запису та підготовки даних для матриці критичності.

Усунути зазначений недолік дозволяє застосування процедури аналітико-стохастичного оцінювання ризику негативного впливу на активи критичних інфраструктур, яка є складовою частиною загальної методології забезпечення готовності КІ. Подальше застосування розглянутої методології в сфері

електроенергетики дозволить здійснити еволюційний перехід до гібридної кіберенергетичної інфраструктури (рис. 2.10).

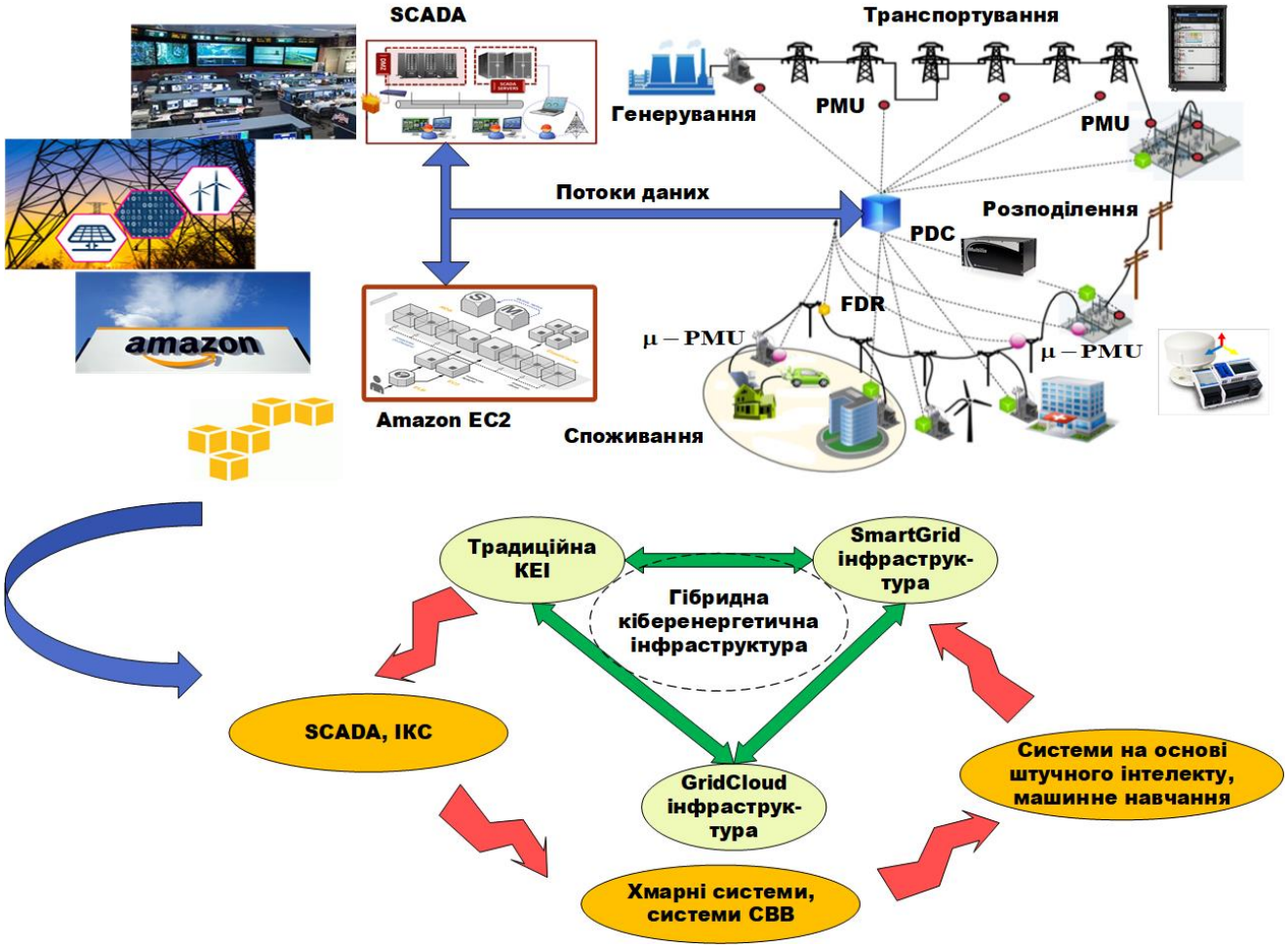


Рис. 2.10 Концепція переходу до гібридної кіберенергетичної інфраструктури

Відповідно до представленої концепції (рис. 2.10) перехід від типової (класичної) критичної енергетичної інфраструктури здійснюється в два етапи, а саме: на першому етапі здійснюється перехід до GridCloud інфраструктури, в значній ступіні цьому сприяє впровадження ХМС та ССВВ; на другому етапі за рахунок впровадження штучного інтелекту, машинного навчання здійснюється перехід до SmartGrid інфраструктури. Але попередньо необхідно покращити рівень надійності і готовності фізичних активів КЕІ; знизити високий рівень зносу фізичних активів КЕІ.

В представленій методології (рис. 2.1) значна увага приділяється функційній (ФБ) та інформаційній безпечності (ІБ) активів КІ. Відомо, що різноманітні негативні події у вигляді зловмисних шкідливих впливів та проникнень (ЗВШП), відмов, збоїв, дефектів погіршують ФБ та ІБ критичних інфраструктур. Безумовно це знижує рівень готовності, збільшує ризик негативних впливів на інфраструктурні активи та сприяє виникненню аварій КІ з важкими наслідками. Класифікаційна схема ризику негативних впливів на активи КІ зображена на рис. 2.11.

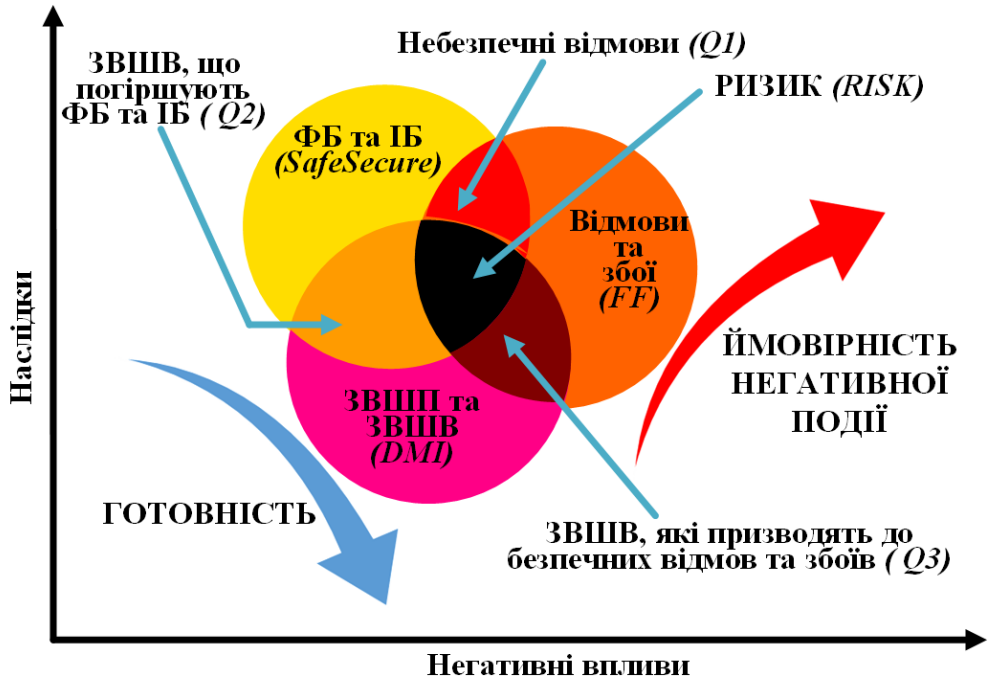


Рис. 2.11 Структурна діаграма ризику негативних впливів на активи КІ

Відповідно до рис. 2.11 зі збільшенням ймовірності негативних подій та зниженням рівня готовності виникає ризик для активів КІ, теоретико-множинна модель якого записується так:

$$\mathrm{Risk} = Q_1 \cap Q_2 \cap Q_3, \tag{2.3}$$

де Q_1 – множина небезпечних відмов КІ, які виникають внаслідок дії звичайних відмов та збоїв інфраструктурних активів і погіршення їхньої функційної й інформаційної безпечності; Q_2 – множина ЗВШВ, що погіршують

функційну та інформаційну безпечність активів КІ; Q_3 – множина ЗВШВ, які призводять до безпечних відмов та збоїв активів КІ.

Від ТММ у вигляді співвідношення (2.3) здійснюється перехід до аналітико-стохастичної моделі ризику негативних впливів на активи КІ, яка записується у вигляді співвідношення

$$R_{CrI} = \left(1 - K_{\Gamma_{CrI}}\right) L_{ПНД_{CrI}}, \tag{2.4}$$

де $K_{\Gamma_{CrI}}$ – КГ критичної інфраструктури з урахуванням негативних впливів на її активи; $L_{ПНД_{CrI}}$ – показник причинно-наслідкової декомпозиції (ПНД) негативних впливів на активи КІ.

У виразі (2.4) показник $L_{ПНД_{CrI}}$ визначається на основі використання алгебри причинно-наслідкових комплексів (ПНК), яка була розроблена і впроваджена в складних людино-машинних системах професором В. О. Твєрдохлєбовим та його колегами. Ілюстративний приклад щодо розрахунку ризику негативних впливів на активи КЕІ наведено у розділах чотири та п’ять.

2.3 Логіко-ймовірнісна модель готовності критичної інфраструктури

Згідно загальної концепції дисертаційного дослідження та відповідно до класифікаційної схеми ризику КІ (рис. 2.11) негативні впливи представляються у вигляді ЗВШВ, на реалізацію яких впливають зовнішні і внутрішні фактори природнього та штучного походження. Дія ЗВШВ моделюється з застосуванням як стохастичного, так і детерміністського підходів (рис. 2.8).

Кортежна модель конкретної критичної інфраструктури записується у вигляді співвідношень (1.9), (1.10). У якості базової (опорної) розглядається логіко-ймовірнісна модель готовності критичної інфраструктури, до складу якої входять фізичні, кібернетичні та хмарні активи. Модель записується у вигляді

$$\text{Availability}_{CI} = 1 - P\left\{\left[UA_{PhA} \cup DMI\right] \cup \left[\left(UA_{CbrA} \cup DMI\right) \cap \left(UA_{CldA} \cup DMI\right)\right]\right\}, \tag{2.5}$$

де UA_{PhA} – подія, яка полягає в неготовності ФА критичної інфраструктури;

UA_{CbrA} – подія, яка полягає в неготовності КБА критичної інфраструктури; UA_{CldA} – подія, яка полягає в неготовності ХМА критичної інфраструктури; DMI – ЗВШВ на активи критичної інфраструктури.

Для оцінного стохастичного моделювання поведінки критичної інфраструктури з урахуванням негативного впливу на її активи застосовується наступна система обмежень:

$$\Im = \begin{cases} \theta \subset \Theta, \vartheta_k = \varnothing, k \notin i, i = \overline{1,n}; \\ \varphi \subset \Theta, \vartheta_f = \varnothing, f \in j, j = \overline{1,m}; \\ \varepsilon \subset \Theta, \vartheta_p = \varnothing, p \notin s, s = \overline{1,\ell}; \\ \rho \subset \Theta, \vartheta_g = \varnothing, g \in z, z = \overline{1,h}; \\ K_{\Gamma_{i,s}}(t) \geq K^*_{\Gamma_0}; \\ K_{\Gamma_{j,z}}(t) < K^*_{\Gamma_0}; \\ C_{min_0} \leq C_0 \leq C_{max_0}; \\ C_0 > C_{max_0}; \end{cases} \tag{2.6}$$

де $\Theta = \theta \cup \varphi \cup \varepsilon \cup \rho$ – множина значень показника цикломатичної складності ϑ (ЦКС) [101], значення якого відповідають сукупності графів ІТС напівмарковського процесу моделювання (НПМ) поведінки критичної інфраструктури (далі скорочено, графів НПМ); $\theta = \{\vartheta_i\}_{i=1}^{n}$ – множина ІТС, яка відповідає значенню показника ЦКС для графів НПМ без поглинаючих станів; $\varphi = \{\vartheta_j\}_{j=1}^{m}$ – множина ІТС, яка відповідає значенню показника ЦКС для графів НПМ з поглинаючими станами; $\varepsilon = \{\vartheta_s\}_{s=1}^{\ell}$ – множина ІТС, що відповідає значенню показника ЦКС для графів НПМ, які не містять станів вразливості та дефектів; $\rho = \{\vartheta_s\}_{s=1}^{\ell}$– множина ІТС, що відповідає значенню показника ЦКС для графів НПМ, які містять стани вразливості та дефектів; ϑ_k, ϑ_f – значення показника ЦКС для графів НПМ, які містять поглинаючи стани; ϑ_p, ϑ_g – значення показника ЦКС для графів НПМ, які містять стани вразливості та дефектів; K_{Γ_0} –

граничні допустимі значення КГ критичної інфраструктури; C_0 – граничні витрати на підтримання необхідного рівня готовності критичної інфраструктури.

В системі обмежень (2.6) показник ЦКС визначається як

$$\vartheta = E - V + 2,$$

де E – кількість переходів (ребер) графу $G = (V, E)$ НПМ; V – кількість станів (вершин) для графу $G = (V, E)$ НПМ.

В наступному розділі дисертаційної роботи представлено результати аналітико-стохастичного моделювання готовності КІ, які було отримано завдяки використанню розглянутих теоретичних положень.

Висновки до розділу 2

1. Сформульовано концепцію наукових досліджень, яка полягає в створенні надійних та безпечних хмарних систем критичних інфраструктур з сервіс-орієнтованим розподіленням ресурсів.

2. На основі запропонованої концепції наукових досліджень розроблено структуру методології забезпечення готовності хмарних систем критичних інфраструктур, яка представлена у вигляді сукупності принципів, моделей, методів оцінювання функційної безпечності, методів забезпечення готовності, методів вибору, оцінки характеристик готовності, енергоефективності та інформаційної технології тестування ХМС КІ.

3. Для забезпечення готовності хмарних систем критичних інфраструктур розроблено принцип реконфігурування та комбінованої надлишковості сервіс-орієнтованих ресурсів ХМС КІ; принцип компліментарності архітектурної побудови КІ; принцип оперативного моніторингу компонентів критичної енергетичної інфраструктури на основі застосування систем синхронізованих векторних вимірювань; принцип управління готовністю критичною енергетичною інфраструктурою за інформаційно-технічним станом з застосуванням сервіс-орієнтованих хмарних ресурсів.

4. На основі представленої схеми моделювання поведінки критичних

інфраструктур, яка базується на причинно-наслідковому аналізі негативного впливу на їхні фізичні, кібернетичні та хмарні активи, розроблено аналітико-стохастичну модель ризику негативного впливу на інфраструктурні активи і логіко-ймовірнісну модель готовності КІ.

5. Подальше застосування розглянутої методології дозволить розробити методи оцінювання і забезпечення готовності критичних інфраструктур; підвищити функціональність, інформативність контуру їхнього управління за рахунок застосування хмарних систем; знизити невизначеність процедури оцінювання ризиків негативного впливу на активи КІ; здійснити еволюційний перехід до гібридної кіберенергетичної інфраструктури.

Основні положення цього розділу викладені у публікаціях автора [8, 74, 75, 76, 99, 101].

РОЗДІЛ 3
АНАЛІТИКО-СТОХАСТИЧНІ МОДЕЛІ КРИТИЧНИХ ІНФРАСТРУКТУР

3.1 Теоретико-множинна модель інформаційно-технічних станів критичної інфраструктури

Для реалізації загальної методології оцінювання готовності критичних інфраструктур (рис. 2.1) необхідно побудувати відповідний модельний ряд, який представляє собою сукупність аналітико-стохастичних моделей [102]. Процес побудови пропонуємих до розгляду аналітико-стохастичних моделей базується на використанні апарату формалізації процесів зміни ІТС інфраструктурних компонентів, врахуванні негативних факторів зовнішнього та внутрішнього впливу на їхню безпечність [103]; принципах аналізу і управління безпечністю критичних інфраструктур. На рис. 3.1 зображена схема формалізації процесів, які впливають на функційну та інформаційну безпечність КІ.

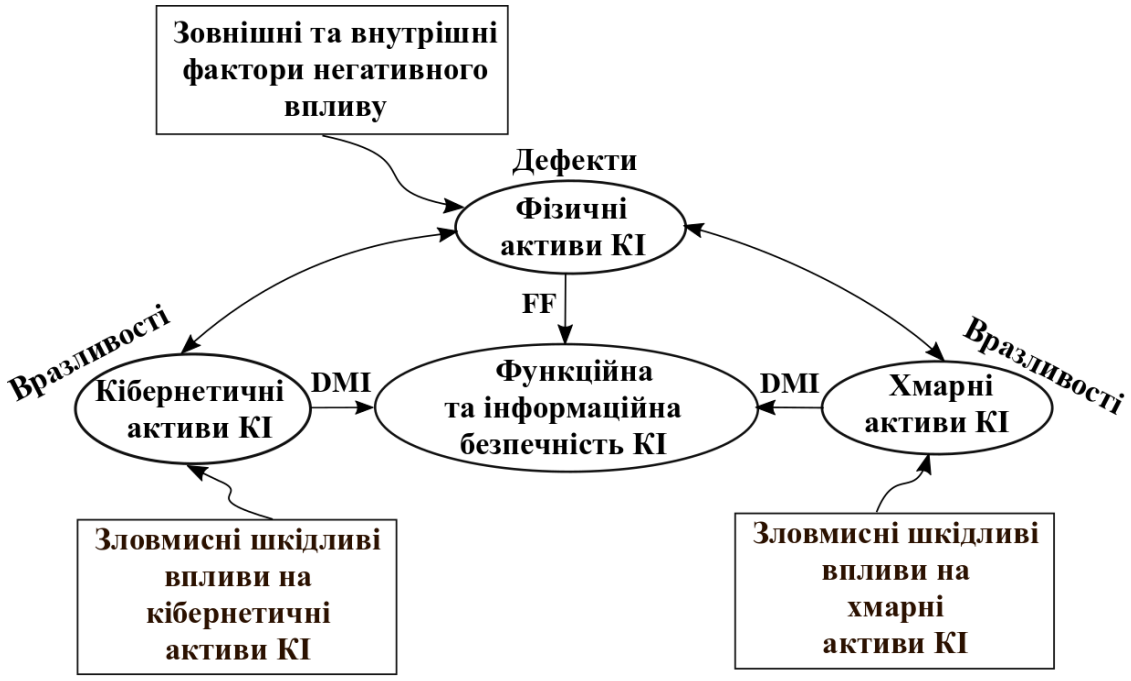


Рис. 3.1 – Схема формалізації процесів, які впливають на ФБ та ІБ КІ

Враховуючи зображений формалізований опис (рис. 3.1) та результати аналізу негативних факторів впливу на активи КІ, який виконано в розділі 2, для

множини інформаційно-технічних станів критичної інфраструктури $M_{CI} = \left\{ M_{FF}^{PhA}, M_{DMI}^{CbrA}, M_{DMI}^{CldA}, M_{SS}^{CI} \right\}$ за умови існування відображень $\Omega(x_i)$, $\Omega(w_j)$ теоретико-множинна модель інформаційно-технічних станів інфраструктури може бути записана у вигляді

$$H_{PhA}^{CI} = \left\{ (x_1, y_1) \middle| x_1 \in M_{FF}^{PhA} \wedge y_1 \in M_{SS}^{CI} \wedge \Omega(x_1) = y_1 \right\}, \quad (3.1)$$

$$H_{CbrA}^{CI} = \left\{ (x_2, y_2) \middle| x_2 \in M_{DMI}^{CbrA} \wedge y_2 \in M_{SS}^{CI} \wedge \Omega(x_2) = y_2 \right\}, \quad (3.2)$$

$$H_{CldA}^{CI} = \left\{ (x_3, y_3) \middle| x_3 \in M_{DMI}^{CldA} \wedge y_3 \in M_{SS}^{CI} \wedge \Omega(x_3) = y_3 \right\}, \quad (3.3)$$

$$N_{CbrA}^{PhA} = \left\{ (w_1, z_1) \middle| w_1 \in M_{DMI}^{CbrA} \wedge z_1 \in M_{FF}^{PhA} \wedge \Omega(w_1) = z_1 \right\}, \quad (3.4)$$

де M_{FF}^{PhA} – множина відмов та дефектів фізичних активів критичної інфраструктури; M_{DMI}^{CbrA} – множина зловмисних шкідливих впливів на кібернетичні активи критичної інфраструктури; M_{DMI}^{CldA} – множина зловмисних шкідливих впливів на хмарні активи критичної інфраструктури; M_{SS}^{CI} – множина інформаційно-технічних станів фізичних, кібернетичних та хмарних активів, які впливають на функційну та інформаційну безпечність критичної інфраструктури.

Використовуючи отриману ТММ у якості опорної моделі, перейдемо до розгляду оцінної аналітико-стохастичної моделі надійності критичної енергетичної інфраструктури з системою моніторингу інформаційно-технічних станів.

3.2 Аналітико-стохастична модель надійності критичної енергетичної інфраструктури з системою моніторингу інформаційно-технічних станів

Однією з основних вимог до критичних інфраструктур є забезпечення необхідного рівня їхньої надійності, живучості у випадках виникнення різних видів відмов та інших негативних подій. Вирішення цієї проблеми в значній мірі залежить від ефективного використання за призначенням системи моніторингу ІТС критичних інфраструктур, що функціонує в різних режимах контролю та діагностування. Тому доцільно розглянути деякі аспекти моделювання надійності

КІ з системою моніторингу їхніх ІТС.

В цьому сенсі певний інтерес викликає архітектурно-орієнтований підхід до оцінки рівня надійності та визначення тестових послідовностей програмного забезпечення систем управління КІ по результатам моніторингу їхнього ІТС, який представлено в [104]. Теоретичною основою зазначеного підходу є опорні моделі “зростання”, які використовуються для обґрунтування необхідного рівня надійності ПЗ на стадії його тестування [105,106]. Певний інтерес з точки зору аналізу можливостей структурного моніторингу складних технічних систем викликає матеріал, який відображено в роботах [107].

Оригінальне технічне рішення для системи моніторингу компонентів КІ з використанням бездротової сенсорної (радіосенсорної) мережі і результати імітаційного моделювання в середовищі MöbiusXMLParser викладені в [108]. Науковою основою для моделювання в [108] є коректно обгрунтоване використання апарату марковських ланцюгів і структурована побудова об’єкта моделювання за допомогою мереж Петрі.

Однак, в зазначених роботах недостатньо повно висвітлено особливості функціонування системи моніторингу КІ в різних режимах застосування за призначенням. А саме, в режимах контролю інформаційно-технічного стану (КТС) і діагностування. Для вирішення цього завдання доцільно використовувати напівмарковські моделі, які адекватно відображають властивості та деякі особливості функціонування системи моніторингу КІ.

3.2.1 Напівмарковські моделі моніторингу інформаційно-технічних станів компонентів критичної інфраструктури

Відповідно до загальної методології (рис. 2.1) забезпечення ефективного функціонування критичних інфраструктур при пріоритеті їх надійності та безпеки повинен виконуватися принцип архітектурної компліментарності (рис. 2.4). Зазначений принцип покладено в основу методу управління КІ за інформаційно-технічним станом, який більш детально розглянуто в розділі 5. Згідно з цим методом управління готовністю критичної інфраструктури здійснюється при

безперервному моніторингу інформаційно-технічних станів її компонентів. На рис. 3.2 зображено класифікаційну схему процесів моніторингу інформаційно-технічиих станів компонентів КІ.

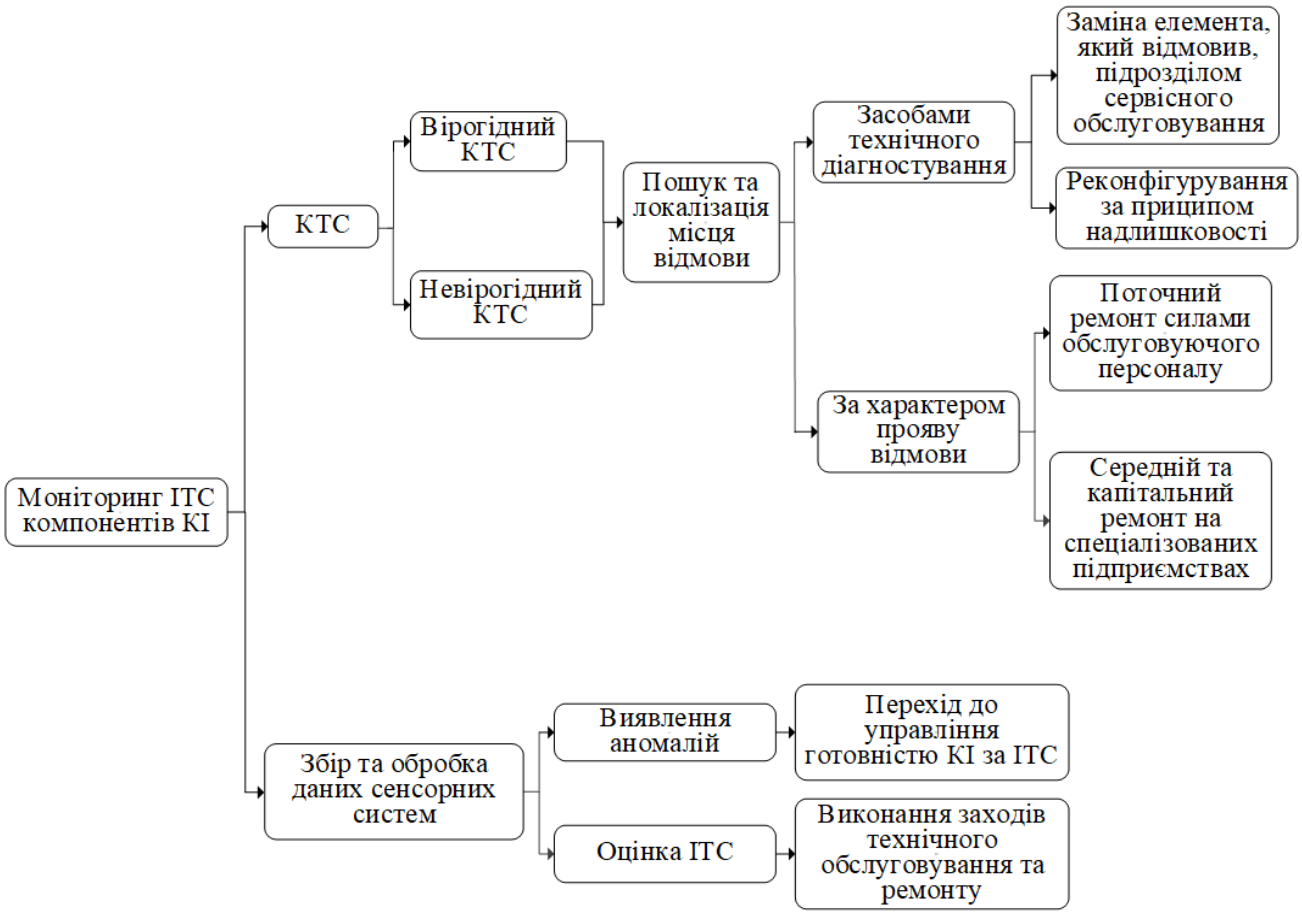


Рис. 3.2 Класифікаційна схема процесів моніторингу інформаційно-технічиих станів компонентів КІ

Згідно з зображеною класифікаційною схемою (рис. 3.2) перспективна система моніторингу компонентів КІ повинна працювати в двох режимах, а саме, контроля інформаційно-технічного стану, збора та обробки даних сенсорних систем. Виходячи з зазначеного, побудуємо моделі моніторингу КІ [109] з урахуванням результатів КТС та технічного діагностування [110] компонентів інфраструктури. Подальші розрахунки були реалізовані на основі застосування напівмарковського процесу моделювання. Перевагу було надано напівмарковським моделям (НПММ) у порівнянні з марковськими саме тому, що використання НПММ надає можливість враховувати стохастичне та

детерміністське різноманіття режимів застосування КІ за призначенням.

На рис. 3.3 зображено граф станів однієї з найбільш розповсюджених напівмарковських моделей моніторингу інформаційно-технічних станів компонентів КІ з КТС. Множина станів цієї НПММ записується у вигляді $\forall\ S_i \in S,\ S = \{S_0, S_1, S_2\} \exists\ G = (V, E)$, де S_0 – працездатний стан (ПРС) компонентів КІ; S_1 – стан КТС компонентів КІ; S_2 – непрацездатний стан (НПРС) компонентів КІ. Вважається, що з встановленою періодичністю, яка не є випадковою величиною і відповідає тривалості експлуатації $T \in [0, t]$ компонентів КІ, на протязі детермінованого інтервалу часу $\tau_{ктс}$ проводиться контроль їхнього інформаційно-технічного стану. Початковий стан компонентів КІ в момент часу $t = 0$ описується значеннями імовірностей $P_0(0) = 1,\ P_1(0) = P_2(0) = 0$.

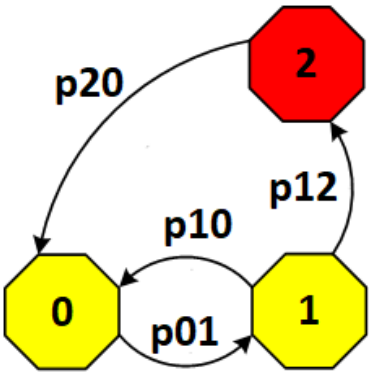


Рис. 3.3 Граф станів НПММ моніторингу інформаційно-технічних станів компонентів критичної інфраструктури з КТС

Застосовуючи відомий спосіб побудови НПММ [111], згідно з представленим на рис. 3.3 графом станів розглянемо яким чином формуються складові матриці $|Q_{ij}(t)|$ незалежних функцій розподілення часу перебування компонентів КІ в *i*-у стані перед переходом в *j*-й стан. Враховуючи періодичність проведення КТС, функція розподілення часу для переходу зі стану S_0 в стан S_1 записується так:

$$Q_{01}(t)=\begin{cases}0, & t<T;\\ 1, & t\geq T.\end{cases} \tag{3.5}$$

Якщо за результатами КТС відмов компонентів КІ не виявлено, то перехід зі стану S_1 в стан S_0 за час *t* здійснюється з функцією розподілення

$$Q_{10}(t)=\begin{cases}0, & t<\tau_{ктс};\\ 1, & t\geq \tau_{ктс}.\end{cases} \tag{3.6}$$

При виникненні під час проведення КТС відмов перехід зі стану S_1 в стан S_2 характеризується ймовірністю

$$Q_{12}(t)=1-e^{-\lambda t}, \tag{3.7}$$

де λ – інтенсивність відмов компонентів КІ під час проведення КТС.

Роботи по відновленню ПРС компонентів КІ (перехід $S_2 \to S_0$) виконуються за випадковий час з функцією розподілення

$$Q_{20}(t)=1-(1+\mu t)e^{-\mu t}, \tag{3.8}$$

де μ – інтенсивність відновлення ПРС компонентів КІ, що відповідає закону Ерланга [10].

Результати моделювання для запропонованої НПММ у вигляді імовірнісної залежності $P_0(T_0,T_в)$ коефіцієнта готовності компонентів КІ від середньої наробітки на відмову та середнього часу їхнього відновлення зображено на рис. 3.4.

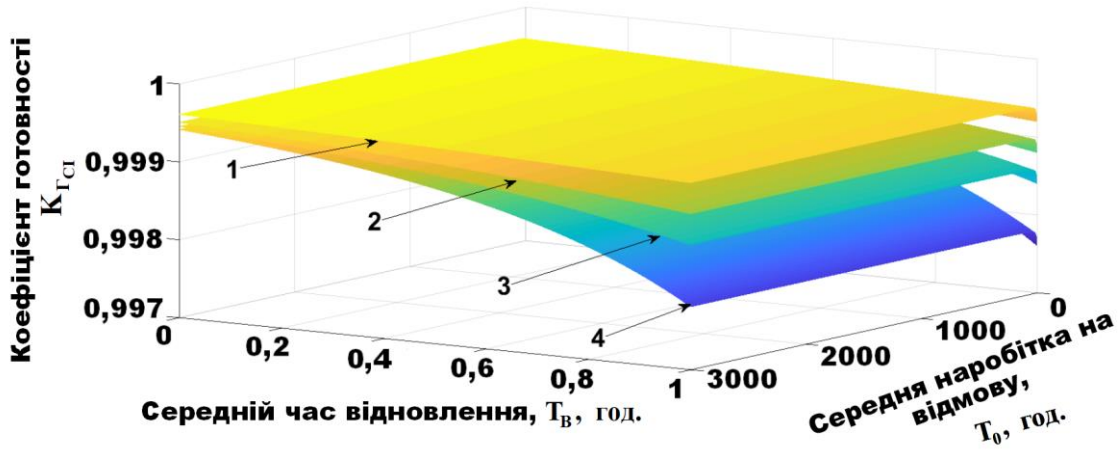


Рис. 3.4 Кількісні результати моделювання для $T=5000$ год. за умов: 1) $\tau_{ктс}=1$ хв. хв.; 2) $\tau_{ктс}=1{,}5$ хв.; 3) $\tau_{ктс}=2$ хв. хв.; 4) $\tau_{ктс}=3$ хв.

Отримані результати моделювання (рис. 3.4) є занадто оптимістичними, тому що не враховуються негативні ситуації, які пов'язані з наявністю різноманітних вразливостей, помилок обслуговуючого персоналу [112] та прихованих відмов. Саме зазначені негативні явища породжують каскадні ефекти в сфері застосування КЕІ [113], що мають важкі наслідки. Тому має сенс розглянути другу модель, яка описує ситуацію, коли проводиться недостовірний КТС (рис. 3.1) компонентів КЕІ.

На відміну від попередньої, друга модель, яка пропонується, враховує реальні ситуації, під час реалізації яких виникають певні негаразди по відношенню до компонентів КЕІ, а саме: через невірогідний КТС не вдається локалізувати та знайти місце відмови (несправності); під час проведення контролю інформаційно-технічних станів компонентів КЕІ виникають приховані відмови і виникає потреба у проведенні другого циклу КТС і виконанні додаткових заходів технічного діагностування. Для запропонованої моделі напівмарковський процес описується графом станів, який зображено на рис. 3.5.

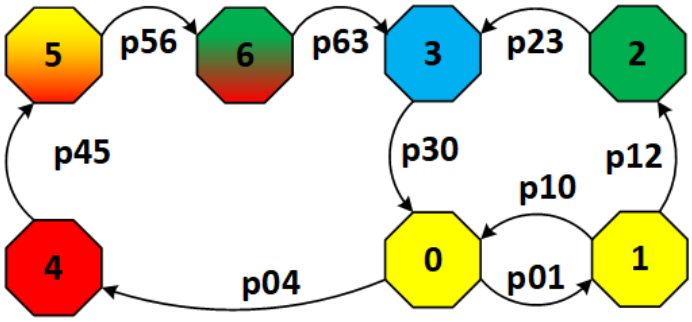


Рис. 3.5 Граф станів НПММ моніторингу інформаційно-технічних станів компонентів КЕІ з невірогідним КТС

Відповідно до рис. 3.5 множина станів НПММ записується у вигляді $\forall\ S_i \in S,\ S = \{S_0, S_1, S_2, S_3, S_4, S_5, S_6\} \exists\ G = (V, E)$, де S_0 – ПРС компонентів КЕІ; S_1 – стан КТС компонентів КЕІ, на протязі якого виникають раптові та помилкові відмови; S_2 – стан технічного діагностування компонентів КЕІ після виникнення відмов під час проведення КТС, тобто в цьому стані здійснюється пошук та

локалізація місця відмови; S_3 – стан відновлення ПРС компонентів КЕІ після виникнення раптових відмов в ході КТС та після виконання заходів технічного діагностування, а також після виявлення прихованої відмови і наступного циклу КТС-технічне діагностування зі стану прихованої відмови; S_4 – стан прихованої відмови, коли компоненти КЕІ знаходяться в НПРС, але вважаються працездатними; S_5 – стан КТС компонентів КЕІ, коли вони знаходяться у стані прихованої відмови; S_6 – стан технічного діагностування компонентів КЕІ, коли вони знаходяться у стані прихованої відмови. Початкові стани відповідають значенням імовірностей $P_0(0)=1$, $P_i(0)=0$, де $i=\overline{1,6}$. По аналогії з попередньою моделлю вважається, що з встановленою періодичністю, яка не є випадковою величиною і відповідає тривалості експлуатації $T\in[0,t]$ компонентів КЕІ, на протязі детермінованого інтервалу часу $\tau_{ктс}$ проводиться контроль їхнього інформаційно-технічного стану.

Решта розподілень для матриці $|Q_{ij}(t)|$ задаються за умови виконання наступних припущень: а) перехід $S_1 \to S_2$ відбувається за випадковий інтервал часу, розподілений за законом Ерланга 2-го порядку з параметром λ_1; б) перехід $S_2 \to S_3$ відбувається за випадковий інтервал часу, розподілений за експоненціальним законом з параметром λ_2; в) перехід $S_3 \to S_0$ відбувається за випадковий інтервал часу, розподілений за законом Ерланга 4-го порядку з параметром μ; г) перехід $S_0 \to S_4$ – по гіперекспоненціальному закону [104] з параметрами λ_3, λ_4; д) перехід $S_5 \to S_6$ – за випадковий час, розподілений за законом Ерланга 3-го порядку з параметром λ_5; е) перехід $S_6 \to S_3$ – за випадковий час, розподілений за експоненціальним законом з параметром λ_6.

Тоді, елементи матриці $|Q_{ij}(t)|$, які відповідають функціям розподілення часу для переходів $S_i \to S_j$, записуються так:

$$Q_{12}(t)=1-(1+\lambda_1 t)e^{-\lambda_1 t}, \tag{3.9}$$

$$Q_{23}(t) = 1 - e^{-\lambda_2 t}, \tag{3.10}$$

$$Q_{30}(t) = 1 - \left(1 + \mu t + \frac{(\mu t)^2}{2} + \frac{(\mu t)^3}{6}\right) e^{-\mu t}, \tag{3.11}$$

$$Q_{04}(t) = 1 - \frac{\lambda_4}{\lambda_4 - \lambda_3} e^{-\lambda_3 t} + \frac{\lambda_3}{\lambda_4 - \lambda_3} e^{-\lambda_4 t}, \tag{3.12}$$

$$Q_{56}(t) = 1 - \left(1 + \lambda_5 t + \frac{(\lambda_5 t)^2}{2}\right) e^{-\lambda_5 t}, \tag{3.13}$$

$$Q_{63}(t) = 1 - e^{-\lambda_6 t}. \tag{3.14}$$

Елементи матриці $\left|Q_{ij}(t)\right|$ для переходів $S_0 \to S_1$ та $S_1 \to S_0$ записуються за допомогою формул (3.5), (3.6). Виконавши нетривіальні розрахунки, згідно з методикою, яка викладена в [1,10], отримаємо співвідношення для розрахунку стаціонарного коефіцієнта готовності та решти імовірнісних залежностей $P_k(T)$, де $k = \overline{1,6}$, у вигляді

$$K_{\Gamma_{CI}} = P_0(T) = \frac{\alpha_1\beta_5(1 - C_1) - \alpha_2\beta_6(1 - C_2)}{A}, \tag{3.15}$$

$$P_1(T) = \frac{2\beta_1(\alpha_1 C_1 - \alpha_2 C_2)}{A}, \tag{3.16}$$

$$P_2(T) = \frac{\beta_2(1 - C_3(1 + \gamma))(\alpha_1 C_1 - \alpha_2 C_2)}{A}, \tag{3.17}$$

$$P_3(T) = \frac{\tau_в[1 - C_3(\alpha_1 C_1 - \alpha_2 C_2)(1 + \gamma)]}{A}, \tag{3.18}$$

$$P_4(T) = \frac{[1 - \alpha_1 C_1 + \alpha_2 C_2][T - G]}{A}, \tag{3.19}$$

$$P_5(T) = \frac{\beta_3(1 - \alpha_1 C_1 + \alpha_2 C_2)}{A}, \tag{3.20}$$

$$P_6(T) = \frac{\beta_4(1 - \alpha_1 C_1 + \alpha_2 C_2)}{A}, \tag{3.21}$$

де

$$A=\alpha_1\beta_5(1-C_1)-\alpha_2\beta_6(1-C_2)+(\alpha_1C_1-\alpha_2C_2)\left[2\beta_1+\beta_2[1-(1+\gamma)C_3]\right]+$$

$$+\tau_в[1-C_3(1+\gamma)(\alpha_1C_1-\alpha_2C_2)]+(1-\alpha_1C_1+\alpha_2C_2)\left[(T-G)+\beta_4+\beta_3\right],$$

$$G=\frac{\alpha_1\lambda_4(1-C_1)+\xi T(\alpha_2C_2-\alpha_1C_1)-\alpha_2\lambda_3(1-C_2)}{\xi(1-\alpha_1C_1+\alpha_2C_2)},$$

$$C_1=e^{-\lambda_3T},\ C_2=e^{-\lambda_4T},\ C_3=e^{-\lambda_1\tau_{ктс}},$$

$$\alpha_1=\frac{\lambda_4}{\lambda_4-\lambda_3},\ \alpha_2=\frac{\lambda_3}{\lambda_4-\lambda_3},$$

$$\beta_1=\frac{1}{\lambda_1},\ \beta_2=\frac{1}{\lambda_2},\ \beta_3=\frac{3}{\lambda_5},\ \beta_4=\frac{1}{\lambda_6},\beta_5=\frac{1}{\lambda_3},\beta_6=\frac{1}{\lambda_4},$$

$$\gamma=\lambda_1\tau_{ктс},\ \xi=\lambda_3\lambda_4,\ \tau_в=\frac{4}{\mu}.$$

На рис. 3.6 згідно з (3.15) відображено залежність $K_{Г_{СІ}}(T_0,T_В)$ від середньої наробітки на відмову T_0 та середнього часу відновлення $T_В$ компонентів КЕІ [109]. Моделювання виконувалося для параметрів, які задавалися за умов, що $\lambda_4>\lambda_3$. Решта параметрів задавалася наступним чином: $T_0=1/\lambda_4$ та $T_В=4/\mu_3$, λ_2=1/100 год.$^{-1}$, λ_3 = 1/5000 год.$^{-1}$, λ_1=1/1000 год.$^{-1}$, λ_5=1/200 год.$^{-1}$; λ_6=1/1000 год.$^{-1}$.

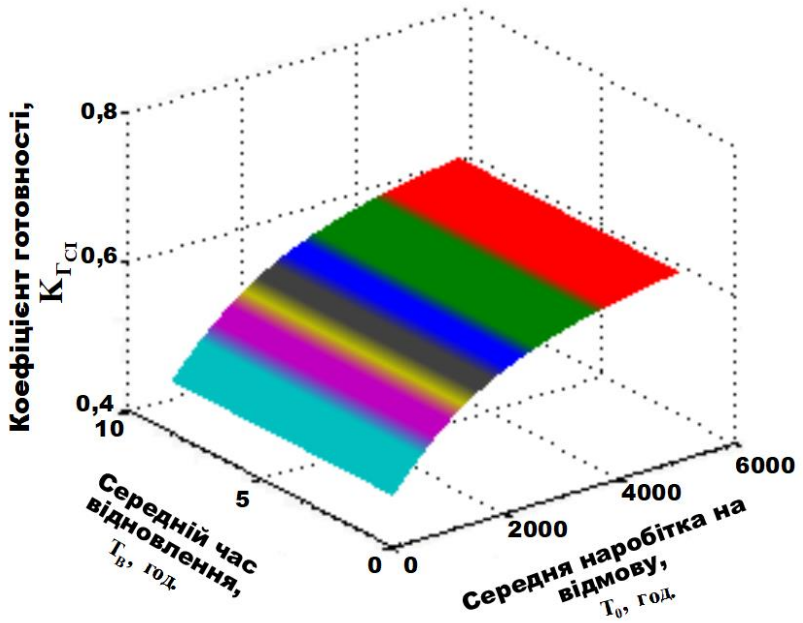


Рис. 3.6 Залежність КГ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що T=5000 год., $\tau_{КТС}=3$ хв.

На рис. 3.7–3.12 зображено графіки імовірнісних залежностей $P_k(T)$, де $k=\overline{1,6}$; для моделювання застосовувалися співвідношення (3.16)–(3.21) .

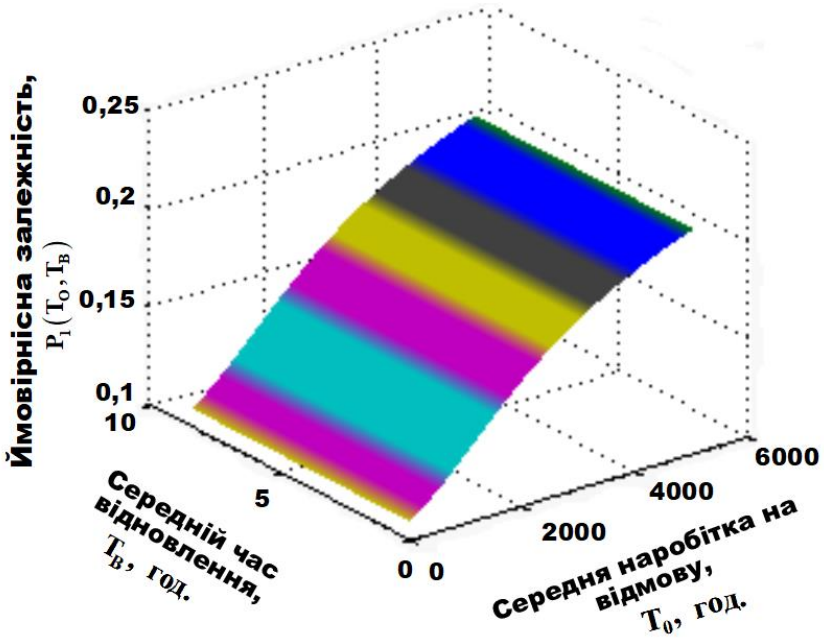


Рис. 3.7 Ймовірнісна залежність $P_1(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що T=5000 год., $\tau_{КТС}=3$ хв.

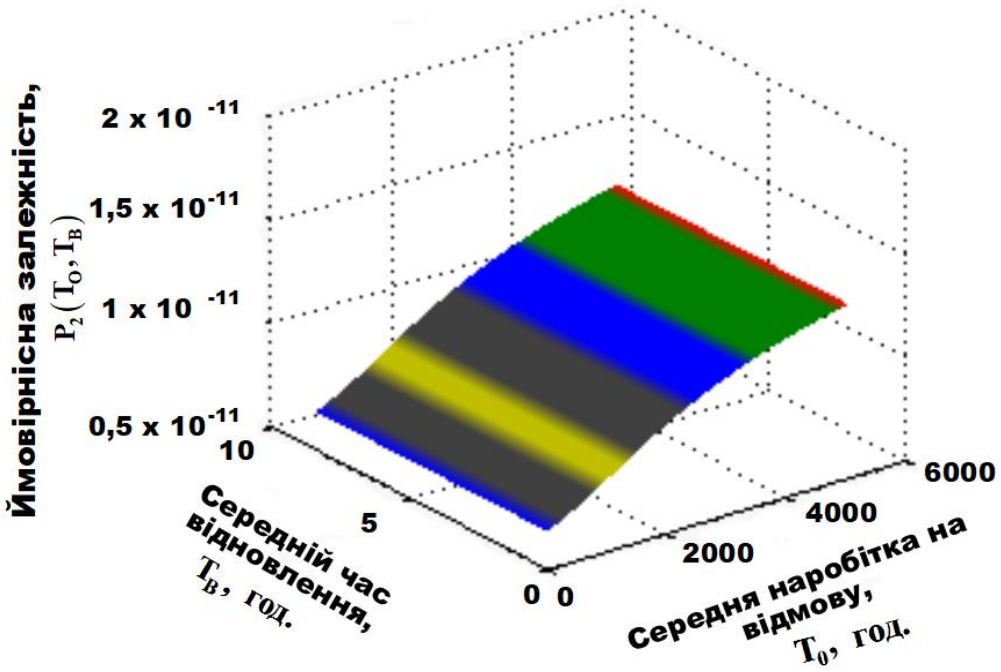


Рис. 3.8 Ймовірнісна залежність $P_2(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що T=5000 год., $\tau_{КТС}=3$ хв.

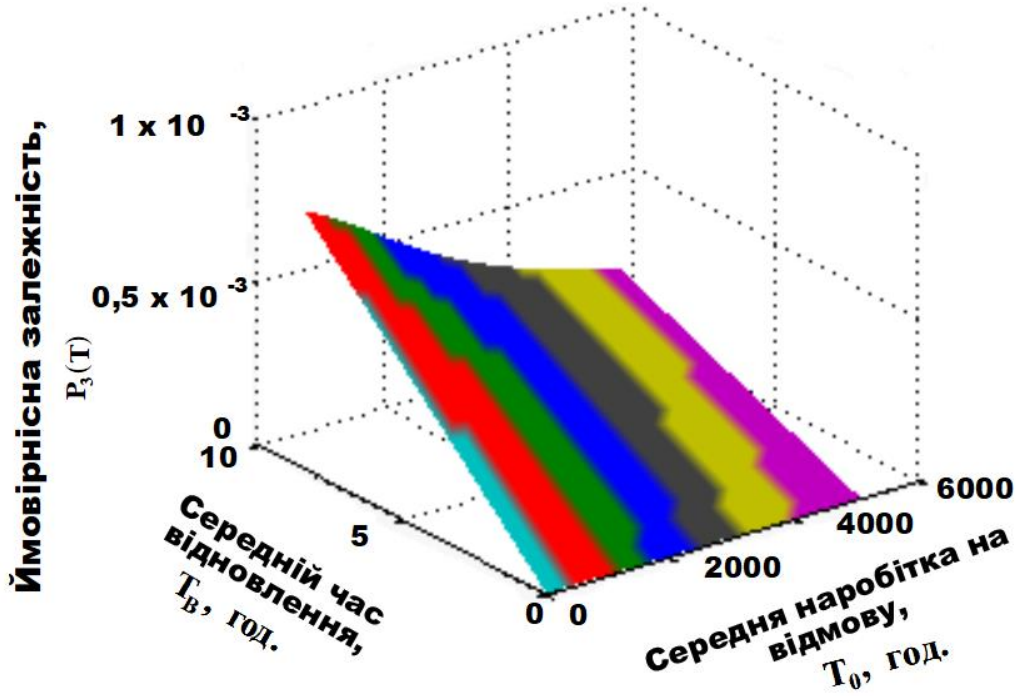


Рис. 3.9 Ймовірнісна залежність $P_3(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=5000 год., $\tau_{КТС} = 3$ хв.

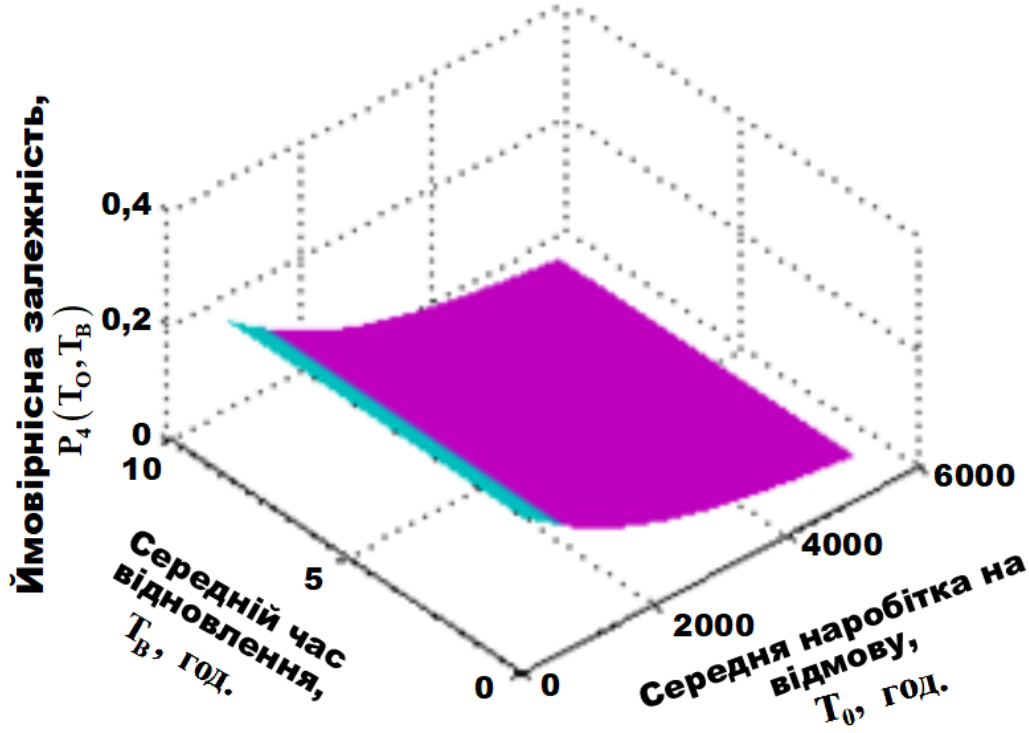


Рис. 3.10 Ймовірнісна залежність $P_4(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=5000 год., $\tau_{КТС} = 3$ хв.

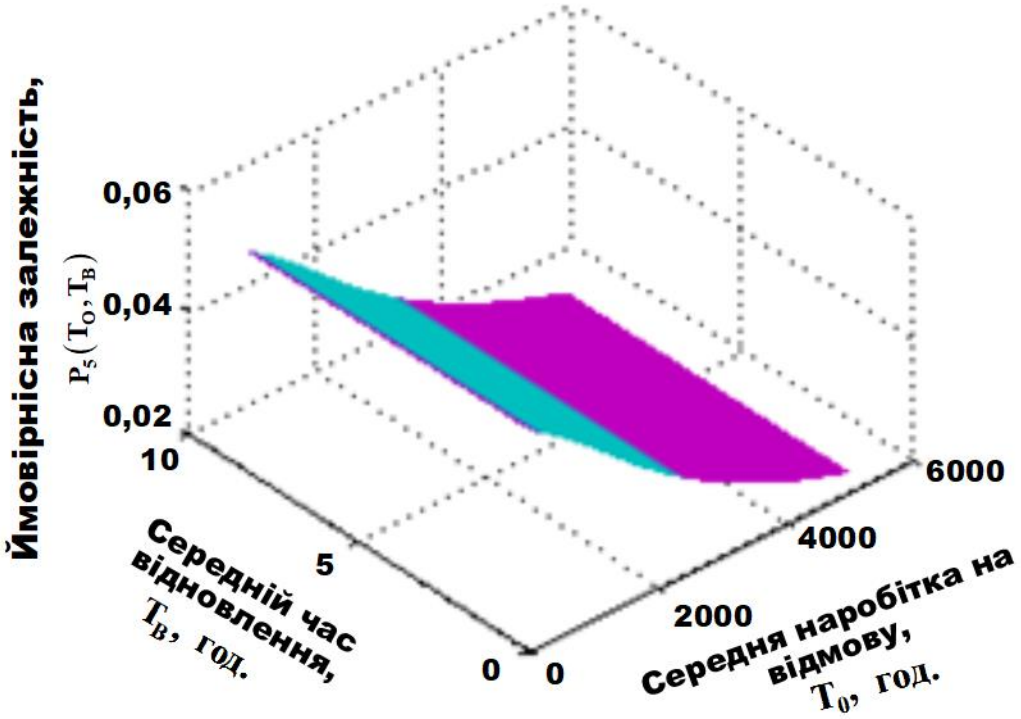


Рис. 3.11 Ймовірнісна залежність $P_5(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=5000 год., $\tau_{КТС} = 3$ хв.

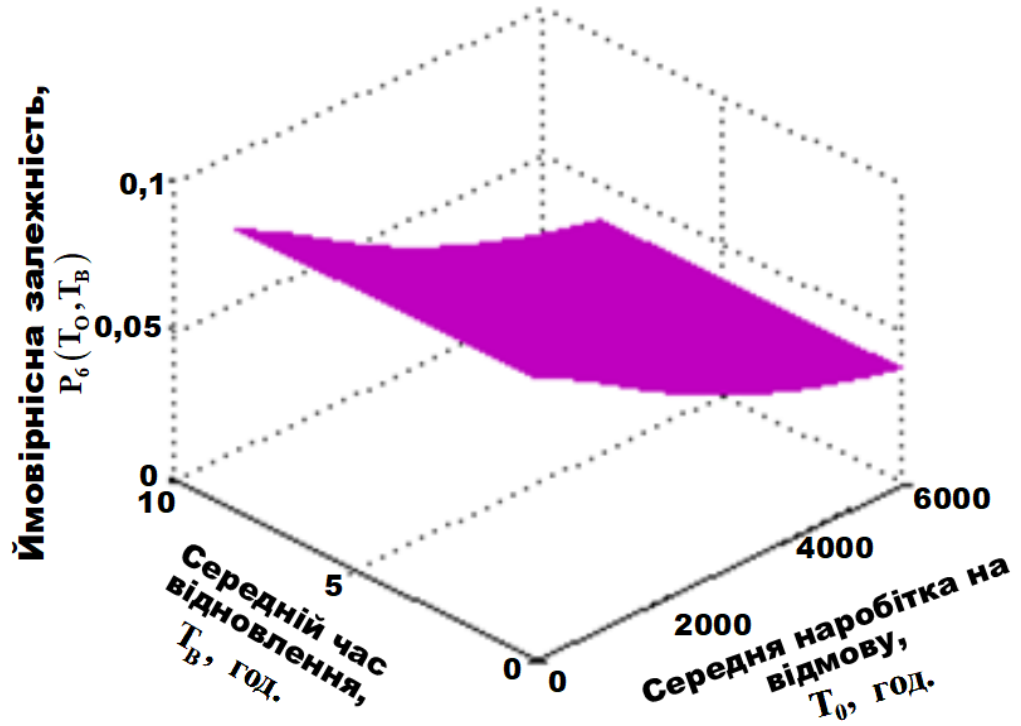


Рис. 3.12 Ймовірнісна залежність $P_6(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=5000 год., $\tau_{КТС} = 3$ хв.

Отримані результати моделювання (рис. 3.6–3.12) свідчать, що існуюча система моніторингу ІТС КЕІ не відповідає вимогам забезпечення необхідного рівня функційної та інформаційної безпечності інфраструктури ($K_{\Gamma_{CI_{max}}} \approx 0,62$). Для усунення цієї проблеми було запропоновано спільне використання систем ССВВ та ХМС. Застосування додаткових модулів системи синхронізованих векторних вимірювань та відповідних хмарних сервісів AWS надає можливість перетворити існуючу систему моніторингу інформаційно-технічних станів компонентів критичної енергетичної інфраструктури (рис. 3.5) (система А) в більш сучасну систему оперативного моніторингу.

Робота цих систем може бути описана за допомогою формальної граматики $L = \left\langle S_{L_i}, Q_{L_{ij}}(t), G_L, \Theta_L, R_{L_r} \right\rangle$, де S_{L_i} – множина станів S_i моделі системи L; $Q_{L_{ij}}(t)$ – множина функцій розподілу для напівмарковської моделі системи L для переходів $S_i \to S_j$; G_L – граф станів $G = (V, E)$ для НПММ системи L; Θ_L – показник цикломатичної складності НПММ системи L; R_{L_r} – множина r-ої кількості гілок напівмарковської моделі системи L. Для системи А перші дві нотації $S_{A_i}, Q_{A_{ij}}(t)$ відповідної граматики А доповнюються наступними чотирма нотаціями:

$$G_A = (7,9);\ \Theta_A = 4;\ R_{A_1} = S_0 \underset{\exists Q_{10}(t)}{\overset{\exists Q_{01}(t)}{\leftrightarrows}} S_1 \xrightarrow{\exists Q_{12}(t)} S_2 \xrightarrow{\exists Q_{23}(t)} S_3 \xrightarrow{\exists Q_{30}(t)} S_0;$$

$$R_{A_2} = S_0 \xrightarrow{\exists Q_{04}(t)} S_4 \xrightarrow{\neg\left(Q_{45}(t) \in \left|Q_{ij}(t)\right|\right)} S_5 \xrightarrow{\exists Q_{56}(t)} S_6 \xrightarrow{\exists Q_{63}(t)} S_3.$$

Третя напівмарковська модель описує роботу системи Б і є логічним продовженням другої моделі (рис. 3.5) для випадку вірогідного контролю інформаційно-технічних станів. Перші дві нотації $S_{Б_i}, Q_{Б_{ij}}(t)$ записуються у відповідності до графу станів, зображеному на рис. 3.13. Решта нотацій граматики Б записується у вигляді

$$G_Б = (5,7);\ \Theta_Б = 4;\ R_{Б_1} = S_0 \underset{\exists Q_{10}(t)}{\overset{\exists Q_{01}(t)}{\leftrightarrows}} S_1 \xrightarrow{\exists Q_{12}(t)} S_2 \xrightarrow{\exists Q_{20}(t)} S_0;$$

$$R_{Б_2} = S_0 \xrightarrow{\exists Q_{03}(t)} S_3 \xrightarrow{\neg\left(Q_{34}(t) \in \left|Q_{ij}(t)\right|\right)} S_4 \xrightarrow{\exists Q_{40}(t)} S_0 .$$

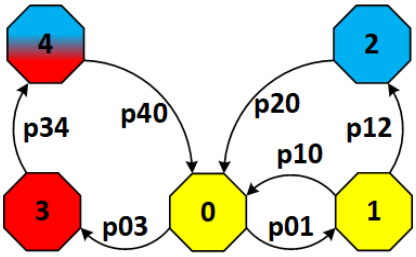


Рис. 3.13 Граф станів НПММ моніторингу інформаційно-технічних станів компонентів КЕІ з вірогідним КТС

Результати порівняльного аналізу системи моніторингу інформаційно-технічних станів критичної інфраструктури з вірогідним контролем (система Б) та існуючою системою моніторингу ІТС компонентів критичної інфраструктури з невірогідним КТС (система А) представлено в таблиці 3.1.

Таблиця 3.1

Результати порівняльного аналізу систем моніторингу інформаційно-технічних станів критичних інфраструктур

Середній час наробітки на відмову, год.	Коефіцієнт готовності		Виграш
	Система моніторингу ІТС КІ з невірогідним КТС (граматика А)	Система оперативного моніторингу ІТС КІ з вірогідним КТС (граматика Б)	
1000	0,4512	0,9862	0,535
2000	0,5234	0,9930	0,4696
3000	0,5617	0,9947	0,433
4000	0,5835	0,9952	0,4117
5000	0,5952	0,9963	0,4011
6000	0,6251	0,9975	0,3724

Отримані результати свідчать про безумовну перевагу системи Б над системою А. Виграш в значеннях коефіцієнта готовності складає понад 37%.

3.2.2 Напівмарковська модель протікання аварії критичної енергетичної інфраструктури

Відомо, що на готовність КЕІ при її застосуванні за призначенням впливає множина факторів, значна кількість яких в силу свого негативного характеру дії приводить до серйозних порушень функціональної безпеки інфраструктури. Внаслідок чого порушуються складні комплементарні зв'язки [114] між різними інфраструктурними компонентами, що може надавати руйнівний вплив на зовнішнє середовище та на економіку держави і створює серйозну загрозу життю людей.

Аналіз найбільш відомих аварій КЕІ [102] свідчить, що для більшості з них можна виділити наступні загальні ознаки:

1) зовнішні та внутрішні фактори негативного впливу;

2) поодинокі відключення ЛЕП;

3) помилки обслуговуючого персоналу (операторів) КЕІ;

4) вразливості ІКС КЕІ;

5) відключення системи підтримки прийняття рішень (СППР);

6) каскадні відключення ЛЕП;

7) повне відключення КЕІ.

На рис. 3.14 зображено структурно-логічну схему протікання аварії КЕІ, яка враховує зазначені етапи.

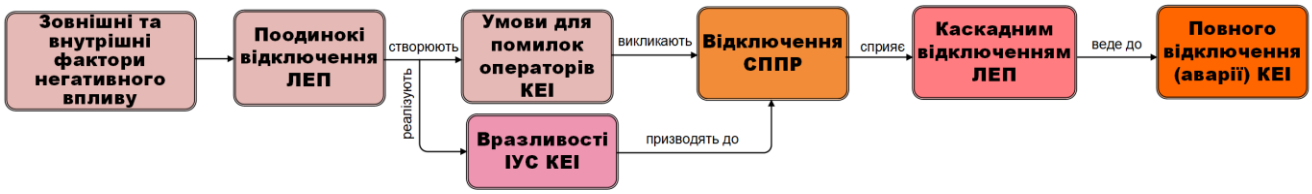


Рис. 3.14 Структурно-логічна схема протікання аварії КЕІ

Методологічні засади для побудови аналогічних моделей протікання аварій КЕІ на основі застосування марковських процесів розглянуто в [115, 116]. У той же час для моделювання складних зв'язків між компонентними складовими КЕІ,

які описуються різноманітними стохастичними залежностями, краще застосовувати апарат моделювання напівмарковських процесів [117, 118]. Для оцінного напівмарковського моделювання поведінки КЕІ під час протікання аварії застосовується система обмежень (2.6). Вважається також, що КЕІ представляє собою сукупність критично важливих об’єктів, до складу яких входять відповідні критичні системи (КС). Для спрощення формалізованого опису інформаційно-технічних станів КС та КЕІ застосовуються такі нотації: M_S^{CrEI} – множина ІТС КЕІ, в яких інфраструктура виконує основні функції за призначенням; M_S^{CrS} – множина ІТС критичних систем, які впливають на виконання основних функцій КЕІ за призначенням, $M_S^{CrS} \subset M_S^{CrEI}$; M_F^{CrEI}– множина відмов, несправностей КЕІ; M_R^{CrEI} – множина ІТС, в яких виконуються заходи по відновленню працездатності КЕІ; M_F^{CrS} – множина відмов (несправностей), вразливостей та порушень КС; M_R^{CrS} – множина ІТС, в яких виконуються заходи по відновленню працездатності КС, які впливають на виконання основних функцій КЕІ за призначенням.

Отже, за умови $\exists\, M_S^{CrS},\ M_S^{CrS} \subset M_S^{CrI}$ та $\exists\, M_F^{CrS},\ M_F^{CrI},\ M_R^{CrS},\ M_R^{CrI}$ існує відображення, яке записується у вигляді [119]

$$\Omega 1 : M_F^{CrEI} \Rightarrow M_R^{CrEI} \equiv H = \left\{ (x, y) \middle| x \in M_F^{CrEI} \wedge y \in M_R^{CrEI} \wedge \Omega 1(x) = y \right\}, \qquad (3.22)$$

$$\Omega 2 : M_F^{CrS} \Rightarrow M_R^{CrS} \equiv N = \left\{ (w, z) \middle| w \in M_F^{CrS} \wedge z \in M_R^{CrS} \wedge \Omega 2(w) = z \right\}. \qquad (3.23)$$

Нотації, які записуються за допомогою співвідношень (3.22), (3.23) слід розглядати як теоретико-множинну модель КЕІ, від якої доцільно перейти до оцінного моделювання.

У якості прикладу розглянемо напівмарковську модель аварії КЕІ міста Севастополя, яка відбулася в 2012 р. [102, 113]. Відомо, що до складу зазначеної КЕІ входили підстанція (місто Бахчисарай) та дві підключені до неї лінії електропередачі (основна і резервна). Для запропонованої моделі напівмарковський процес описується графом станів, який зображено на рис. 3.15. Відповідно до рис. 3.15 множина станів НПММ записується у вигляді

$\forall\ S_i \in S,\ S=\{S_0,S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8\} \exists\ G=(V,E)$, де S_0 – працездатний стан критичної енергетичної інфраструктури; S_1 – контроль інформаційно-технічного стану, в ході якого виникають раптові відмови основної лінії електропередачі; S_3 – контроль інформаційно-технічного стану, в ході якого виникають раптові відмови резервної лінії електропередачі; S_5 – контроль інформаційно-технічного стану, в ході якого виникають раптові відмови ПТС; S_2 – відновлення працездатного стану основної лінії електропередачі після раптової відмови; S_4 – відновлення працездатного стану резервної лінії електропередачі після раптової відмови; S_7 – стан прихованої відмови ПТС; S_8 – контроль інформаційно-технічного стану ПТС, яка знаходиться в стані прихованої відмови; S_6 – стан відновлення працездатного стану ПТС після раптової відмови, яка виявлена в ході проведення першого циклу контролю інформаційно-технічного стану, або після прихованої відмови, яка виявлена в ході проведення другого циклу контролю інформаційно-технічного стану.

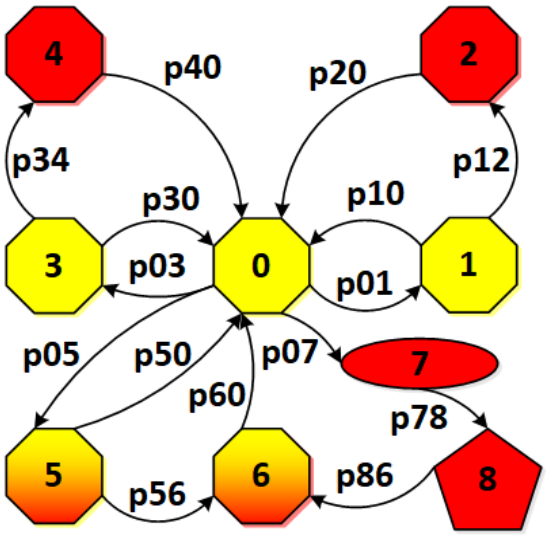


Рис. 3.15 Граф станів НПММ протікання аварії КЕІ міста Севастополя

Початкові стани відповідають значенням імовірностей $P_0(0)=1$, $P_i(0)=0$, де $i=\overline{1,8}$. Крім того, вважається, що з встановленою періодичністю, яка не є випадковою величиною і відповідає тривалості експлуатації $T \in [0,t]$ компонентів

критичної енергетичної інфраструктури, на протязі детермінованого інтервалу часу $\tau_{ктс}$ проводиться контроль їхнього інформаційно-технічного стану. Відповідно до моделюємої ситуації елементи матриці $\left|Q_{ij}(t)\right|$, які відповідають функціям розподілення часу для переходів $S_i \to S_j$, записуються у вигляді

$$Q_{12}(t) = 1 - e^{-\lambda_1 t}, \tag{3.24}$$

$$Q_{34}(t) = 1 - e^{-\lambda_2 t}, \tag{3.25}$$

$$Q_{56}(t) = 1 - e^{-\lambda_3 t}, \tag{3.26}$$

$$Q_{07}(t) = 1 - \frac{\lambda_5}{\lambda_5 - \lambda_4} e^{-\lambda_4 t} + \frac{\lambda_4}{\lambda_5 - \lambda_4} e^{-\lambda_5 t}, \tag{3.27}$$

$$Q_{20}(t) = 1 - (1 + \mu_1 t) e^{-\mu_1 t}, \tag{3.28}$$

$$Q_{40}(t) = 1 - (1 + \mu_2 t) e^{-\mu_2 t}, \tag{3.29}$$

$$Q_{60}(t) = 1 - \left(1 + \mu_3 t + \frac{(\mu_3 t)^2}{2} + \frac{(\mu_3 t)^3}{6}\right) e^{-\mu_3 t}. \tag{3.30}$$

Елементи матриці $\left|Q_{ij}(t)\right|$ для переходів $S_0 \to S_1$, $S_1 \to S_0$, $S_0 \to S_3$, $S_3 \to S_0$, $S_0 \to S_5$, $S_5 \to S_0$ та $S_8 \to S_6$ записуються аналогічно за допомогою формул (3.5), (3.6). Застосувавши граматику B, охарактеризуємо складність пропонуємої моделі, для якої перші дві нотації $S_{B_i}, Q_{B_{ij}}(t)$ доповнюються наступними шістьма нотаціями:

$$G_B = (9{,}15);\ \Theta_B = 8;\ R_{B_1} = S_0 \xleftrightarrow[\exists Q_{10}(t)]{\exists Q_{01}(t)} S_1 \xrightarrow{\exists Q_{12}(t)} S_2 \xrightarrow{\exists Q_{20}(t)} S_0;$$

$$R_{B_2} = S_0 \xleftrightarrow[\exists Q_{30}(t)]{\exists Q_{03}(t)} S_3 \xrightarrow{\exists Q_{34}(t)} S_4 \xrightarrow{\exists Q_{40}(t)} S_0;$$

$$R_{B_3} = S_0 \xleftrightarrow[\exists Q_{50}(t)]{\exists Q_{05}(t)} S_5 \xrightarrow{\exists Q_{56}(t)} S_6 \xrightarrow{\exists Q_{60}(t)} S_0;$$

$$R_{B_4} = S_0 \xrightarrow{\exists Q_{07}(t)} S_7 \xrightarrow{\neg\left(Q_{78}(t) \in \left|Q_{ij}(t)\right|\right)} S_8 \xrightarrow{\exists Q_{86}(t)} S_6 \xrightarrow{\exists Q_{60}(t)} S_0.$$

При обчисленні пропонуємої напівмарковської моделі (рис. 3.15) слід враховувати складність моделі, яка описується за допомогою граматики B. Крім

того, доцільно враховувати невизначеність, яка виникає при обчисленні деяких перехідних імовірностей p_{ij} для трьох напівмарковських моделей, які описуються граматиками А–В. В табл. 3.2 наведено результати порівняльного аналізу складності зазначених моделей. Згідно табл. 3.2 рівень складності моделей визначається невизначеністю трьох перехідних імовірностей p_{ij}.

Таблиця 3.2

Порівняльний аналіз складності напівмарковських моделей, які описуються граматиками А–В

Напівмарков-ська модель з граматикою	Нотації складності моделі	Перехідні імовірності p_{ij} з невизначеністю	Характеристика невизначеності перехідних імовірностей p_{ij}
А	$G_A = (7,9)$; $\Theta_A = 4$	p_{45}	Невизначеність виникає у зв'язку зі складністю знаходження відповідної величини $Q_{ij}(t)$, яка визначає перехід зі стану прихованої відмови в стан КТС, тому що прихована відмова виникає з деякою ймовірністю у випадковий момент часу, а закінчується завжди у невипадковий момент [111] початку контролю інформаційно-технічних станів компонен-тів КЕІ
Б	$G_Б = (5,7)$; $\Theta_Б = 4$	p_{34}	
В	$G_B = (9,15)$; $\Theta_B = 8$	p_{78}	

Застосувавши методику, яка викладена в [102,111], для розрахунку стаціонарного коефіцієнта готовності $K_{Г_{СЕІ}}$ та стаціонарних імовірностей $P_k(T)$,

де $k=\overline{1,8}$, отримаємо такі співвідношення:

$$K_{\Gamma_{CEI}}=P_0(T)=\frac{\alpha_1\beta_4(1-k_4)-\alpha_2\beta_5(1-k_5)}{A}, \tag{3.31}$$

$$P_1(T)=\frac{\beta_1 L(1-k_1)}{A}, \tag{3.32}$$

$$P_2(T)=\frac{\tau_{в_1} L(1-k_1)}{A}, \tag{3.33}$$

$$P_3(T)=\frac{\beta_2 L(1-P_2)}{A}, \tag{3.34}$$

$$P_4(T)=\frac{\tau_{в_2} L(1-k_2)}{A}, \tag{3.35}$$

$$P_5(T)=\frac{\beta_3 L(1-k_3)}{A}, \tag{3.36}$$

$$P_6(T)=\frac{\tau_{в_3}(1-2L-LP_3)}{A}, \tag{3.37}$$

$$P_7(T)=\frac{(1-3L)(T-G)}{A}, \tag{3.38}$$

$$P_8(T)=\frac{\tau_{ктс_3}(1-3L)}{A}, \tag{3.39}$$

де

$$A=\alpha_1\beta_4(1-k_4)-\alpha_2\beta_5(1-k_5)+L\left[(1-k_1)(\beta_1+\tau_{в_1})+(1-k_2)(\beta_2+\tau_{в_2})+(1-k_3)(\beta_3+\tau_{в_3})\right]+$$

$$+(1-3\alpha_1k_4+3\alpha_2k_5)\left[T+\tau_{ктс_3}+\tau_{в_3}-G\right],$$

$$G=\frac{\alpha_1\lambda_5(1-k_4)+3\xi T(\alpha_2k_5-\alpha_1k_4)-\alpha_2\lambda_4(1+k_5)}{\xi(1-3\alpha_1k_4+3\alpha_2k_5)},$$

$$\alpha_1=\frac{\lambda_5}{\lambda_5-\lambda_4},\ \alpha_2=\frac{\lambda_4}{\lambda_5-\lambda_4},\ \beta_1=\frac{1}{\lambda_1},\ \beta_2=\frac{1}{\lambda_2},\ \xi=\lambda_4\lambda_5,$$

$$\beta_3=\frac{1}{\lambda_3},\ \beta_4=\frac{1}{\lambda_4},\ \beta_5=\frac{1}{\lambda_5},\ T_O=\sum_{i=1}^{5}\beta_i,$$

$$\tau_{в_1}=\frac{2}{\mu_1},\ \tau_{в_2}=\frac{2}{\mu_2},\ \tau_{в_3}=\frac{4}{\mu_3},\ T_В=\tau_{в_1}+\tau_{в_2}+\tau_{в_3}$$

$$k_1 = e^{-\lambda_1 \tau_{ктс1}},\ k_2 = e^{-\lambda_2 \tau_{ктс2}}, k_3 = e^{-\lambda_3 \tau_{ктс3}},\ k_4 = e^{-\lambda_4 T},\ k_5 = e^{-\lambda_5 T},$$

$$L = \alpha_1 k_4 - \alpha_2 k_5.$$

На рис. 3.16 згідно з (3.31) відображено залежність $K_{\Gamma_{CEI}}(T_0, T_B)$ від середньої наробітки на відмову T_0 та середнього часу відновлення T_B компонентів критичної енергетичної інфраструктури. Моделювання виконувалося для параметрів, які задавалися за умов, що $\lambda_5 > \lambda_4$, $\mu_3 > \mu_1$, $\tau_{ктс1} = \tau_{ктс2} = \tau_{ктс3}$. Решта параметрів задавалася наступним чином: T=3000 год., $\lambda_1 = \lambda_2 = \lambda_3$=1/1000 год.$^{-1}$, λ_4=1/2000 год.$^{-1}$, $\mu_1 = \mu_2$=1/2 год.$^{-1}$.

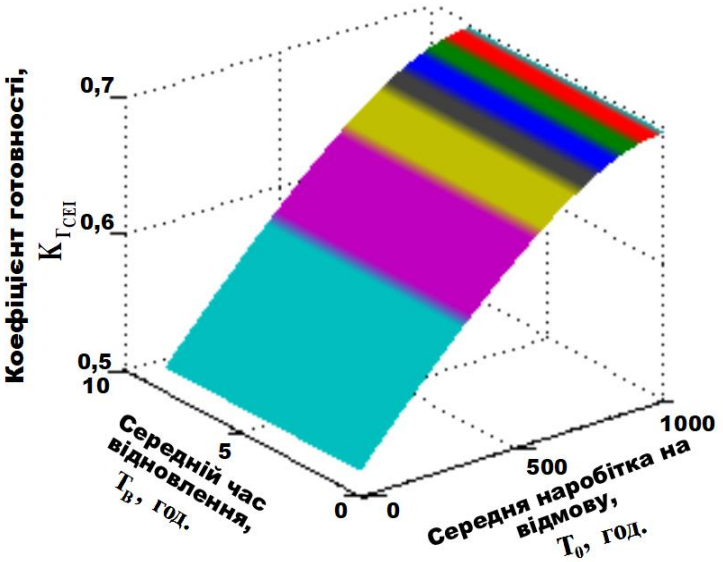


Рис. 3.16 Залежність КГ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що T=3000 год., $\tau_{КТС} = 3$ хв.

На рис. 3.17–3.24 зображено графіки імовірнісних залежностей $P_k(T)$, де $k = \overline{1,8}$; для моделювання застосовувалися співвідношення (3.32)–(3.39).

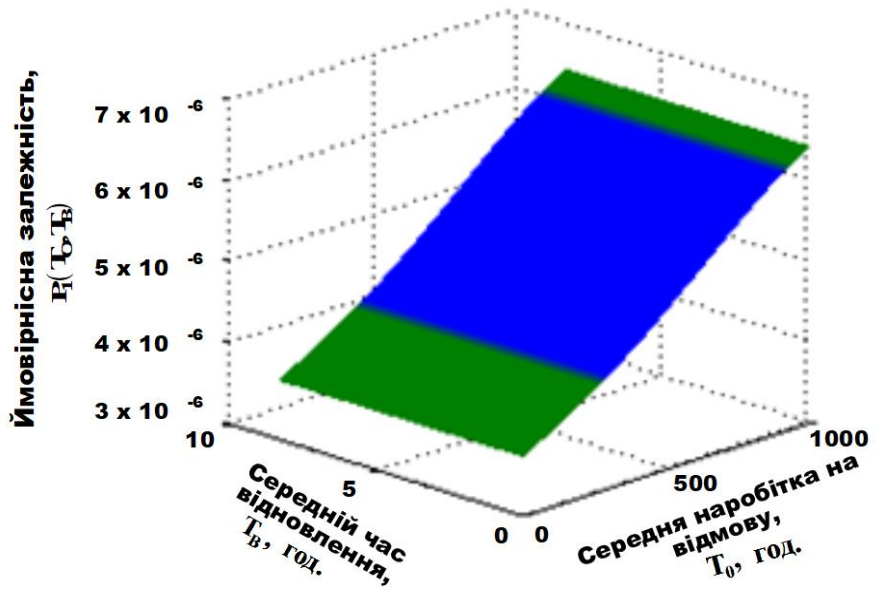


Рис. 3.17 Ймовірнісна залежність $P_1(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

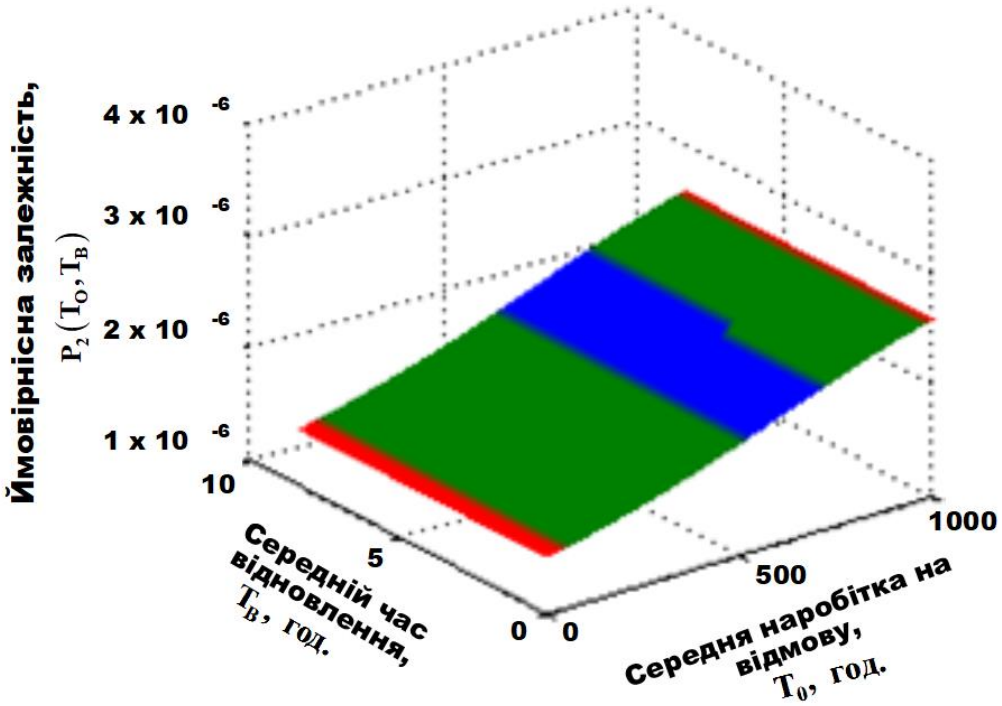


Рис. 3.18 Ймовірнісна залежність $P_2(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

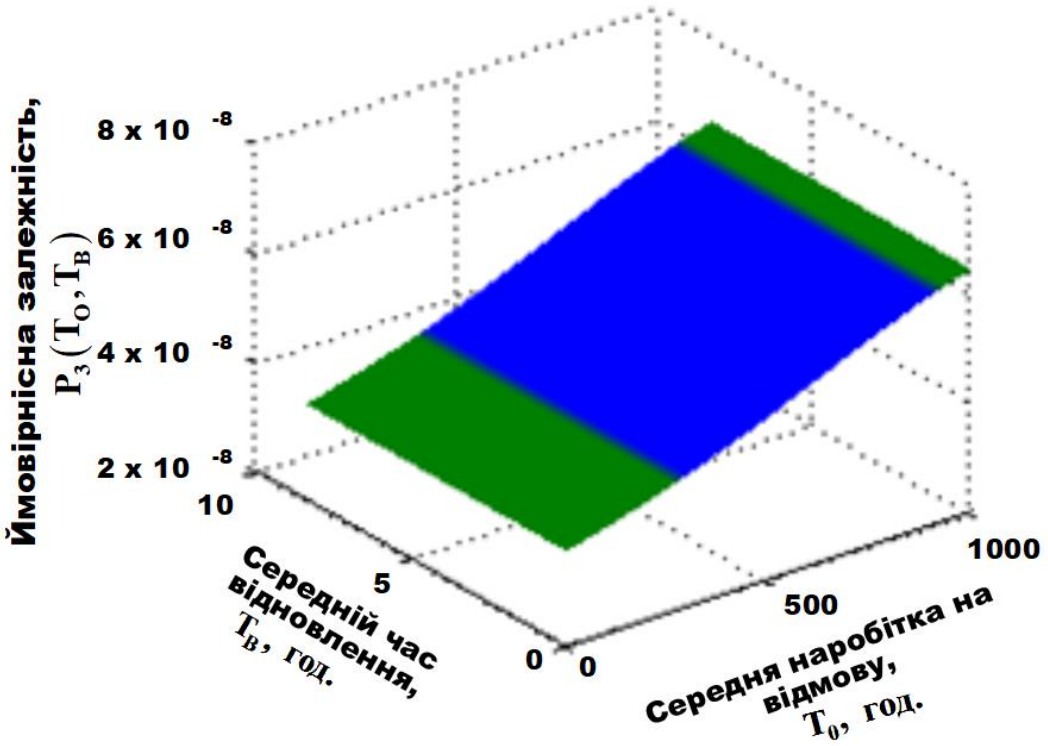


Рис. 3.19 Ймовірнісна залежність $P_3(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

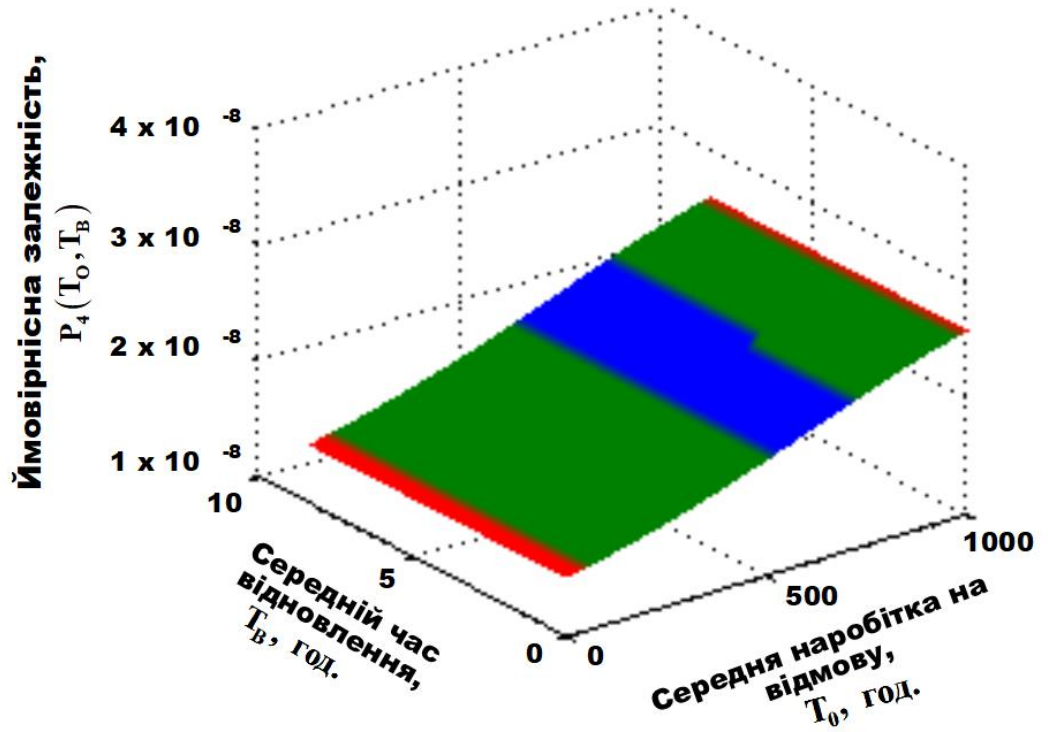


Рис. 3.20 Ймовірнісна залежність $P_4(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

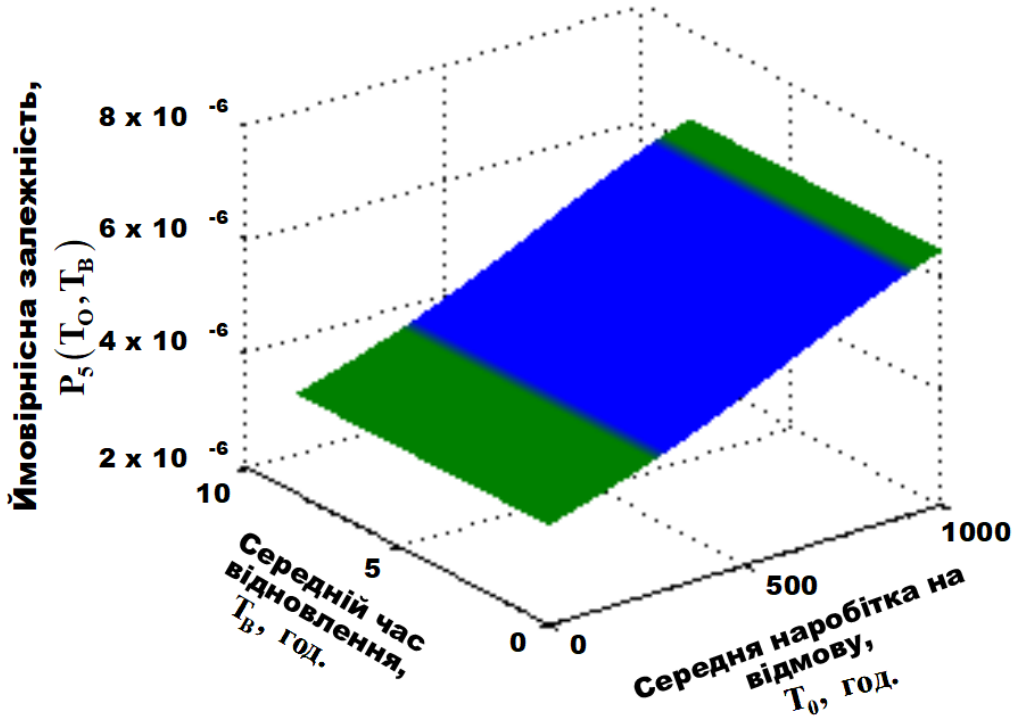


Рис. 3.21 Ймовірнісна залежність $P_5(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

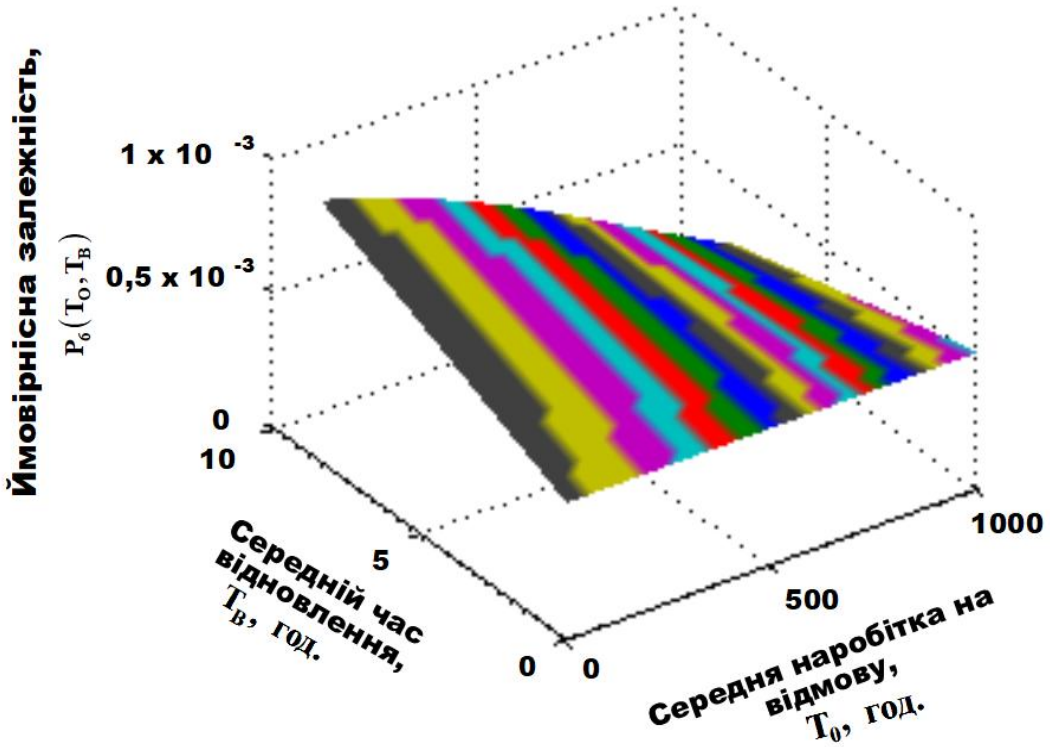


Рис. 3.22 Ймовірнісна залежність $P_6(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

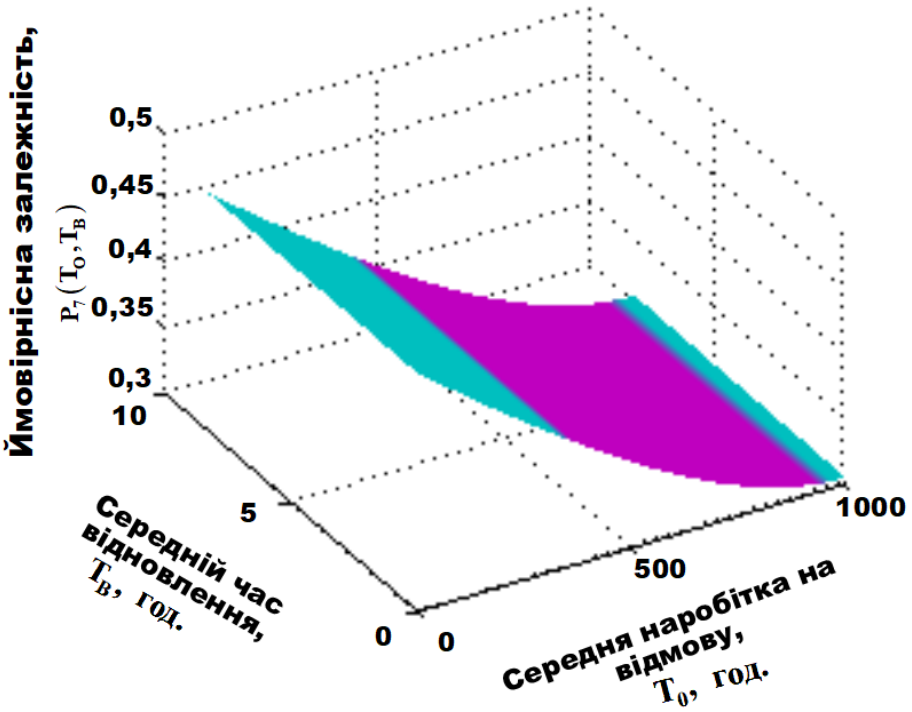


Рис. 3.23 Ймовірнісна залежність $P_7(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

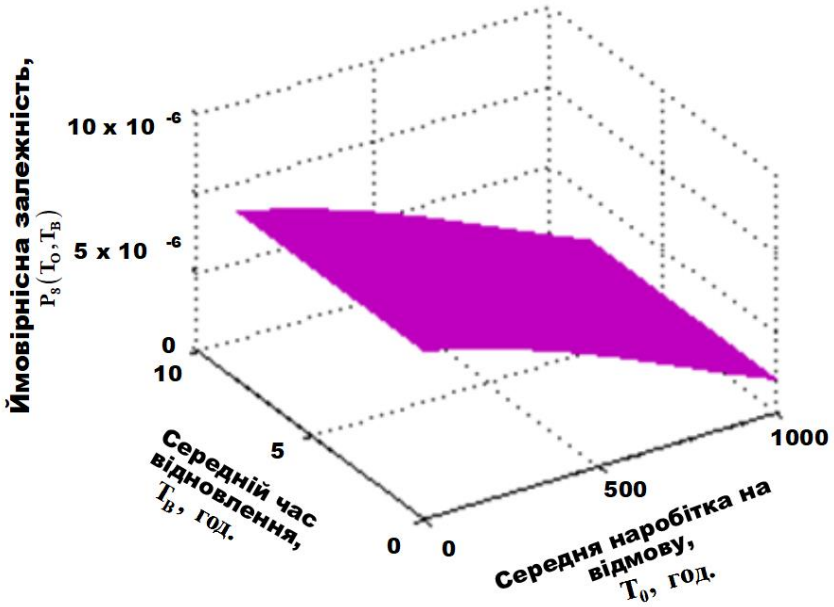


Рис. 3.24 Ймовірнісна залежність $P_8(T_0, T_B)$ компонентів КЕІ від середньої наробітки на відмову та середнього часу відновлення за умови, що Т=3000 год., $\tau_{КТС} = 3$ хв.

Результати моделювання (рис. 3.16) свідчать, що для приведеного прикладу аварії КЕІ, коефіцієнт готовності інфраструктури складає $K_{Г_{СЕІ}} = 0,535,...,0,695$. Отримані значення коефіцієнта готовності (рис. 3.4, 3.6, 3.16) свідчать про низьку

ефективність застосування за призначенням типової системи моніторингу КЕІ та нездатність при її використанні забезпечити функційну безпечність компонентів інфраструктури. Ці обставини підтверджують необхідність використання ССВВ та хмарних систем з метою підвищення готовності і функційної безпечності критичної енергетичної інфраструктури за рахунок проведення оперативного моніторингу інформаційно-технічних станів компонентів інфраструктури.

3.3 Метод напівмарковскього моделювання готовності хмарної інфраструктури

Згідно з концепцією та методологією наукових досліджень (рис. 2.1) вважається, що застосування ХМС і створення відповідних хмарних активів дозволить покращити функціональність та інформативність оперативного моніторингу ІТС компонентів критичних інфраструктур. Розглянемо яким чином виконується моделювання поведінки та оцінювання готовності хмарної інфраструктури, до складу якої входять ХМС, що розгортаються у вигляді фізичних і віртуальних машин.

3.3.1 Постановка завдання оцінювання готовності хмарної інфраструктури на основі напівмарковського моделювання

Застосовуючи результати аналізу хмарних інфраструктур (розділи 1, 2), виконаєм постановку завдання щодо оцінювання рівня готовності хмарної інфраструктури, яка складається з певної кількості ХМС, що розгортаються у вигляді фізичних та віртуальних машин. Не прив’язуючись до конкретної хмарної реалізації, припустимо, що ХМІ включає до свого складу сукупність фізичних машин, засобів контролю і управління, різне мережеве обладнання. На базі ФМ, що входять до складу хмарного інформаційного центру, розгортаються засоби віртуалізації (або віртуальні машини), що складаються з певної кількості центральних процесорів, оперативних запам’ятовуючих пристроїв і дискових пристроїв для зберігання інформації [120]. Крім того, вважається, що згідно з принципом реконфігурування (рис. 2.3), ФМ та ВМ об’єднуються в підсистеми, що працюють в гарячому, теплому та холодному режимах. Представлена модель в

кортежній формі записується у вигляді співвідношення (2.1), складовими якого є

$$M^{Hot} = M_{PM}^{Hot} \cup M_{VM}^{Hot},\ M^{Warm} = M_{PM}^{Warm} \cup M_{VM}^{Warm},\ M^{Cold} = M_{PM}^{Cold} \cup M_{VM}^{Cold}, \quad (3.40)$$

$$x^{Hot} = x_{PM}^{Hot} \cup x_{VM}^{Hot},\ x^{Warm} = x_{PM}^{Warm} \cup x_{VM}^{Warm},\ x^{Cold} = x_{PM}^{Cold} \cup x_{VM}^{Cold}, \quad (3.41)$$

де $M_{PM}^{Hot} = \bigcup_{i=1}^{n} M_{PM_i}^{Hot}$ – множина ФМ гарячої підсистеми хмарної інфраструктури; $M_{VM}^{Hot} = \bigcup_{i=1}^{m} M_{VM_i}^{Hot}$ – множина ВМ гарячої підсистеми хмарної інфраструктури; $M_{PM}^{Warm} = \bigcup_{i=1}^{n} M_{PM_i}^{Warm}$ – множина ФМ теплої підсистеми хмарної інфраструктури; $M_{VM}^{Warm} = \bigcup_{i=1}^{m} M_{VM_i}^{Warm}$ – множина ВМ теплої підсистеми хмарної інфраструктури; $M_{PM}^{Cold} = \bigcup_{i=1}^{n} M_{PM_i}^{Cold}$ – множина ФМ холодної підсистеми хмарної інфраструктури; $M_{VM}^{Cold} = \bigcup_{i=1}^{m} M_{VM_i}^{Cold}$ – множина ВМ холодної підсистеми хмарної інфраструктури;

Тоді, виходячи з зазначеного, для конкретної хмарної інфраструктури, яка задається у вигляді кортежу (2.1), (3.40), (3.41), шляхом застосування методу напівмарковського моделювання можна виконати оцінювання готовності ХМІ відповідно до наступної системи вимог і обмежень:

$$\Im = \begin{cases} K_{\Gamma_{IaaS\ Cloud}}(T) \geq K_{\Gamma_0}; \\ C_{min_0} \leq C_0 \leq C_{max_0}; \\ n_h \geq 1,\ n_w \geq 1,\ n_c \geq 1; \end{cases} \quad (3.42)$$

де K_{Γ_0} – гранично припустиме значення стаціонарного коефіцієнта готовності хмарної інфраструктури; T – загальний час застосування ХМІ за призначенням; n_h – кількість ФМ та ВМ гарячої підсистеми; n_w – кількість ФМ та ВМ теплої підсистеми; n_c – кількість ФМ та ВМ холодної підсистеми; $C_0 \in \left[C_{min_0}; C_{max_0}\right]$ – граничні витрати на підтримання необхідного рівня готовності хмарної інфраструктури.

Отже, використовуючи представлену кортежну модель (2.1), (3.40), (3.41), у відповідності з критерієм (3.42) необхідно розв’язати задачу первинного аналітико-стохастичного оцінювання та подальшого забезпечення рівня готовності хмарної інфраструктури.

3.3.2 Етапи методу оцінювання готовності хмарної інфраструктури на основі напівмарковського моделювання

Розглянемо яким чином виконується моделювання поведінки та оцінка готовності хмарної інфраструктури, до складу якої входять ХМС, що розгортаються у вигляді ФМ і ВМ. Для розв’язування завдання у відповідності з критерієм (3.34) застосуємо окремий метод.

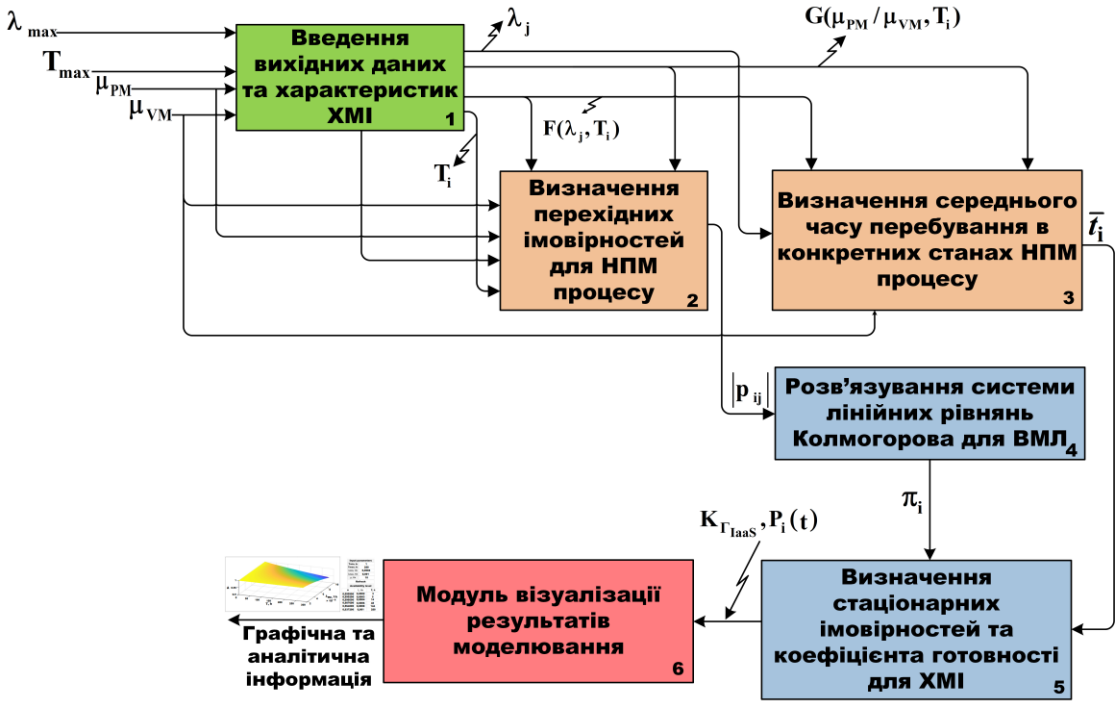


Рис. 3.25 Функціональна діаграма методу оцінювання готовності хмарної інфраструктури за результатами напівмарковського моделювання

Після аналізу відомих методів перевагу було надано методу напівмарковського моделювання на основі використання вкладених марковських ланцюгів (ВМЛ), який включає наступні кроки:

1) аналіз класифікаційної схеми забезпечення готовності хмарної інфраструктури з декількома підсистемами фізичних і віртуальних машин;

2) аналіз властивостей, основних характеристик, режимів функціонування хмарної інфраструктури та можливих зловмисних шкідливих проникнень в контур управління ХМІ, які впливають на ефективність її застосування за призначенням;

3) формалізоване визначення, характеристика основних станів та побудова відповідної моделі готовності хмарної інфраструктури;

4) оцінка готовності хмарної інфраструктури у відповідності з функціональною діаграмою (рис. 3.25) методу оцінювання готовності хмарної інфраструктури на основі напівмарковського моделювання.

3.4 Напівмарковські моделі хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин

Важлива роль в забезпеченні готовності хмарної інфраструктури відводиться моніторингу інформаційно-технічних станів ХМС, які розвертаються у вигляді декількох підсистем фізичних та віртуальних машин. Тому, керуючись основними положеннями методології наукових досліджень, розглянемо яким чином будуються та обчислюються напівмарковські моделі хмарної інфраструктури, до складу якої входить інтегрована система моніторингу ІТС фізичних і віртуальних машин.

3.4.1 Особливості архітектурної побудови хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин

Впродовж процесу розроблення моделей відповідно до запропонованого методу (рис. 3.25) було враховано можливості щодо створення сучасної інтегрованої системи моніторингу інформаційно-технічних станів ХМС [74] на основі розгортання мереж мікросервісів і віртуальних моніторів. Розширення моніторингових функцій на основі застосування сервісів та потужних інформаційно-обчислювальних ресурсів відомого хмарного провайдера AWS створює чудові умови щодо реалізації достовірного контроля інформаційно-технічних станів критичних інфраструктур. На рис. 3.26 зображена спрощена

структурна схема ХМІ з трьома підсистема ФМ та ВМ і інтегрованою системою моніторингу їхніх інформаційно-технічних станів. Відповідно до рис. 3.26 та згідно з принципом реконфігурування і комбінованої надлишковості сервіс-орієнтованих ресурсів хмарних систем критичних інфраструктур (рис. 2.3) за допомогою інтегрованої системи моніторингу здійснюється контроль ІТС й технічне діагностування компонентів інфраструктури.

Вважається, що згідно [121] за допомогою використання інтегрованої системи моніторингу (рис. 3.26) в разі необхідності розв'язується завдання щодо міграції ресурсів ФМ та ВМ; також вважається, що управління готовністю КІ за їхнім інформаційно-технічним станом може здійснюватися за результатами моніторингу ІТС інфраструктурних компонентів.

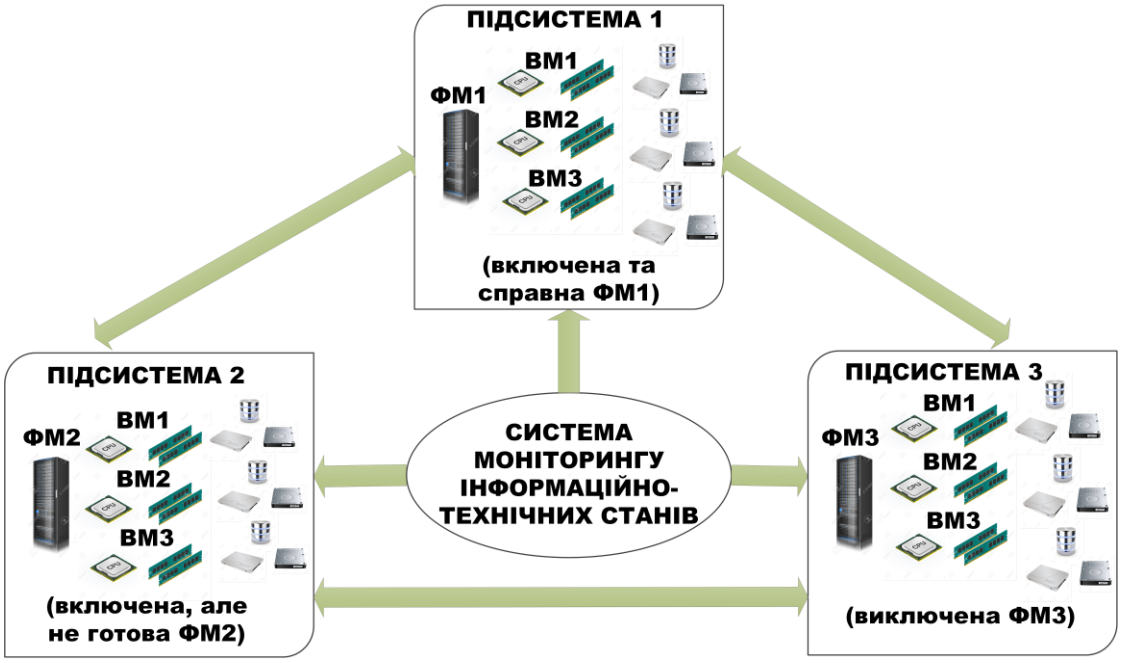


Рис. 3.26 Спрощена структурна схема ХМІ з трьома підсистема ФМ та ВМ і інтегрованою системою моніторингу ІТС

Розглянемо роль та місце інтегрованої системи моніторингу в розв'язуванні завдань щодо оцінки рівня готовності хмарної інфраструктури за результатами напівмарковського моделювання поведінки відповідних ХМС.

3.4.2 Напівмарковська модель готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних машин

У якості ключової розглянемо НПММ готовності хмарної інфраструктури з трьома ФМ та інтегрованою системою моніторингу їхніх інформаційно-технічних станів [32]. Будемо вважати, що наявність сучасних мікросервісів AWS надає можливість проводити вірогідний КТС фізичних машин хмарної інфраструктури, включаючи міграцію їхніх ресурсів. Фактично НПММ, яка пропонується до розгляду, містить три підсистеми по одній фізичній машині, тобто $n_h = n_w = n_c = 1$. По відношенню до фізичних машин ХМІ діють такі припущення: а) ФМ гарячої підсистеми в початковий момент часу $t = 0$ знаходяться у включеному стані і виконують завдання застосування за призначенням; б) ФМ теплої підсистеми в момент часу $t = 0$ включені та знаходяться в режимі очікування застосування за призначенням; в) ФМ холодної підсистеми розглядаються як абсолютно надійні і в момент часу $t = 0$ знаходяться у виключеному стані. Граф станів моделі зображено на рис. 3.27.

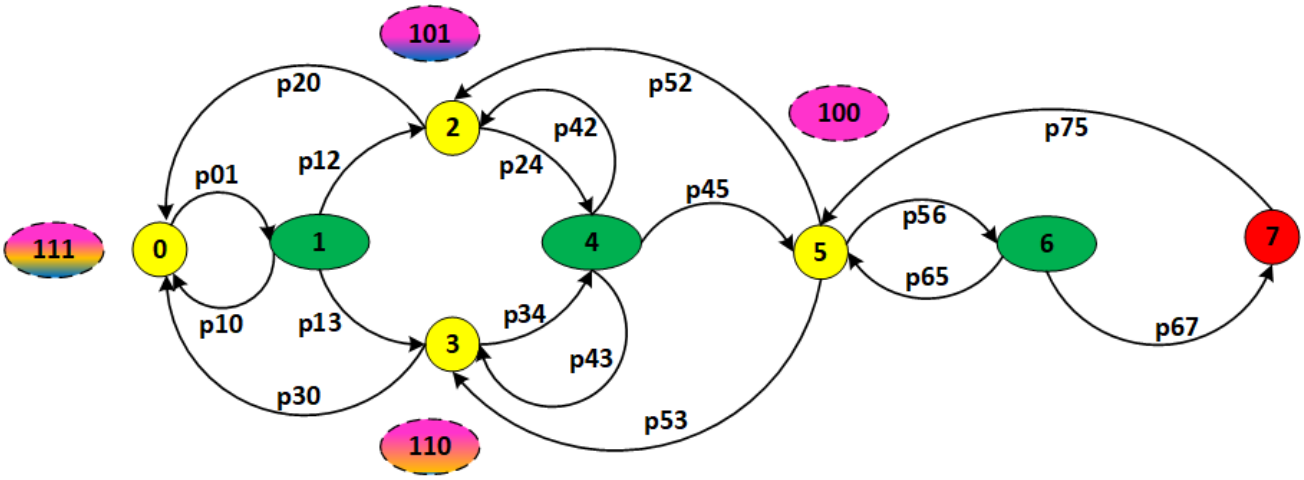


Рис. 3.27 Граф станів ключової НПММ готовності ХМІ з трьома ФМ та інтегрованою системою моніторингу інформаційно-технічних станів

Відповідно до рис. 3.27 множина станів НПММ записується у вигляді $\forall\, S_i \in S,\ S = \{S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7\} \exists\, G = (V_1, E_1)$, де S_0 – працездатний стан ХМІ; S_1, S_4, S_6 – КТС, в ході якого виникають раптові відмови ФМ; S_2 – стан міграції ресурсу, коли здійснюється заміна гарячої ФМ в стані відмови на працездатну теплу фізичну машину або відновлення ПРС (далі, скорочено

пояснюється як відповідна заміна); S_3 – стан міграції ресурсу, коли здійснюється заміна гарячої ФМ на холодну; S_5 – стан міграції ресурсу, коли здійснюється заміна теплої ФМ на холодну; S_7 – непрацездатний стан ХМІ, тобто всі ФМ відмовили або не відповідають ресурсним вимогам.

Початкові стани відповідають значенням імовірностей $P_0(0)=1$, $P_i(0)=0$, де $i=\overline{1,7}$. Крім того, вважається, що з встановленою періодичністю, яка не є випадковою величиною і відповідає тривалості експлуатації $T\in[0,t]$ фізичних машин ХМІ, на протязі детермінованого інтервалу часу $\tau_{ктс}$ проводиться контроль їхнього інформаційно-технічного стану. Ситуація, яка моделюється, описується за допомогою матриці $\left|Q_{ij}(t)\right|$. Елементи матриці відповідають функціям розподілення часу для переходів $S_i \to S_j$ і записуються у вигляді

$$Q_{12}(t)=Q_{13}(t)=Q_{45}(t)=Q_{67}(t)=1-e^{-\gamma t}, \tag{3.43}$$

$$Q_{20}(t)=Q_{30}(t)=Q_{75}(t)=1-(1+\mu_1 t)e^{-\mu_1 t}, \tag{3.44}$$

$$Q_{52}(t)=Q_{53}(t)=1-(1+\mu_2 t)e^{-\mu_2 t}, \tag{3.45}$$

де γ – інтенсивність раптових відмов фізичних машин; μ_1 – інтенсивність міграції теплої та холодної фізичних машин в гарячу підсистему і відновлення працездатності холодної ФМ хмарної інфраструктури; μ_2 – інтенсивність міграції холодної ФМ в теплу підсистему хмарної інфраструктури.

Елементи матриці $\left|Q_{ij}(t)\right|$ для переходів $S_0 \to S_1$, $S_2 \to S_4$, $S_3 \to S_4$, $S_5 \to S_6$ та $S_1 \to S_0$, $S_4 \to S_2$, $S_4 \to S_3$, $S_6 \to S_5$ записуються аналогічно за допомогою формул (3.5), (3.6). Основні нотації граматики Г для аналізу складності пропонуємої моделі записуються так:

$$G_\Gamma=(8,17);\ \Theta_\Gamma=11;\ R_{\Gamma_1}=S_0 \underset{\exists Q_{10}(t)}{\overset{\exists Q_{01}(t)}{\longleftrightarrow}} S_1 \xrightarrow{\exists Q_{12}(t)} S_2 \xrightarrow{\exists Q_{20}(t)} S_0;$$

$$R_{\Gamma_2}=S_0 \underset{\exists Q_{10}(t)}{\overset{\exists Q_{01}(t)}{\longleftrightarrow}} S_1 \xrightarrow{\exists Q_{13}(t)} S_3 \xrightarrow{\exists Q_{30}(t)} S_0;$$

$$R_{\Gamma_3}=S_2 \underset{\exists Q_{42}(t)}{\overset{\exists Q_{24}(t)}{\longleftrightarrow}} S_4 \xrightarrow{\exists Q_{45}(t)} S_5 \xrightarrow{\exists Q_{52}(t)} S_2;$$

$$R_{\Gamma_4} = S_3 \xleftarrow[\exists Q_{43}(t)]{\exists Q_{34}(t)} S_4 \xrightarrow{\exists Q_{45}(t)} S_5 \xrightarrow{\exists Q_{53}(t)} S_3;$$

$$R_{\Gamma_5} = S_5 \xleftarrow[\exists Q_{65}(t)]{\exists Q_{56}(t)} S_6 \xrightarrow{\exists Q_{67}(t)} S_7 \xrightarrow{\exists Q_{75}(t)} S_5.$$

Виконавши нетривіальні розрахунки, отримаємо співвідношення для визначення величини стаціонарного коефіцієнта готовності $K_{\Gamma_1}(t)$ та відповідних імовірностей $\pi_i(t)$ ХМІ з інтегрованою системою моніторингу інформаційно-технічних станів фізичних машин, де $i = \overline{0,7}$, у вигляді

$$K_{\Gamma_1}(t) = \pi_0(t) + \pi_2(t) + \pi_3(t) + \pi_5(t), \tag{3.46}$$

$$\pi_0(t) = P_0 \frac{\overline{t_0}}{U}, \qquad \pi_2(t) = P_2 \frac{\overline{t_2}}{U}, \qquad \pi_3(t) = P_3 \frac{\overline{t_3}}{U}, \tag{3.47}$$

$$\pi_5(t) = P_5 \frac{\overline{t_5}}{U}, \qquad U = \sum_{i=0}^{7} P_i \overline{t_i}. \tag{3.48}$$

Співвідношення для визначення складових, які входять у вирази (3.46)–(3.48), надано в додатку В.

На рис. 3.28 зображено графік залежності $K_{\Gamma_1}(T)$, який отримано з використанням співвідношень (3.46)–(3.48).

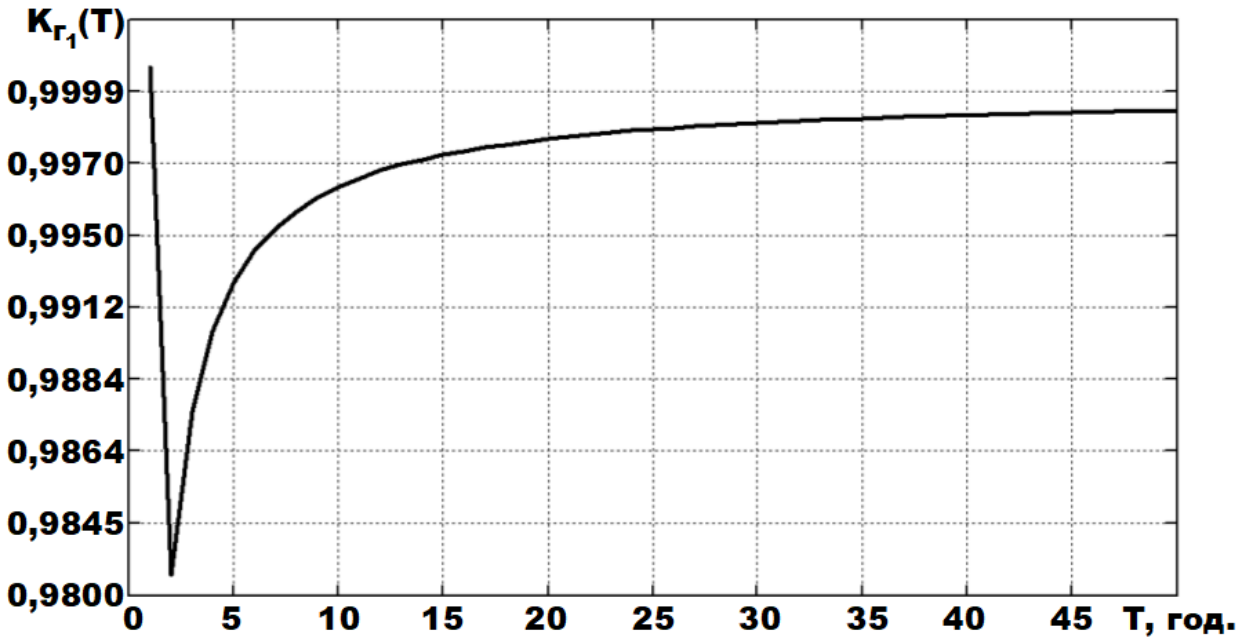


Рис. 3.28 Залежність $K_{\Gamma_1}(T)$ для $T = 500$ год., $\gamma = 0,002$ 1/год., $\mu = 5$ 1/год.

Отримані результати моделювання (рис. 3.14) свідчать про досить високий рівень готовності ХМІ, що є підставою для побудови більш складних архітектурних рішень на основі використання запропонованої ключової НПММ (рис. 3.27). Наприклад, на рис. 3.29 зображено граф станів для перспективної НПММ готовності ХМІ, до складу якої входять три підсистеми з дев'ятьма фізичними машинами, тобто $n_h = n_w = n_c = 3$. Аналогічна модель готовності ХМІ тільки для випадку, коли $n_h = n_w = n_c = 2$ представлена в [122].

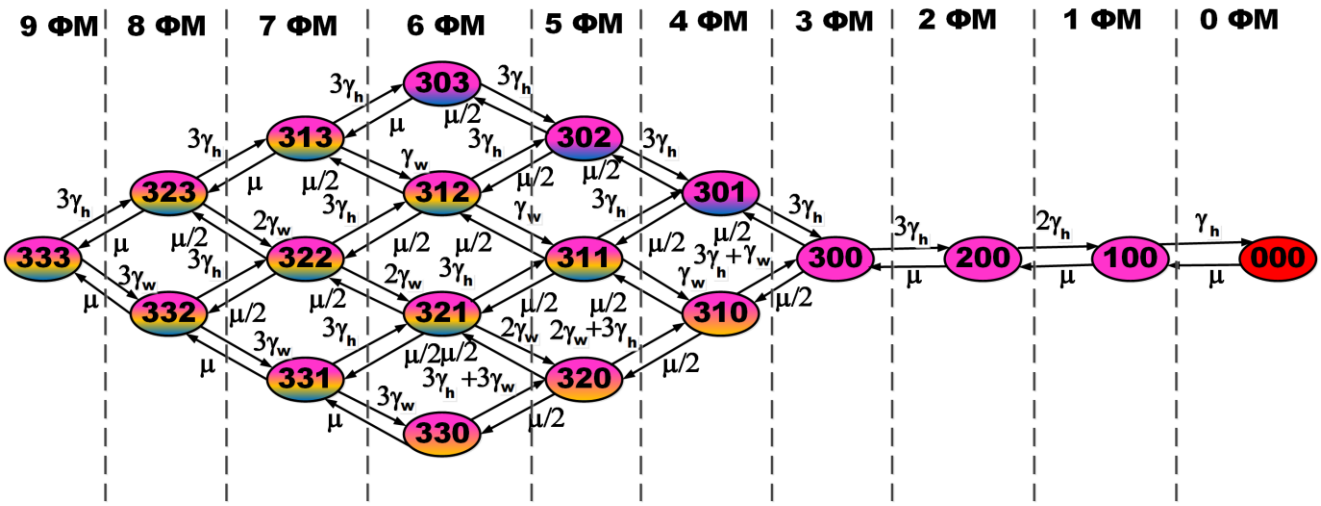


Рис. 3.29 Граф станів НПММ готовності ХМІ з дев'ятьма ФМ

Для представленої перспективної моделі готовності ХМІ (рис. 3.29) прийняті такі припущення: а) в початковий момент часу $t = 0$ всі дев'ять ФМ знаходяться в ПРС стані; б) за допомогою інтегрованої системи моніторингу здійснюється вірогідний КТС теплої та гарячої підсистем ФМ; 3) ФМ холодної підсистеми розглядаються як абсолютно надійні та в початковий момент часу знаходяться у вимкненому стані; 4) ФМ теплої підсистеми ввімкнені та знаходяться в режимі очікування застосування за призначенням; 5) при відмові ФМ гарячої підсистеми фізичні машини теплої та холодної підсистем з попередньо визначеною інтенсивністю (вважається, що дорівнюється значенню інтенсивності відмов фізичних машин гарячої підсистеми) замінюють фізичні машини, що відмовили; 6) у випадку відмови ФМ теплої підсистеми вони замінюються (з інтенсивністю відмов машин теплої підсистеми) на физичні

машини холодної підсистеми, які знаходяться в ПРС стані; 7) ФМ теплої та холодної підсистем після відновлення прцездатності фізичних машин гарячої підсистеми, які відмовили, повертаються (з інтенсивністю відновлення ФМ гарячої або теплої підсистем) в початкові стани.

Тоді, за умови дії системи вимог і обмежень (3.34) коефіцієнт готовності ХМІ можна визначити за допомогою співвідношення

$$K_{\Gamma_2}(t) = 1 - P_{0,0,0}(t), \tag{3.49}$$

де $P_{0,0,0}(t)$ – ймовірність події, яка полягає в тому, що в ХМІ не залишиллося жодної працездатної ФМ, тобто інфраструктура непрацездатна.

Безумовно НПММ готовності хмарної інфраструктури, граф станів якої представлено на рис. 3.29, є дуже складною, а її розв'язування потребує значних витрат часу та обчислювальних ресурсів. Тому обчислення моделі та отримання кількісних результатів моделювання розглядається як перспектива для подальших наукових досліджень.

Певну зацікавленість викликає моделювання негативних подій, які виникають внаслідок дії зловмисних шкідливих впливів. Наприклад, коли виникають приховані відмови ФМ. На рис. 3.30 зображено граф станів НПММ готовності ХМІ з трьома ФМ та інтегрованою системою моніторингу для випадку прихованих відмов.

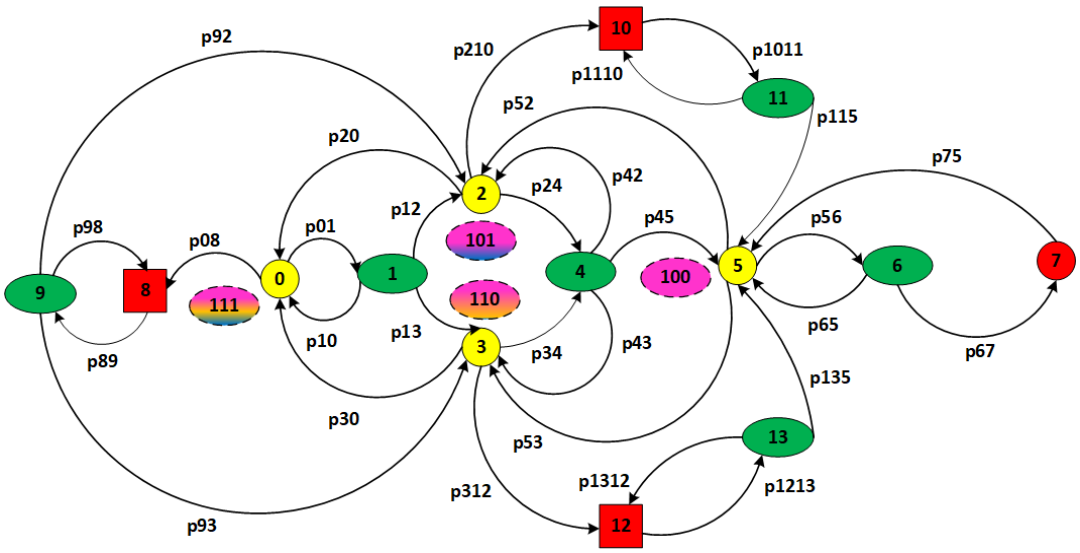
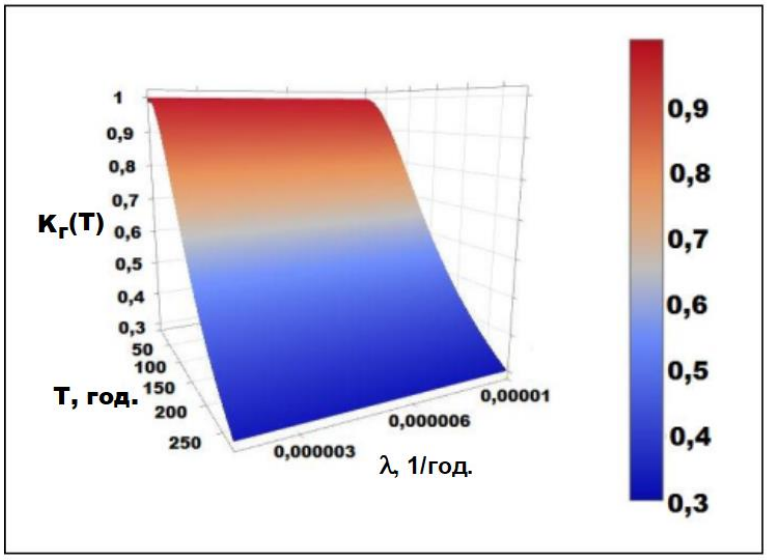


Рис. 3.30 Граф станів ключової НПММ готовності ХМІ з трьома ФМ та інтегрованою системою моніторингу для випадку прихованих відмов

На відміну від попередньої моделі граф станів НПММ, який представлено на (рис. 3.30), включає стани прихованих відмов S_8, S_{10}, S_{12} та стани додаткових циклів контролю інформаційно-технічних станів S_9, S_{11}, S_{13}. Коефіцієнт готовності ХМІ розраховується за допомогою співвідношення [74]

$$K_{\Gamma_3}(t) = \pi_0 + \pi_2 + \pi_3 + \pi_5. \qquad (3.50)$$

У виразі (3.50) стаціонарні імовірності π_0, π_2, π_3, π_5 визначаються, відповідно, як імовірності перебування ХМІ в працездатних станах S_0, S_2, S_3, S_5. Результати кількісних розрахунків представлено на рис. 3.31, 3.32.

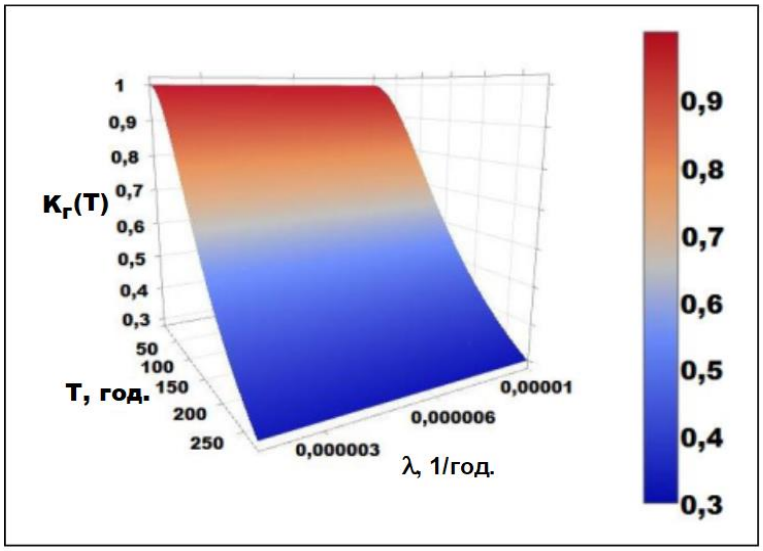


Вхідні параметри	
Tmin, год.:	1
Tmax, год.:	280
λmin, 1/год.	0,000005
λmax, 1/год.	0,00001
μ, 1/год.	8

Рівень готовності

$K_г(T)$	λ, 1/год.	T, год.
0,999901	0,000005	2
0,997204	0,000006	10
0,988526	0,000007	20
0,974270	0,000008	30
0,943517	0,000009	45
0,903494	0,00001	60

Рис/ 3.31 Залежність $K_{\Gamma_3}(T)$ для $T = 250$ год., $\mu = 8$ 1/год.



Вхідні параметри	
Tmin, год.:	1
Tmax, год.:	280
λmin, 1/год.	0,000005
λmax, 1/год.	0,00001
μ, 1/год.	10

Рівень готовності

$K_г(T)$	λ, 1/год.	T, год.
0,999917	0,000005	2
0,997208	0,000006	10
0,988531	0,000007	20
0,974273	0,000008	30
0,943519	0,000009	45
0,903498	0,00001	60

Рис. 3.32 Залежність $K_{\Gamma_3}(T)$ для $T = 250$ год., $\mu = 10$ 1/год.

Найбільш складною є перспективна модель ХМІ, яка побудована на основі попередньої НПММ для $n_h = n_w = n_c = 3$ (рис. 3.29) за умови дії зловмисних шкідливих впливів, що призводять до прихованих відмов. Граф станів для пропонуємої моделі (рис. 3.33) будується з урахуванням дії всієї сукупності негативних факторів по аналогії з графом станів для НПММ, який зображено на рис. 3.30.

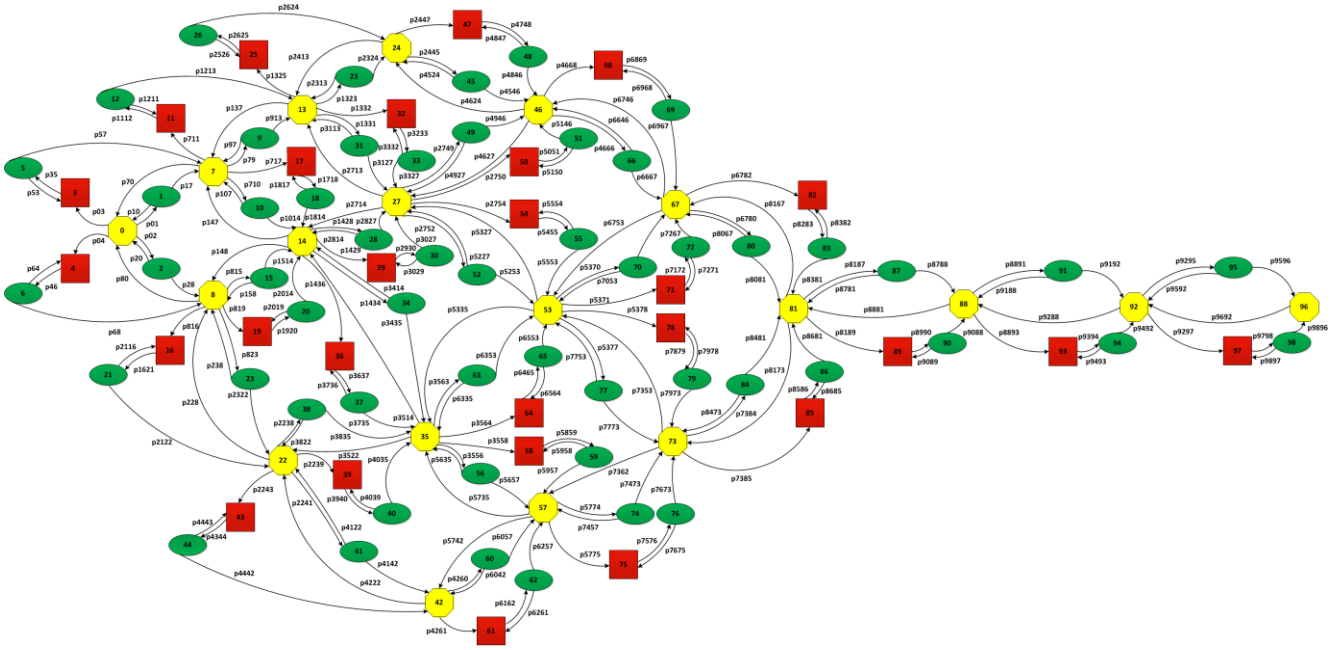


Рис. 3.33 Граф станів НПММ готовності ХМІ з дев’ятьма ФМ для випадку, коли діють зловмисні шкідливі впливи, що призводять до прихованих відмов

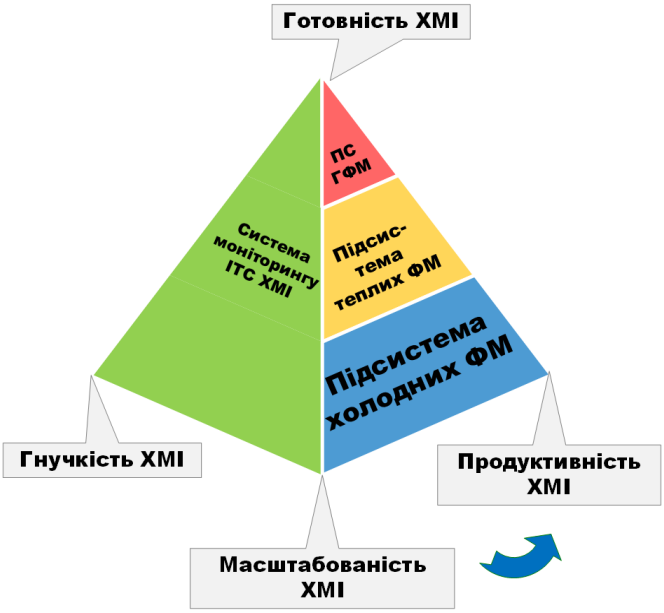
Отримані результати моделювання підтверджують, що запропоновані НПММ (рис. 3.27, 3.30) адекватно відображають ситуацію, коли внаслідок дії зловмисних шкідливих впливів виникають приховані відмови фізичних машин і суттєво знижується рівень готовності хмарної інфраструктури. Порівняльний аналіз свідчить, що у цьому випадку нижнє значення коефіцієнта готовності ХМІ зменшується з 0,98 (рис. 3.28) до майже 0,9 (рис. 3.31, 3.32).

3.4.3 Особливості масштабованого використання віртуального ресурсу хмарної інфраструктури з декількома підсистемами фізичних машин

Масштабоване використання віртуального ресурсу ХМІ реалізується згідно з класифікаційною схемою метамоделі забезпечення готовності інфраструктури,

яка описана в [123] і зображена на рис. 3.34. В буквальному сенсі властивість масштабованості означає, що хмарний провайдер надає користувачам стільки сервіс-орієнтованих віртуальних ресурсів відповідно до договору SLA про надаваємі послуги, скільки їм потрібно. Це завдання хмарний провайдер водночас розв'язує, забезпечуючи виконання вимог SLA по гнучкості управління, енергоспоживанню та надійності ХМІ (рис. 3.34).

а)



б)

Рис. 3.34 Класифікаційна схема метамоделі забезпечення готовності ХМІ з урахуванням вимог: а) масштабованості та надійності; б) енергоспоживання і гнучкості управління

Як видно з рис. 3.34 метамодель має форму піраміди, сторони якої відображені у вигляді окремих положень концепції забезпечення готовності ХМІ. Одне з найважливіших місць концепції займає положення по масштабованому наданню розподілених віртуальних ресурсів, що реалізується за рахунок своєчасного підключення (відключення) додаткових ФМ, на базі яких розвертається певна кількість ВМ, створюючи таким чином відповідний обчислювальний ресурс. Важлива роль також відводиться системі моніторингу ІТС ХМІ, за допомогою якої здійснюється КТС, діагностування та технічне (профілактичне) обслуговування компонентних складових інфраструктури.

3.4.4 Напівмарковська модель готовності хмарної інфраструктури з декількома підсистемами фізичних та віртуальних машин

З урахуванням особливостей надання масштабованих віртуальних ресурсів розглянемо яким чином можна оцінювати готовність хмарної інфраструктури, до складу якої входить три підсистеми ФМ та ВМ. На рис. 3.35 зображено класифікаційну схему зловмисних шкідливих впливів на готовність хмарної інфраструктури. Відповідно до рис. 3.35 оцінювання готовності ХМІ здійснюється на основі аналізу об’єктивних і суб’єктивних факторів впливу на фізичні та віртуальні машини, які можуть привести до наступних негативних подій:

1) деградація та неможливість застосування за призначенням накопичувачів даних;

2) відмова та відключення хмарного сховища;

3) відключення хмарного ресурсу під впливом агресивних дій зовнішнього середовища;

4) відключення інфраструктури внаслідок помилок обслуговуючого персоналу (застосування помилкового коду);

5) випадкові відключення серверів;

6) кібератаки, які викликають перевищення пропускної спроможності вхідних інформаційних каналів (DDoS) та застосування зловмисного ПЗ.

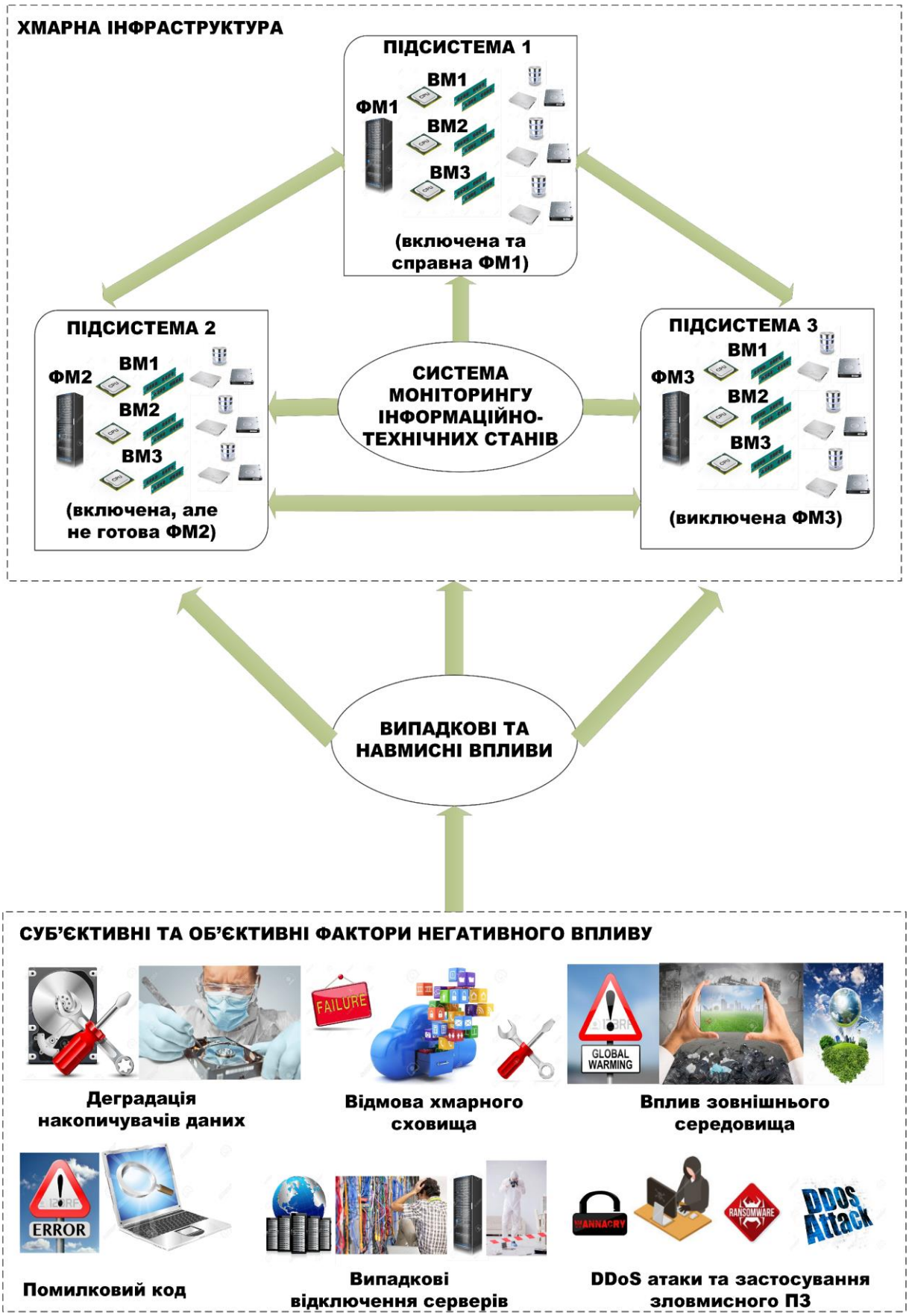


Рис. 3.35 Класифікаційна схема ЗВШВ на готовність ХМІ, до складу якої входять три підсистеми фізичних та віртуальних машин

Результати аналізу свідчать, що наслідки дії ЗВШВ (рис. 3.35) можуть проявлятися у вигляді раптових та прихованих відмов. Виходячи з зазначеного, процес оцінювання готовності ХМІ пропонується реалізувати як напівмарковський. У якості теоретичного базису пропонується розглянути НПММ готовності ХМІ з трьома підсистема фізичних та віртуальних машин для випадку їхніх раптових відмов, що виявляються за допомогою миттєвого контролю інформаційно-технічних станів ФМ і ВМ [76]. Хмарна інфраструктура вважається непрацездатною, а її ресурс недоступним, коли відмовляють всі три ФМ, на основі яких розвертаються ВМ. У той же час фізична машина зі складу інфраструктури вважається працездатною до тих пір поки є працездатною хоча б одна віртуальна машина, яка розвернута на базі розглядаємої ФМ. На рис. 3.36 зображено граф станів цієї моделі.

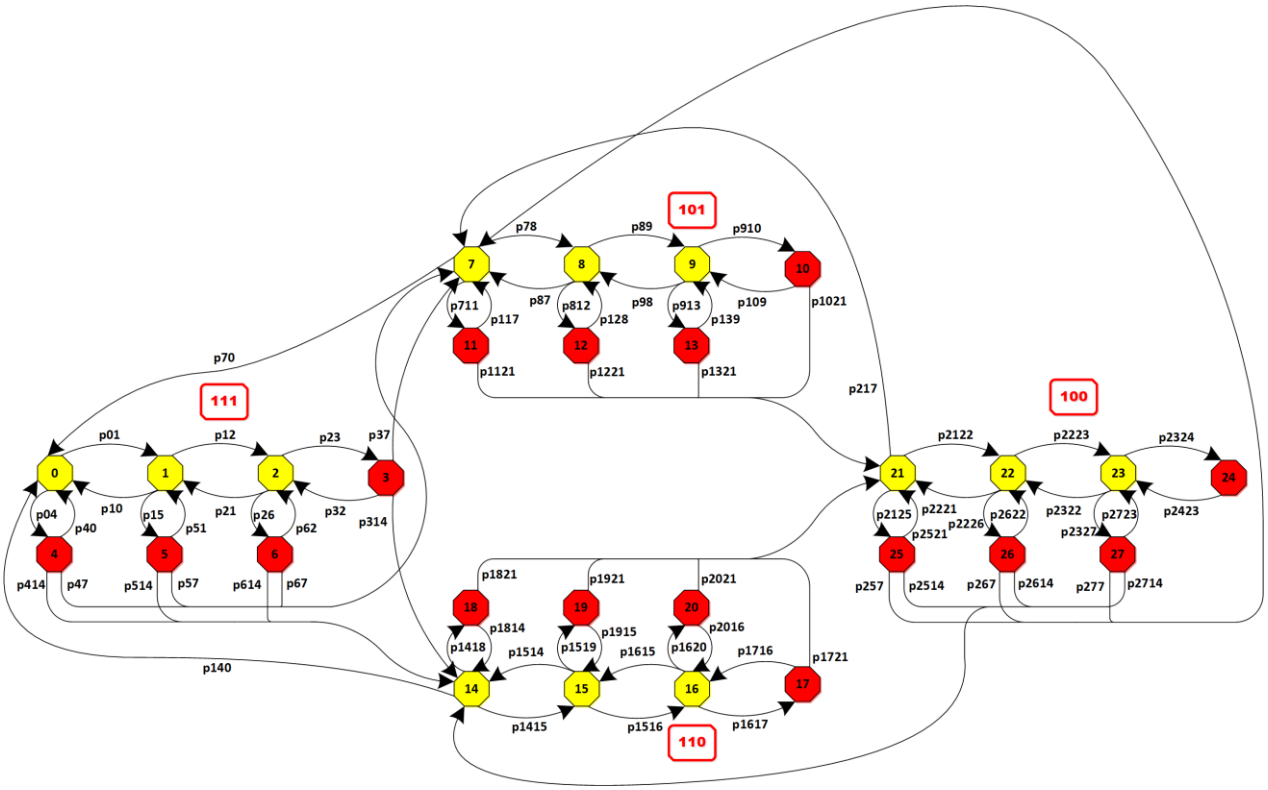


Рис. 3.36 Граф станів НПММ готовності ХМІ з трьома підсистемами фізичних та віртуальних машин і миттєвим КТС

Згідно приведеного графу станів напівмарковської моделі (рис. 3.36) готовності хмарної інфраструктури для множини працездатних станів ФМ та ВМ

можна записати наступні нотації: $\forall\ S_i \in S,\ S = \{S_0, S_1, ..., S_{27}\} \exists\ G_Д = (28, 67)$, $\Theta_Д = 41$, $S_{PM}^{VP} = \{S_0, S_1, S_2, S_7, S_8, S_9, S_{14}, S_{15}, S_{16}, S_{21}, S_{22}, S_{23}\}$, $S_{PM}^{VM} \subset S$. На цьому ж графі (рис. 3.36) червоним кольором позначається множина непрацездатних станів фізичних та віртуальних машин хмарної інфраструктури, тобто $S_{PM}^{VP*} = \{S_3, S_4, S_5, S_6, S_{10}, S_{11}, S_{12}, S_{13}, S_{17}, S_{18}, S_{19}, S_{20}, S_{24}, S_{25}, S_{26}, S_{27}\}$, $S_{PM}^{VP*} \subset S$. Отже, $S = S_{PM}^{VM} \cup S_{PM}^{VP*}$. Крім того, для побудови адекватної НПММ слід взяти до уваги наступні припущення: а) у разі відмови ФМ або ВМ виконується міграція ресурсу з теплої або холодної підсистем; б) якщо тепла та холодна підсистеми порожні, то ФМ, яка відмовила, ремонтується з метою відновлення ПРС [124]; в) час перебування ФМ та ВМ в працездатних станах S_i перед переходом в непрацездатні стани S_j розподілений за експоненціальним законом з функцією розподілення $Q_{ij}(t) = 1 - e^{-\lambda_i t}$, де λ_i – інтенсивність відмов ФМ та ВМ; г) час перебування ФМ або ВМ в непрацездатних станах S_j (тобто в станах ремонту, міграції) перед переходом в працездатні стани S_j розподілений за законом Ерланга другого порядку [111, 125] з функцією розподілення $Q_{ji}(t) = 1 - (1 + \mu_j t)e^{-\mu_j t}$, де μ_j – інтенсивність відновлення ПРС стану (тобто ремонту, міграції) ФМ або ВМ.

Враховуючи стаціонарний режим перебування ФМ, ВМ ХМІ в відповідних станах та справедливість виконання умови $\sum_{i=0}^{27} \pi_i = 1$, можна визначити величину КГ за формулою

$$K_{Г_4}(t) = \pi_0 + \pi_1 + \pi_2 + \pi_7 + \pi_8 + \pi_9 + \pi_{14} + \pi_{15} + +\pi_{16} + \pi_{21} + \pi_{22} + \pi_{23}. \qquad (3.51)$$

Від представленої НПММ (рис. 3.36), яка відображає теоретичні аспекти оцінювання рівня готовності ХМІ з декількома підсистема ФМ, ВМ та миттєвим КТС, перейдемо до моделі, що враховує нюанси проведення контроля інформаційно-технічних станів відповідних хмарних систем інфраструктури. Для цього побудуємо НПММ готовності ХМІ з урахуванням тривалості проведення

контроля інформаційно-технічних станів фізичних та віртуальних машин. Відповідно, граф станів пропонуємої моделі, що враховує зазначені нюанси, та основні співвідношення щодо розрахунку коефіцієнта готовності ХМІ наведено в додатку Г.

Отримана НПММ (рис. 3.36) може бути застосована як для визначення КГ, так і для оцінки інших показників надійності хмарної інфраструктури. Кількісні оцінки показників надійності ХМІ з трьома підсистемами ФМ та ВМ за умови проведення миттєвого контролю їхніх інформаційно-технічних станів і заданого рівня готовності інфраструктури представлено в табл. 3.3.

Таблиця 3.3

Кількісні оцінки показників надійності ХМІ з трьома підсистемами фізичних та віртуальних машин і миттєвим КТС

№ з/п	Рівень готовності ХМІ та показники надійності фізичних і віртуальних машин		
	Коефіцієнт готовності ХМІ	Середня наробітка до відмови ФМ та ВМ, год.	Інтенсивність відновлення ФМ та ВМ, 1/год.
1.	0,99	2380	4
2.		2083	5
3.		1667	8
4.		1562	10
5.		1316	20
6.		1219	30
7.		1110	40
8.		1020	50

Отримані результати напівмарковського моделювання (табл. 3.3) можуть бути застосовані для обгрунтування граничних величин показників надійності ФМ та ВМ, які будуть відповідати вимогам забезпечення необхідного рівня готовності хмарної інфраструктури.

3.5 Напівмарковська модель готовності хмарної інфраструктури з урахуванням зловмисних шкідливих впливів

Відомо, що хмарна інфраструктура як і решта кібернетичних активів КІ є об'єктом негативних шкідливих впливів, включаючи хакерські атаки та втручання спільноти зловмисників. Атака може здійснюватися за сценарієм, аналогічним тому, що був реалізований в 2017 році в Україні, коли завдяки успішно проведеній кібератаці була частково паралізована національна інфраструктура, а також нанесені суттєві збитки економіці держави за рахунок вимушеного простою промислових підприємств [126]. Враховуючи актуальність зазначеної проблеми, зробимо спробу побудувати НПММ готовності хмарної інфраструктури за умов, коли на неї здійснюється зловмисний шкідливий вплив у вигляді кібератаки, наслідки якої проявляються у вигляді відмов та збоїв відповідного сервіс-орієнтованого ресурсу [127].

У якості прикладу дії зловмисного шкідливого впливу розглянемо відомий випадок хакерської атаки на українські кібернетичні активи з застосуванням двох відомих комп'ютерних вірусів WannaCry та Petya Ransomware. Припустимо, що на хмарну інфраструктуру з конфігурацією, яка зображена на рис. 3.34, здійснюється зловмисний шкідливий вплив за сценарієм, що передбачає використання зазначених вірусів. В цьому випадку для аналізу ЗВШВ пропонується використовувати класифікаційну схему, яка представлена на рис. 3.34 [75]. Відповідно до класифікаційної схеми (рис. 3.34) можна виділити дві фази реалізації кібератаки, а саме: 1) під час реалізації першої фази вірус WannaCry, розповсюджений спільнотою зловмисників в замаскованому вигляді як оновлення деякого ПЗ, проникає в систему та взламує її захист; 2) під час другої фази вірус Petya Ransomware шифрує дані, які зберігаються в системі. Після чого

користувачеві у разі необхідності використовувати зашифровані дані пропонується заплатити певні кошти для отримання ключів доступу, тобто вірус діє як типовий зловмисник-вимагач.

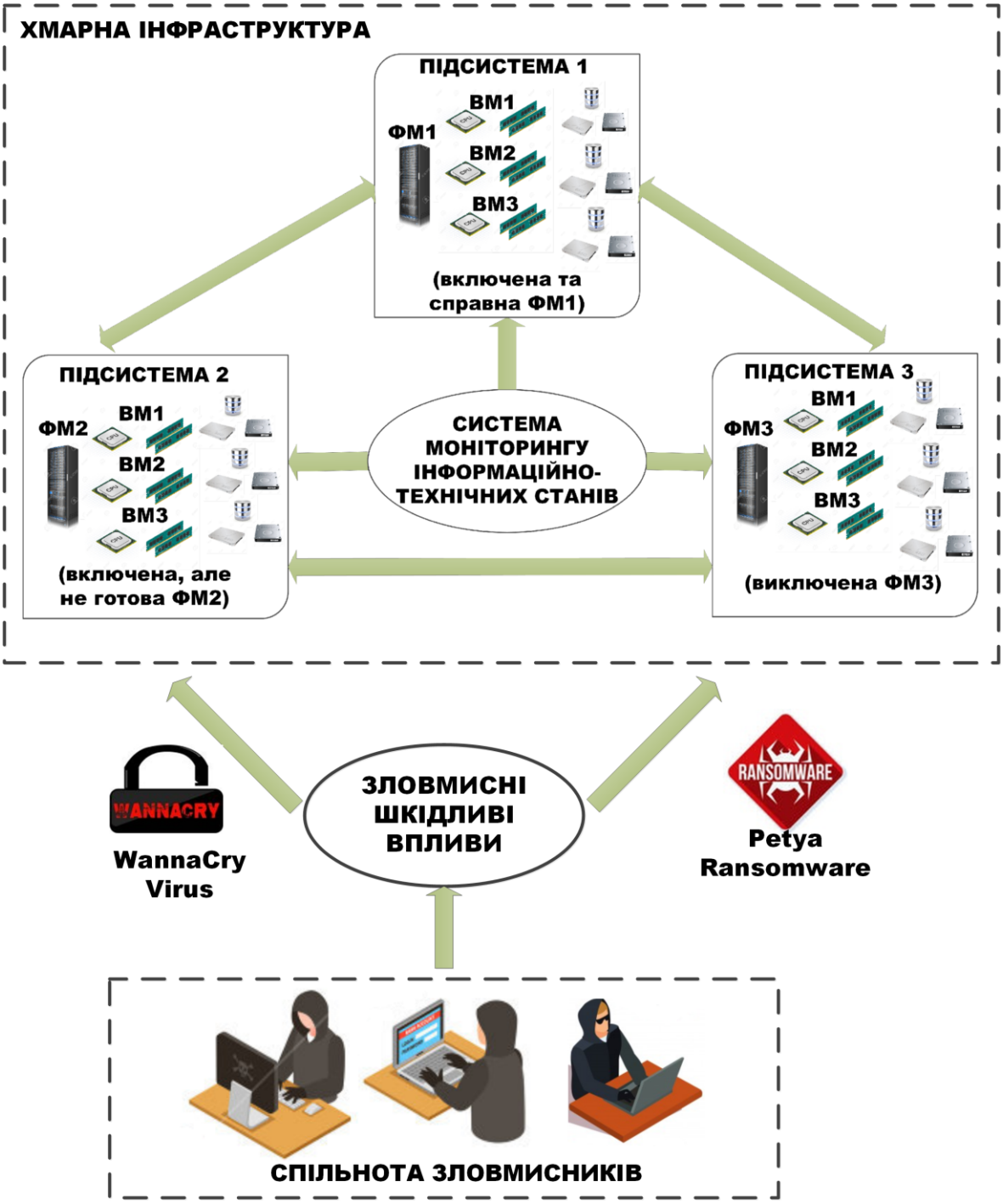


Рис. 3.34 Класифікаційна схема ЗВШВ на готовність ХМІ відповідно до сценарію кібератаки з використанням вірусів WannaCry і Petya Ransomware

На рис. 3.35 зображено граф станів НПММ готовності ХМІ для випадку, коли ЗВШВ реалізуються за сценарієм кібератаки, класифікаційна схема якої

наведена на рис. 3.34. Стосовно пропонуємої до розгляду моделі [30] застосовуються припущення, аналогічні припущенням для НПММ, граф станів якої зображено на рис. 3.30. Крім того, вважається, що ЗВШВ призводять до порушень, які проявляються у вигляді прихованих відмов.

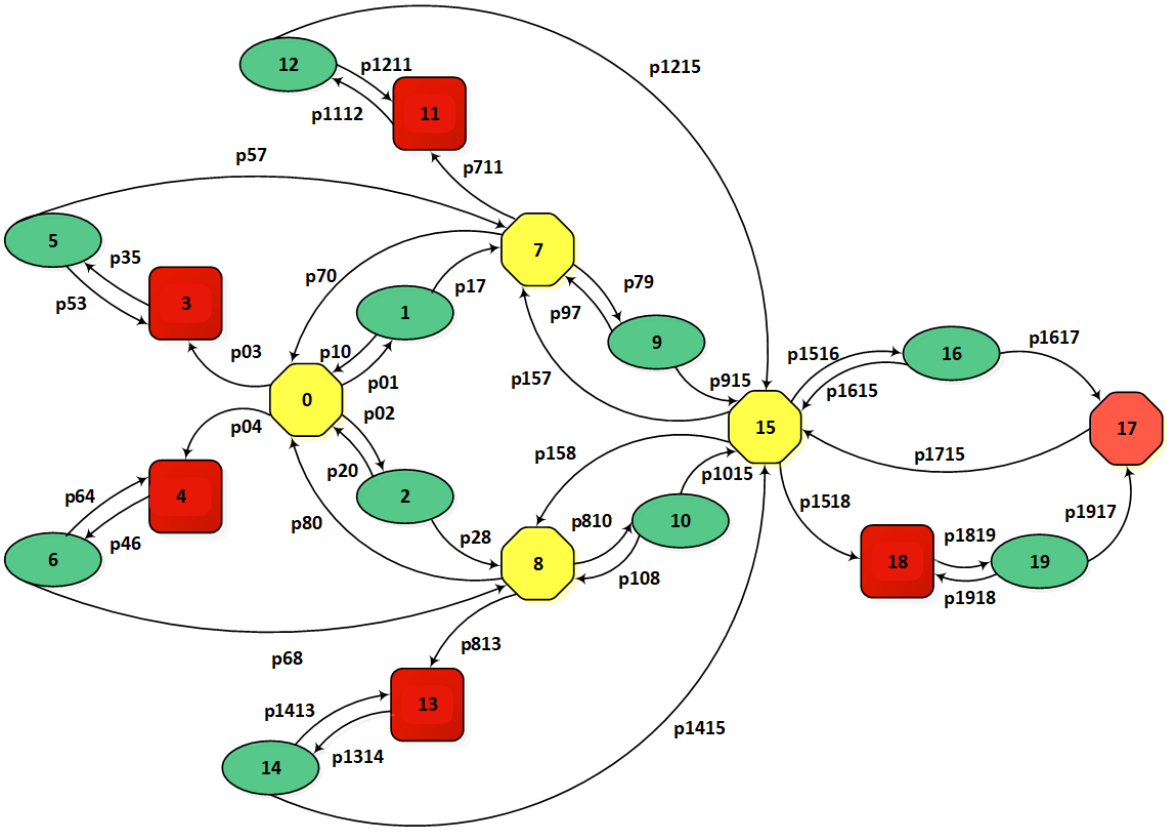


Рис. 3.35 Граф станів НПММ готовності хмарної інфраструктури з урахуванням зловмисних шкідливих впливів

Відповідно до рис. 3.35 множина станів НПММ записується у вигляді $\forall\ S_i \in S,\ S = \{S_0, S_1, ..., S_{19}\} \exists\ G_E = (20, 38),\ \Theta_E = 20$. Множина станів (рис. 3.35) $S_{AI} = \{S_0, S_7, S_8, S_{15}\}$, $S_{AI} \subset S$, коли всі три ФМ знаходяться у працездатному стані визначає загальний ПРС стан інфраструктури. Під час кібератаки за рахунок дії вірусів ХМІ переходить в стани прихованої відмови, тобто $S_{HF} = \{S_3, S_4, S_{11}, S_{13}, S_{18}\}$, $S_{HF} \subset S$. За допомогою інформаційно-технічних станів, які утворюють відповідну множину $S_{TIMS} = \{S_1, S_2, S_5, S_6, S_9, S_{10},\ S_{12}, S_{14}, S_{16}, S_{19}\}$, $S_{TIMS} \subset S$, описується ситуація, коли обслуговуючий персонал інфраструктури

робить спробу, застосовуючи систему моніторингу ІТС фізичних машин, реалізувати захисні функції (функції протидії) відносно активності дії комп'ютерних вірусів та інших типів зловмисних шкідливих впливів і проникнень. Отже, $S = S_{AI} \cup S_{HF} \cup S_{TIMS}$. В табл. 3.4 відображено переходи S_{ij} та перехідні імовірності p_{ij} відповідних гілок дії комп'ютерних вірусів WannaCry і Petya Ransomware. Враховуючи виконання умови $\sum_{i=0}^{19} \pi_i = 1$, можна визначити величину КГ за формулою

$$K_{\Gamma_5}(t) = \pi_0 + \pi_7 + \pi_8 + \pi_{15}. \tag{3.52}$$

Таблиця 3.4

Перехідні імовірності для НПММ готовності ХМІ, що описують дію комп'ютерних вірусів

Гілка активації вірусу WannaCry	Гілка розповсюдження вірусу Petya Ransomware
$S_0 \xrightarrow{p_{03}} S_3 \xrightarrow{p_{35}} S_5 \xrightarrow{p_{57}} S_7$	$S_0 \xrightarrow{p_{04}} S_4 \xrightarrow{p_{46}} S_6 \xrightarrow{p_{68}} S_8$ $S_7 \xrightarrow{p_{711}} S_{11} \xrightarrow{p_{1112}} S_{12} \xrightarrow{p_{1215}} S_{15}$ $S_8 \xrightarrow{p_{813}} S_{13} \xrightarrow{p_{1314}} S_{14} \xrightarrow{p_{1415}} S_{15}$ $S_{15} \xrightarrow{p_{1518}} S_{18} \xrightarrow{p_{1819}} S_{19} \xrightarrow{p_{1917}} S_{17}$

Основні співвідношення щодо розрахунку коефіцієнта готовності хмарної інфраструктури з урахуванням зловмисних шкідливих впливів і проникнень наведено в [75, 76, 111, 123]. На рис. 3.36 зображено результати моделювання у вигляді залежності коефіцієнта готовності хмарної інфраструктури від інтенсивності відмов фізичних машин та часу їхнього функціонування. Кількісні результати моделювання (рис. 3.36) отримано для різних значень співвідношень інтенсивностей дії комп'ютерних вірусів двох типів, тобто для велични $\xi = \lambda_3 / \lambda_4$.

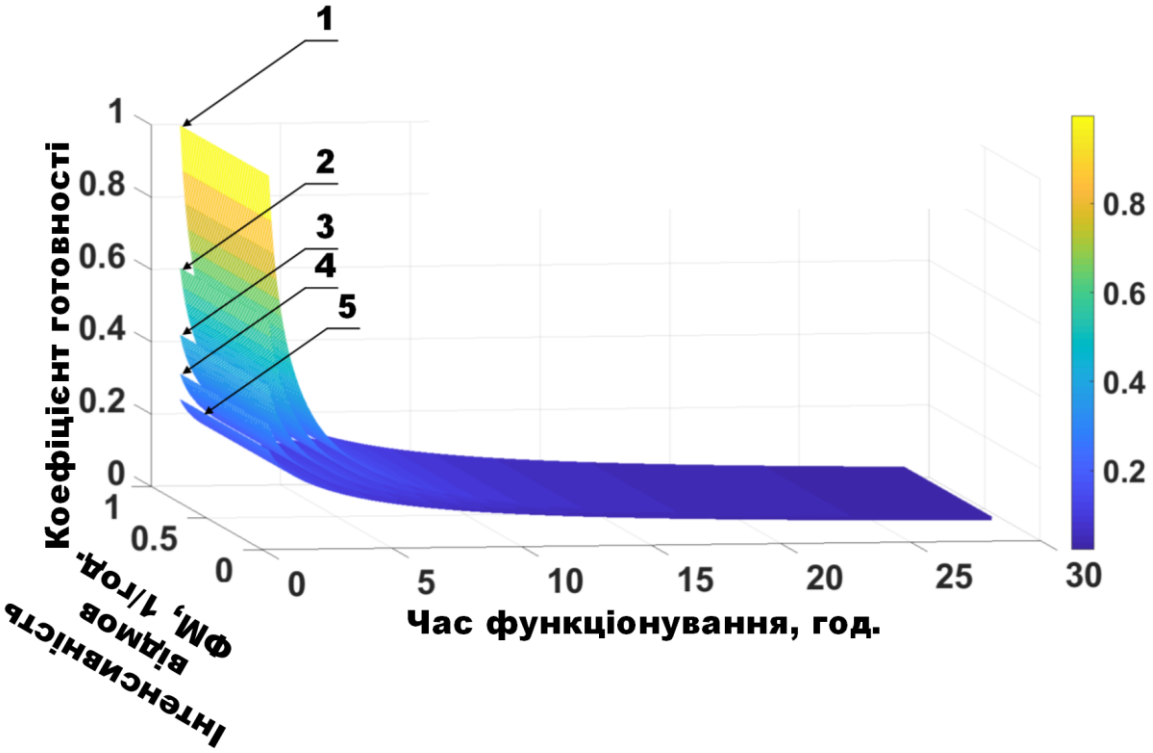


Рис. 3.36 Залежність $K_{\Gamma_5}(T)$ для співвідношення інтенсивностей дії комп'ютерних вірусів з $\xi = \lambda_3/\lambda_4$, коли: 1 – $\xi = 0,2$; 2 – $\xi = 0,21$; 3 – $\xi = 0,22$; 4 – $\xi = 0,235$; 5 – $\xi = 0,25$

Отримані результати моделювання (рис. 3.36) адекватно відтворюють ситуацію, яка реально відбувалася в 2017 році, коли за 2 години дії ЗВШВ майже всі IT компанії втратили доступ до своїх кібернетичних та хмарних активів.

Висновки до розділу 3

1. Розроблено аналітико-стохастичні моделі готовності КІ, які отримано на основі використання апарату формалізації процесів зміни інформаційно-технічних станів інфраструктурних компонентів та врахування негативних факторів зовнішнього і внутрішнього впливу на їхню безпеку.

2. Запропоновано метод напівмарковського моделювання, який надає змогу отримати оцінки готовності КІ, фактично відтворюючи їхню поведінку в умовах дії різноманітних негативних факторів впливу. Результати моделювання можуть бути використані для обґрунтування граничних показників надійності та функційної безпечності компонентів КІ.

3. Відповідно до запропонованого методу розроблено такі базові моделі: напівмарковська модель готовності ХМІ з інтегрованою системою моніторингу інформаційно-технічних станів фізичних машин; напівмарковська модель готовності ХМІ з декількома підсистемами фізичних та віртуальних машин; напівмарковська модель готовності ХМІ з урахуванням зловмисних шкідливих впливів. Розширення моніторингових функцій на основі застосування сервісів та потужних інформаційно-обчислювальних ресурсів відомих хмарних провайдерів створює сприятливі умови щодо реалізації вірогідного контролю інформаційно-технічних станів критичних інфраструктур.

4. Отримані напівмарковські моделі можуть бути застосовані як для визначення коефіцієнта готовності, так і для оцінки інших показників надійності хмарної та інших критичних інфраструктур.

5. Результати моделювання підтверджують доцільність застосування модулів синхронізованих векторних вимірювань і сервіс-орієнтованого хмарних ресурсів для створення інтегрованої системи оперативного моніторингу інформаційно-технічних станів критичної енергетичної інфраструктури. Застосування додаткових модулів ССВВ та відповідних хмарних сервісів AWS надає можливість підвищити вірогідність контролю інформаційно-технічних станів компонентів критичної енергетичної інфраструктури на 37%.

Основні положення цього розділу викладені у публікаціях автора [32, 74–76, 102, 103, 109, 110, 113, 115, 116, 120, 123, 127].

РОЗДІЛ 4
МЕТОДИ ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ КРИТИЧНИХ ІНФРАСТРУКТУР

4.1 Аналітико-стохастичний метод побудови структурних схем безпеки кібернетичних активів критичних інфраструктур

За результатами аналізу, які наведено в розділі один, витікає, що хмарні системи можна розглядати як перспективні засоби по забезпеченню функційної та кібернетичної безпечності КІ. Зокрема, в роботах [128, 129] розглядається можливість застосування хмарних активів для підвищення рівня готовності системи SCADA як однієї з найважливіших компонентів контуру управління КІ. Оцінювання виконувалось за умов, що до складу інфраструктури входять хмарні активи. Тому важливо дослідити як хмарні активи можуть впливати на безпеку кібернетичних активів КІ при існуванні певних зловмисних шкідливих впливів, кіберзагроз, враховуючи механізми їхньої реалізації [130] та наслідки для компонентів системи управління інфраструктурою, включаючи її програмне забезпечення [131].

Отже, для новоутвореної структури (рис. 1.13) виникає актуальне завдання, яке полягає в розробці основних положень методології оцінювання функційної безпечності (тобто з урахуванням конкретних інформаційно-технічних станів) критичних інфраструктур, які базуються на аналітико-стохастичному моделюванні внутрішніх та зовнішніх факторів негативного впливу на активи КІ і визначенні відповідних ризиків.

4.1.1 Етапи реалізації методу побудови структурних схем безпеки кібернетичних активів критичних **інфраструктур**

Для розв’язування завдання визначення рівня функційної безпечності КІ було запропоновано застосовувати аналітико-стохастичний метод побудови структурних схем безпеки (ССБ) [132], схему алгоритму реалізації якого зображено на рис. 4.1.

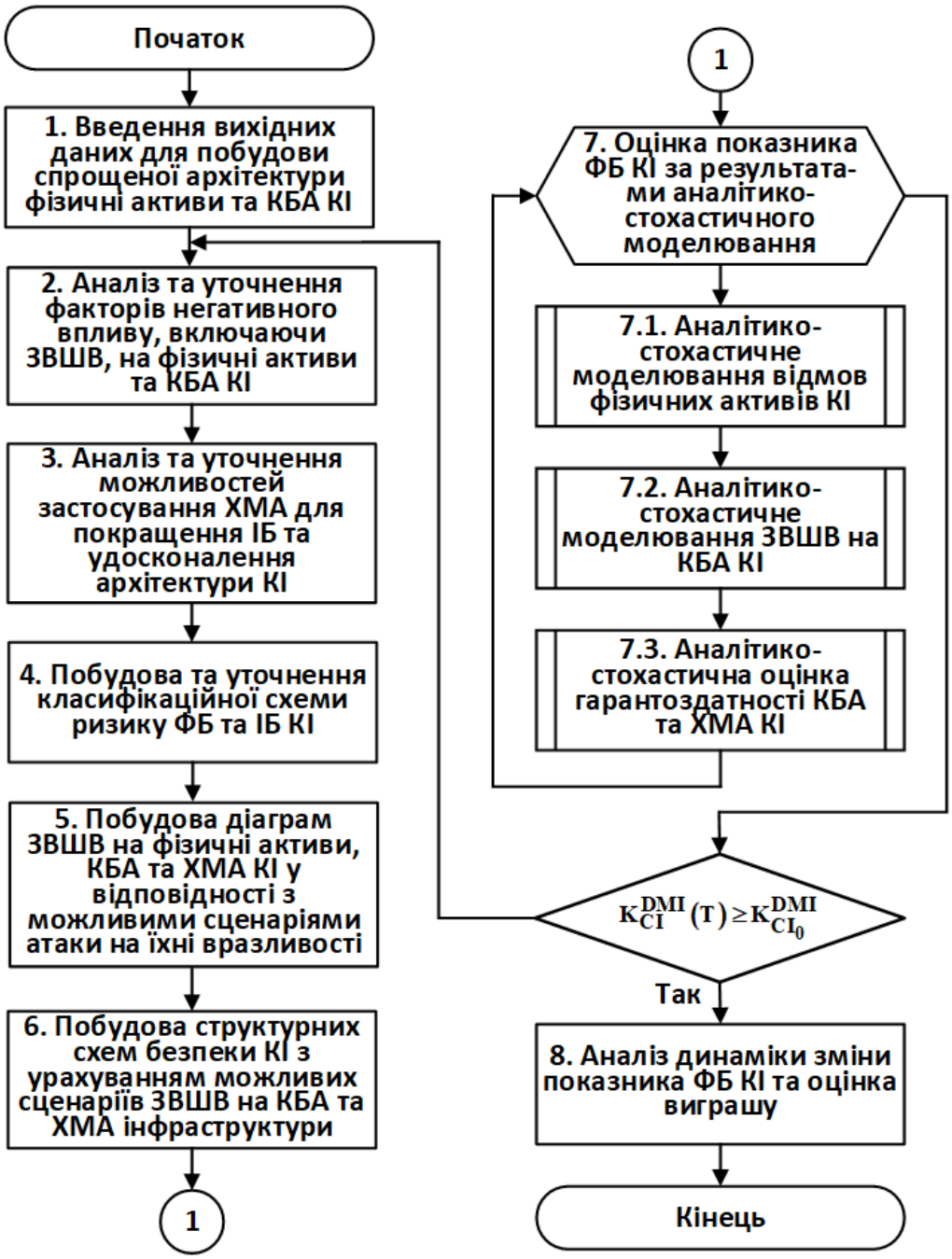


Рис. 4.1 Схема алгоритму реалізації етапів аналітико-стохастичного методу побудови ССБ кібернетичних активів КІ

Враховуючи, що перші п’ять етапів методу розглянуто в попередніх розділах дисертаційного дослідження, зосередимо увагу на шостому етапі реалізації методу побудови структурних схем безпеки кібернетичних активів критичних інфраструктур (рис. 4.1). Фактично побудова основних елементів ССБ починається з розгляду можливих сценаріїв ЗВШВ, які будуються з урахуванням відомого досвіду кібератак. Далі виконується аналітико-стохастичне

моделювання (етап 7) на основі використання апарату моделювання напівмарковських процесів. Отримані результати моделювання застосовуються для аналізу динаміки зміни рівня функційної безпечності критичної інфраструктури та оцінки виграшу (етап 8).

4.1.2 Аналітико-стохастичне моделювання відмов фізичних активів критичних інфраструктур

Для моделювання відмов фізичних активів критичних інфраструктур можуть застосовуватися різноманітні методи. Перевага надається аналітико-стохастичним методам, які у більшості випадків реалізуються у відповідності зі схемою, яка зображена на рис. 2.8.

Серед аналітико-стохастичних методів, які враховують ІТС досліджуваних систем особливу увагу слід приділити апарату моделювання на основі напівмарковських процесів [133]. Як було вже відмічено в другому та третьому розділах, у порівнянні з марковськими [134] перевагу було надано напівмарковським моделям саме тому, що використання НПММ надає можливість враховувати різноманітні режими застосування фізичних активів КІ за призначенням, коли тривалість перебування інфраструктури може розглядатися як випадкова величина з різними законами розподілу (наприклад, час відновлення, час діагностування та пошуку несправності і т.і.), так і детермінована величина (наприклад, час проведення контролю інформаційно-технічних станів (КТС), час виконання технічного обслуговування і т.і.).

Для упорядкування та визначення послідовності виникнення тих, чи інших негативних подій стосовно до фізичних активів КІ можуть застосовуватися детерміністські підходи. Наприклад, в [135, 136] розглянуто один з таких підходів, реалізований на основі використання методу декомпозиції складних подій, які призводять до аварій КІ.

4.1.3 Аналітико-стохастичне моделювання зловмисних шкідливих впливів на кібернетичні активи критичних інфраструктур

Моделювання виконується згідно з функціональною схемою реалізації сценарію ЗВШВ. В залежності від умов, припущень та обмежень, що

спостерігаються та вводяться, пропонується застосовувати як апарат марковського моделювання [131, 134], так і апарат напівмарковського моделювання [137, 138] ЗВШВ на кібернетичні активи КІ. Слід зауважити, що застосування апарату марковського моделювання ЗВШВ на кібернетичні активи критичних інфраструктур вимагає попереднього обгрунтування з урахуванням динаміки розвитку процесів за умов, коли спостерігається марковська властивість. Такі умови, наприклад, можуть виникати, коли кібератака реалізується в певний поточний момент часу і їй не передує попередній збір інформації про об’єкт атаки, тобто відсутній етап цільового фішингу. Але як свідчить аналіз наслідків успішно проведених кібератак на вітчизняну критичну інфраструктуру [139, 140], завжди існує деякий період, так званої, предісторії, на якому проводиться цільовий фішинг. У цьому випадку марковська властивість не спостерігається і тому необхідно застосовувати інші немарковські моделі ЗВШВ. На переконання автора найкраще для цього підходить апарат моделювання напівмарковських процесів, який в подальшому застосовується при оцінці функційної безпечності КІ з урахуванням ризиків негативного впливу на їхні активи.

Для побудови адекватних моделей ЗВШВ визначається тривалість інтервалу загального циклу оцінювання рівня безпеки кібернетичних активів КІ та формулюється складна подія, що відбувається на певному інтервалі часу. Після чого виконується декомпозиція зазначеної події та з застосуванням теорем складання і множення імовірностей визначається комплексний показник безпеки.

Аналітико-стохастичне моделювання може виконуватися для декількох сценаріїв ЗВШВ. Результати моделювання в подальшому використовуються для вибору найкращого варіанту захисту від кібератак, включаючи побудову електронного периметру кібербезпеки.

4.2 Метод оцінювання функційної безпечності критичних інфраструктур з урахуванням ризику негативних впливів на їхні активи

Відповідно до рис. 4.1 четвертий етап побудови структурної схеми безпеки присвячено побудові та уточненню класифікаційної схеми ризику функційній безпечності критичних інфраструктур (рис. 2.11). Після чого на сьомому етапі

виконується оцінка показника функційної безпечності критичних інфраструктур. Тому слід приділити особливу увагу розробці методичного апарату оцінювання функційної безпечності критичних інфраструктур з урахуванням ризику зловмисних шкідливих впливів на їхні активи.

4.2.1 Етапи реалізації методу оцінювання функційної безпечності критичних інфраструктур з урахуванням ризику негативних впливів на їхні активи

Запропонований метод складається з таких етапів:

1) розробка функціональної схеми реалізації зловмисних шкідливих впливів на активи критичної інфраструктури;

2) побудова діаграм системних відмов критичної інфраструктури з урахуванням зловмисних шкідливих впливів на інфраструктурні активи;

3) оцінка комплексного показника безпеки активів критичної інфраструктури за результатами аналітико-стохастичного моделювання;

4) кількісна оцінка ризику негативного впливу на активи критичної інфраструктури;

5) оцінка показника безпеки КІ з урахуванням ризику негативного впливу на активи інфраструктури.

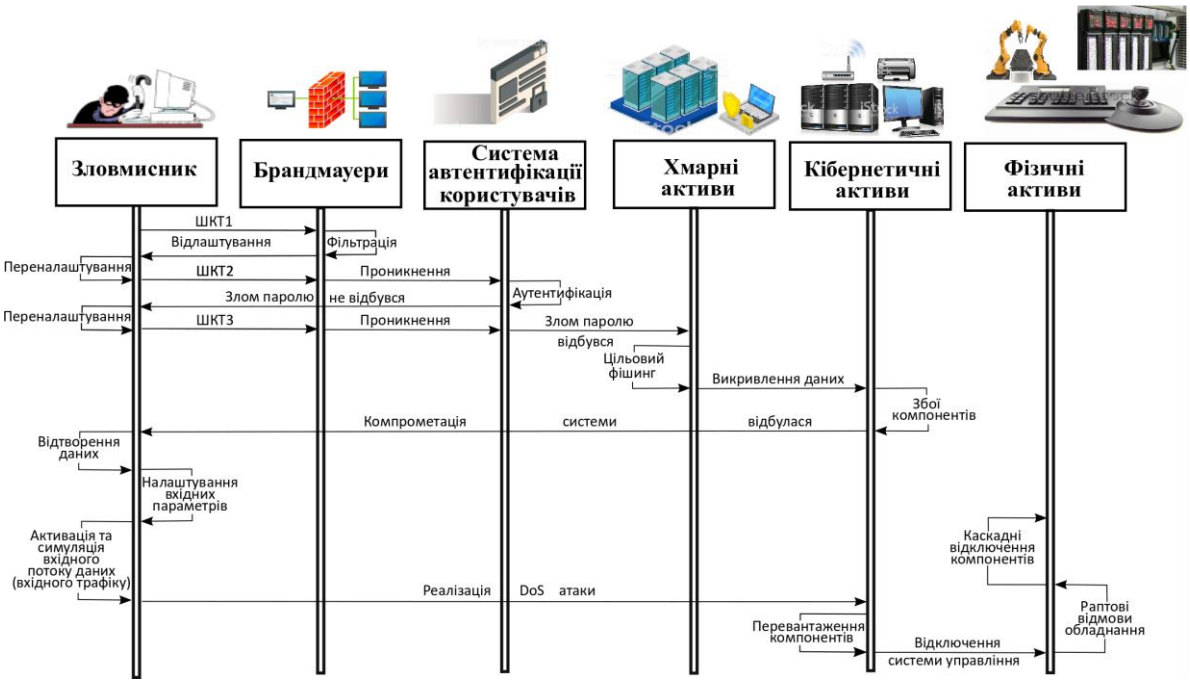


Рис. 4.2 Функціональна схема сценарію реалізації ЗВШВ на активи КІ

Первинно на основі відомого досвіду розробляється сценарій розвитку ЗВШВ. У якості прикладу розглянемо сценарій кібератаки, функціональна схема реалізації якого представлена на рис. 4.2. Вважатимемо, що зловмисники створюють і застосовують шкідливий трафік (ШКТ), який впливає на фізичні, кібернетичні та хмарні активи критичної інфраструктури.

Діючи відповідно до зображеної функціональної схеми (рис. 4.2), зловмисники прагнуть досягти таких цілей [141]:

1) створити умови щодо проникнення через брандмауери, тобто уникнути дій, пов'язаних з виконанням функцій фільтрації вхідних інформаційних потоків;

2) отримати доступ до КБА без автентифікаційної процедури перевірки паролю або здійснити злом паролю;

3) проникнути в систему, тобто здійснити її злом, компрометацію, викривлення інформації; замінити корисну інформацію на сфальсифіковану або реалізувати інформаційне перевантаження КБА та хмарних активів для припинення доступу до них;

4) створити умови (наприклад, DoS атака, розгортання шкідливої бот-мережі), коли за рахунок відключення КБА та хмарних активів виникають відмови компонентів, які утворюють фізичні активи критичної інфраструктури.

На наступному етапі з урахуванням можливих сценаріїв реалізації ЗВШВ (рис. 4.2) будуються діаграми системних відмов (ДСВ) критичної інфраструктури. Порядок побудови ДСВ для кібернетичних та хмарних активів критичної інфраструктури, які водночас утворюють відповідні мережеві рівні інформаційно-керуючої системи КІ типу SCADA, представлено в [132].

На рис. 4.3 зображено спрощену архітектурну реалізацію кібернетичних та хмарних активів системи SCADA КІ. Головна особливість наведеної архітектури полягає в утворенні паралельно підключеного контуру хмарних активів AWS, який працює за принципом функціональної та ресурсної надмірності.

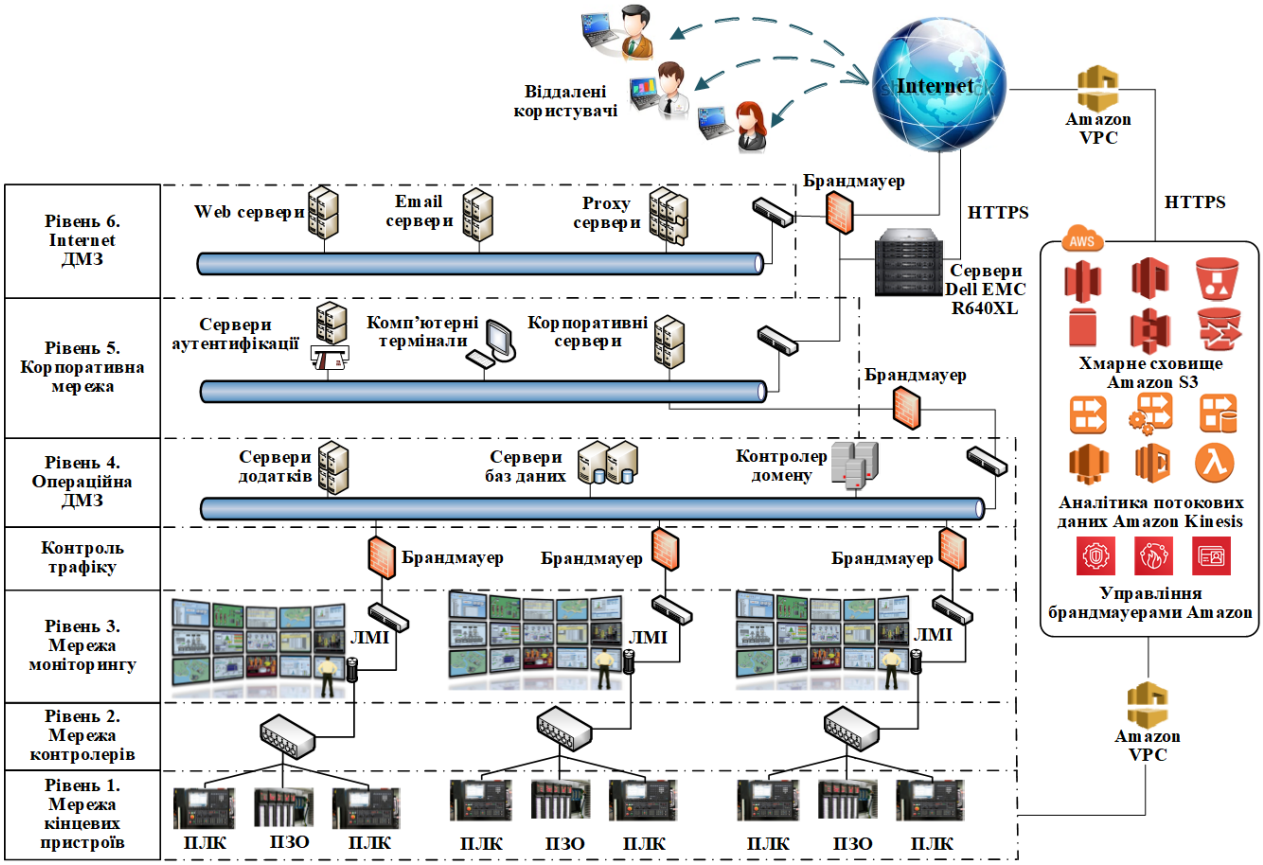


Рис. 4.3 Спрощена архітектурна реалізація кібернетичних [142] та хмарних активів системи SCADA критичної інфраструктури

Згідно з рис. 4.3 серверні системи, прилади кіберзахисту, кінцеві пристрої утворюють шість мережевих рівнів, що мають певні вразливості через які реалізуються загрози інформаційній безпеці та гарантоздатності [143] SCADA критичної інфраструктури.

В таблиці 4.1 відзначені наступні аспекти інформаційної безпеки та гарантоздатності системи SCADA критичної інфраструктури, забезпеченню яких сприяє застосування AWS: A1 – аварійне відновлення і резервне копіювання кібернетичних активів SCADA критичної інфраструктури; A2 – узагальнення викликів, які обумовлені несправностями та змінами вимог і умов застосування за призначенням SCADA критичної інфраструктури; A3 – покращення аналізу забезпечення відмовостійкості кібернетичних активів SCADA КІ; A4 – багатоверсійні обчислення у контексті факторів еволюційного розвитку кібернетичних активів SCADA КІ.

Таблиця 4.1

Застосування AWS для забезпечення інформаційної безпеки та гарантоздатності системи SCADA критичної інфраструктури

Назва сервісу AWS	Призначення сервісу AWS	Аспекти забезпечення інформаційної безпеки та гарантоздатності SCADA КІ на основі AWS			
		A1	A2	A3	A4
Управління брандмауерами Amazon	Гнучке управління процесами фільтрації трафіку	–	–	+	–
Аналітика потокових даних Amazon Kinesis	Прийом, обробка, аналіз аномалій, розподілення та доставка інформаційних потоків даних	–	+	+	+
Хмарне сховище Amazon S3	Запис та збереження даних великих обсягів	+	–	+	+
Віртуальна приватна хмара Amazon VPC	Створює захищені приватні мережі та підмережі без відображення IP-адрес в Internet	+	+	–	–

На рис. 4.4 зображено діаграму системної відмови SCADA КІ з урахуванням зловмисних шкідливих впливів на кібернетичні та хмарні активи інфраструктури.

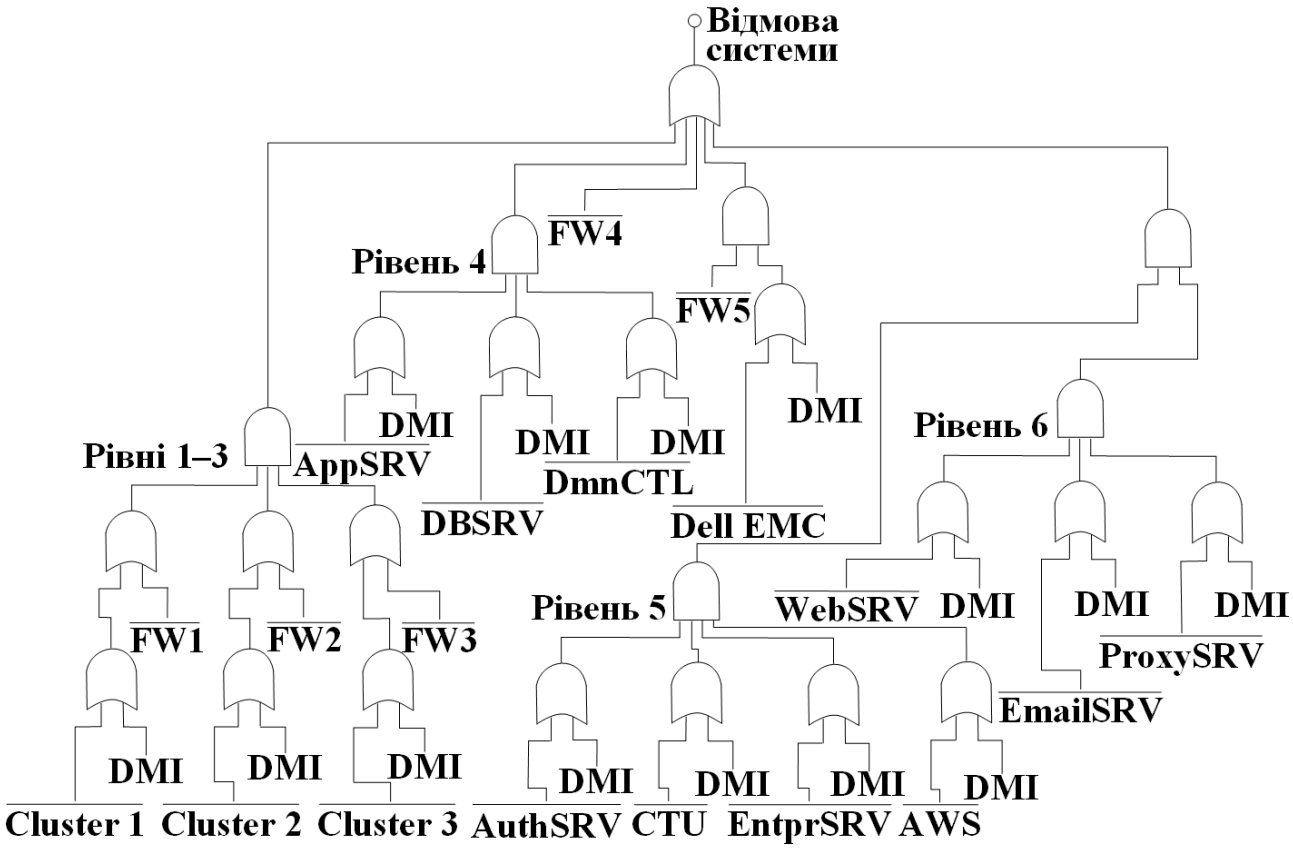


Рис. 4.4 Діаграма системної відмови кібернетичних та хмарних активів SCADA КІ

Відповідно до ДСВ, яка зображена на рис. 4.4, комплексна ймовірнісна оцінка готовності кібернетичних та хмарних активів SCADA КІ може бути визначена так:

$$\text{UnAvailability} = P\left(\Phi\left(X\right)=0\right) = P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \overline{FW4} \cup \right.$$

$$\left. \cup \left[\overline{FW5} \cap \left(\overline{\text{Dell EMC}} \cup DMI\right)\right]\right\}, \tag{4.1}$$

$$UA_{1-3} = \left\{\left[\overline{\text{Cluster1}} \cup DMI\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{\text{Cluster2}} \cup DMI\right] \cup \overline{FW2}\right\} \cap$$

$$\cap \left\{\left[\overline{\text{Cluster3}} \cup DMI\right] \cup \overline{FW3}\right\}, \tag{4.2}$$

$$UA_4 = \left[\overline{\text{AppSRV}} \cup DMI\right] \cap \left[\overline{\text{DBSRV}} \cup DMI\right] \cap \left[\overline{\text{DmnCTL}} \cup DMI\right], \tag{4.3}$$

$$UA_5 = \left[\overline{\text{AuthSRV}} \cup DMI\right] \cap \left[\overline{\text{CTU}} \cup DMI\right] \cap \left[\overline{\text{EntprSRV}} \cup \right.$$

$$\left. \cup DMI\right] \cap \left[\overline{\text{AWS}} \cup DMI\right], \tag{4.4}$$

$$UA_6 = \left[\overline{WebSRV} \cup DMI\right] \cap \left[\overline{EmailSRV} \cup DMI\right] \cap \left[\overline{ProxySRV} \cup DMI\right], \qquad (4.5)$$

де $\overline{\text{Dell EMC}}$ – подія, яка полягає в неготовності універсальної серверної платформи для IT-інфраструктур [144], яка розгорнута на основі масштабованої системної архітектури для збереження великих обсягів даних, проведення складних обчислювальних операцій та розподілення вхідних потоків даних (вхідного трафіку); $\overline{AWS}$ – подія, що полягає в неготовності сервіс-орієнтованих ресурсів хмарного провайдера Amazon, характеристику яких наведено в табл. 4.1.

Тоді ймовірність події, яка полягає в тому, що всі кібернетичні та хмарні активи SCADA КІ будуть доступні може бути записана у вигляді

$$\text{Availability} = 1 - \text{UnAvailability} = 1 - P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \overline{FW4} \cup \right.$$

$$\left. \cup \left[\overline{FW5} \cap \left(\overline{\text{Dell EMC}} \cup DMI\right)\right]\right\}. \qquad (4.6)$$

Характеристика складових, які входять у співвідношення (4.1)–(4.6), наведена в [132]. Отже, необхідно виконати моделювання і дослідити, яким чином застосування додаткових сервісів AWS впливає на загальний рівень функційної безпечності кібернетичних та хмарних активів системи SCADA КІ (рис. 4.3).

4.2.2 Аналітико-стохастична модель функційної безпечності інформаційно-керуючої системи критичної інфраструктури з урахуванням зловмисних шкідливих впливів на її кібернетичні та хмарні активи

Застосовуючи спрощену архітектурну реалізацію (рис. 4.3) та діаграму системної відмови (рис. 4.4), отримаєм оцінку функційної безпечності ІКС типу SCADA КІ, з урахуванням зловмисних шкідливих впливів на її кібернетичні та хмарні активи. Отримаєм кількісні значення комплексного показника ФБ без урахування вартості наслідків ЗВШВ для поданого сценарію (рис. 4.1), коли всі зазначені процеси відбуваються як напівмарковські, враховуючи випадкові події, які трапляються на інтервалах застосування за призначенням брандмауерів та відповідних підсистем SCADA КІ (рис. 4.3, 4.4). Сукупність цих інтервалів утворює загальний робочий цикл або цикл оцінювання, протягом якого відбувається складна подія Q (рис. 4.5).

Відповідно до рис. 4.5 випливає, що комплексний показник функційної безпечності W_{SCADA} можна визначити як ймовірність події Q, застосувавши відомі теореми складання та множення ймовірностей, а саме [134, 138]:

$$W_{SCADA} = \rho K_{\Gamma_{SCADA}} + [1-\rho] K_{\Gamma_{SCADA}}, \quad (4.7)$$

де ρ – ймовірність успішного виконання брандмауером функцій фільтрації вхідних та вихідних інформаційних потоків (вхідного та вихідного трафіків); $K_{\Gamma_{SCADA}}$ – стаціонарний коефіцієнт готовності SCADA КІ.

Рис. 4.5 Загальний цикл оцінювання рівня ФБ SCADA КІ

Для визначення складових співвідношення (4.7) застосуємо апарат моделювання напівмарковських процесів та метод побудови структурних схем безпеки [132]. На рис. 4.6 зображено граф станів напівмарковської моделі функціонування брандмауера (БДМ), на яку поширюються дії системи обмежень (2.6).

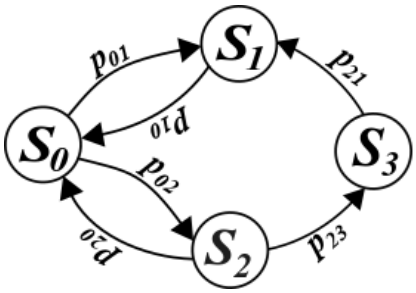


Рис. 4.6 Граф станів напівмарковської моделі функціонування БДМ

У процесі функціонування (рис. 4.6) БДМ може перебувати в чотирьох станах:

1) стан S_0 – БДМ працює в нормальному режимі та успішно виконує операції фільтрації як вхідного, так і вихідного трафіків SCADA КІ;

2) стан S_1 – заміна кодових ключів, завдяки чому виконується компенсація ЗВШВ на кібернетичні та хмарні активи SCADA КІ;

3) стан S_2 – зловмисники здійснюють цільовий фішинг;

4) стан S_3 – система скомпрометована і не може використовуватися обслуговуючим персоналом за призначенням; вважається, що кібернетичні та хмарні активи SCADA КІ недоступні.

Запропоновану до розгляду НПММ (рис. 4.6) можна інтерпретувати наступним чином. Як свідчить відомий досвід кодові ключи замінюються з певною періодичністю $T_{ЗК}$. Процедура заміни триває час $\tau_{ЗК}$. Тому функції розподілення часу для переходів $S_0 \to S_1$, $S_1 \to S_0$ задаються у вигляді

$$Q_{01}(t) = \begin{cases} 0, & t < T_{ЗК}; \\ 1, & t \geq T_{ЗК}; \end{cases} \tag{4.8}$$

$$Q_{10}(t) = \begin{cases} 0, & t < \tau_{ЗК}; \\ 1, & t \geq \tau_{ЗК}. \end{cases} \tag{4.9}$$

Для решти переходів $S_i \to S_j$, $S_j \to S_i$ елементи матриці $\left|Q_{ij}(t)\right|$ записуються як

$$Q_{02}(t) = \begin{cases} 1 - e^{-\gamma_{цф} t}, & t < T_{ЗК}; \\ 1, & t \geq T_{ЗК}; \end{cases} \tag{4.10}$$

$$Q_{20}(t) = \begin{cases} 1 - \left[1 + \gamma_{кбз} t + \dfrac{(\gamma_{кбз} t)^2}{2}\right] e^{-\gamma_{кбз} t}, & t < T_{ЗК}; \\ 1, & t \geq T_{ЗК}; \end{cases} \tag{4.11}$$

$$Q_{23}(t) = \begin{cases} 1 - e^{-\gamma_{км} t}, & t < T_{ЗК}; \\ 1, & t \geq T_{ЗК}. \end{cases} \tag{4.12}$$

В виразах (4.8)–(4.12) застосовуються такі параметри: $\gamma_{цф}$ – інтенсивність проведення цільового фішингу зловмисниками на інтервалі часу тривалістю $T_{ЗК} \in [0, t]$; $\gamma_{кбз}$ – інтенсивність забезпечення кіберзахисту системи (цільовий

фішинг не досяг успіху); $\gamma_{км}$ – інтенсивність компрометації системи (цільовий фішинг досяг успіху). По аналогії з попередніми моделями основні нотації граматики Є для аналізу складності пропонуємої НПММ (рис. 4.6) записуються у вигляді

$$G_Є = (4,6);\ \Theta_Є = 4;\ R_Є = S_0 \xleftarrow[\exists Q_{20}(t)]{\exists Q_{02}(t)} S_2 \xrightarrow{\neg\left(Q_{23}(t) \in \left|Q_{ij}(t)\right|\right)} S_3 \xleftarrow[\exists Q_{03}(t)]{\exists Q_{30}(t)} S_0 .$$

Крім того, припустимо, що для представленої НПММ (рис. 4.6) початкові стани відповідають значенням імовірностей $P_0(0)=1$, $P_i(0)=0$, де $i=\overline{1,3}$. Тоді, прийнявши до уваги рівняння $\sum\limits_{i=0}^{n} \pi_i = 1$, де $n=3$, та, враховуючи, що $\forall\ \pi_i \in \Pi$, $\Pi = \{\pi_0, \pi_1, \pi_2, \pi_3\} \exists \{p_{ij} : \pi(p_{ij})\}$, відповідно до [111, 138] отримаєм такі розрахункові співвідношення:

$$F_{ij}(t) = 1 \to P_{ij}(\infty), \tag{4.13}$$

$$P_{ij}(\infty) = p_{ij} = \int\limits_0^{\infty} \prod_{k \neq j} \left[1 - Q_{ik}(\tau)\right] dQ_{ij}(\tau), \tag{4.14}$$

$$\pi_0 = \frac{1}{1 + p_{01} + p_{02}(1 + 2p_{23})}, \tag{4.15}$$

$$\pi_1 = \left[p_{01} + p_{02}p_{23}\right]\pi_0, \tag{4.16}$$

$$\pi_2 = p_{02}\pi_0,\ \pi_3 = 1 - \left[\pi_0 + \pi_1 + \pi_2\right], \tag{4.17}$$

$$\rho = \pi_0 + \pi_2, \tag{4.18}$$

де $F_{ij}(t)$ – функція розподілення часу перебування в стані S_i перед переходом в стан S_j; p_{ij} – перехідна ймовірність зі стану S_i в стан S_j.

На рис. 4.7 відповідно до ДСВ (рис. 4.4) зображено структурну схему надійності кібернетичних та хмарних активів системи SCADA КІ, що побудована з урахуванням послідовності подій, логіка реалізації яких визначається співвідношеннями (4.1)–(4.7). За допомогою ССН можна визначити внесок кожного елементу в загальний рівень надійності системи.

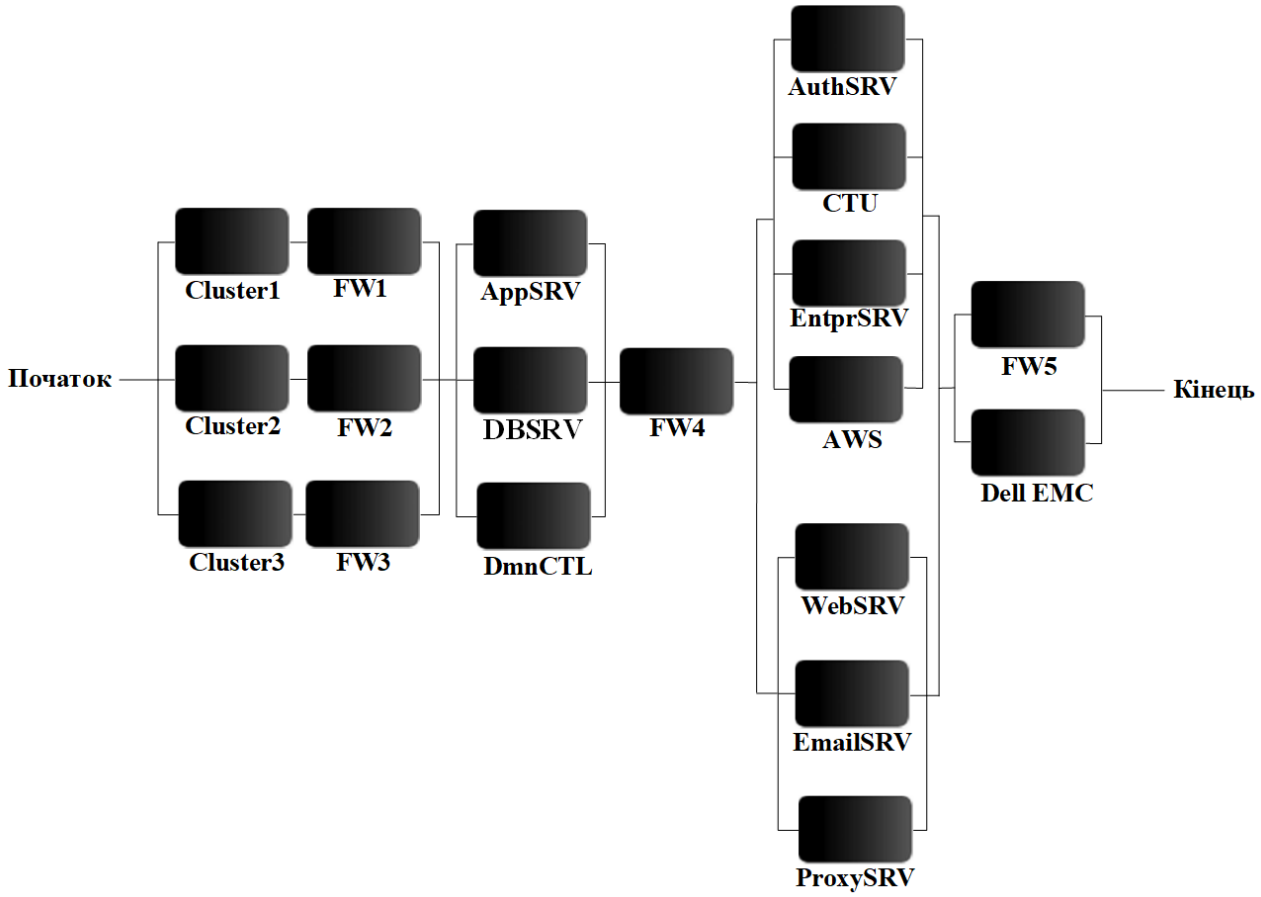


Рис. 4.7 Структурна схема надійності кібернетичних та хмарних активів системи SCADA КІ

Використовуючи зображену ССН (рис. 4.7), співвідношення для визначення стаціонарного коефіцієнта готовності кібернетичних та хмарних активів SCADA КІ можна записати у вигляді

$$K_{\Gamma_{SCADA}} = A_{SCADA} = \{1-[1-A_{Cluster1}A_{FW1}]\times[1-A_{Cluster2}A_{FW2}]\times[1-A_{Cluster3}A_{FW3}]\}\times$$
$$\times\{1-[1-A_{AppSRV}]\times[1-A_{DBSRV}]\times[1-A_{DmnCTL}]\}\times\{1-[1-A_{AuthSRV}]\times$$
$$\times[1-A_{CTU}]\times[1-A_{EntprSRV}]\times[1-A_{WebSRV}]\times[1-A_{EmailSRV}]\times[1-A_{AWS}]\times$$
$$\times[1-A_{ProxySRV}]\}\times\{1-[1-A_{FW5}]\times[1-A_{Dell\ EMC}]\}\times A_{FW4}. \qquad (4.19)$$

Співвідношення (4.8)–(4.19) пов’язані між собою аналітико-стохастичною залежністю і можуть бути використані для визначення комплексного показника ФБ W_{SCADA} (4.7) з урахуванням доступності кібернетичних та хмарних активів SCADA критичної інфраструктури.

На рис. 4.8 зображено результати моделювання із застосуванням розробленого аналітико-стохастичного апарату у вигляді тривимірної залежності комплексного показника ФБ W_{SCADA} від інтенсивності компрометації активів $\gamma_{км}$ та тривалості цільового фішингу $T_{цф}$ кібернетичних і хмарних активів системи SCADA КІ. На рис. 4.9 зображено результати обчислення ймовірності $P_{SCADA}(\gamma_{км})$ компрометації активів SCADA КІ за умови, що атака здійснюється за сценарієм, функціональна схема реалізації якого зображена на рис. 4.2.

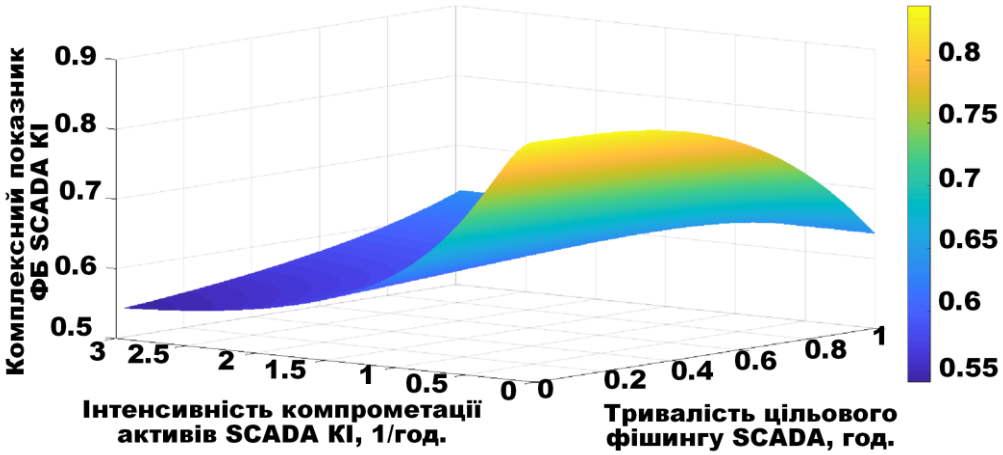


Рис. 4.8 Залежність $W_{SCADA}(\gamma_{км}, T_{цф})$ системи SCADA КІ

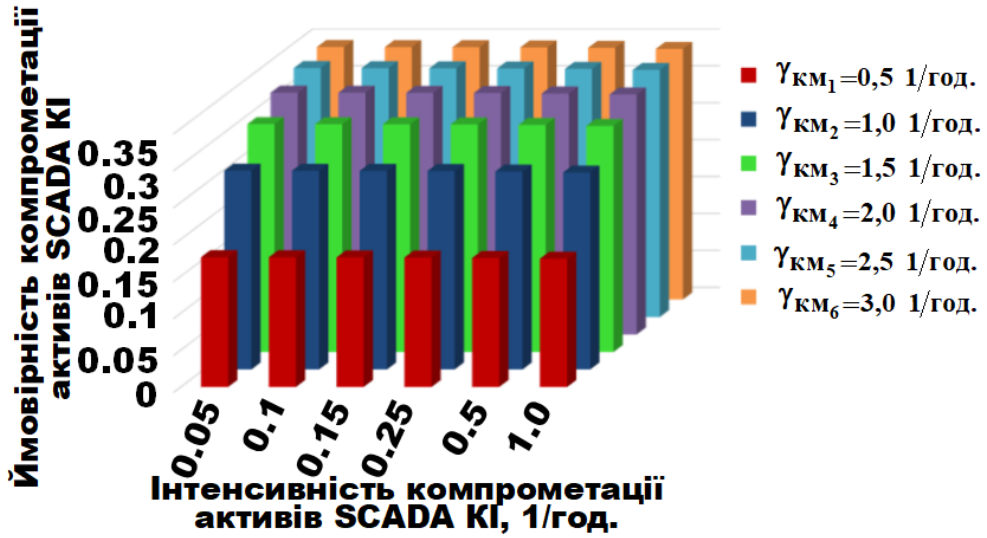


Рис. 4.9 Залежність $P_{SCADA}(\gamma_{км})$ системи SCADA КІ

Отримані результати моделювання (рис. 4.8) підтверджують доцільність застосування додаткових хмарних ресурсів для підтримання необхідного рівня

функційної безпечності SCADA КІ. Тим не менш, результати моделювання (рис. 4.9) водночас підтверджують, що зловмисні шкідливі впливи на основі реалізації процедури цільового фішингу майже на 35% підвищують ймовірність компрометації кібернетичних та хмарних активів SCADA критичної інфраструктури, суттєво знижуючи загальний рівень готовності системи.

4.2.3 Аналітико-стохастична модель гарантоздатності кібернетичних та хмарних активів критичної інфраструктури

У якості прикладу розглянемо яким чином можна побудувати та обчислити модель гарантоздатності КЕІ, враховуючи, що в структурі її системи управління є розподілення функцій енергоінфраструктури між фізичними, кібернетичними та хмарними активами SCADA. Розширити функції SCADA критичної енергетичної інфраструктури щодо аварійного відновлення, резервного копіювання та зберігання інформації вважається можливим шляхом застосування хмарних систем. Залучення активів системи SCADA щодо виконання основних функцій критичної енергетичної інфраструктури представлено в табл. 4.2.

Таблиця 4.2

Залучення активів системи SCADA щодо виконання основних функцій КЕІ

Функції КЕІ	Активи SCADA КЕІ		
	ФА	КА	ХМА
Транспортування	+	+	–
Розподілення	+	+	+
Споживання	–	+	+

В табл. 4.3 представлено результати порівняльного аналізу можливостей різних типів активів, які входять до складу КЕІ щодо виконання аварійного відновлення, резервного копіювання та зберігання інформації. На підставі виконаного аналізу розширюються можливості щодо побудови аналітико-стохастичної моделі готовності кібернетичних та хмарних активів SCADA критичної енергетичної інфраструктури, яка враховує як різноманітні відмови, так і ЗВШВ.

Таблиця 4.3

Аналіз можливостей активів КЕІ, ХМС та SCADA

Типи активів систем та інфраструктур		Функції відновлення та зберігання інформації		
		Аварійне відновлення	Резервне копіювання	Зберігання інформації
КЕІ	ФА	–	–	–
	КА	–	+	+
ХМС	ФА	–	+	–
	КА	+	+	+
SCADA КЕІ з ХМС	ФА	–	+	–
	КА	+	+	+

Будемо вважати, що на систему SCADA КЕІ, архітектура якої представлена на рис. 4.3, здійснюється атака за певним сценарієм з використанням ЗВШВ на її фізичні та кібернетичні активи. Припустимо, що у відповідності зі сценарієм, враховуючи результати відомого досвіду ЗВШВ на фізичні та кібернетичні активи національної критичної енергоінфраструктури [13], атака реалізується в декілька етапів, а саме:

1) на першому етапі здійснюється цільовий фішинг (ЦФ);

2) на другому етапі можливе розкриття інформації (РЗІ) внаслідок здійснення ЦФ;

3) на третьому етапі система може бути цілковито скомпрометована за рахунок фальсифікації (ФСФ) та підміни інформації (ПДМ).

Вочевидь, щоб розробити ефективні заходи кіберзахисту від ЗВШВ, попередньо необхідно створити теоретичний базис реалізації атаки на кібернетичні та хмарні активи КЕІ. На думку автора у якості математичного апарату варто застосовувати теорію бінарних відношень [145, 146]. Згідно з розв’язуваємим завданням досить зручно встановлювати відповідність між елементами $a \in \mathrm{A}$, $b \in \mathrm{B}$ та $c \in \mathrm{C}$ через їхні бінарні відношення, де $\mathrm{A} = \bigcup_{\mathrm{i} \in \mathrm{I}} a_{\mathrm{i}}$, $\mathrm{B} = \bigcup_{\mathrm{j} \in \mathrm{J}} b_{\mathrm{j}}$, $\mathrm{C} = \bigcup_{\mathrm{r} \in \mathrm{R}} c_{\mathrm{r}}$ є відповідними множинами

елементів. Наприклад, запис $\exists\, \rho \subset A \times B$ означає, що існує багатозначна функція ρ [147], яка деякому елементу a_i з множини A ставить у відповідність елемент b_j з множини B та задається як декартів добуток, тобто $A \times B = \{(a,b) | a \in A, b \in B\}$. Звідси, справедливим є твердження, якщо пара $(a_i, b_j) \in \rho$, то пара a_i та b_j знаходиться у відношенні ρ. Інакше кажучи, запис $a_i \rho b_j$ означає, що елементи a_i та b_j знаходяться у відношенні ρ. Отже, бінарне відношення $\rho \subset A \times B$ множин A та B розглядається як підмножина декартівого добутку $A \times B$. Аналогічно можна задати бінарне відношення $\sigma \subset B \times C$ множин C та B. Від загальної теорії перейдемо до розгляду прикладних аспектів дисертаційного дослідження.

Аналіз відомих кібератак на національну КЕІ [148] свідчить, що для досягнення загальної мети атака здійснюється в декілька етапів. При цьому спостерігається чітка послідовність виконання етапів та залежність наступних етапів кібератаки від попередніх. Припустимо, що на поточний момент часу завдяки ЦФ зловмисниками здійснено розкриття інформації. Ця обставина надає їм змогу поетапно реалізувати атаку, діаграма, якої зображена на рис. 4.10.

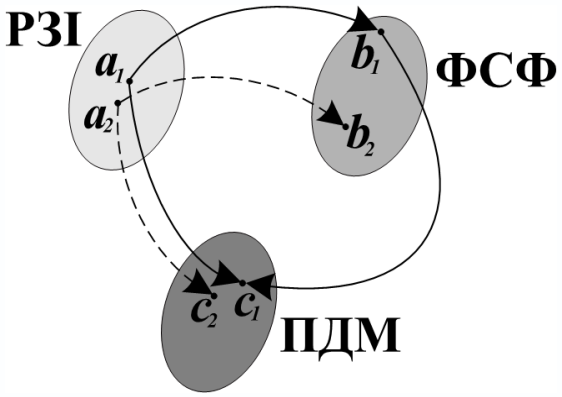


Рисунок 4.10 – Діаграма етапів реалізації кібератаки

Відповідно до зображеної діаграми (рис. 4.10) отримали переходи, які дають можливість класифікувати атаку за рівнем успішності ЗВШВ та ввести такі визначення.

Визначення 1. *Кібератака вважається атакою з високим рівнем*

успішності ЗВШВ, якщо реалізуються переходи РЗІ $\longrightarrow$ *ФСФ* $\longrightarrow$ *ПДМ та РЗІ* $\longrightarrow$ *ПДМ (позначені суцільною лінією).*

Визначення 2. *Кібератака вважається атакою з середнім рівнем успішності ЗВШВ, якщо реалізуються переходи РЗІ* $\longrightarrow$ *ФСФ та РЗІ* $\longrightarrow$ *ПДМ (позначені пунктирною лінією).*

Визначення 3. *Кібератака вважається атакою з низьким рівнем успішності ЗВШВ, якщо реалізуються переходи РЗІ* $\longrightarrow$ *ФСФ або РЗІ* $\longrightarrow$ *ПДМ (позначені пунктирною лінією).*

У той же час, спираючись на відомий досвід кібератак на КЕІ, треба розуміти, що без виконання початкового етапу РЗІ наступні етапи фальсифікації та підміни інформації реалізувати неможливо. В табл. 4.4 наведено формалізми на основі бінарних відношень, які описують етапи реалізації кібератак на КБА системи SCADA КІ.

Таблиця 4.4

Бінарні відношення, які описують етапи реалізації кібератак на КБА системи SCADA КІ

Переходи етапів реалізації кібератаки	Бінарні відношення
РЗІ $\longrightarrow$ ФСФ	$\rho \subset A \times B \longleftrightarrow \rho = \{(a,b) \mid a \in \rho, b \in \rho\}$
ФСФ $\longrightarrow$ ПДМ	$\sigma \subset B \times C \longleftrightarrow \sigma = \{(b,c) \mid b \in \sigma, c \in \sigma\}$
РЗІ $\longrightarrow$ ПДМ	$\delta \subset A \times C \longleftrightarrow \delta = \{(a,c) \mid a \in \delta, c \in \delta\}$

Застосовуючи діаграму (рис.4.10), визначення 1–3 та формалізми, які наведено в табл. 4.4, сформулюємо і доведемо такі теореми.

Теорема 1. *Необхідною та достатньою умовою для реалізації кібератаки з високим рівнем успішності на кібернетичні активи критичної інфраструктури є виконання умови транзитивності бінарних відношень відповідних переходів.*

Доведення. На рис. 4.10 переходи РЗІ $\longrightarrow$ ФСФ, ФСФ $\longrightarrow$ ПДМ та

РЗІ $\longrightarrow$ ПДВ (позначені суцільною лінією) між собою поєднані. Тоді, застосовуючи формалізми табл. 4.4, отримаєм добуток бінарних відношень ρ та σ у вигляді [146, 149]

$$\rho \circ \sigma = \underset{(a,b)}{\mathrm{C}} \underset{c}{\mathrm{V}} (a,b) \in \rho \wedge (b,c) \in \sigma = (a,c),$$

де $\underset{(a,b)}{\mathrm{C}}$ – класифікатор або символ абстракції по змінним a та b; $\underset{c}{\mathrm{V}}$ – квантор існування по змінній c.

Як результат отримали рівняння $\rho \circ \sigma = \delta = (a,c)$, яке свідчить, що утворена множина $\mathrm{G} = \{(a,b),(b,c),(a,c)\}$ відповідає транзитивному бінарному відношенню. ■

Теорема 2. *Необхідною та достатньою умовою для реалізації кібератаки з середнім рівнем успішності на кібернетичні активи критичної інфраструктури є не виконання умови транзитивності бінарних відношень відповідних переходів.*

Доведення. На рис. 4.10 переходи РЗІ $\longrightarrow$ ФСФ та РЗІ $\longrightarrow$ ПДВ (позначені пунктирною лінією) між собою не поєднуються, що підтверджує не виконання умови транзитивності. Тоді, застосовуючи формалізми табл. 4.4, отримаєм добуток бінарних відношень ρ та δ у вигляді [149]

$$\rho \Delta_1 \delta = \underset{(a,(b,c))}{\mathrm{C}} (a,b) \in \rho \wedge (a,c) \in \delta \neq \rho \circ \delta .$$

Як результат отримали нерівняння, яке свідчить, що умова транзитивності бінарних відношень не виконується.

Після отримання зазначеного теоретичного базису перейдемо до побудови діаграм зловмисних шкідливих впливів. На рис. 4.11–4.15 зображено діаграми зловмисних шкідливих впливів на фізичні та кібернетичні активи системи SCADA КЕІ, які реалізуються згідно описаного сценарію. Слід зазначити, що на діаграмах ЗВШВ перший, другий, третій кластери, які позначено як Clusters 1–3, утворюються шляхом об’єднання елементів мережі контролю та оперативного моніторингу станів (рис. 4.3) КЕІ та системи SCADA. Всього передбачається розглянути п’ять можливих сценаріїв здійснення ЗВШВ. Відповідно на рис. 4.12–4.15 відображено діаграми для

першого сценарію. Характеристика видів ЗВШВ представлена в табл. 4.5. Загальний аналіз наслідків ЗВШВ на активи системи SCADA КЕІ з урахуванням перших чотирьох зазначених сценаріїв наведено в додатку Д; характеристика п'ятого сценарія (рис. 4.16) представлена в табл. 4.6.

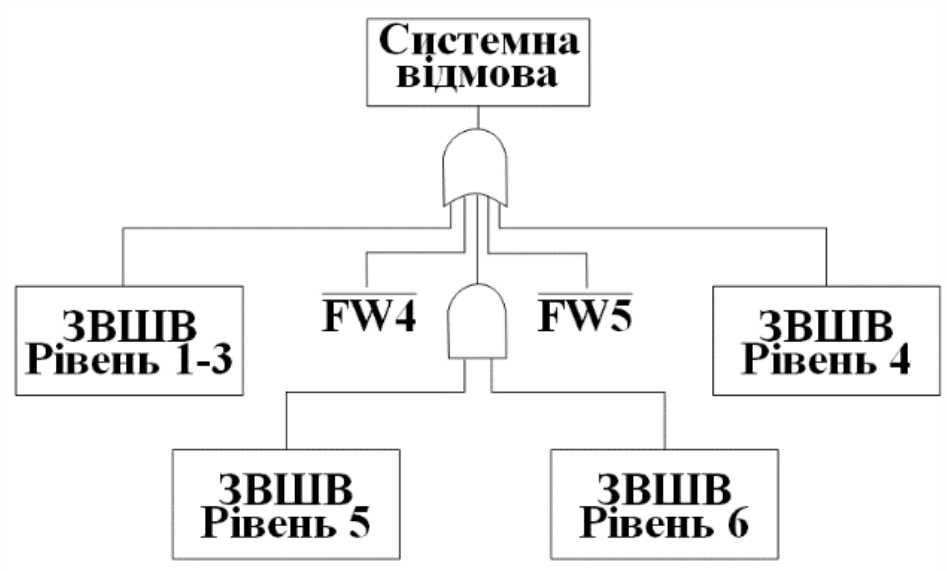


Рис. 4.11 Діаграма ЗВШВ на фізичні та КБА активи системи SCADA КЕІ

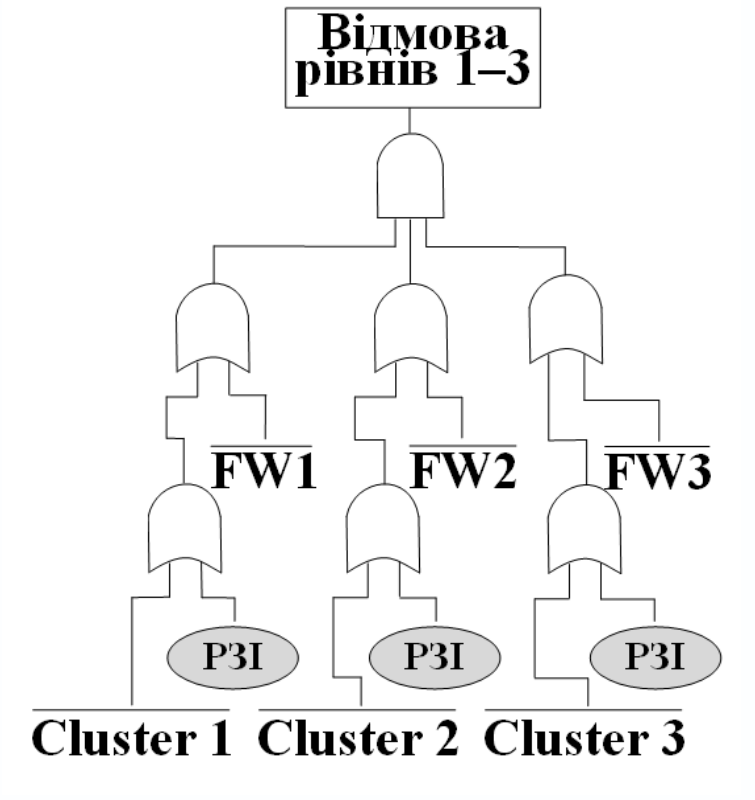


Рис 4.12 Діаграма ЗВШВ на перший, другий та третій мережеві рівні SCADA КЕІ

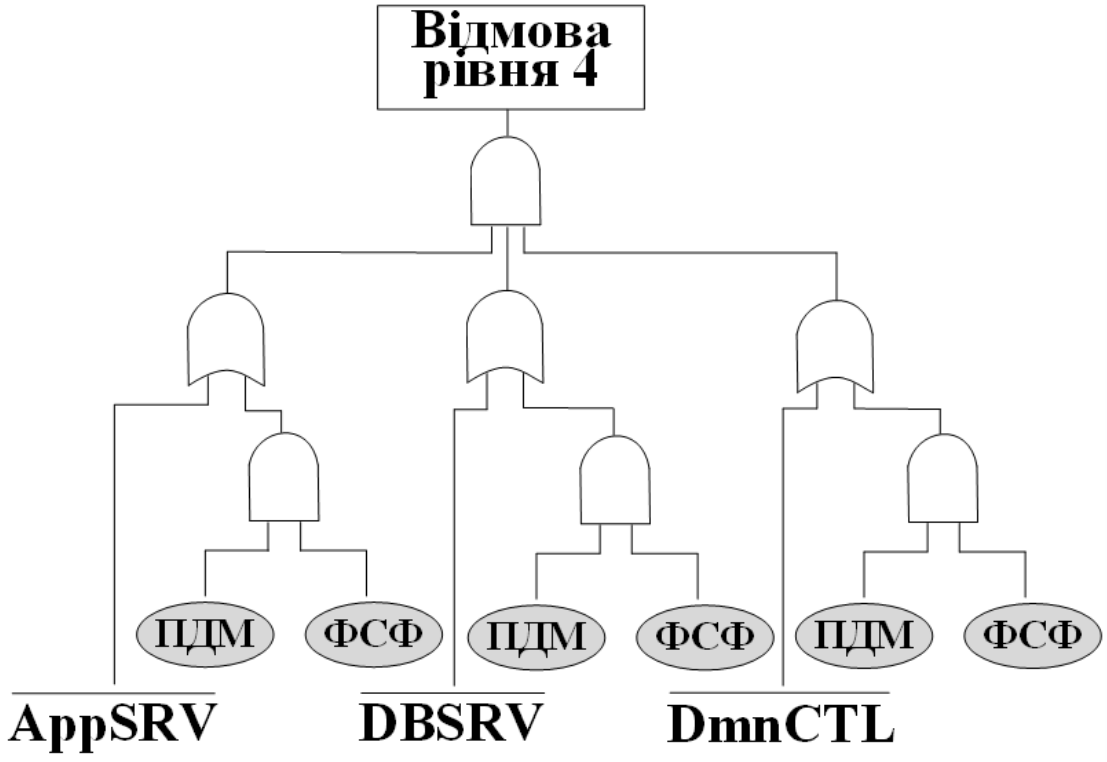


Рис. 4.13 Діаграма ЗВШВ на четвертий мережевий рівень SCADA KEI

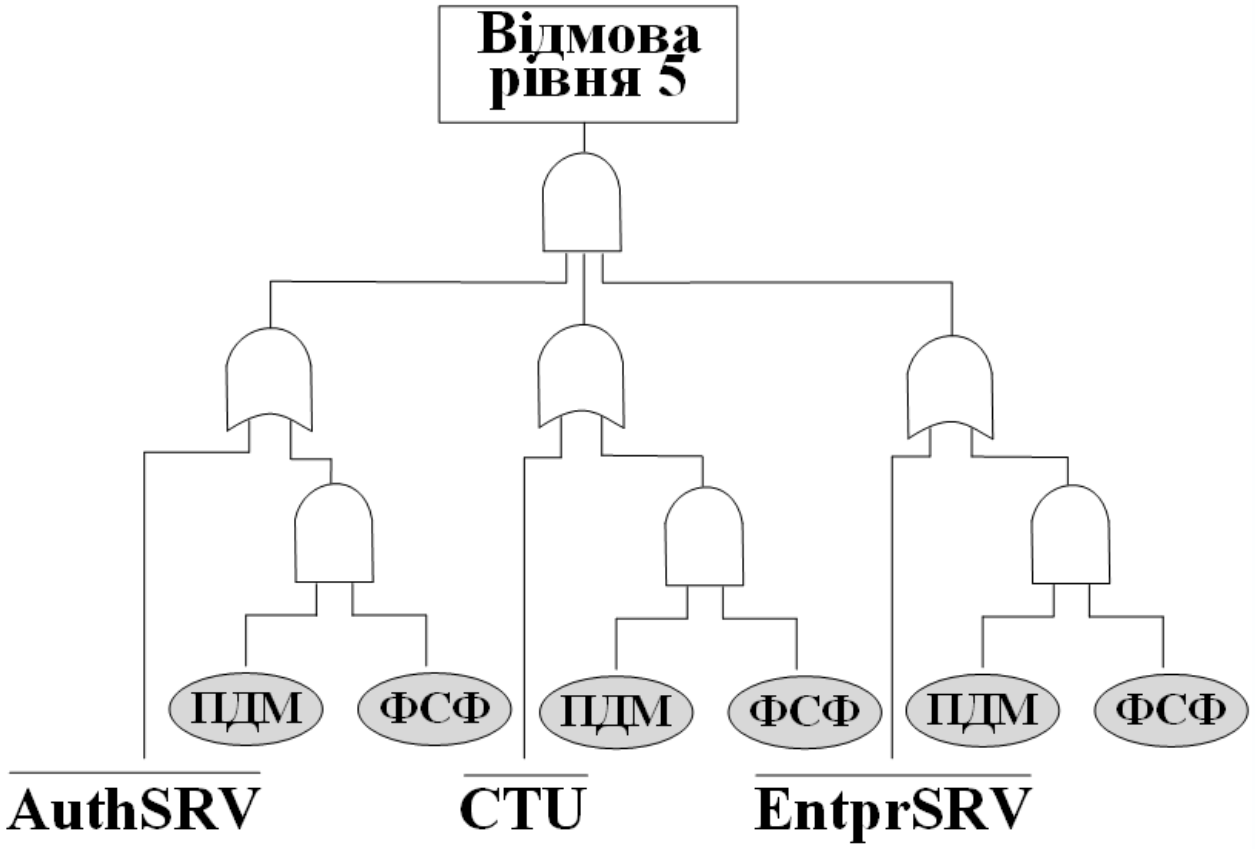


Рис. 4.14 Діаграма ЗВШВ на п’ятий мережевий рівень SCADA KEI

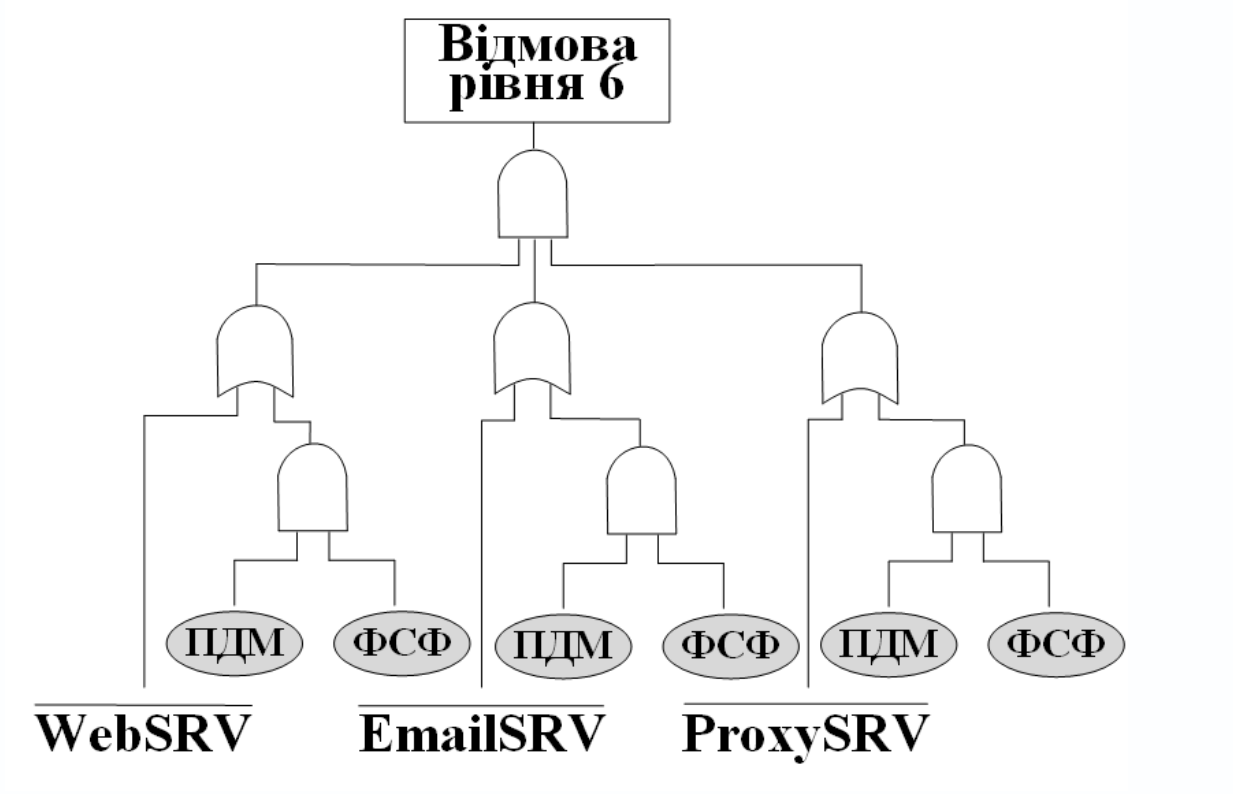


Рис. 4.15 Діаграма ЗВШВ на шостий мережевий рівень SCADA КЕІ

Таблиця 4.5

Характеристика видів ЗВШВ на активи системи SCADA КЕІ

Вид ЗВШВ	Загальна характеристика
Розкриття інформації	1. Здійснюється ЦФ шляхом збору, обробки та аналізу службової інформації корпоративних мереж КЕІ, включаючи моніторинг інформації, яка курсує у вхідних каскадах мережевих рівнів системи SCADA. 2. Виконується ЦФ електронної пошти керівників підрозділів КЕІ. 3. Здійснюється крадіжка облікових даних для доступу до системи SCADA КЕІ.
Фальсифікація інформації	1. За результатами ЦФ здійснюється всебічне вивчення системи SCADA, тобто вивчаються структурна побудова, програмне та апаратне забезпечення, навантаження і тому інше. 2. Розробка та впровадження вбудованого шкідливого програмного забезпечення для управління обладнанням компонентів КЕІ. 3. Викривлення інформації, яка курсує в інфокомунікаційних системах мережевого рівня SCADA КЕІ.

Продовження таблиці 4.5

Вид ЗВШВ	Загальна характеристика
Підміна інформації	1. Проникнення в серверні системи мережевого рівня SCADA КЕІ. 2. Інформація управління викривляється та повністю замінюється неправдивою інформацією. 3. Повна компрометація системи за рахунок доступу до інформаційного ресурсу. 4. Команди управління обслуговуючого персоналу системи SCADA замінюються на шкідливі команди зловмисників за рахунок чого здійснюється синхронізоване дистанційне відключення компонентів КЕІ. 5. Комплексні зловмисні шкідливі впливи, які реалізуються у вигляді: віддаленого відключення резервних блоків живлення пунктів управління компонентами КЕІ; одночасних фейкових телефонних дзвінків, які відволікають та ускладнюють роботу операторів та обслуговуючого персоналу системи SCADA КЕІ; розгортання бот мережі, що знищує дані необхідні для управління обладнанням.

Таблиця 4.6

Характеристика п’ятого сценарія ЗВШВ на активи SCADA КЕІ

Вид ЗВШВ	Компоненти, на які направлена дія ЗВШВ	Наслідки ЗВШВ	Рівень успішності ЗВШВ
Розкриття інформації	Програмовані логічні контролери, протиаварійне захисне обладнання, сенсорні модулі, людино-машинні інтерфейси, які утворюють пер-ший, другий, третій кластери мережі контролю та оперативного моніторингу, ХМС AWS, які утворюють хмарні активи SCADA КЕІ	Отримання доступу до інформаційного ресурсу та ХМА системи SCADA КЕІ, реалізація функцій аварій-ного відновлювання і резервного копіювання неможлива	Високий

Продовження таблиці 4.6

Вид ЗВШВ	Компоненти, на які направлена дія ЗВШВ	Наслідки ЗВШВ	Рівень успішності ЗВШВ
Фальсифікація інформації	Серверні та інфокомуніка-ційні системи, контролери доменів, комп'ютерні термінали четвертого, п'ятого, шостого мере-жевих рівнів, хмарні активи SCADA КЕІ	Викривлення даних контуру управління КІ з застосу-ванням інформацій-ного ресурсу КБА та ХМА системи SCADA КЕІ, реалізація функцій аварій-ного відновлювання і резервного копіювання не-можлива	Високий
Підміна інформації	Серверні та інфокомуніка-ційні системи, контролери доменів, комп'ютерні термінали четвертого, п'ятого, шостого мереже-вих рівнів, хмарні системи AWS, які утворюють хмарні активи SCADA КЕІ	Компрометація системи, заміна вірогідних даних неправдивими, застосування зловмисниками кібернетич-них та хмарних активів SCADA для відключення компонентів КЕІ з блокуванням дій обслуго-вуючого персоналу, реаліза-ція функцій аварійного відновлювання і резервного копіювання неможлива	Високий

Для подальшої розбудови аналітико-стохастичної моделі та отримання результатів моделювання необхідно розглянути чотири важливих припущення, які стосуються узгодженості сценаріїв реалізації ЗВШВ з архітектурною побудовою активів системи SCADA КЕІ і урахуванням відповідних мережевих рівнів, а саме:

1) перший сценарій ЗВШВ реалізується для архітектури системи SCADA КЕІ, до складу якої не входять хмарні активи;

2) другий, третій, четвертий, п'ятий сценарії ЗВШВ реалізуються для перспективної архітектури фізичних, кібернетичних та хмарних активів системи SCADA КЕІ, яку відображено на рис. 4.3;

3) функції аварійного відновлювання та резервного копіювання дозволяють

повністю усунути наслідки ЗВШВ;

4) коефіцієнт готовності ХМС по шкалі HAL задається не менше ніж 0,9999 [150].

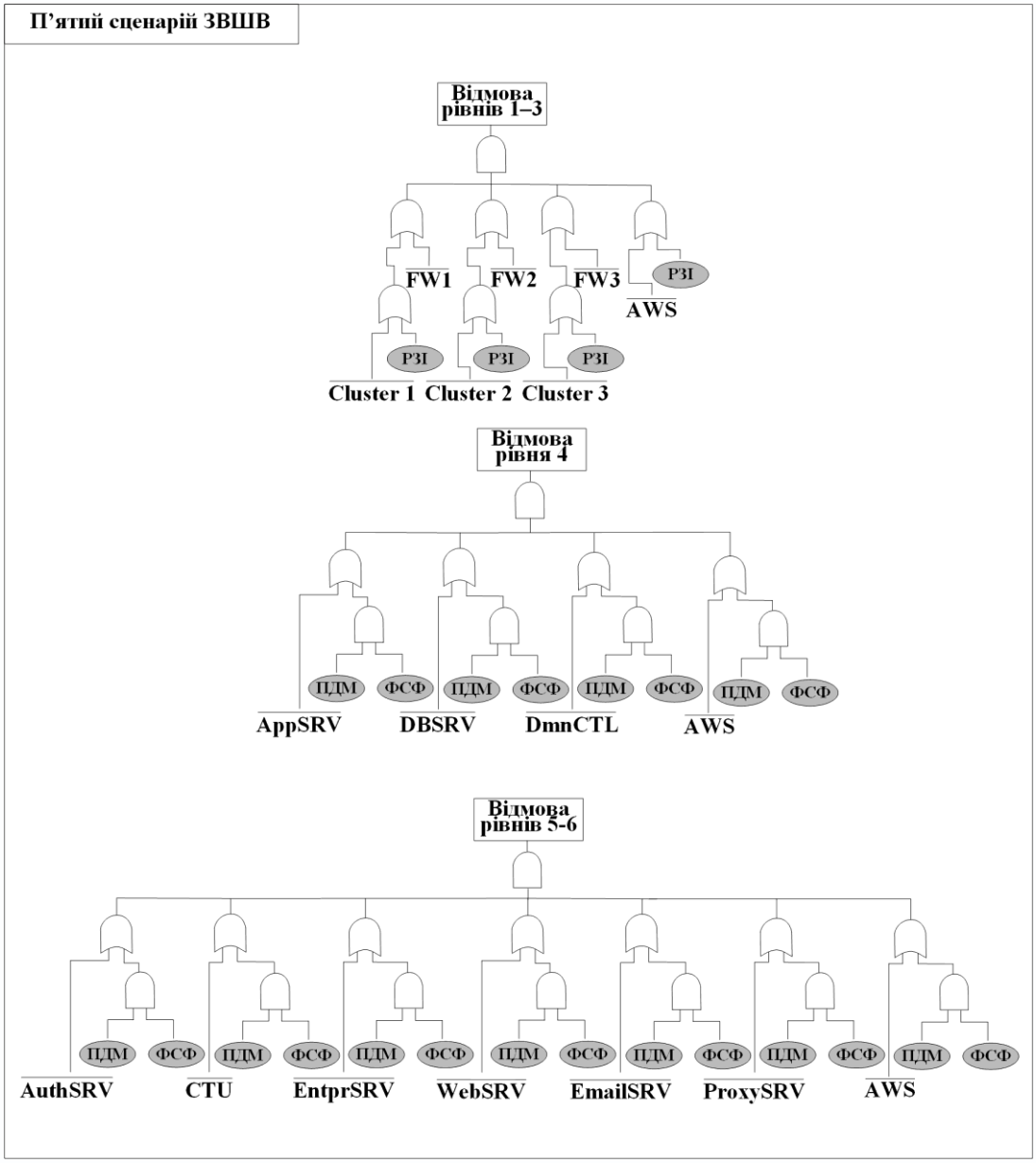


Рис. 4.16 П'ятий сценарій ЗВШВ на активи системи SCADA КЕІ

Відповідно до рис. 4.11–4.15 ймовірність складної події, яка полягає в неготовності активів системи SCADA КЕІ за результатами реалізації першого сценарію ЗВШВ, можна записати наступним чином [132]:

$$\text{UnAvailability} = P\left(\Phi\left(X\right)=0\right) = P\left\{UA_{1-3_j} \cup UA_{4_j} \cup \left[UA_{5_j} \cap UA_{6_j}\right] \cup \right.$$

$$\left. \cup \overline{FW4} \cup \overline{FW5}\right\}, \qquad (4.20)$$

$$UA_{1-3_1} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$

$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\}, \quad (4.21)$$

$$UA_{4_1} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$

$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\}, \quad (4.22)$$

$$UA_{5_1} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$

$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\}, \quad (4.23)$$

$$UA_{6_1} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$

$$\cap \left\{\overline{ProxySRV} \cup \left[TI \cap SI\right]\right\}, \quad (4.24)$$

де ID – подія, яка полягає в реалізації ЗВШВ у вигляді РЗІ; TI – подія, яка полягає в реалізації ЗВШВ у вигляді ФСФ; SI – подія, яка полягає в реалізації ЗВШВ у вигляді ПДМ; *j* – номер відповідного сценарію ЗВШВ.

Відповідно до рис. 4.16 ймовірність складної події, яка полягає в неготовності активів системи SCADA КЕІ за результатами реалізації п’ятого сценарію ЗВШВ, можна визначити як

$$UA_{1-3_4} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$

$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\} \cap \left\{\overline{AWS} \cup ID\right\}, \quad (4.25)$$

$$UA_{4_4} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$

$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (4.26)$$

$$UA_{5_4} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$

$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{AWS} \cup \left[TI \cap SI\right]\right\}, \quad (4.27)$$

$$UA_{6_4} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$

$$\cap \left\{\overline{ProxySRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{AWS} \cup \left[TI \cap SI\right]\right\}. \quad (4.28)$$

Характеристика перших чотирьох сценаріїв ЗВШВ наведена в додатку Д. Керуючись пропозиціями, які надано в [132–134], та застосовуючи отримані вирази

(4.20)–(4.28), перейдемо від діаграм ЗВШВ на активи системи SCADA KEI (рис. 4.11–4.15) до її структурних схем безпеки. На рис. 4.17 зображено ССБ для п’ятого сценарію ЗВШВ на активи системи SCADA KEI.

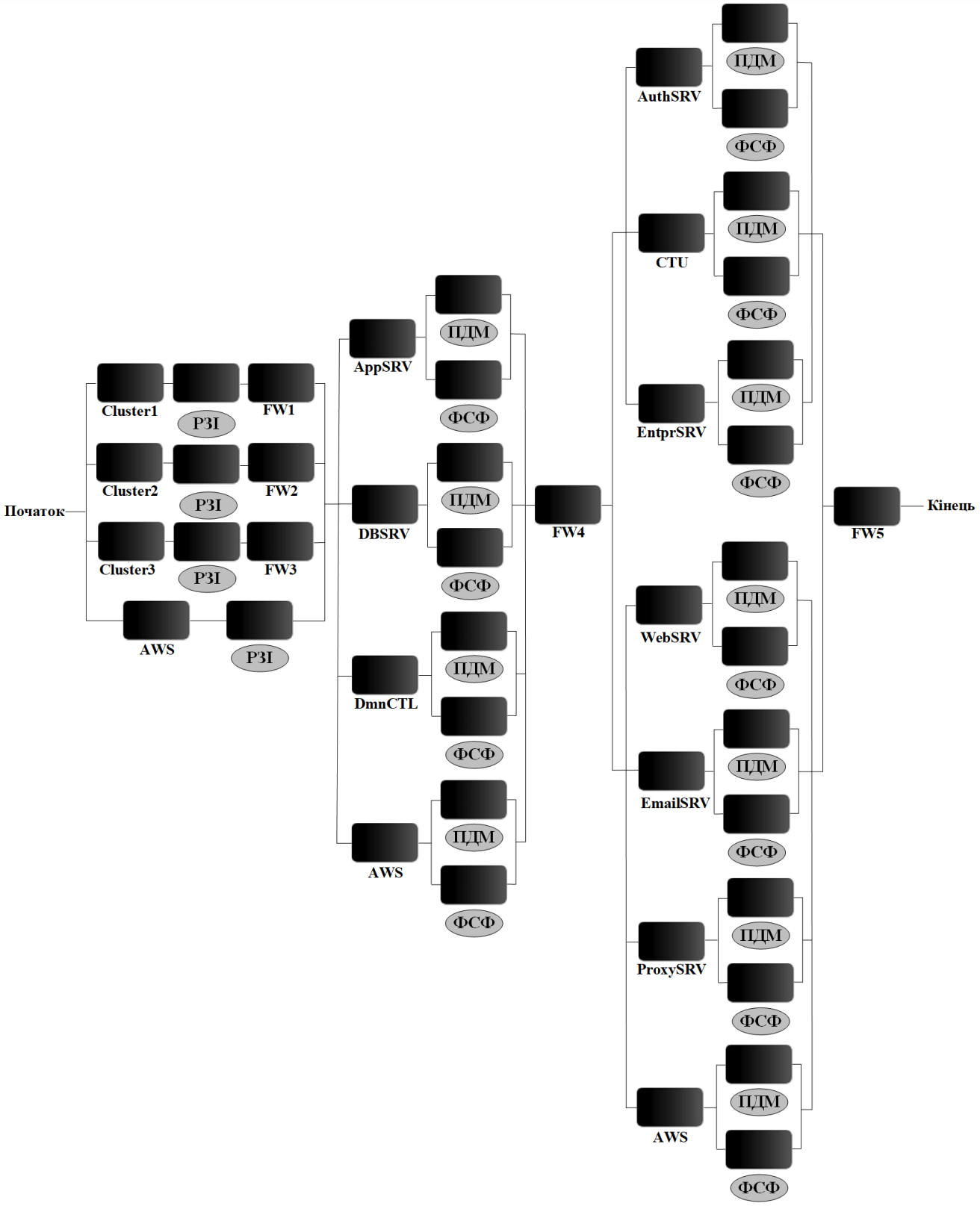


Рис. 4.17 ССБ системи SCADA KEI для п’ятого сценарію ЗВШВ

У якості комплексного показника гарантоздатності активів системи SCADA КЕІ пропонується застосовувати стаціонарний коефіцієнт готовності (СКГ), обгрунтування доцільності використання якого представлено в роботах [132, 134, 151]. В загальному вигляді, враховуючи приведені варіанти архітектурної реалізації (рис. 4.3), значення СКГ системи SCADA КЕІ за умови дії ЗВШВ визначається за допомогою співвідношення:

$$K_{SCADA}^{DMI} = K_{SCADA_1}^{DMI} K_{SCADA_2}^{DMI} K_{SCADA_3}^{DMI} A_{FW_4} A_{FW_5}, \quad (4.29)$$

де $K_{SCADA_1}^{DMI}$ – СКГ першого, другого, третього кластерів SCADA КЕІ; $K_{SCADA_2}^{DMI}$ – СКГ четвертого мережевого рівня SCADA КЕІ; $K_{SCADA_3}^{DMI}$ – СКГ п’ятого та шостого мережевих рівнів SCADA КЕІ; A_{FW_4}, A_{FW_5} – СКГ четвертого та п’ятого брандмауерів, відповідно.

В співвідношенні (4.29) перші три складові визначаються за результатами напівмарковського моделювання ЗВШВ на кібернетичні та хмарні активи SCADA КЕІ. Решта вхідних даних для компонентів SCADA задається у відповідності з процедурою параметризації, яка описана в роботах [132, 134]. Розглянемо основні аналітичні співвідношення, що відображають специфіку реалізації конкретного сценарію ЗВШВ і використовуються для оцінки відповідних складових.

Згідно з ССБ системи SCADA КЕІ для першого сценарію ЗВШВ (додаток Д) стаціонарний коефіцієнт готовності визначається за допомогою наступних виразів:

$$K_{SCADA_1}^{DMI} = 1 - \overline{K}_{SCADA_1}^{DMI}, \quad (4.30)$$

$$\overline{K}_{SCADA_1}^{DMI} = \overline{K}_{SCADA_{11}}^{DMI} \overline{K}_{SCADA_{12}}^{DMI} \overline{K}_{SCADA_{13}}^{DMI}, \quad (4.31)$$

$$\overline{K}_{SCADA_{11}}^{DMI} = 1 - K_{SCADA_{11}}^{DMI}, \ \overline{K}_{SCADA_{12}}^{DMI} = 1 - K_{SCADA_{12}}^{DMI}, \ \overline{K}_{SCADA_{13}}^{DMI} = 1 - K_{SCADA_{13}}^{DMI}, \quad (4.32)$$

$$K_{SCADA_{11}}^{DMI} = A_{Cluster1} A_{FW1} P_{ID}, \quad (4.33)$$

$$K_{SCADA_{12}}^{DMI} = A_{Cluster2} A_{FW2} P_{ID}, \quad (4.34)$$

$$K_{SCADA_{13}}^{DMI} = A_{Cluster3} A_{FW3} P_{ID}, \quad (4.35)$$

$$K_{SCADA_2}^{DMI} = 1 - \overline{K}_{SCADA_2}^{DMI}, \quad (4.36)$$

$$\overline{K}^{DMI}_{SCADA_2} = \overline{K}^{DMI}_{SCADA_{21}} \overline{K}^{DMI}_{SCADA_{22}} \overline{K}^{DMI}_{SCADA_{23}}, \quad (4.37)$$

$$\overline{K}^{DMI}_{SCADA_{21}} = 1 - K^{DMI}_{SCADA_{21}}, \ \overline{K}^{DMI}_{SCADA_{22}} = 1 - K^{DMI}_{SCADA_{22}}, \ \overline{K}^{DMI}_{SCADA_{23}} = 1 - K^{DMI}_{SCADA_{23}}, \quad (4.38)$$

$$K^{DMI}_{SCADA_{21}} = A_{AppSRV} K^{DMI}_{SCADA_{211}}, \ K^{DMI}_{SCADA_{211}} = 1 - \overline{P}_{TI} \overline{P}_{SI}, \ \overline{P}_{TI} = 1 - P_{TI}, \ \overline{P}_{TI} = 1 - P_{SI}, \quad (4.39)$$

$$K^{DMI}_{SCADA_{22}} = A_{DBSRV} K^{DMI}_{SCADA_{221}}, \ K^{DMI}_{SCADA\ 221} = K^{DMI}_{SCADA\ 211}, \quad (4.40)$$

$$K^{DMI}_{SCADA_{23}} = A_{DmnCTL} K^{DMI}_{SCADA_{231}}, \ K^{DMI}_{SCADA\ 231} = K^{DMI}_{SCADA\ 211}, \quad (4.41)$$

$$K^{DMI}_{SCADA_3} = 1 - \overline{K}^{DMI}_{SCADA_3}, \quad (4.42)$$

$$\overline{K}^{DMI}_{SCADA_3} = \overline{K}^{DMI}_{SCADA_{31}} \overline{K}^{DMI}_{SCADA_{32}} \overline{K}^{DMI}_{SCADA_{33}} \overline{K}^{DMI}_{SCADA_{34}} \overline{K}^{DMI}_{SCADA_{35}} \overline{K}^{DMI}_{SCADA_{36}}, \quad (4.43)$$

$$\overline{K}^{DMI}_{SCADA_{31}} = 1 - K^{DMI}_{SCADA_{31}}, \ \overline{K}^{DMI}_{SCADA_{32}} = 1 - K^{DMI}_{SCADA_{32}}, \ \overline{K}^{DMI}_{SCADA_{33}} = 1 - K^{DMI}_{SCADA_{33}}, \quad (4.44)$$

$$\overline{K}^{DMI}_{SCADA_{34}} = 1 - K^{DMI}_{SCADA_{34}}, \ \overline{K}^{DMI}_{SCADA_{35}} = 1 - K^{DMI}_{SCADA_{35}}, \ \overline{K}^{DMI}_{SCADA_{36}} = 1 - K^{DMI}_{SCADA_{36}}, \quad (4.45)$$

$$K^{DMI}_{SCADA_{31}} = A_{AuthSRV} K^{DMI}_{SCADA_{311}}, \ K^{DMI}_{SCADA\ 311} = K^{DMI}_{SCADA\ 211}, \quad (4.46)$$

$$K^{DMI}_{SCADA_{32}} = A_{CTU} K^{DMI}_{SCADA_{321}}, \ K^{DMI}_{SCADA\ 321} = K^{DMI}_{SCADA\ 211}, \quad (4.47)$$

$$K^{DMI}_{SCADA_{33}} = A_{EntprSRV} K^{DMI}_{SCADA_{331}}, \ K^{DMI}_{SCADA\ 331} = K^{DMI}_{SCADA\ 211}, \quad (4.48)$$

$$K^{DMI}_{SCADA_{34}} = A_{WebSRV} K^{DMI}_{SCADA_{341}}, \ K^{DMI}_{SCADA\ 341} = K^{DMI}_{SCADA\ 211}, \quad (4.49)$$

$$K^{DMI}_{SCADA_{35}} = A_{EmailSRV} K^{DMI}_{SCADA_{351}}, \ K^{DMI}_{SCADA\ 351} = K^{DMI}_{SCADA\ 211}, \quad (4.50)$$

$$K^{DMI}_{SCADA_{36}} = A_{ProxySRV} K^{DMI}_{SCADA_{361}}, \ K^{DMI}_{SCADA\ 361} = K^{DMI}_{SCADA\ 211}, \quad (4.51)$$

де P_{ID} – ймовірність ПРС відповідної ресурсної компоненти, яка входить до складу кібернетичних або хмарних активів системи SCADA КЕІ, за умови, що здійснюється ЗВШВ у вигляді РЗІ (табл. 4.5, 4.6); P_{TI} – ймовірність ПРС відповідної ресурсної компоненти, яка входить до складу кібернетичних або хмарних активів системи SCADA КЕІ, за умови, що здійснюється ЗВШВ у вигляді ФСФ (табл. 4.5, 4.6); P_{SI} – ймовірність ПРС відповідної ресурсної компоненти, яка входить до складу кібернетичних або хмарних активів системи SCADA КЕІ, за умови, що здійснюється ЗВШВ у вигляді ПДМ (табл. 4.5, 4.6).

Для отримання оцінки комплексного показника гарантоздатності

кібернетичних та хмарних активів системи SCADA КЕІ згідно співвідношень (4.30)–(4.51) на основі реалізації напівмарковського процесу розроблено відповідний алгоритм. На рис. 4.18 зображено розмічений граф станів напівмарковської моделі з виродженими станами, яка була розроблена в [111], інтерпретована та модифікована в [152] і застосована в дисертаційному дослідженні для визначення імовірнісних оцінок ЗВШВ, коли здійснюється розкриття та фальсифікація інформації. Для напівмарковського моделювання ЗВШВ, коли здійснюється підміна інформації на основі попередньо виконаного цільового фішингу, застосовується НПММ, граф станів якої зображено на рис. 4.6. Процес побудови та обчислення вказаних НПММ з урахуванням необхідних формальних ознак описано в роботах [111, 138, 152]. На рис. 4.19 зображено відповідні імовірносні залежності реалізації зазначених типів ЗВШВ, які отримано за результатами напівмарковського моделювання.

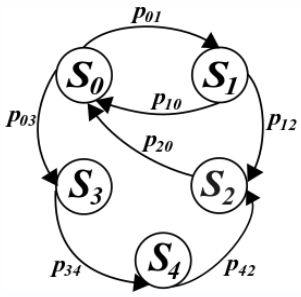


Рис. 4.18 Граф станів напівмарковської моделі зловмисного шкідливого впливу у вигляді РЗІ та ФСФ на активи системи SCADA КЕІ

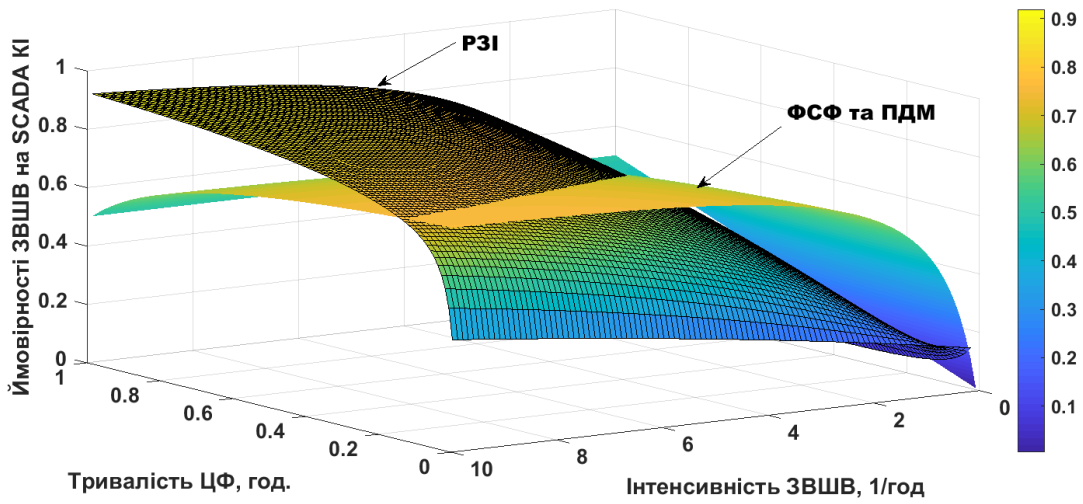


Рис 4.19 Залежності ймовірності реалізації зловмисного шкідливого впливу у вигляді РЗІ, ФСФ та ПДМ для активів системи SCADA КЕІ

Обчислення комплексного показника гарантоздатності (4.29) виконувалися згідно з загально відомими методами. Результати моделювання для отриманих п’ятьох сценаріїв ЗВШВ зображено на рис. 4.20–4.22. При відображенні результатів моделювання (рис. 4.20–4.22) значна увага приділялася визначенню залежностей між комплексним показником гарантоздатності кібернетичних, хмарних активів SCADA KEI та інтенсивністю ЗВШВ, тривалостями інтервалів часу, який витрачається на зміну кодових ключів і цільовий фішинг.

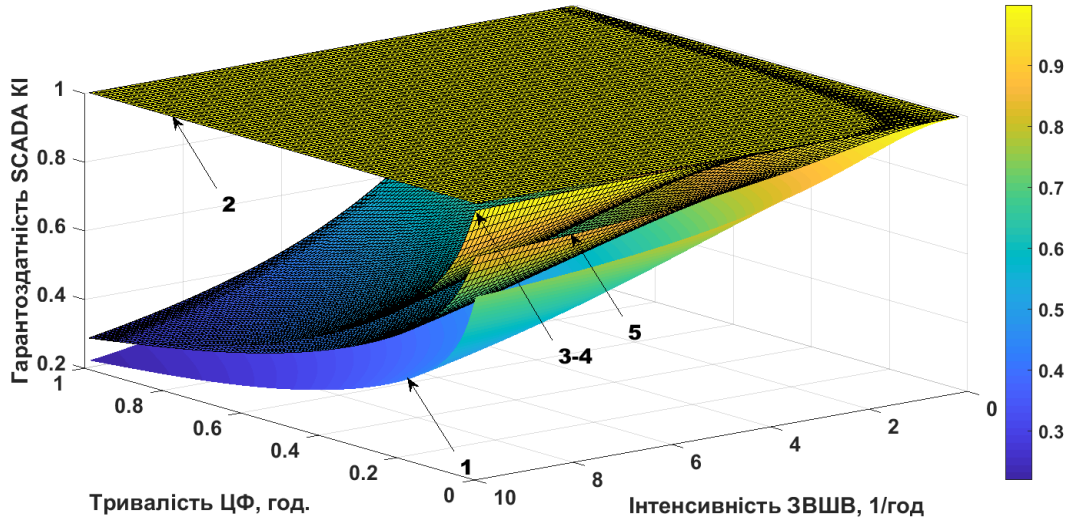


Рисунок 4.20 – Комплексний показник гарантоздатності активів SCADA KEI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну кодових ключів витрачається 3 хвилини

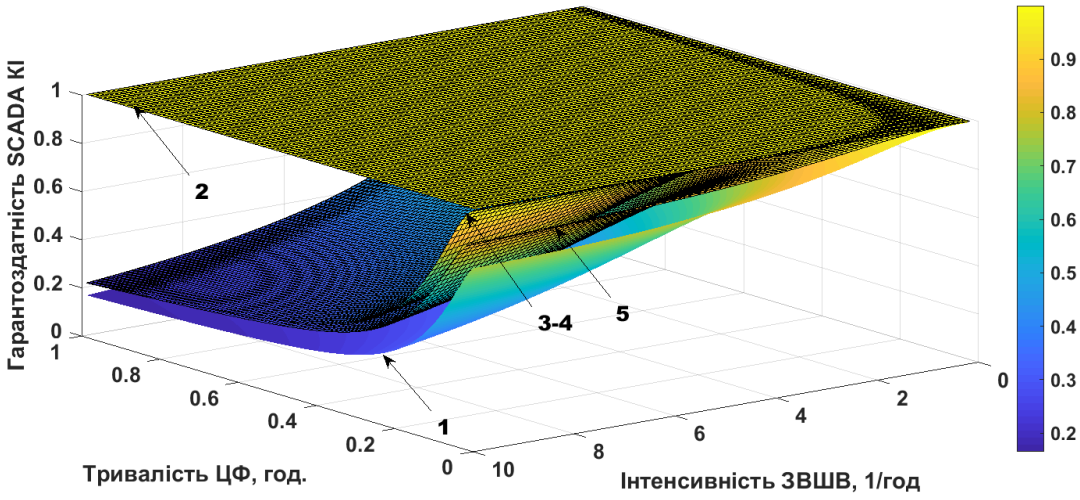


Рис. 4.21 Комплексний показник гарантоздатності активів SCADA KEI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну кодових ключів витрачається 30 хвилин

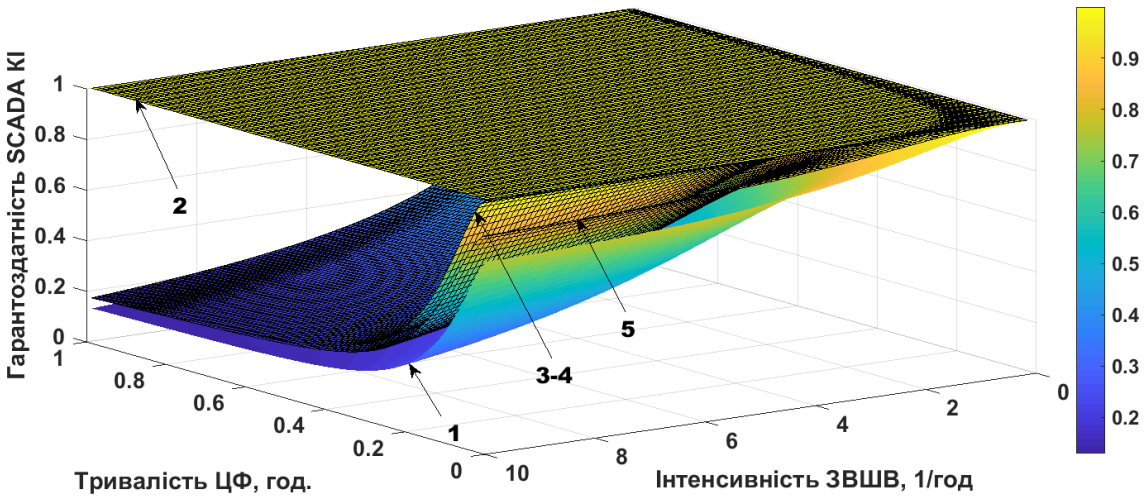


Рис. 4.22 Показник гарантоздатності активів SCADA KEI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну кодових ключів витрачається одна година

Динаміку зміни величини комплексного показника гарантоздатності для другого сценарію ЗВШВ (рис. 4.20–4.22) в залежності від інтенсивності зловмисного шкідливого впливу, тривалостей інтервалів часу, який витрачається на проведення цільового фішингу та зміну кодових ключів відображено на рис. 4.23.

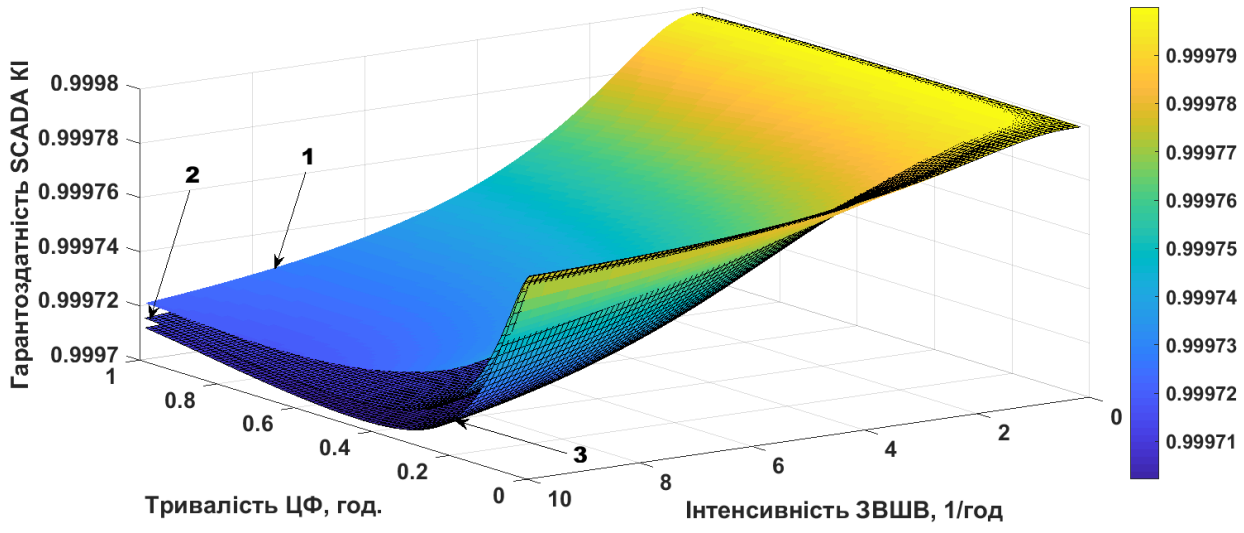


Рис. 4.23 Динаміка зміни величини комплексного показника гарантоздатності активів SCADA KEI для другого сценарію ЗВШВ за умови, що на зміну ключів витрачається: 1 – три хвилини; 2 – тридцять хвилин; 3 – одна година

Оцінимо виграш від використання хмарних систем при створенні хмарних активів SCADA критичної енергетичної інфраструктури з урахуванням дії зловмисних шкідливих впливів шляхом обчислення стаціонарного коефіцієнта неготовності (простою) по формулі

$$\overline{K}_{SCADA}^{DMI} = 1 - K_{SCADA}^{DMI}. \quad (4.52)$$

Результати обчислення стаціонарного коефіцієнта неготовності (СКНГ) кібернетичних та хмарних активів SCADA критичної енергетичної інфраструктури зображено на рис. 4.24–4.26.

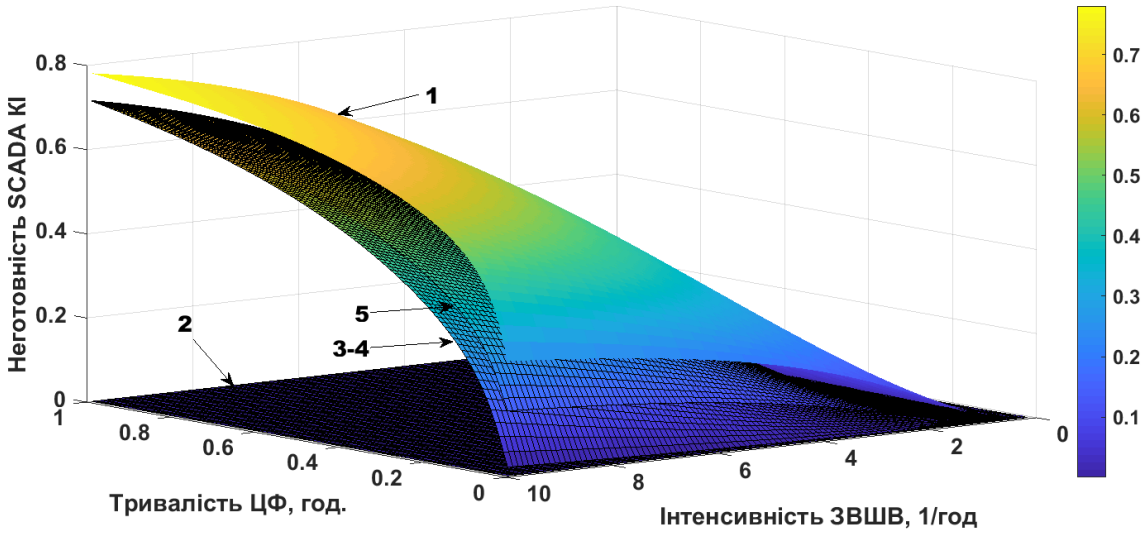


Рис. 4.24 Стаціонарний коефіцієнт неготовності активів SCADA KEI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну кодових ключів витрачається 3 хвилини

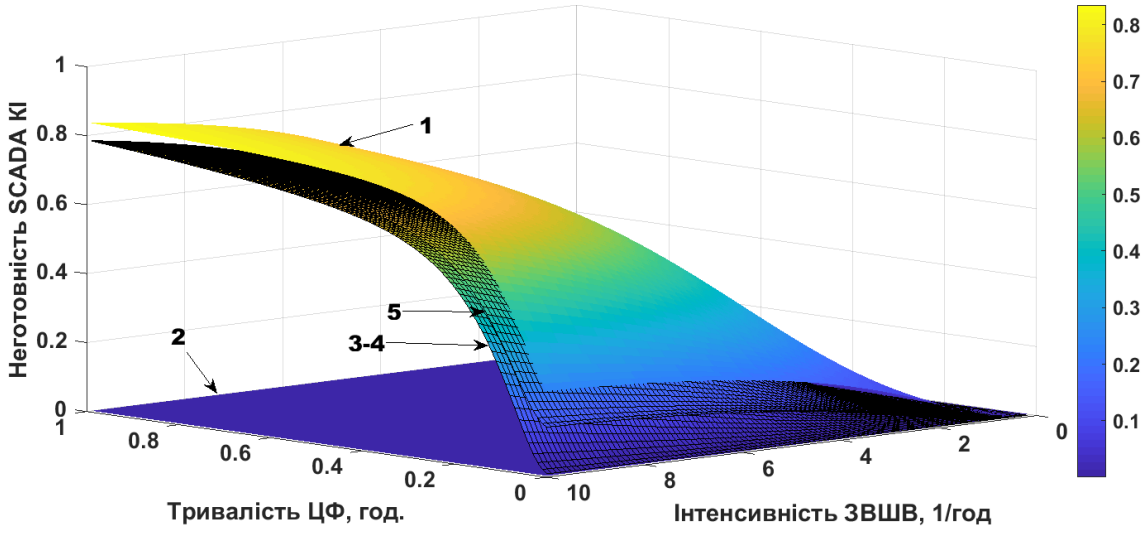


Рис. 4.25 Стаціонарний коефіцієнт неготовності активів SCADA KEI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається 30 хвилин

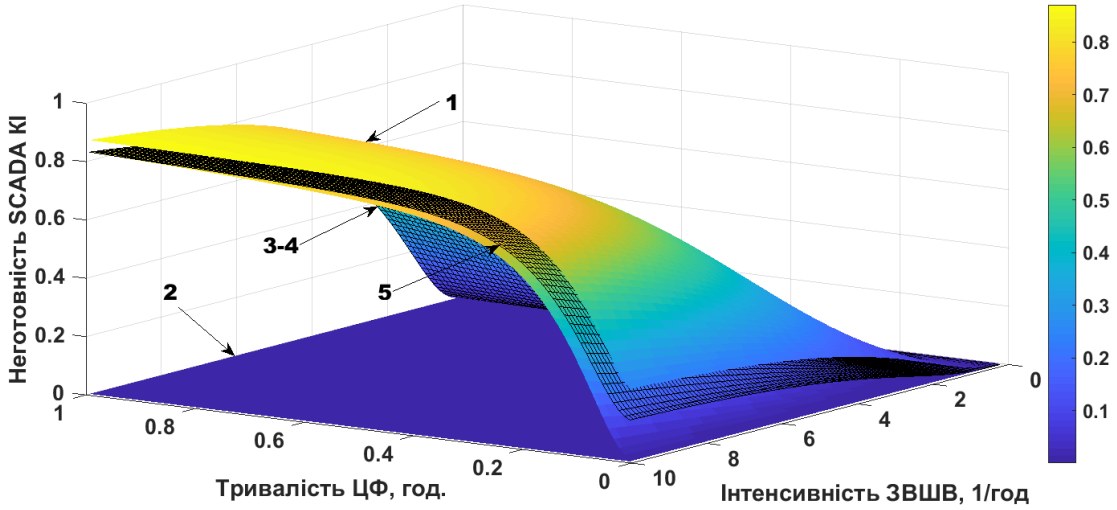


Рис. 4.26 Стаціонарний коефіцієнт неготовності активів SCADA KEI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається одна година

Для покращення наочного уявлення про отриманий виграш обчислимо абсолютну різницю між значеннями СКНГ для відповідних пар сценаріїв ЗВШВ, застосовуючи наступне співвідношення:

$$\Delta_{SCADA} = \left| \overline{K}^{DMI}_{SCADA_{k,h}} - \overline{K}^{DMI}_{SCADA_{2,h}} \right|, \tag{4.53}$$

де k=1,3,4,5 – номери відповідних сценаріїв ЗВШВ; h – номер зрізу СКНГ, для якого виконується обчислення; $\overline{K}^{DMI}_{SCADA_{2,h}}$ – значення h-го зрізу СКНГ для другого сценарію ЗВШВ.

Слід зазначити, що у співвідношенні (4.53) друга складова, яка визначає можливість отримання h-го зрізу СКНГ для другого сценарію ЗВШВ може бути замінена на іншу складову, що дозволяє отримати аналогічну оцінку для будь-якого сценарію. Результати обчислень з застосуванням співвідношень (4.52), (4.53) для конкретних сценаріїв ЗВШВ на активи SCADA KEI представлені на рис. 4.27–4.29. Ці результати отримано за умови, що тривалість цільового фішингу і час, який відводиться на зміну кодових ключів становить три хвилини. Зазначені вхідні параметри обрано не даремно, а саме, виходячи з міркувань необхідності створення найбільш жорстких умов реалізації ЗВШВ. А саме, вважається, що за досить невеликий час ЦФ зловмисники здійснюють атаку на КБА та ХМА системи SCADA

КЕІ з інтенсивністю ЗВШВ, яка дозволяє нанести максимальної шкоди.

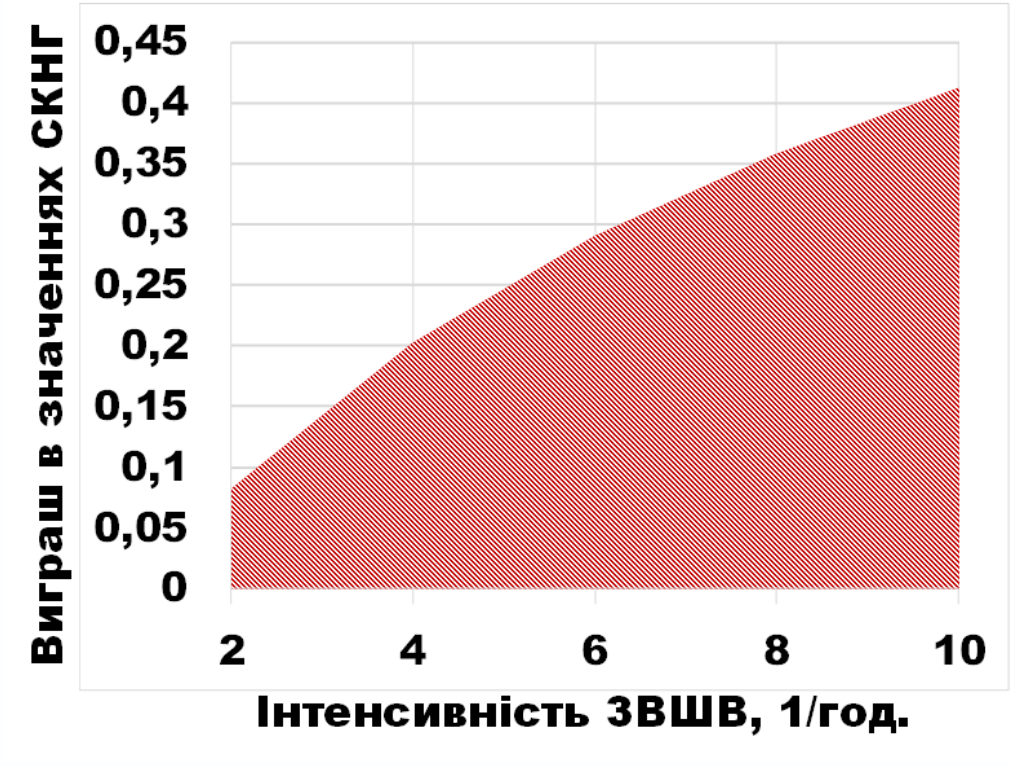


Рис. 4.27 Виграш в СКНГ для 2-го сценарію ЗВШВ у порівнянні з 1-м

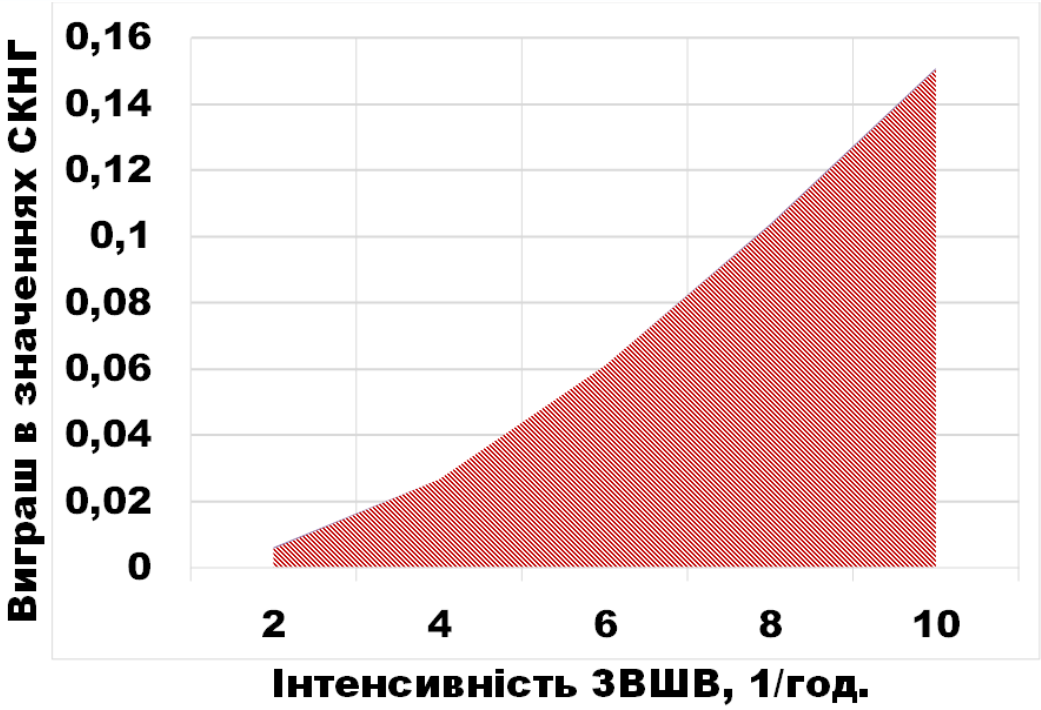


Рис. 4.28 Виграш в СКНГ для 2-го сценарію ЗВШВ у порівнянні з 3-м та 4-м

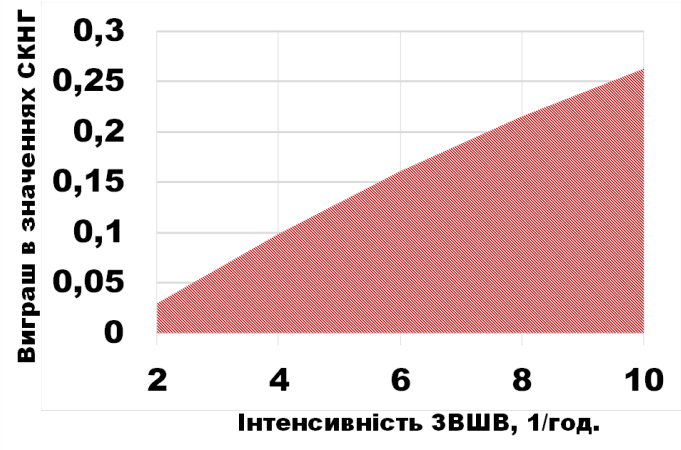


Рис. 4.29 Виграш в СКНГ для 2-го сценарію ЗВШВ у порівнянні з 5-м

Відповідно до рис. 4.27–4.29 найбільш критичною за результатами обчислення СКНГ є ситуація для ЗВШВ, що реалізується за першим сценарієм. Другими за критичністю є третій та четвертий сценарії з однаковим максимальним виграшем лише 15%. Тому будемо розглядати їх як один сценарій і отримаєм розрахунки виграшу в значеннях СКНГ, використовуючи аналогічний підхід, тобто за формулою

$$\Delta_{SCADA} = \left| \overline{K}^{DMI}_{SCADA_{r,h}} - \overline{K}^{DMI}_{SCADA_{3,h}} \right|, \tag{4.54}$$

де r=1,5 – номери відповідних сценаріїв ЗВШВ; h – номер зрізу СКНГ, для якого виконується обчислення; $\overline{K}^{DMI}_{SCADA_{3,h}}$ – значення h-го зрізу СКНГ для третього сценарію ЗВШВ.

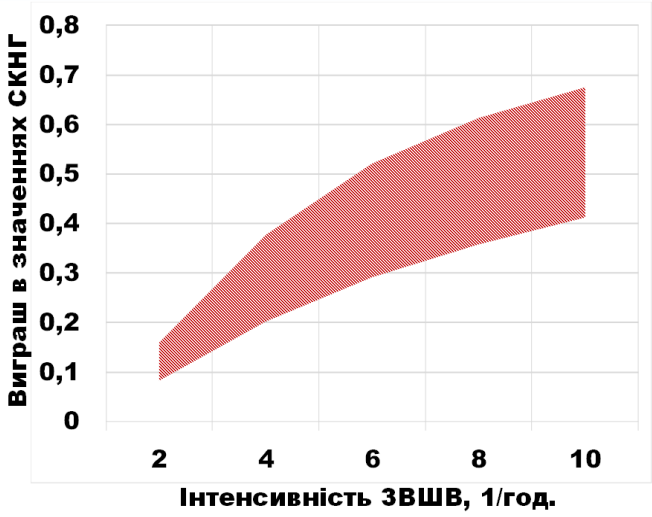


Рис. 4.30 Виграш в СКНГ для 3-го та 4-го сценаріїв ЗВШВ у порівнянні з 1-м

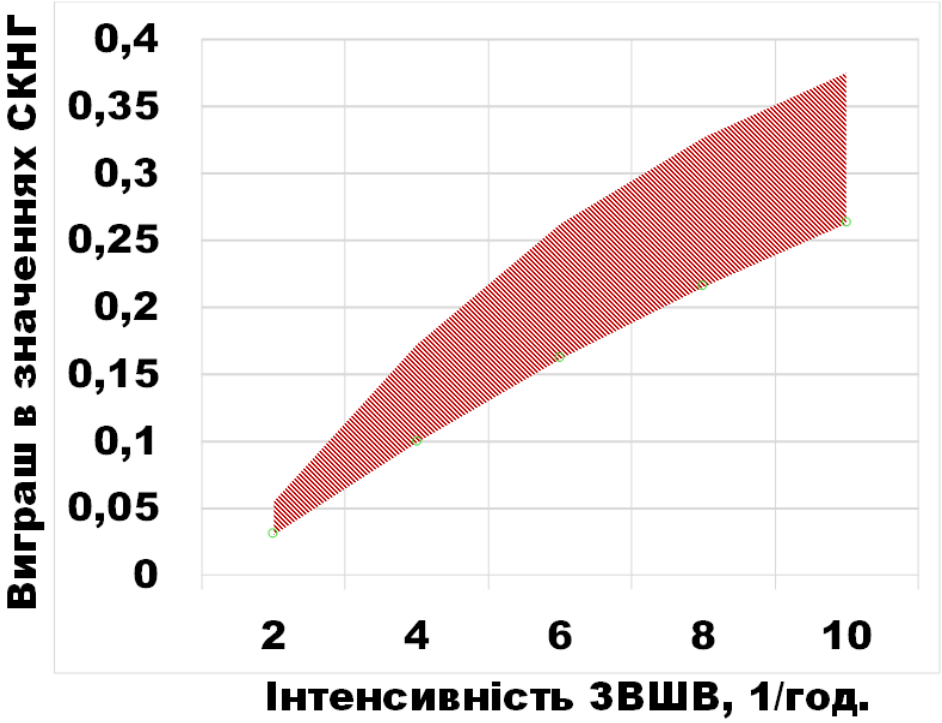


Рис. 4.31 Виграш в СКНГ для 3-го та 4-го сценаріїв ЗВШВ у порівнянні з 5-м

На рис. 4.30, 4.31 представлено результати розрахунків з використанням співвідношень (4.52), (4.54).

Порівняльний аналіз результатів аналітико-стохастичного моделювання гарантоздатності кібернетичних та хмарних активів КІ (рис. 4.27–4.31) свідчить, що при використанні функцій післяаварійного відновлювання та резервного копіювання, які виконуються завдяки застосуванню відповідних хмарних активів, значення стаціонарного коефіцієнта неготовності системи SCADA критичної енергетичної інфраструктури в залежності від реалізуємого сценарію зловмисних шкідливих впливів зменшується від 8,7% до 49,5%. Узагальнені результати аналізу динаміки зміни величини стаціонарного коефіцієнта неготовності (тобто діапазон зменшення значень стаціонарного коефіцієнта неготовності), який визначає фактичний виграш в готовності кібернетичних та хмарних активів системи SCADA критичної енергетичної інфраструктури для найбільш жорстких умов реалізації зловмисних шкідливих впливів наведено в табл. 4.7.

Таблиця 4.7

Аналіз динаміки зміни величини коефіцієнта неготовності системи SCADA КІ з урахуванням дії ЗВШВ

<table>
<tr><th rowspan="2">Порівняльна комбінація сценаріїв ЗВШВ</th><th colspan="2">Загальні параметри ЗВШВ</th><th rowspan="2">Тривалість процедури зміни ключів, хв.</th><th rowspan="2">Зменшення значень СКНГ, %</th></tr>
<tr><th>Тривалість ЦФ, хв.</th><th>Максимальна інтенсивність ЗВШВ, 1/год.</th></tr>
<tr><td>(2;1)
(2;3)
(2;5)
(3;1)
(3;5)</td><td rowspan="15">3</td><td rowspan="15">10</td><td rowspan="5">3</td><td>41,2
15
26,3
26,2
11,25</td></tr>
<tr><td>(2;1)
(2;3)
(2;5)
(3;1)
(3;5)</td><td rowspan="5">10</td><td>36,4
10,1
22
26,3
11,9</td></tr>
<tr><td>(2;1)
(2;3)
(2;5)
(3;1)
(3;5)</td><td rowspan="5">30</td><td>34,9
8,7
20,8
26,2
12,1</td></tr>
<tr><td>(2;1)
(2;3)
(2;5)
(3;1)
(3;5)</td><td rowspan="5">60</td><td>36,6
10,3
22,2
26,3
11,9</td></tr>
</table>

Продовження таблиці 4.7

Порівняльна комбінація сценаріїв ЗВШВ	Загальні параметри ЗВШВ		Тривалість процедури зміни ключів, хв.	Зменшення значень СКНГ, %
	Тривалість ЦФ, хв.	Максимальна інтенсивність ЗВШВ, 1/год.		
(2;1)	6	10	3	49,5
(2;3)				25
(2;5)				34,6
(3;1)				24,5
(3;5)				9,5
(2;1)			10	48,4
(2;3)				23,7
(2;5)				33,4
(3;1)				24,7
(3;5)				9,7
(2;1)			30	49,4
(2;3)				25
(2;5)				34,5
(3;1)				24,5
(3;5)				9,5
(2;1)			60	53,2
(2;3)				29,5%
(2;5)				38,5
(3;1)				23,6
(3;5)				9

Результати, які наведено в табл. 4.7, обгрунтовано доводять, що застосування потужного обчислювального ресурсу хмарних систем дозволяє значно покращити готовність системи SCADA КЕІ та її кібернетичних активів. Ці обставини свідчать, що включення ХМС до складу активів системи SCADA підсилює можливості по підтриманню необхідного рівня безпеки контуру управління КЕІ.

4.2.4 Кількісна оцінка ризику негативного впливу на активи критичної енергетичної інфраструктури з використанням запропонованого методу

У якості наочного прикладу розглянемо як визначається кількісна оцінка ризику критичної енергетичної інфраструктури. На рис. 4.32 зображено кластери КЕІ, які виконують основні функції енергетичної інфраструктури.

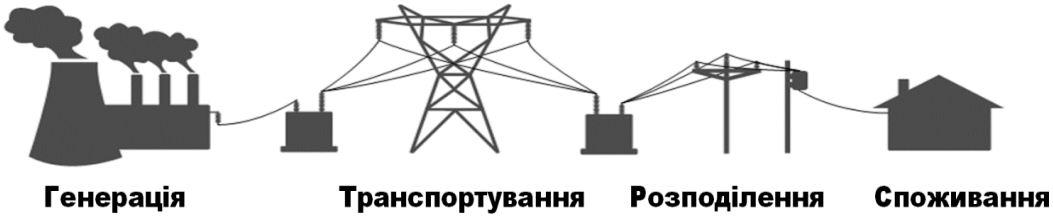


Рис. 4.32 Кластери критичної енергетичної інфрастуктури [153]

Робочий цикл енергозабезпечення за участю кластерів генерації, транспортування, розподілення та споживання у вигляді відповідної схеми функціонування існуючої насьогодні типової КЕІ представлено на рис. 4.33.

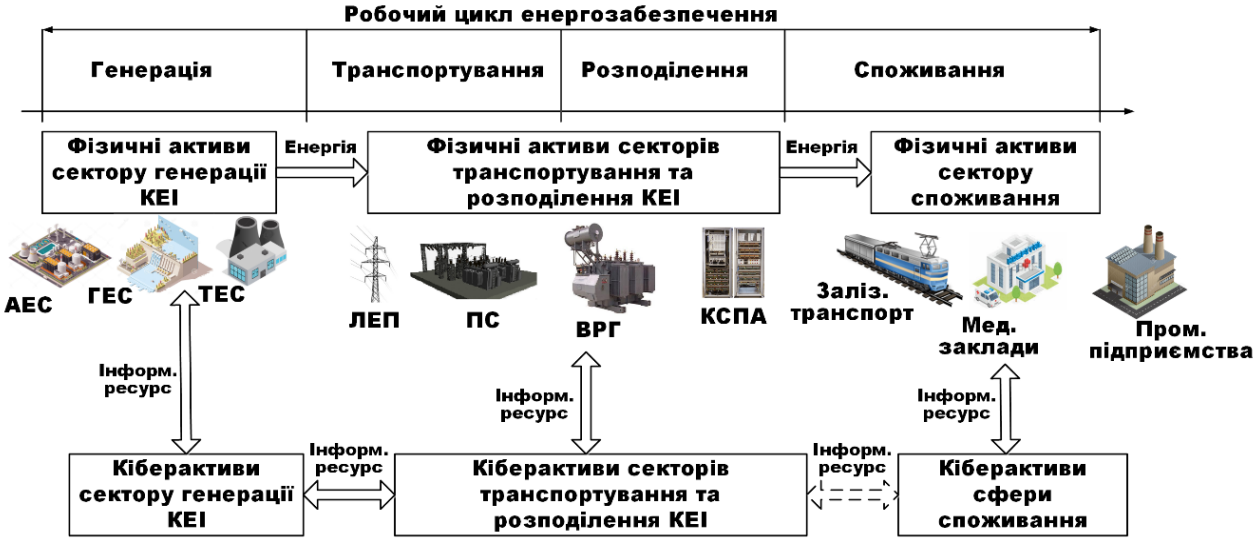


Рис. 4.33 Спрощена схема функціонування типової КЕІ

Процедура кількісної оцінки ризику негативного впливу на активи КЕІ лежить в основі методу забезпечення функційної безпечності інфраструктури, основні етапи реалізації якого у вигляді класифікаційної схеми зображено на рис. 4.33. Відповідно до поданої класифікаційної схеми (рис. 4.33) після ідентифікації негативного впливу на активи критичної енергетичної інфраструктури здійснюється причинно-наслідковий аналіз.

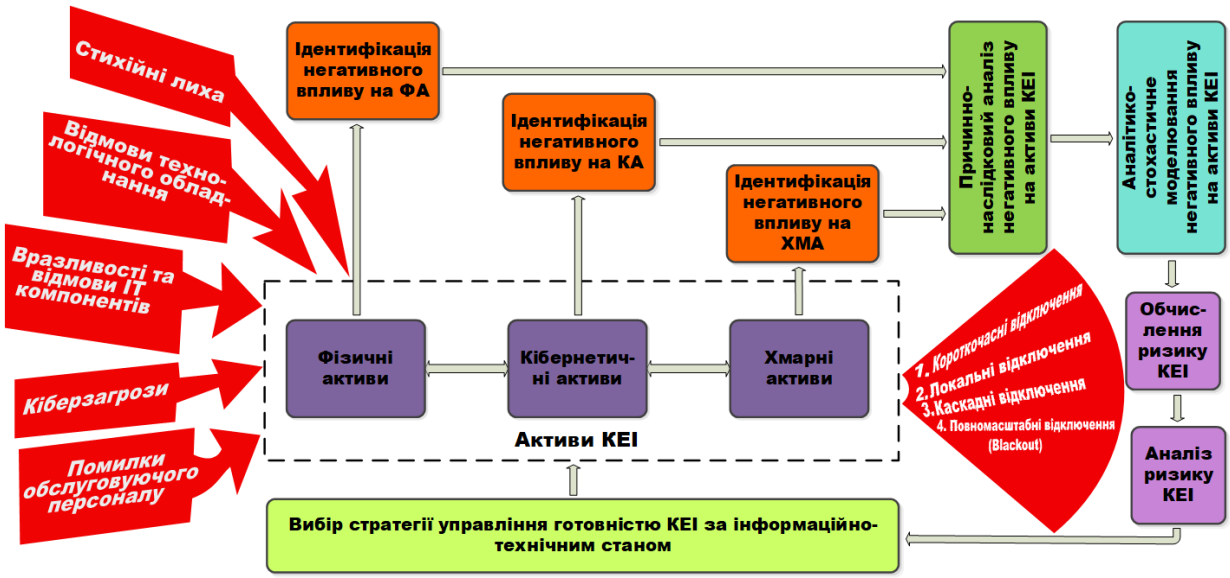


Рис. 4.33 Класифікаційна схема методу забезпечення функційної безпечності КЕІ з урахуванням ризику негативного впливу на її активи

Фактично причинно-наслідковий аналіз надає можливість отримати математичну інтерпретацію подій, пов’язаних з негативним впливом на активи критичної енергетичної інфраструктури, та перейти до їхнього аналітико-стохастичного моделювання. Тоді, згідно з класифікаційною схемою (рис. 4.33) та співвідношенням (2.4) кількісна оцінка ризику негативного впливу на активи КЕІ з урахуванням результатів причинно-наслідкового аналізу та аналітико-стохастичного моделювання може бути визначена так [137]:

$$R_{CrEI} = \left(1 - K_{\Gamma_{CrEI}}\right) L_{ПНД_{CrEI}}, \qquad (4.55)$$

де $K_{\Gamma_{CrEI}}$ – КГ критичної енергетичної інфраструктури; $L_{ПНД_{CrEI}}$ – показник причинно-наслідкової декомпозиції негативної події для КЕІ.

В співвідношенні (4.55) показник ПНД $L_{ПНД_{CrEI}}$ визначається за допомогою схеми причинно-наслідкового комплексу протікання негативної події для критичної енергетичної інфраструктури. Відповідно з дослідженнями, виконаними в [137], етапу побудови ПНК передує етап побудови структурно-логічної схеми протікання негативної події для критичної енергетичної інфраструктури. Зокрема, на рис. 4.34 зображено схему ПНК протікання першого етапу аварії Blackout 2003 року [154], яка будується у відповідності з принципами,

викладеними в [155].

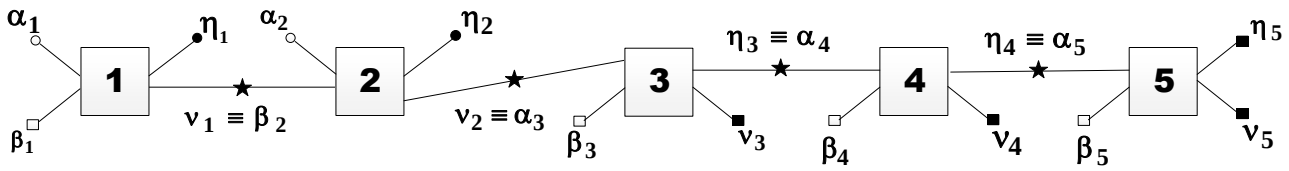


Рис. 4.34 Схема причинно-наслідкового комплексу протікання аварії Blackout 2003 року

На наступному кроці виконується логіко-цифрове представлення результатів причинно-наслідкової декомпозиції, яка у вигляді причинно-наслідкового комплексу зображена на рис. 4.34. Логічною основою процедури виконання ПНД є використання унікальних властивостей операції додавання по модулю два XOR, що фактично надає змогу отримувати коди розроблених ПНК. Більш детально принципи побудови причинно-наслідкових комплексів та сутність методу ПНД аварій критичної енергетичної інфраструктури розглянуто в наступному розділі дисертаційної роботи. На рис. 4.35 зображено результати кількісної оцінки ризику аварії критичної енергетичної інфраструктури $R_{CEI}(\lambda_1,\lambda_2)$ в залежності від інтенсивностей відмов компонентних складових критичної енергетичної інфраструктури та помилок обслуговуючого персоналу (ОП).

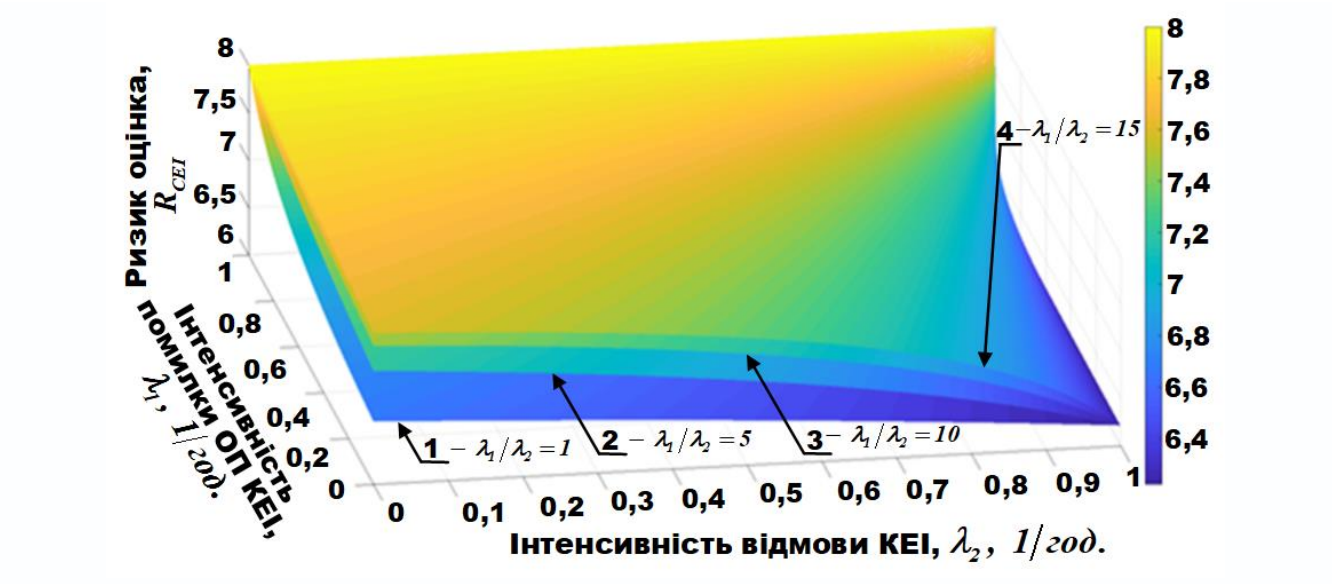


Рис. 4.35 Кількісна оцінка ризику аварії КЕІ

Аналіз результатів моделювання (рис. 4.35) дає змогу здійснити вибір стратегії забезпечення функційної безпечності критичної енергетичної інфраструктури. Зокрема, перевага була віддана стратегії управління готовністю критичної енергетичної інфраструктури за інформаційно-технічним станом.

4.3 Кількісна оцінка показника безпеки перспективних засобів Глобальної морської системи зв'язку та безпеки мореплавства морської критичної інфраструктури

Наступний блок розробленої методології присвячено кількісній оцінці показника безпеки перспективних засобів Глобальної морської системи зв'язку та забезпечення безпеки мореплавства морських рухомих об'єктів МКІ [120]. Насьогодні ГМСЗБ, не дивлячись на вжиті заходи є досить застарілою системою, яка потребує удосконалення та модернізації. В першу чергу це стосується принципу колективного застосування засобів ГМСЗБ, що є неприпустимим з точки зору забезпечення безпеки життя кожної людини [156]. Для цього необхідно розробити та впровадити в практику використання в умовах моря індивідуальних засобів ГМСЗБ. Серед перспективних засобів, які надають можливість перейти від ГМЗСБ колективного застосування до системи індивідуального використання з урахуванням морських районів (МР) [157], слід відзначити бездротові сенсорні мережі (БДСМ або WSN) та ХМС (рис. 4.36).

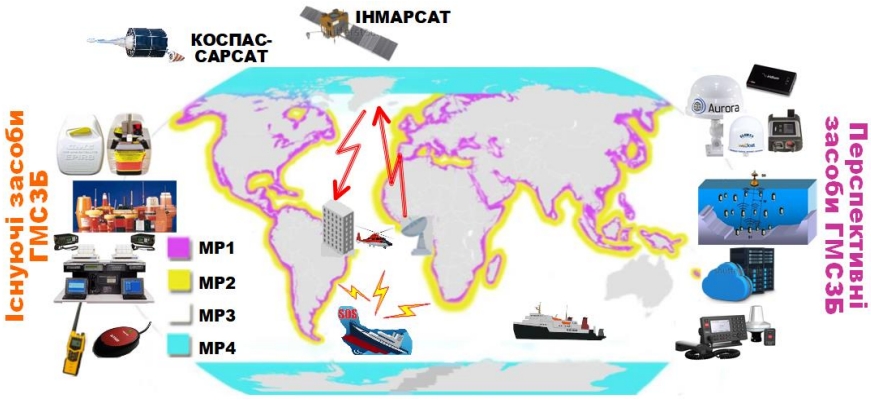


Рис. 4.36 Характеристика засобів ГМСЗБ морських рухомих об'єктів МКІ [157]

Роль та місце бездротових сенсорних мереж, хмарних систем та радіотелекомунікаційних засобів (РТЛКЗ) як перспективних засобів ГМЗСБ

морських рухомих об’єктів МКІ (далі, скорочено ГМСЗБ) відображено на відповідній функціональній схемі (рис. 4.37). Для кращого структурування компонентів ГМСЗБ побудуємо кортежну модель ГМСЗБ. Згідно з рис. 4.37 кортежна модель ГМСЗБ може бути представлена у вигляді

$$GMDSS_{MCI} = \left\{ MS, SS, GS, F_{GMDSS}^{MCI} \right\},$$

$$MS = \left\{ \left\{ M_{MS}^{PhA} \right\}, \left\{ M_{MS}^{CbrA} \right\}, \left\{ x_{MS}^{PhA} \right\}, \left\{ x_{MS}^{CbrA} \right\}, F_{GMDSS}^{MS} \right\},$$

$$SS = \left\{ \left\{ M_{SS}^{PhA} \right\}, \left\{ M_{SS}^{CbrA} \right\}, \left\{ x_{SS}^{PhA} \right\}, \left\{ x_{SS}^{CbrA} \right\}, F_{GMDSS}^{SS} \right\},$$

$$GS = \left\{ \left\{ M_{GS}^{PhA} \right\}, \left\{ M_{GS}^{CbrA} \right\}, \left\{ M_{GS}^{CldA} \right\}, \left\{ x_{GS}^{PhA} \right\}, \left\{ x_{GS}^{CbrA} \right\}, \left\{ x_{GS}^{CldA} \right\}, F_{GMDSS}^{GS} \right\},$$

де MS – компоненти морського сегменту ГМСЗБ; SS – компоненти космічного сегменту ГМСЗБ; GS – компоненти наземного сегменту ГМСЗБ.

Розглянемо принцип застосування за призначенням існуючих засобів ГМСЗБ згідно функціональної схеми (рис. 4.37) в звичайному режимі та під час проведення пошуково-рятувальної операції (ПРО).

В звичайному режимі компоненти, які згідно кортежної моделі $GMDSS_{MCI}$ утворюють множини MS, SS та GS застосовуються для того, щоб забезпечити розв’язування комплексу завдань по забезпечнню стійкого зв’язку та навігації МРО морської критичної інфраструктури. В буквальному сенсі це означає, що за допомогую засобів зв’язку ГМСЗБ “покриваються” всі чотири морських райони світового океану, а саме: район МР1 – засобами зв'язку, що працюють в діапазоні ульракоротких хвиль (відстань до 38 км); МР2 – засобами зв'язку, що працюють в діапазоні середніх хвиль (відстань до 380 км); МР3 – засобами угруповування геостаціонарних штучних супутників землі ІНМАРСАТ забезпечується зв’язок в міжполярній зоні (від 73° північної широти до 73° південної широти); МР4 – засобами зв’язку, що працюють в діапазоні коротких хвиль (в полярній зоні).

Під час проведення ПРО застосовуються засоби угруповування не геостаціонарних супутників КОСПАС/САРСАТ. До універсальних перспективних засобів ГМСЗБ відносяться засоби угруповування не геостаціонарних супутників ІРІДІУМ (рис. 4.37).

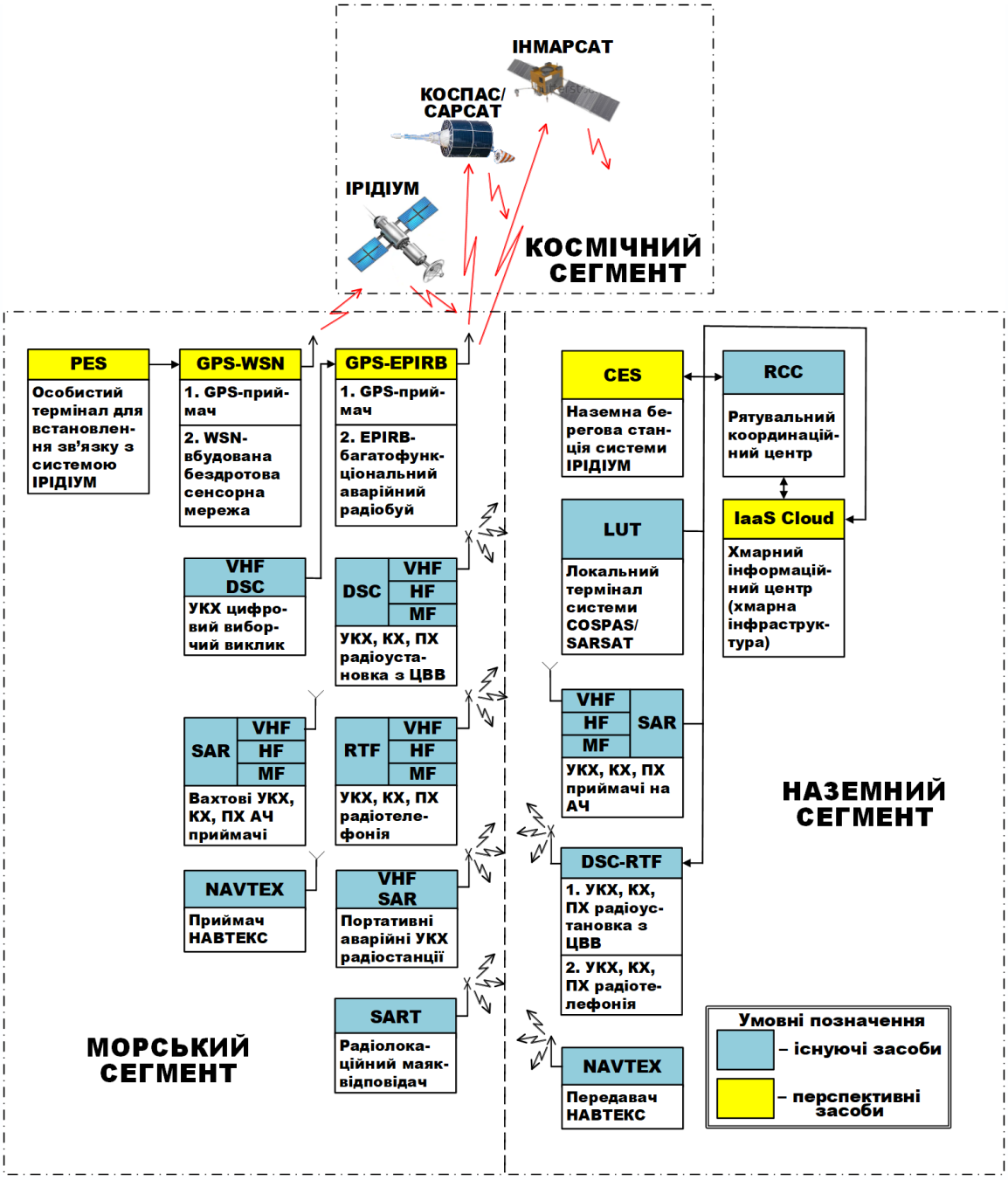


Рис. 4.37 Функціональна схема застосування перспективних засобів ГМСЗБ

На рис. 4.38 зображена діаграма функціонування ГМСЗБ. Діаграма висвітлює аспекти застосування ГМСЗБ за призначенням, включаючи режими використання існуючих і перспективних засобів в звичайних умовах та під час проведення пошуково-рятувальної операції, коли задіюються різноманітні судна, які перебувають в нормальному навігаційному стані.

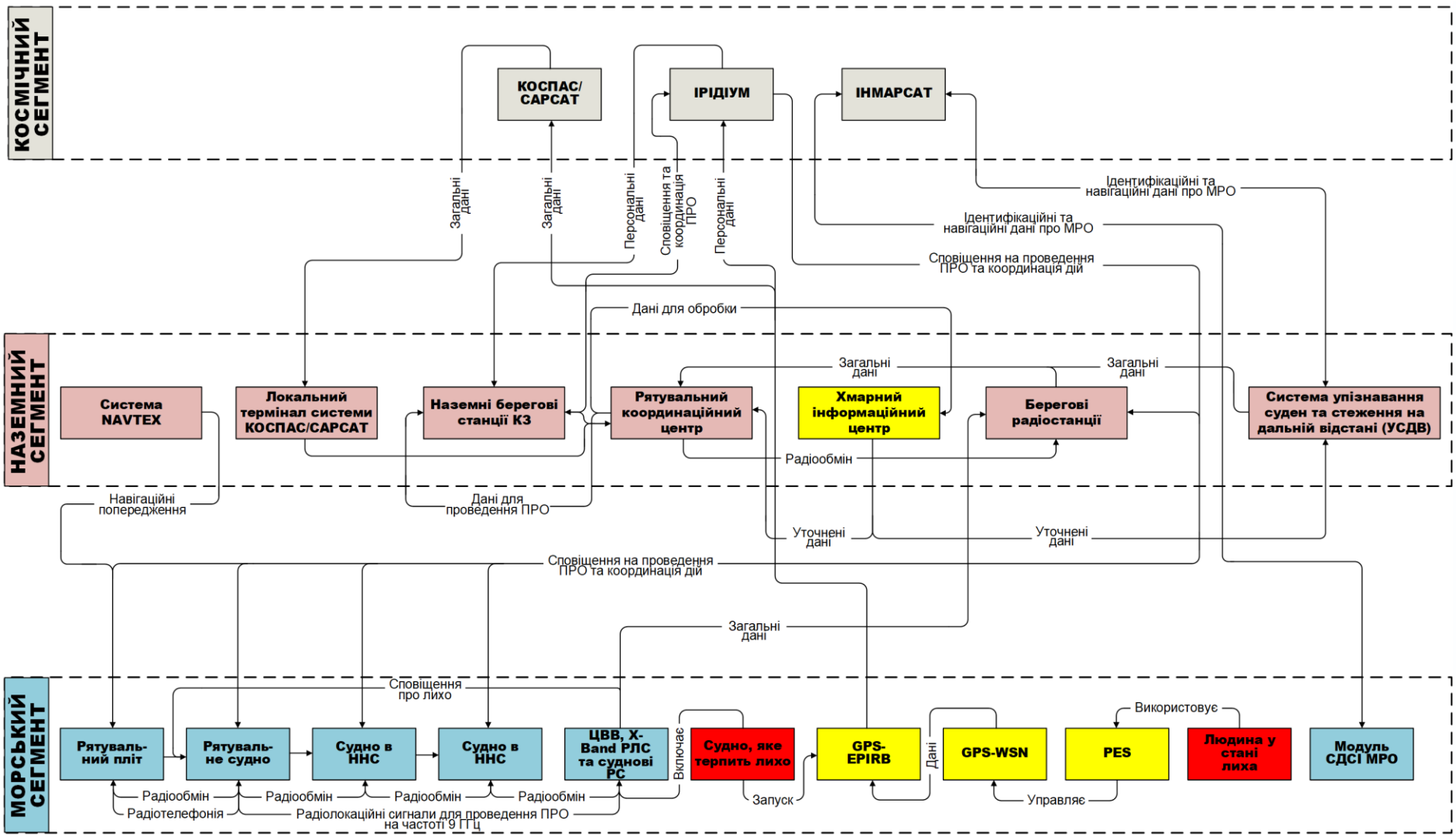


Рис. 4.38 Діаграма функціонування Глобальної морської системи зв’язку та забезпечення безпеки мореплавства

Застосовуючи інформацію про принципи побудови (рис. 4.37), функціонування (рис. 4.38), а також на підставі проведеного аналізу відомих вразливостей (рис. 1.11, 1.15) і загроз (табл. 4.7) було побудовано діаграму впливу ризик-факторів на сегменти (рис. 4.39) та схему реалізації атаки на засоби ГМСЗБ (рис. 4.40).

Таблиця 4.7

Аналіз загроз Глобальній морській системі зв'язку та забезпечення безпеки мореплавства [158]

Вид загрози	Характеристика загрози	Ризик
Розкриття інформації	Зловмисники отримують доступ до конфіденціальної інформації МРО МКІ	Низький
Фальсифікація інформації	Зловмисники змінюють інформацію таким чином, щоб ввести в оману користувачів щодо реальних координат МРО МКІ	Середній
Підміна інформації	Зловмисники за допомогою спеціальних технічних засобів надсилають інформа-цію, яка не відповідає дійсності	Високий

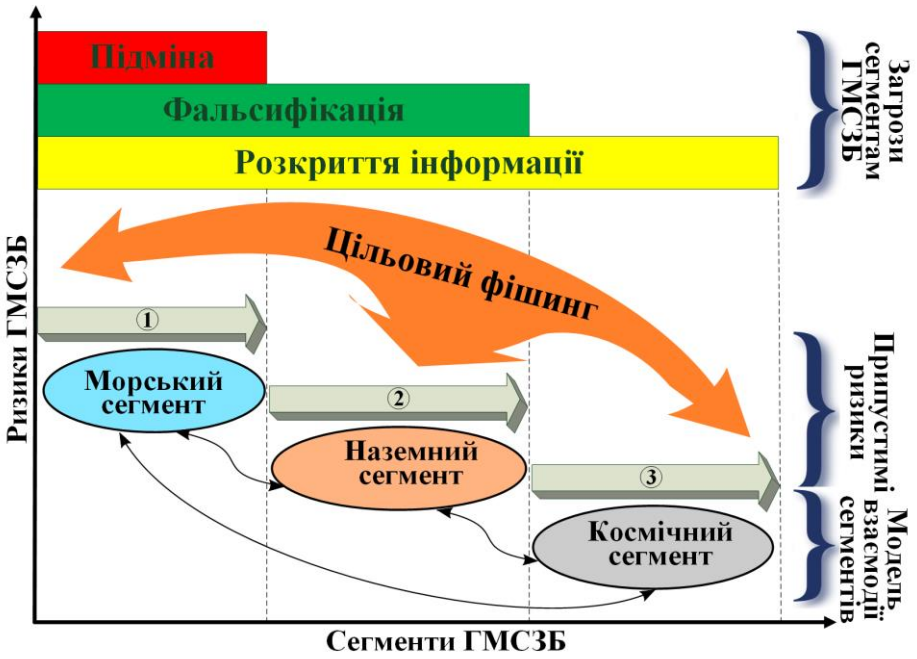


Рис. 4.39 Діаграма впливу ризик-факторів на сегменти ГМСЗБ

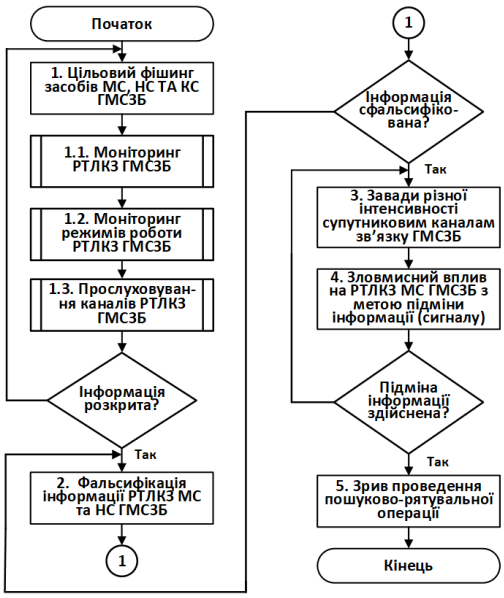


Рис. 4.40 Схема алгоритму реалізації атаки на засоби ГМСЗБ

Далі, враховуючи можливий сценарій атаки CA_k, були побудовані діаграма системної відмови SF_k (рис. 4.41), структурна схема (рис. 4.42) та діаграма ЗВШВ $DMI_k(ID, TI, SI)$ (рис. 4.43) з урахуванням ризик-факторів по виконанню трьох негативних дій, а саме: розкриття, фальсифікація та підміна інформації. Паралельно отримали теоретико-множинну модель $Availability_{ГМСЗБ}$ та здійснили перехід до опорної моделі $A_{ГМСЗБ}$ для визначення коефіцієнта готовності системи ГМСЗБ.

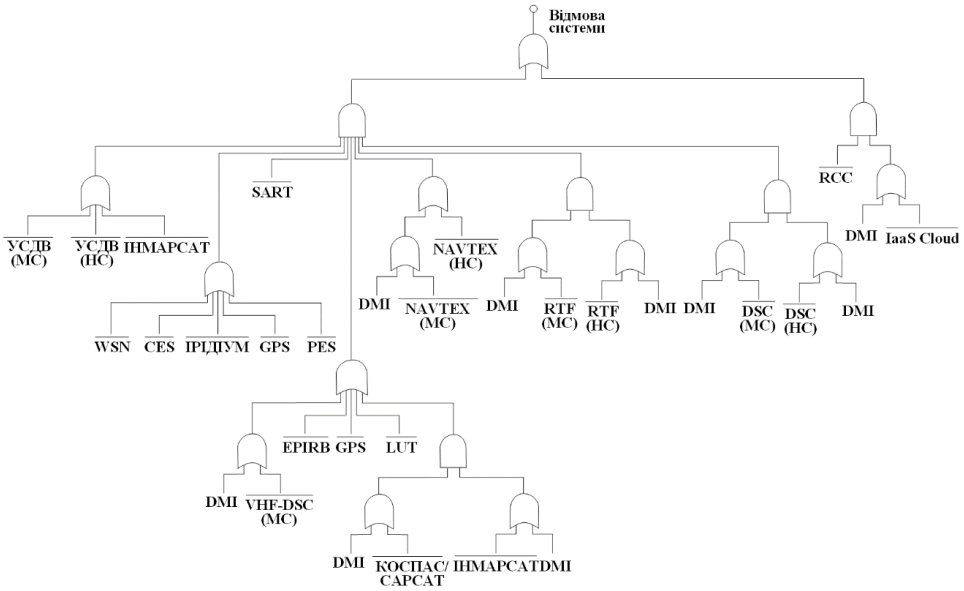


Рис. 4.41 Діаграма системної відмови ГМСЗБ

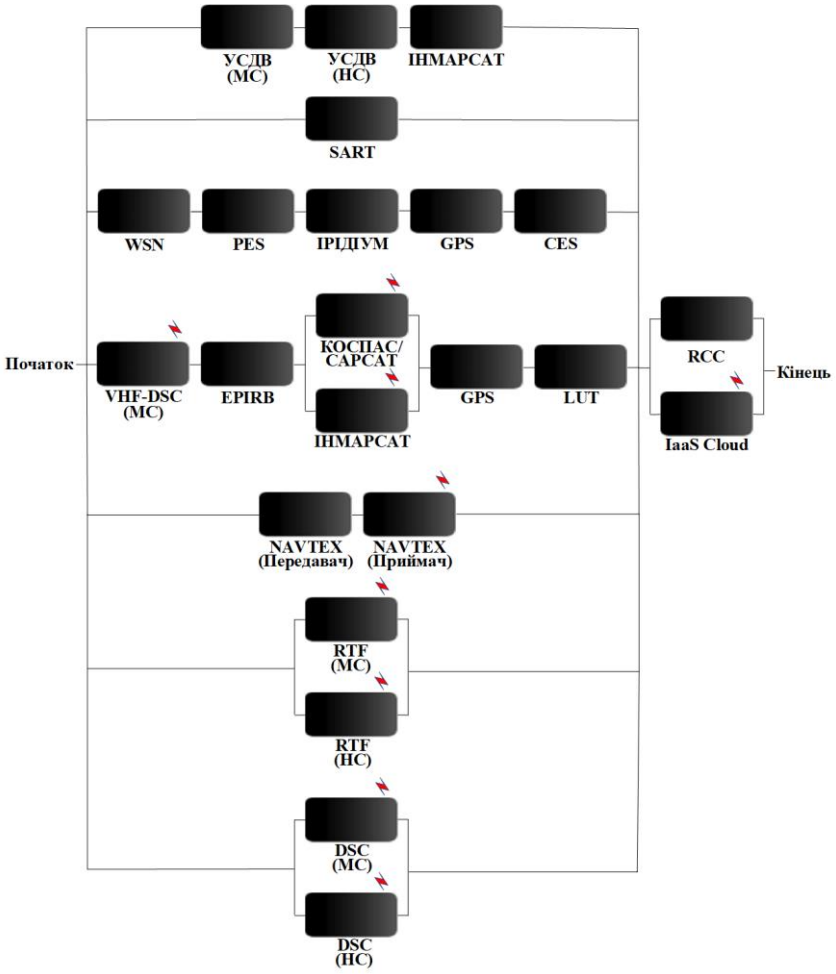


Рис. 4.42 Структурна схема ЗВШВ на засоби ГМСЗБ

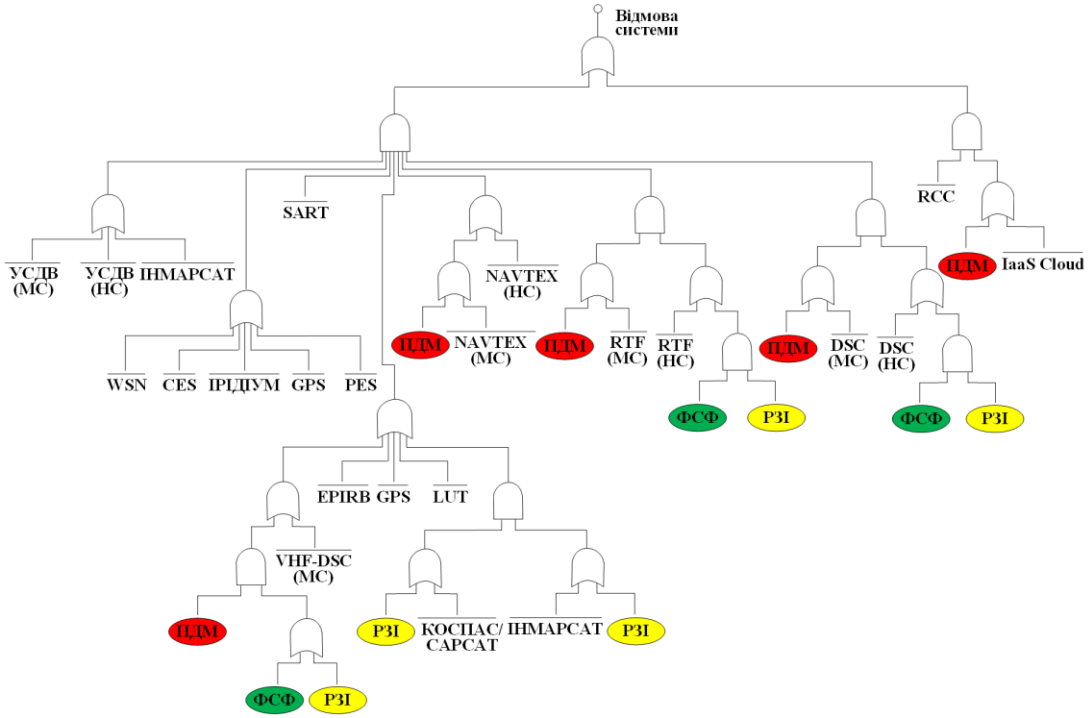


Рис. 4.43 Діаграма зловмисного шкідливого впливу на засоби ГМСЗБ

Застосовуючи відповідний метод, основні положення якого викладено в [132] та попередньо отриманий модельний ряд $W_{ГМСЗБ} = \langle CA_k, SF_k, DMI_k(ID, TI, SI), \quad Availability_{ГМСЗБ}, A_{ГМСЗБ} \rangle$, побудували стуктурну схему безпеки ГМСЗБ, яка зображена на рис. 4.44.

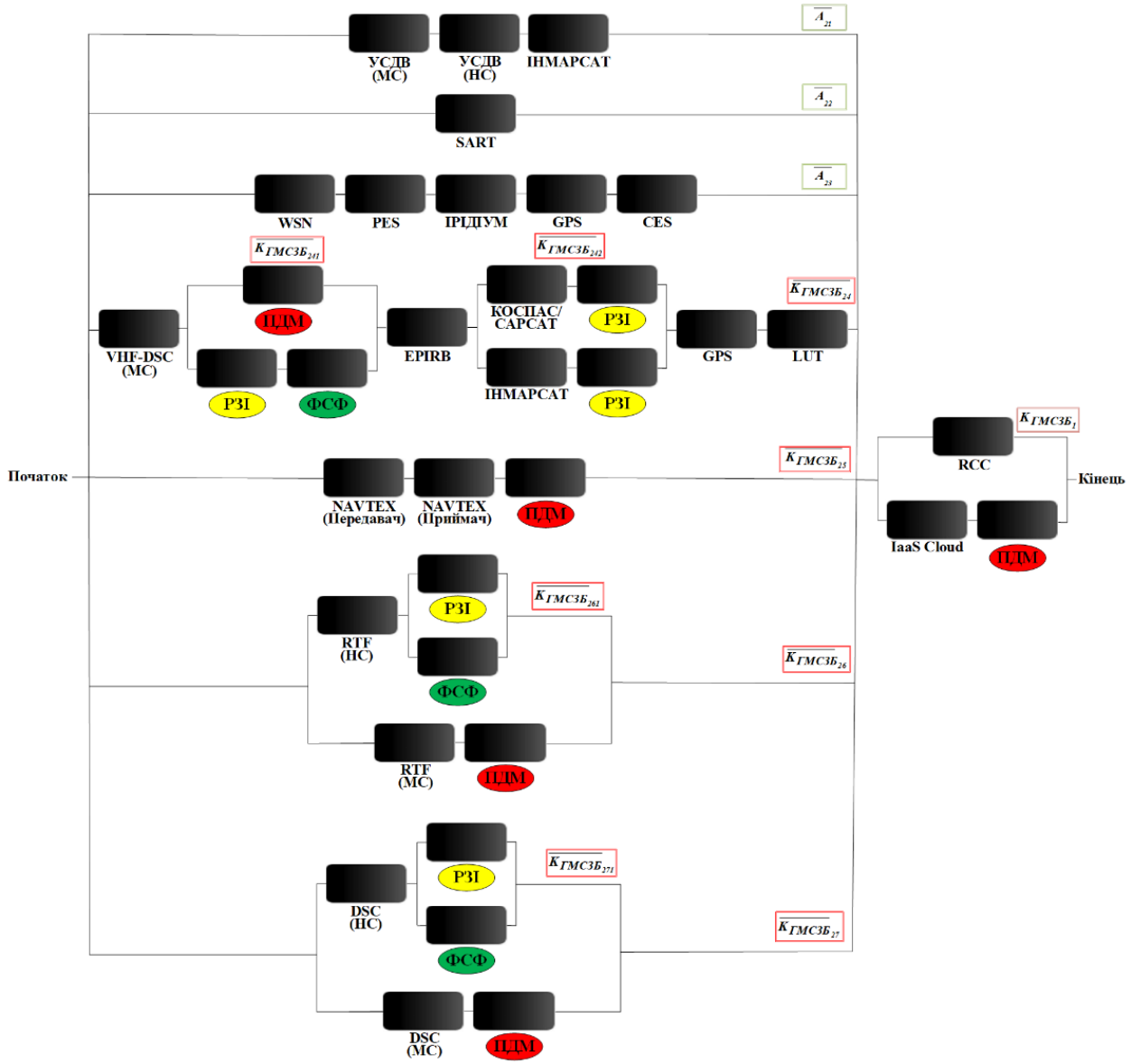


Рис. 4.44 Структурна схема безпеки засобів ГМСЗБ

Напівмарковське моделювання здійснювалося з застосуванням вже розроблених моделей, графи станів яких зображено на рис. 4.6, 4.18. Отже, загальна аналітико-стохастична модель, яка представлена за допомогою ССБ (рис. 4.44) та зазначених графів станів (рис. 4.6, 4.18), записується у вигляді таких співвідношень:

$$K_{ГМСЗБ} = K_{ГМСЗБ_1} K_{ГМСЗБ_2},$$

$$K_{ГМСЗБ_1} = 1 - \{1 - A_{RCC}\}\{1 - A_{IaaS\ Cloud} \cdot P_{ПДМ}\},$$

$$K_{ГМСЗБ_2} = 1 - \overline{A_{21}}\ \overline{A_{22}}\ \overline{A_{23}}\ \overline{K_{ГМСЗБ_{24}}}\ \overline{K_{ГМСЗБ_{25}}}\ \overline{K_{ГМСЗБ_{26}}}\ \overline{K_{ГМСЗБ_{27}}}.$$

На рис. 4.45–4.48 зображено результати кількісної оцінки показника безпеки (ПБ) перспективних засобів ГМСЗБ у порівнянні з існуючими.

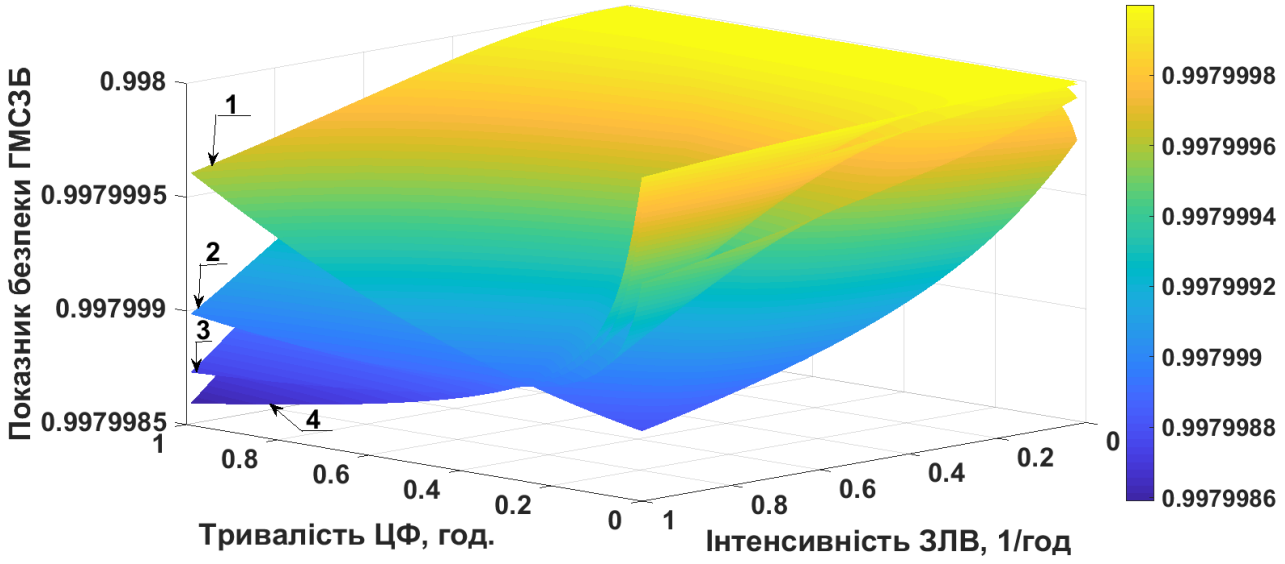


Рис. 4.45 Показник безпеки існуючої системи ГМСЗБ: 1 – $\gamma_{DMI}/\gamma_{tp} = 1$; 2 – $\gamma_{DMI}/\gamma_{tp} = 2$; 3 – $\gamma_{DMI}/\gamma_{tp} = 4$; 4 – $\gamma_{DMI}/\gamma_{tp} = 10$

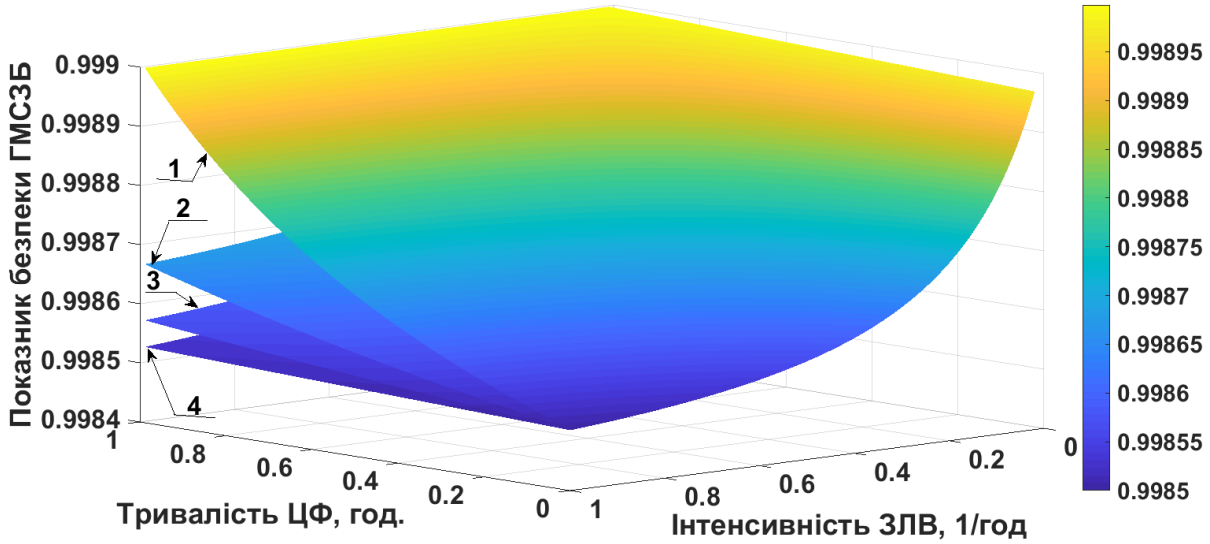


Рис. 4.46 Показник безпеки перспективної системи ГМСЗБ: 1 – $\gamma_{DMI}/\gamma_{tp} = 1$; 2 – $\gamma_{DMI}/\gamma_{tp} = 2$; 3 – $\gamma_{DMI}/\gamma_{tp} = 4$; 4 – $\gamma_{DMI}/\gamma_{tp} = 10$

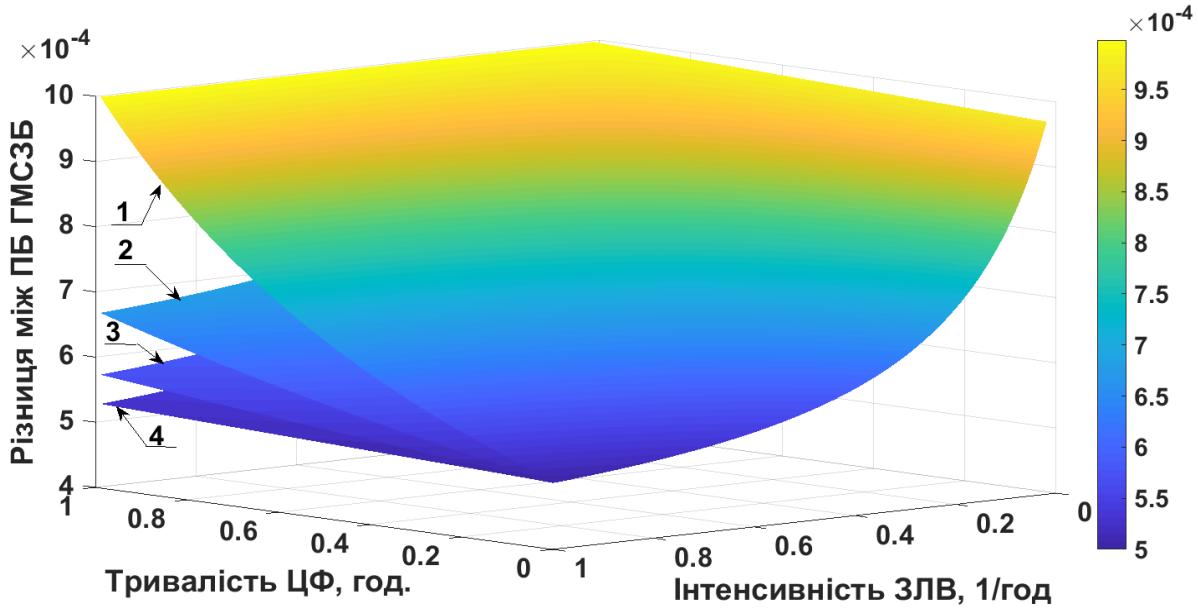


Рис. 4.47 Різниця між ПБ перспективних та існуючих засобів ГМСЗБ: 1 – $\gamma_{DMI}/\gamma_{tp}=1$; 2 – $\gamma_{DMI}/\gamma_{tp}=2$; 3 – $\gamma_{DMI}/\gamma_{tp}=4$; 4 – $\gamma_{DMI}/\gamma_{tp}=10$

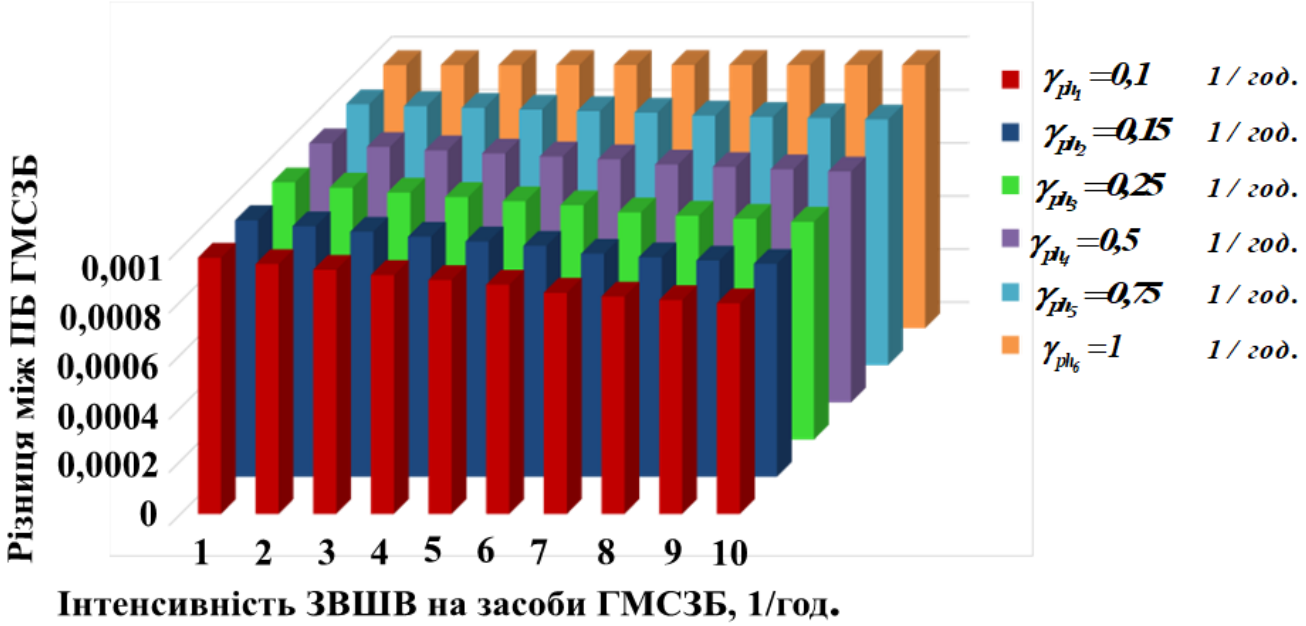


Рис. 4.48 Різниця між ПБ перспективних та існуючих засобів ГМСЗБ з урахуванням інтенсивності цільового фішингу та інших ЗВШВ

Аналіз результатів моделювання (рис. 4.45–4.48) свідчить, що застосування бездротових сенсорних мереж та хмарних систем з метою покращити роботу ГМСЗБ є виправданим, оскільки цей варіант дає певний виграш в значеннях показника безпеки.

Моделювання здійснювалося з урахуванням можливостей зловмисників реалізовувати відповідні сценарії атаки. Вважалося, що перед початком атаки попередньо зловмисниками здійснюється цільовий фішинг. Отриману за результатами цільового фішингу інформацію зловмисники можуть використовувати для порушення режиму конфіденціального ведення переговорів, введення в оману тощо. Далі ця інформація може бути сфальсифікована і використовуватися цілеспрямовано, що у будь-яклму випадку спричинить втрати, включаючи не санкціоноване проникнення в систему управління морським рухомим об’єктом МКІ.

Висновки до розділу 4

1. Наведено основні положення методології оцінювання функційної безпечності критичних інфраструктур, які базуються на аналітико-стохастичному моделюванні внутрішніх та зовнішніх факторів негативного впливу на активи КІ і визначенні відповідних ризиків.

2. Розроблено аналітико-стохастичний метод побудови структурних схем безпеки з урахуванням зловмисних шкідливих впливів на кібернетичні активи критичних інфраструктур. В основу методу покладено моделювання поведінки критичних інфраструктур відповідно до сценарію реалізації кібератаки та визначення рівня функційної безпечності КІ.

3. Виконано оцінювання комплексного показника гарантоздатності кібернетичних та хмарних активів інформаційно-керуючої системи SCADA КЕІ з урахуванням трьох типів зловмисних шкідливих впливів, а саме, розкриття, фальсифікація та підміна інформації. За результатами моделювання встановлено, що застосування відповідних хмарних активів у структурі системи SCADA КЕІ дозволяє суттєво підвищити її рівень готовності; виграш в значеннях стаціонарного коефіцієнта неготовності становить від 8,7% до 49,5% (див. табл. 4.7).

4. Розроблено метод оцінювання функційної безпечності критичної енергетичної інфраструктури з урахуванням ризику негативних впливів на її активи. З застосуванням запропонованого методу виконано аналітико-

стохастичне оцінювання ризику аварії критичної енергетичної інфраструктури за одним з відомих сценаріїв її реалізації. Кількісні результати моделювання зображено на рис. 4.35.

5. З застосуванням запропонованого методу отримано кількісні оцінки показника безпеки перспективних засобів Глобальної морської системи зв’язку та забезпечення безпеки мореплавства морських рухомих об’єктів морської критичної інфраструктури. У якості перспективних засобів ГМСЗБ запропоновано застосовувати бездротові сенсорні мережі та хмарні системи, що надає можливість підвищити значення ймовірнісного показника безпеки на 0,001 (рис. 4.48).

Основні положення цього розділу викладені у публікаціях автора [128–138, 120].

РОЗДІЛ 5
МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

5.1 Метод причинно-наслідкової декомпозиції аварій критичної енергетичної інфраструктури

Від методів оцінювання перейдемо до розгляду методів забезпечення готовності критичних інфраструктур. Зважаючи на те, що за останні п’ять років найчутливішою і найвразливішою ланкою національної безпеки держави була критична енергетична інфраструктура, розробку відповідних методів почнемо з виконання причинно-наслідкового та компаративістичного аналізу найбільш відомих аварій КЕІ. Фактична мета дослідження полягає в підвищенні точності оцінки ризику негативних подій для КЕІ з урахуванням негативного впливу на фізичні і кібернетичні активи інфраструктури. В першу чергу розглянемо принцип побудови причинно-наслідкового комплексу відомої аварії КЕІ.

5.1.1 Принцип побудови причинно-наслідкового комплексу протікання аварії критичної енергетичної інфраструктури

Процес побудови ПНК протікання аварії критичної енергетичної інфраструктури розглянемо в ракурсі реалізації одного з етапів методу причинно-наслідкової декомпозиції [155, 159]. Слід зазначити, що для покращення процедури аналізу аварій КЕІ метод ПНД доповнено методом компаративістичного аналізу. Послідовне застосування цих методів дозволить попередити відмови та відключення компонентів критичної енергетичної інфраструктури, а також запобігти аваріям КЕІ. На рис. 5.1 зображено етапи реалізації зазначених методів.

Зважаючи на специфіку застосування за призначенням КЕІ, відмови та відновлення критично важливих об’єктів, вплив вразливостей програмного забезпечення на готовність як компонентних складових, так і інфраструктури в цілому, була розглянута наступна теоретико-множинна модель:

$$\forall\ CrS_{\ell} \in CrEI,\ CrEI = \bigcup_{\ell=1}^{L}\{CrS_{\ell}\} \text{ та } S_{CrS}^{j} \in S_{CrEI},\ S_{CEI} = \bigcup_{j=1}^{J}\{S_{CrS}^{j}\} \exists$$

$$\exists\ TSM = \{CrEIS, CrSS, CrEIF, CrEIR, CrSF, CrSR\}, \quad (5.1)$$

$$\Omega 1: CrEIF \Rightarrow CrEIR \equiv H = \{(x,y) | x \in CrEIF \wedge y \in CrEIR \wedge \Omega 1(x) = y\}, \quad (5.2)$$

$$\Omega 2: CrSWV \Rightarrow CrSWP \equiv N = \{(w,z) | w \in CrSWV \wedge z \in CrSWP \wedge \Omega 2(w) = z\}, \quad (5.3)$$

де $CrEIS = \{CrEIS_i\}_{i=1}^{N}$ – множина станів КЕІ, які визначають її функційну безпечність; $CrSS = \{CrSS_j\}_{j=1}^{M}$, $CrSS \subset CrEIS$ – множина станів критичних систем, які входять до складу КЕІ, що визначають їхню ФБ; $CrEIF = \{CrEIF_p\}_{p=1}^{Q}$, $CrEIR = \{CrEIR_d\}_{d=1}^{U}$ – множина станів відмов та відновлень працездатних станів КЕІ, відповідно; $CrSWV = \{CrSWV_g\}_{g=1}^{H}$, $CrSWP = \{CrSWP_z\}_{z=1}^{V}$ – множина станів вразливостей програмного забезпечення критичних систем та множина станів пом’якшення дії вразливостей ПЗ КС, відповідно.

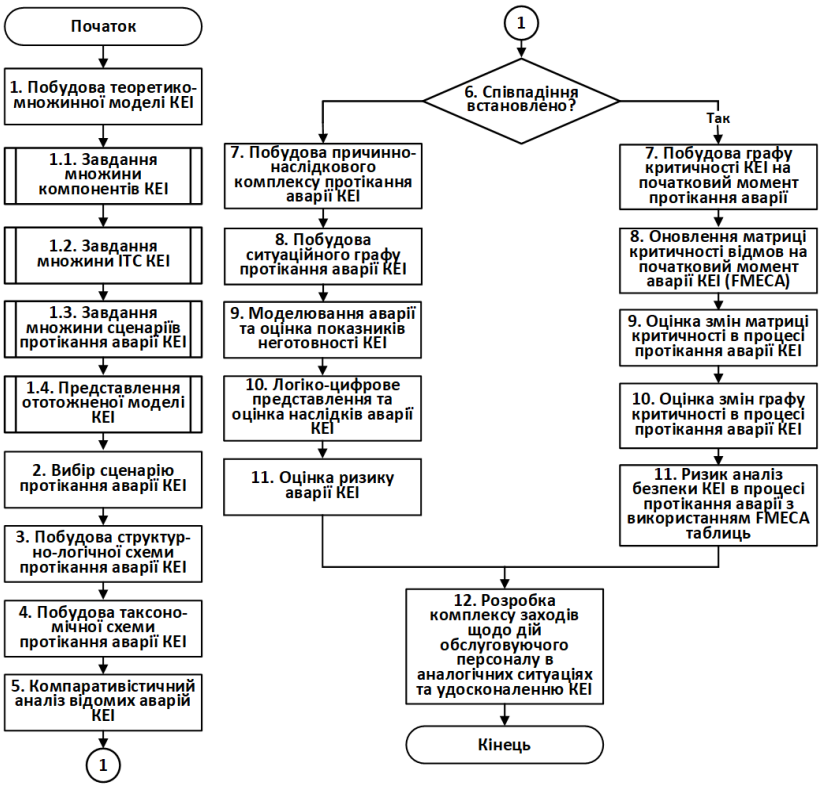


Рис. 5.1 Схема алгоритму реалізації етапів методу ПНД та методу компаративістичного аналізу аварії критичної енергетичної інфраструктури

Згідно з рис. 5.1 за умови наявності співпадіння реалізується гілка відповідно до методу ризик-аналізу безпеки з використанням ієрархії матриць критичності, який розроблено д.т.н. Брежнєвим Є.В. В іншому випадку, реалізується гілка відповідно до методу ПНД аварії КЕІ.

Для побудови ПНК за результатами компаративістичного аналізу, застосовуючи структурно-логічну схему протікання аварії КЕІ, формуються відповідні групи причин, наслідків та супроводжуючих їх умов. Групи об'єднуються в елементарні причинно-наслідкові ланки. В свою чергу, ланка будується у формі детермінованого автомата, а сукупність ланок об'єднується в причинно-наслідкові комплекси, які відповідають вимогам структурного автомата [160], і в представленому дисертаційному дослідженні застосовуються для визначення показника ПНД негативних подій для КЕІ. На рис. 5.2 зображено структуру причинно-наслідкової ланки, яка згідно з [155, 159, 160] виконує три операції по відношенню до групи "причини-умови", а саме: $\omega(\alpha,\beta)$ – операція поєднання; $h(\omega(\alpha,\beta))$ – операція перетворення; $\kappa(h(\omega(\alpha,\beta)))$ – операція розщеплення.

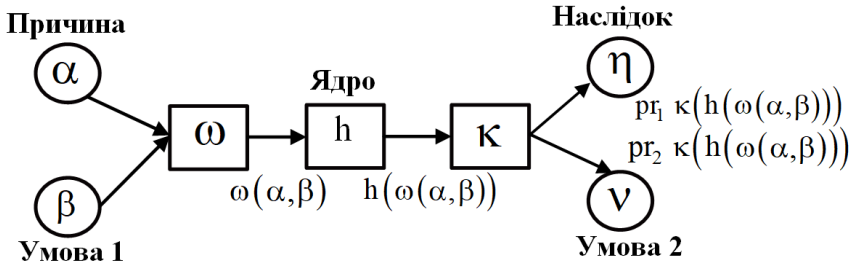


Рис. 5.2 Схема позначення компонентів в структурі причинно-наслідкової ланки [1]

Кожна з груп для причинно-наслідкової ланки, яка зображена на рис. 5.2, відносно негативних подій, пов'язаних з аварією КЕІ, може бути певним чином інтерпретована. Наприклад, в групі причини до умови 1 відносяться кваліфікація обслуговуючого персоналу, зношення електрообладнання, витрати на технічне

обслуговування та ремонт і т.і., а до причини – помилка обслуговуючого персоналу, коротке замикання, збільшення навантаження в мережах електропостачання, погіршення погодних умов тощо. Тоді до групи наслідків відносяться фінансові збитки, втрати необхідних потужностей, загибель людей і т.і., а до умови 2 відносяться моральне та технічне старіння обладнання, відсутність сучасної системи оперативного моніторингу ІТС компонентів КЕІ, низький рівень автоматизації процесів транспортування та розподілення електроенергії, відсутність можливості реалізувати масштабні інфраструктурні проєкти, тощо. Послідовність розвитку тих чи інших негативних подій визначає з'єднання ланок ПНК. Найбільш наочно це спостерігається у разі виникнення каскадних відмов електромережі, коли, наприклад, відключення однієї ЛЕП, яке відображається в групі наслідків першої ланки послідовно з'єднується з групою умов для другої ланки, що відображає функціонування другої ЛЕП. Зокрема, таке з'єднання ПНК можна інтерпретувати так: відключенння однієї ЛЕП створило умови для перевантаження іншої ЛЕП і т.і.

Застосування отриманих ПНК дозволить структурувати компоненти КЕІ, побудувати відповідні оцінні моделі та визначити рівень функційної безпечності інфраструктури в цілому.

5.1.2 Структурно-логічна схема протікання аварії критичної енергетичної інфраструктури

Як було зазначено в розділі 4 процесу побудови ПНК передує розробка структурно-логічної схеми типу "порушення-вразливість", яка відображає загальний характер протікання аварії КЕІ. У якості прикладу на рис. 5.3 представлена структурно-логічна схема протікання першого етапу аварії Blackout 2003 року [161–163].

На схемі (рис. 5.3) джерела вразливості, стан яких впливає на безпеку КЕІ зображено у формі еліпса; порушення в функціонуванні стандартних операційних процедур позначені прямокутниками. Крім того, на схемі позначено решту важливих для функційної безпечності КЕІ систем та установ, а саме: мережа обміну та передачі інформації в цифровому форматі ECAR, система оцінки та

прогнозу інформаційно-технічних станів компонентів інфраструктури (SE), система аналізу непередбачених ситуацій в реальному часі (RTCA), системний регулятор розподілення електроенергії (компанія MISO). Детальна характеристика подій, що відбувалися відповідно до структурно-логічної схеми, яка зображена на рис. 5.3, надана в роботах [161–164].

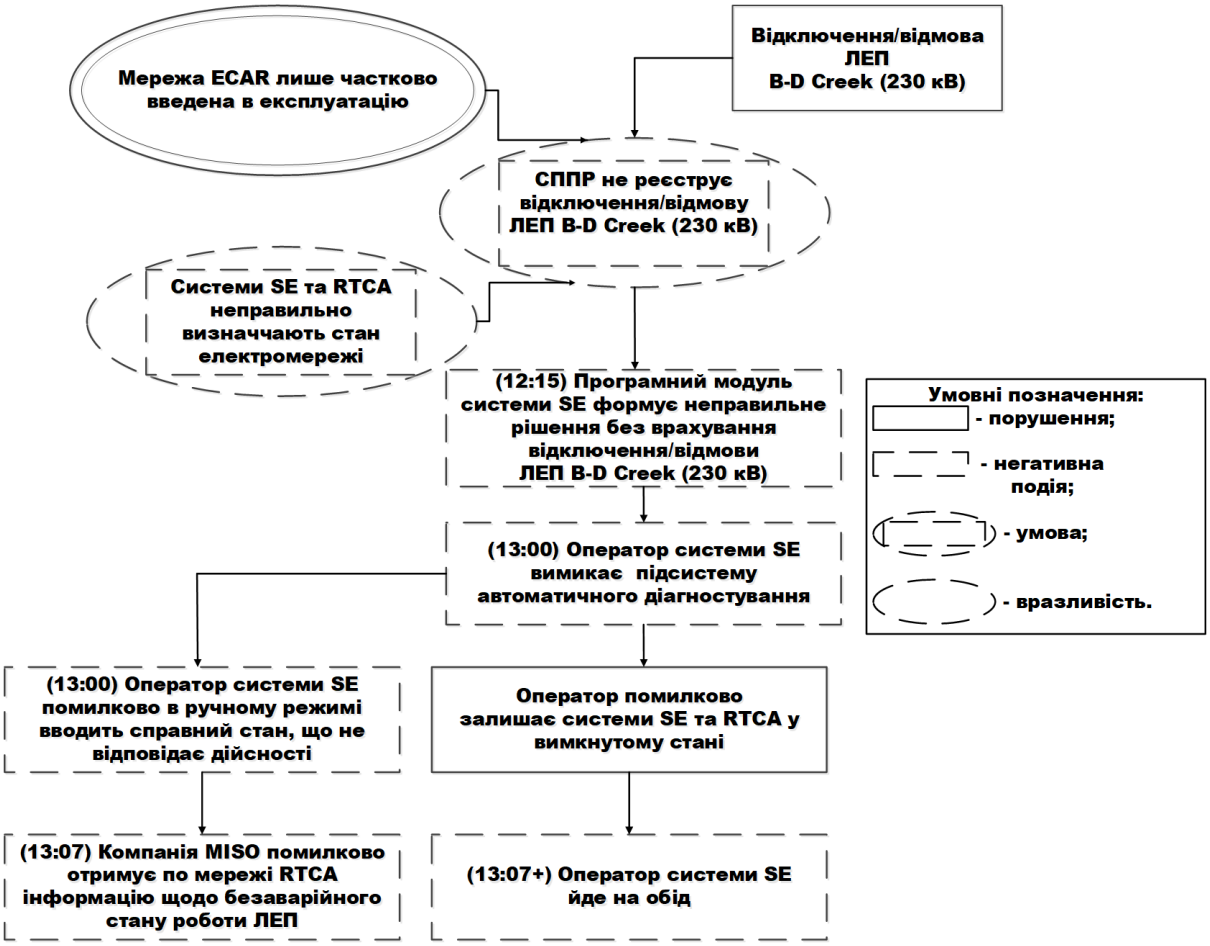


Рис. 5.3 Структурно-логічна схема протікання першого етапу аварії Blackout 2003 року [162]

Зображена структурно-логічна схема (рис. 5.3) допомогає встановити послідовність і хронологію негативних подій, що в сукупності відображають процес протікання аварії. Однак, цієї інформації недостатньо для виконання причинно-наслідкової декомпозиції. Тому на наступному кроці виконується інформаційний аналіз додаткових чинників впливу, здійснюється облік відповідних класифікаційних ознак в поєднанні з детальним аналізом внутрішніх, зовнішніх об’єктивних та суб’єктивних факторів негативного впливу на процеси

функціонування КЕІ (КС), що дозволяє побудувати і здійснити перехід від структурно-логічної до класифікаційної схеми протікання аварії (рис. 5.4) [136].

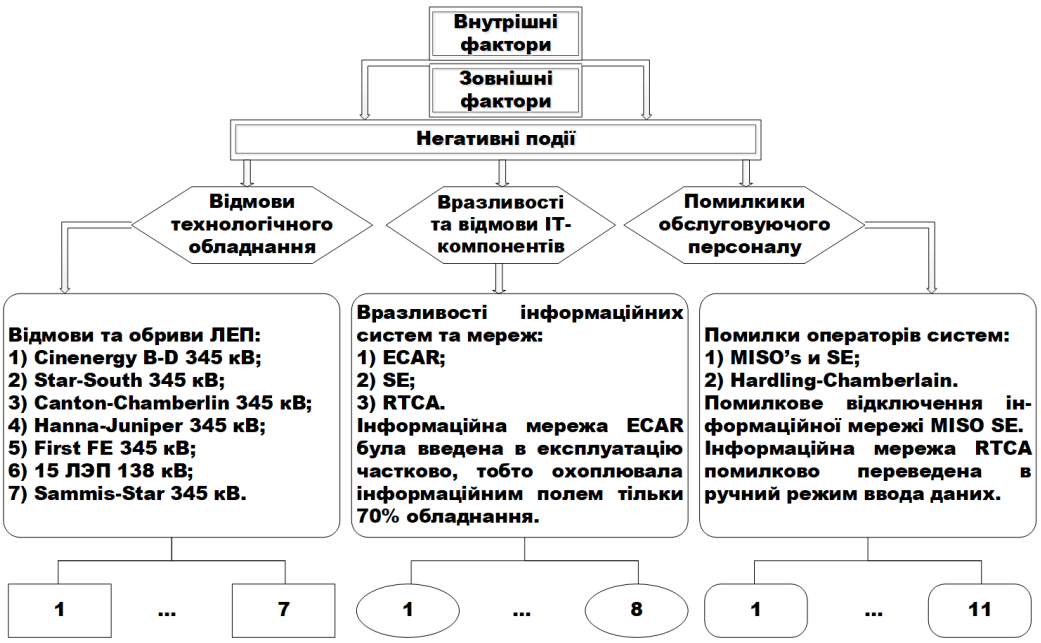


Рис. 5.4 Класифікаційна схема протікання першого етапу аварії Blackout 2003 року

Наступні етапи відповідно до схеми їхньої реалізації (рис. 5.1) реалізуються наступним чином:

1) виконується компаративістичний аналіз відомих аварій КЕІ;

2) будується ПНК у відповідності з методом причинно-наслідкової декомпозиції протікання аварії КЕІ;

3) від ПНК здійснюється перехід до ситуаційного графу протікання аварії КЕІ;

4) виконується аналітико-стохастичне моделювання аварії та показників готовності (неготовності) КЕІ;

5) логіко-цифрове представлення та оцінка наслідків аварії КЕІ.

6) на передостанньому етапі визначається величина ризику аварії КЕІ з застосуванням результатів аналітико-стохастичного моделювання та логіко-цифрового оцінювання наслідків аварії інфраструктури.

Останній етап реалізується шляхом розробки комплексу заходів щодо дій

обслуговуючого персоналу з метою запобігання аналогічним негативним подіям, включаючи перехід до управління готовністю КЕІ за інформаційно-технічним станом її компонентних складових. Всі ці заходи дозволять формулювати рекомендації щодо зменшення ризиків аварій КЕІ.

5.1.3 Причинно-наслідкова декомпозиція аварії критичної енергетичної інфраструктури

Відповідно до принципів побудови, які викладено в [155, 160], структурно-логічна схема (рис. 5.3), доповнена класифікаційною схемою послідовності негативних подій (рис. 5.4), трансформується в схему ПНК протікання аварії КЕІ. Зокрема, на рис. 5.5 зображена схема ПНК протікання першого етапу Blackout 2003 р. [162–164], яка побудована за результатами причинно-наслідкової декомпозиції негативних подій [136], що спостерігалися під час протікання зазначеної аварії КЕІ.

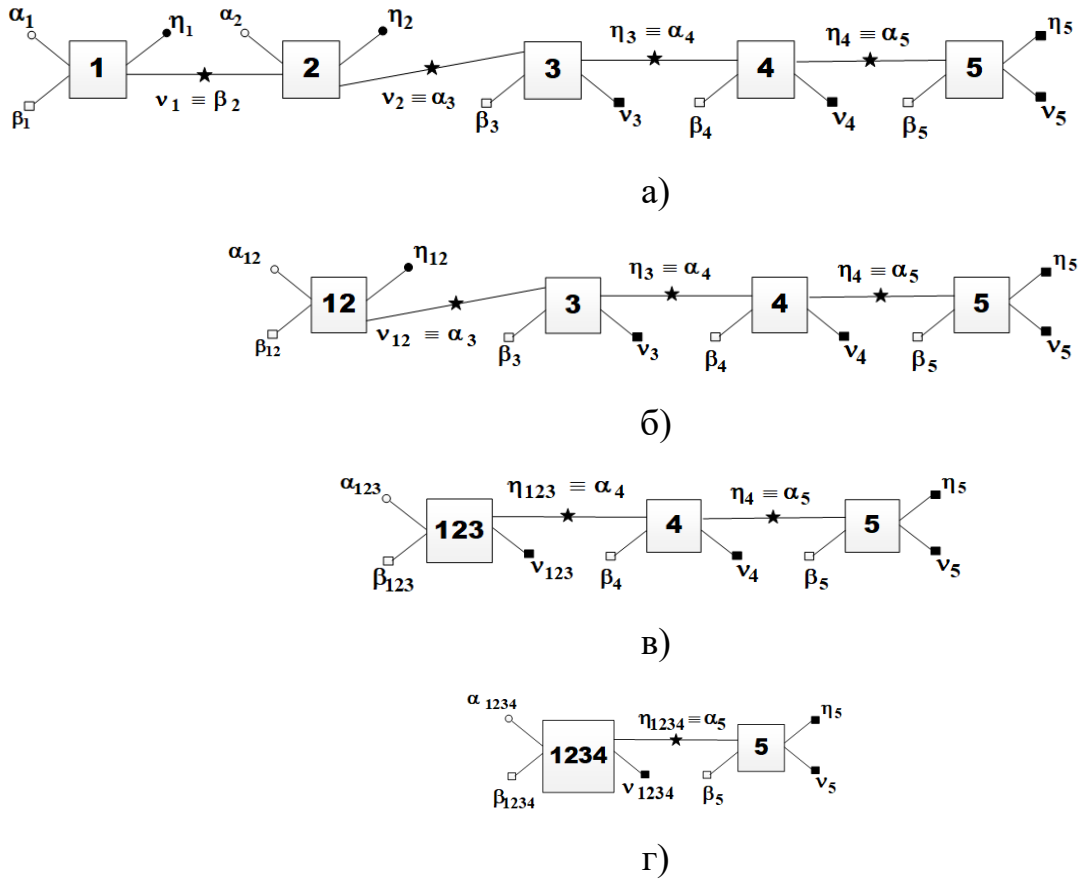


Рис. 5.5 Схема ПНК протікання першого етапу Blackout 2003 р.: а) загальна схема ПНК; б) схема ПНК для згортки 1-ої та 2-ої ланок причинно-наслідкових зв’язків; в) схема ПНК для згортки 1-ої, 2-ої та 3-ої ланок причинно-наслідкових зв’язків; в) схема ПНК для згортки 1-ої, 2-ої, 3-ої та 4-ої ланок причинно-наслідкових зв’язків

Операції композиції ланок реалізуються на основі ототожнення вузлів. Кожна операція композиції дає нову структуру взаємозв'язків ланок [155, 160]. Охарактеризуємо їх.

1. Для пропонуємої до розгляду структури перша та друга ланки (рис. 5.5 а) представляють собою стандартну операцію (O_2) для паралельного з'єднання ланок по групам причини та наслідки, які визначаються тотожністю $\nu_1 \equiv \beta_2$. А саме, для першої та другої ланок $O_2(H_1, H_2)$ записуються такі оператори [155, 160]:

1.1) $\omega_3(\alpha_1, \alpha_2)$ – причина; β_1 – умова 1;

1.2) $\omega_4(\eta_1, pr_1(\kappa_2(h_2(\omega_2(\alpha_2, \beta_2^*)))))$ – наслідок; $pr_2(\kappa_2(h_2(\omega_2(\alpha_2, \beta_2^*))))$ – умова 2 при $\beta_2^* = pr_2(\kappa_1(h_1(\omega_1(\alpha_1, \beta_1))))$.

2. Згортка першої та другої ланок з третьою ланкою (рис. 5.5, б) виконується як стандартна операція (O_3) для паралельного з'єднання ланок причинно-наслідкових зв'язків по групам причини та наслідки, яка визначається тотожністю $\nu_1 \equiv \alpha_2$. Для цих ланок $O_3(H_1, H_2)$ задаються такі оператори:

2.1) α_1 – причина; $\omega_3(\beta_1, \beta_2)$ – умова 1;

2.2) $\omega_4(pr_1(\kappa_2(h_2(\omega_2(\alpha_2^*, \beta_2)))))$ – наслідок; $pr_2(\kappa_2(h_2(\omega_2(\alpha_2^*, \beta_2))))$ – умова 2 при $\alpha_2^* = pr_2(\kappa_1(h_1(\omega_1(\alpha_1, \beta_1))))$.

3. Для структури, яка розглядається, згортка першої, другої, третьої ланок та четвертої ланки (рис. 5.5, в) представляють собою стандартну операцію (O_1) для паралельного з'єднання ланок причинно-наслідкових зв'язків по групам причини і наслідки, які визначаються тотожністю $\eta_1 \equiv \alpha_2$. А саме, в ланці $O_1(H_1, H_2)$, для згортки першої, другої, третьої ланок та четвертої ланок визначаються наступні оператори:

3.1) α_1 – причина; $\omega_2(\beta_1, \beta_2)$ – умова 1;

3.2) β_1 – умова 1; $pr_1(\kappa_2(h_2(pr_1\ (\kappa_1(h_1(\omega_1(\alpha_1, \beta_1)))))))$ – наслідок; $\omega_4(\nu_1, \nu_2)$ –

умова 2.

4. Згортка першої, другої, третьої, четвертої і п’ятої ланок (рис. 5.5, г) представляє собою стандартну операцію (O_1) і записується по аналогії з пунктом 3.

Записана таким чином математична інтерпретація ПНК дозволяє: а) усунути невизначеність і систематизувати взаємозв’язки, взаємодію компонентів (КС), процесів для КЕІ, які розглядаються; б) використовувати ланки причинно-наслідкових зв’язків (рис. 5.5) для здійснення аналітико-стохастичного моделювання.

5.1.4 Аналітико-стохастичне моделювання протікання аварії критичної енергетичної інфраструктури

Скористаємося структурованими, логічно обґрунтованими зв’язками між ланками ПНК (рис. 5.5) для побудови напівмарковської моделі протікання аварії КЕІ. Побудову моделі реалізуємо в два етапи.

На першому етапі з використанням отриманої схеми ПНК встановлюється послідовність логічних переходів, на основі якої будується ситуаційний граф станів. В якості наочного прикладу розглянемо схему, що зображена на рис. 5.5, а, для якої запишемо наступну послідовність логічних переходів:

1) $\beta_1 \to \nu_1 \equiv \beta_2 \to \nu_2 \equiv \alpha_3 \to \eta_3 \equiv \alpha_4 \to \eta_4 \equiv \alpha_5 \to \eta_5$;

2) $\alpha_1 \to \eta_1$, $\alpha_2 \to \eta_2$;

3) $\beta_3 \to \nu_3$, $\beta_4 \to \nu_4$, $\beta_5 \to \nu_5$.

Охарактеризуємо кожну з отриманих послідовностей. Як ми бачимо, перша післідовність реалізується у вигляді структури причинно-наслідкових ланок і комплексів (ПНК1) [155, 160]. Друга група переходів представлена причинно-наслідковими ланками $\alpha_1 \to \eta_1$ (ПНЛ1) та $\alpha_2 \to \eta_2$ (ПНЛ2) без врахування групи умов. Третя група переходів представлена умовними ланками $\beta_3 \to \nu_3$(УЛ3), $\beta_4 \to \nu_4$(УЛ4), $\beta_5 \to \nu_5$ (УЛ5) без врахування групи причин та наслідків. На рис. 5.6 зображено ситуаційний граф станів протікання першого етапу Blackout 2003 року, який відповідає зазначеній послідовності логічних переходів.

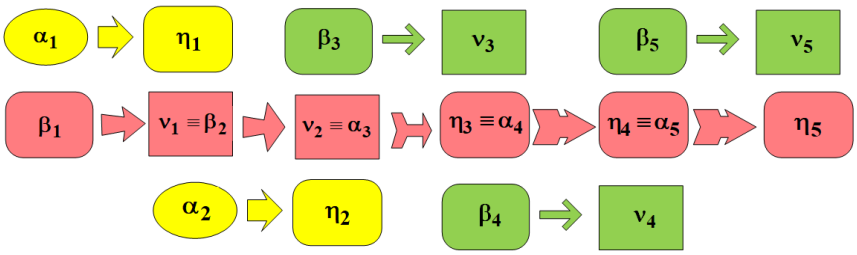


Рис. 5.6 Ситуаційний граф протікання першого етапу Blackout 2003 р.

Кожна із зазначених послідовностей логічних переходів (рис. 5.6) описує конкретні ситуації розвитку аварії КЕІ та може бути використана для реалізації наступного етапу аналітико-стохастичного моделювання. На другому етапі з використанням зображеного на рис. 5.6 ситуаційного графа будуються марковські (ММ), напівмарковські моделі (рис. 5.7) для послідовності негативних подій за участю різних компонентних складових КЕІ, і визначається оцінка показника функційної безпечності КЕІ. Аналіз, який виконано в [136, 164], свідчить про те, що складна випадкова подія, яка розглядається як аварія КЕІ, протікає як послідовність A_i, де $i = 1,...,N$ – сукупність відмов, несправностей технологічного обладнання, вразливостей ІТ-компонентів критичної енергетичної інфраструктури. Ймовірність випадкової події визначається як

$$P(A) = P\left[\bigcap_{i=1}^{N}\left\{A^i\right\}\right] = \prod_{i=1}^{N} P(A_i). \qquad (5.4)$$

У якості показника функційної безпечності пропонується використовувати коефіцієнт готовності критичної енергетичної інфраструктури ($K_{\Gamma_{CrEI}}$), під яким будемо розуміти ймовірність того, що в будь-який момент часу інфраструктурне утворення знаходиться в стані готовності, яке дозволяє в повному обсязі виконувати завдання функціонального призначення за умови відсутності неприйнятних ризиків. Тоді, з врахуванням (5.4) значення коефіцієнта готовності КЕІ визначається наступним чином:

$$K_{\Gamma_{CrEI}} = \prod_{j=1}^{m} K_{\Gamma_j}, \qquad (5.5)$$

де $j = 1,...,m$ – сукупність критичних систем зі складу КЕІ, які знаходяться під впливом і-ї послідовності негативних подій; K_{Γ_j} – коефіцієнт готовності j-ї

критичної системи зі складу КЕІ.

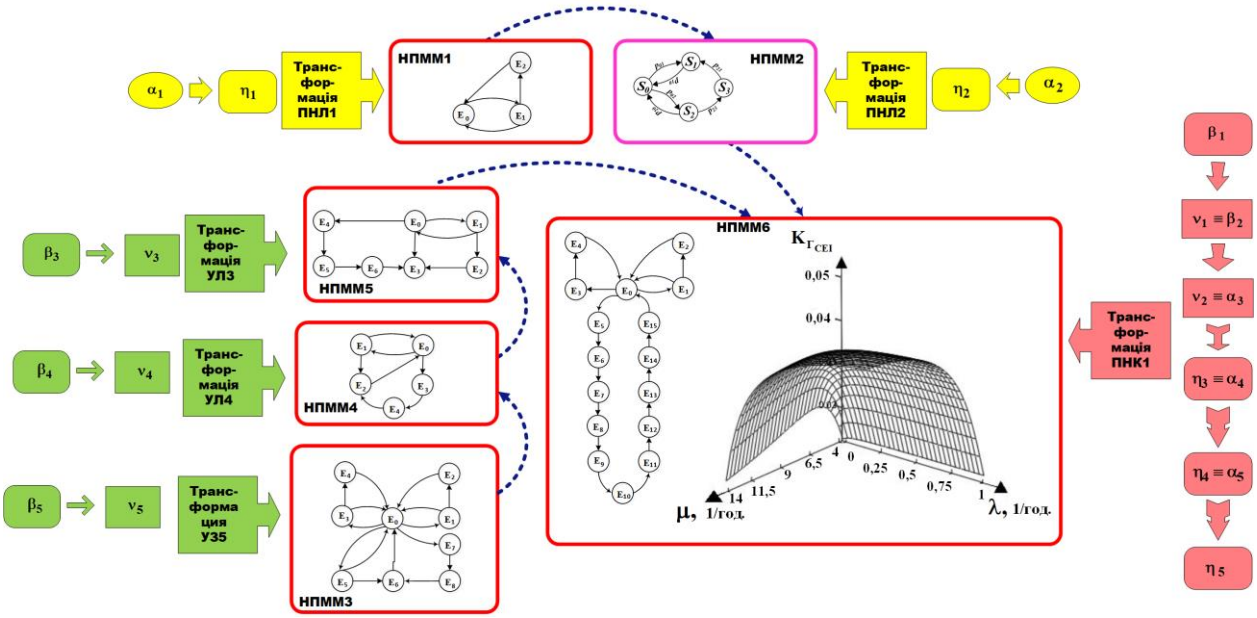


Рис. 5.7 Схема трансформації ситуаційного графа ПНК протікання аварії КЕІ в графи станів марковських та напівмарковських моделей

Більш детально результати розрахунків значень K_{Γ_j} для різних компонентних складових КЕІ на основі застосування апарату моделювання марковських та напівмарковських процесів наведено в [8, 113, 165, 166]. Після виконання аналітико-стохастичного моделювання, що є досить трудомістким і складним з математичної точки зору процесом, доцільно розробити апарат логіко-цифрового представлення результатів причинно-наслідкового декомпозиції.

5.1.5 Логіко-цифрове представлення причинно-наслідкової декомпозиції аварії критичної енергетичної інфраструктури

Необхідність реалізації даного кроку пов’язана з прагненням розробити відповідну інформаційну технологію, яку було б зручно використовувати для обчислення ризику КЕІ, використовуючи співвідношення (4.55). Логічною основою апарату цифрового представлення результатів ПНД аварії КЕІ є використання унікальних властивостей операції підсумовування по модулю два XOR, що фактично дозволяє отримати коди для розроблених причинно-наслідкового комплексу, причинно-наслідкових та умовних ланок (рис. 5.7). Нижче наводяться результати обчислень з застосуванням операції XOR [136].

1. Для ПНЛ1 та ПНЛ2, відповідно, отримали результат у вигляді

$$\alpha_1 \oplus \eta_1 = 0,\ \alpha_2 \oplus \eta_2 = 0. \tag{5.6}$$

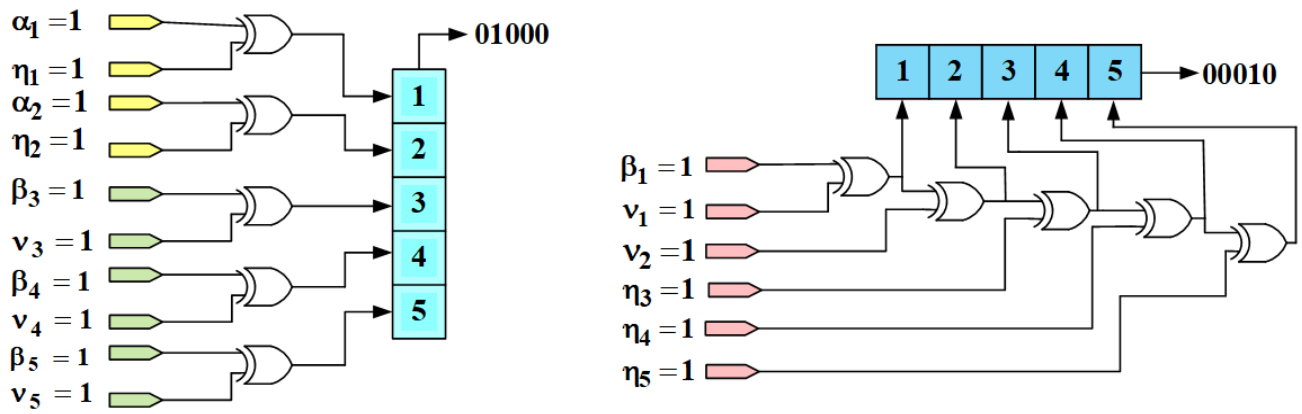
2. Для УЛ3, УЛ4, УЛ5, відповідно, застосовуються співвідношення

$$\beta_3 \oplus \nu_3 = 0,\ \beta_4 \oplus \nu_4 = 0,\ \beta_5 \oplus \nu_5 = 0. \tag{5.7}$$

3. Для ПНК1 отримали наступні співвідношення:

$$\beta_1 \oplus \nu_1 = 0,\ \beta_2 \oplus \nu_2 = 1,\ \alpha_3 \oplus \eta_3 = 0,\ \alpha_4 \oplus \eta_4 = 1,\ \alpha_5 \oplus \eta_5 = 0. \tag{5.8}$$

Схемні реалізації для операції підсумовування по модулю два з урахуванням співвідношень (5.6)–(5.8) зображено на рис. 5.8.



а) б)

Рис. 5.8 Схеми логіко-цифрового представлення ПНД аварії КЕІ: а) для ПНЛ1, 2 та УЛ3–УЛ5; б) для ПНК1

Результатом обчислень є кодові послідовності: а) 00010 – код причинно-наслідкового комплексу ПНК1; б) 01000 – код для причинно-наслідкових ланцюгів ПНЛ1 та ПНЛ2, умовних ланцюгів УЛ3–УЛ5. Оцінка ризику аварії КЕІ (рис. 4.35) з урахуванням результатів аналітико-стохастичного моделювання та логіко-цифрового представлення, коли $L_{ПНД_{CrEI}} = 8$, була отримана відповідно до співвідношення (4.55). Не складає труднощів помітити, що при зміні конфігурації ПНК, ПНЛ та УЛ (рис. 5.7, 5.8) змінюються кодові послідовності, що свідчить про чутливість запропонованої операції для розв’язування завдань по визначенню значення показника причинно-наслідкового декомпозиції $L_{ПНД_{CrEI}}$ аварій КЕІ.

Дійсно довжина ПНК та величина $L_{ПНД_{CrEI}}$ будуть більшими для випадку аварій типу Blackout [162–164] хоча б тому, що відбуваються каскадні відключення, які протікають за принципом ланцюгової реакції.

5.2 Метод компаративістичного аналізу аварій критичної енергетичної інфраструктури

На п’ятому етапі реалізації пропонуємих методів (рис. 5.1) виконується компаративістичний аналіз відомих аварій КЕІ з метою встановити загальні ознаки різноманітних негативних подій за участю компонентних складових КЕІ. Метод реалізується у формі перехресного аналізу інформації про аварії КЕІ, тобто у певній послідовності задаються питання. Зокрема, питання, що стосуються стану критично важливих об’єктів зі складу КЕІ можуть задаватися у наступній формі [136, 167]:

1. В чому полягала аварія X об’єкту A? (В чому полягала передаварійна ситуація X^* на об’єкті A?).

2. Що було причиною аварії X об’єкту A? (Що було причиною передаварійної ситуації X^* на об’єкті A?).

3. Як розвивалася аварія X на об’єкті A? (Як розвивалася передаварійна ситуація X^* на об’єкті A?).

4. Як реагувала на аварійну ситуацію X система управління (СУ) об’єктом A? (Як реагувала на передаварійну ситуацію X^* СУ об’єктом A?).

5. Чому аварія X не була відвернена СУ об’єктом A? (Завдяки яким особливостям СУ передаварійна ситуація X^* не привела до аварії X на об’єкті A?).

6. Чи можлива подібна аварія Y на об’єкті B? (Чи можлива подібна передаварійна ситуація Y^* на об’єкті B?).

7. Чи можлива поява подібної причини виникнення аварії Y на об’єкті B? (Чи можлива поява подібної причини передаварійній ситуації Y^* на об’єкті B?).

8. Як могла б розвиватися аварія Y на об’єкті B? (Як могла б розвиватися передаварійна ситуація Y^* на об’єкті B?).

9. Як реагувала б на аварійну ситуацію Y СУ об’єктом B? (Як реагувала б на

передаварійну ситуацію Y^* СУ об’єктом В?).

10. Можна було б запобігти аварії Y СУ об’єктом В? (Завдяки яким особливостям СУ об’єктом В передаварійна ситуація Y^* не привела б/або привела до аварії Y на об’єкті В?).

Зазначені питання становлять основу методики перехресного аналізу. У табл. 5.1 наведено результати перехресного аналізу за матеріалами Північно-Американської і Європейської аварій Blackout (серпень–вересень 2003 р.).

Таблиця 5.1

Результати перехресного аналізу аварій Північно-Американської та Європейської КЕІ

№ з/п	Аналізуємий аспект	Питання	Результат аналізу аварії Європейської КЕІ	Результат аналізу аварії Північно-Американської КЕІ
1.	Тип аварії	Які наслідки аварії?	Відключення основних елементів топології електромережі, знеструмлення 56 млн. населення	Відключення основних елементів топології електромережі, знеструмлення 50 млн. населення
2.	Причина аварії	Що стало причиною аварії об’єктів КЕІ?	Збільшення навантаження призвело до підвищення температури проводів ЛЕП, що викликало провисання проводів і виникнення короткого замикання за рахунок контакту з рослинністю. Навантаження збільшилося через несправність італійських гідроагрегатів	Збільшення навантаження призвело до підвищення температури проводів ЛЕП, що викликало провисання проводів і виникнення короткого замикання за рахунок контакту з рослинністю. Навантаження збільшилося внаслідок спекотного літа, значного збільшення кількості використовуємих кондиціонерів та інших охолоджуючих систем. Зниження надійності КЕІ

Продовження таблиці 5.1

№ з/п	Аналізуємий аспект	Питання	Результат аналізу аварії Європейської КЕІ	Результат аналізу аварії Північно-Американської КЕІ
3.	Як протікала аварія	Як розвивалася аварія на об’єктах КЕІ?	Системи аварійної автоматики швидко відключали та ізолювали ЛЕП з підвищеним навантаженням; вузли та генератори, були не здатні повторно відновити функціонування системи. Внаслідок чого підвищилося навантаження на працездатні компоненти мережі; мережа перейшла в стан глобальної нестійкості. Неузгодженість дій італійських і швейцарських операторів, їхня недбалість	Системи аварійної автоматики швидко відключали та ізолювали ЛЕП з підвищеним навантаженням; вузли та генератори, були не здатні повторно відновити функціонування системи. Внаслідок чого підвищилося навантаження на працездатні компоненти топології мережі; мережа перейшла в стан глобальної нестійкості.
4.	Реакція СУ	Як реагувала на аварійну ситуацію СУ об’єктами КЕІ?	Психологічний фактор вплинув на збільшення масштабів затемнення. Оператори припускатися помилок через неуважність, втому або стресовий стан. Оператори не мали уявлення про справжні масштаби відключень	Психологічний фактор вплинув на збільшення масштабів затемнення. Оператори могли припускатися типових помилок через неуважність, втому або стресовий стан.

Продовження таблиці 5.1

№ з/п	Аналізуємий аспект	Питання	Результат аналізу аварії Європейської КЕІ	Результат аналізу аварії Північно-Американської КЕІ
5.	Особливості застосування СУ	Чому аварія не була відвернена СУ об’єктами КЕІ?	У операторів італійської СУ КЕІ не було доступу до даних, які мали оператори швейцарської СУ КЕІ. Погане володіння ситуацією було посилене відсутністю можливості спільного навчання швейцарських і італійських диспетчерів. Неузгодженість дій обслуговуючого персоналу	У США змінилися умови, які вплинули на надійність системи. А саме, за останні 10-15 років в Північній Америці не було реалізовано жодного проєкту по введенню в дію нового високовольтного обладнання (ЛЕП, трансформаторні підстанції тощо). У той же час електрогенеруючі структури знайшли способи для збільшення споживання електроенергії без введення додаткового високовольтного обладнання

Результати перехресного аналізу (табл. 5.1) були застосовані для розробки ПНК протікання аварії КЕІ (рис. 5.5, 5.6), а також в процесі побудови відповідних аналітико-стохастичних моделей (рис. 5.7). Інформація, яка отримана за результатами перехресного аналізу, може бути використана для формування комплексу заходів по зниженню ризиків негативних подій для КЕІ. Наприклад, цю інформацію можна застосовувати для розробки сценаріїв дій операторів СУ КЕІ в нештатних екстремальних ситуаціях; для розробки симуляторів і відповідної тренажерної апаратури для підготовки операторів СУ інфраструктурою; удосконалення загальної структури управління системою технічного обслуговування та ремонту компонентних складових КЕІ; підготовки

проєктної документації для розробки перспективних систем інфраструктури.

5.3 Метод управління готовністю критичної енергетичної інфраструктури за інформаційно-технічним станом

Наступний блок в структурі загальної методології (рис. 2.1, 2.2) присвячений розробці методу управління готовністю КЕІ за інформаційно-технічним станом. Пропонуємий метод базується на результатах моделювання та оцінювання готовності критичної енергетичної інфраструктури та враховує еволюційні аспекти її розвитку [168]. Розглянемо принципи аналізу та управління безпекою [167], які закладено в відповідні стратегії забезпечення готовності КЕІ.

5.3.1 Принципи аналізу та управління безпекою критичної енергетичної інфраструктури

Зрозуміло, що виконати оцінку інформаційно-технічних станів КЕІ в цілому досить складно. Тому з урахуванням фізичної сутності та з метою спрощення завдання, яке розв’язується, пропонується використовувати теоретико-множинну модель КЕІ, що описується співвідношеннями (5.6)–(5.8). Крім того, додатково будемо керуватися наступними принципами аналізу безпеки КЕІ [167]:

1. Кожна складова ТММ КЕІ (5.6)–(5.8) може бути описана таблицею функційної безпечності SF_i. По аналогії з таблицею FMECA [8] кожному рядку таблиці SF_i ставиться у відповідність стан F_{ij}, $j=1,...,m_j$. Вся множина ІТС КЕІ включає не тільки працездатні стани F_{io}, непрацездатні стани з раптовими (прихованими) відмовами F_{ij}, де $j=1,...,m_j$, з кратними відмовами $F_{ij}^{(h)}$, де $h=2,...,m_j$ згідно з [8], але й стани з відмовами (відключеннями) критичних систем (об’єктів), які виникли внаслідок кібератак та інших ЗВШВ на кіберактиви інфраструктури F_{ik}, де $k=1,...,n_k$ та $F_{ik}^{(c)}$ ($c=2,...,n_k$):

$$MF_i=\left\{F_{io},F_{ij},F_{ij}^{(h)},F_{ik},F_{ik}^{(c)}\right\}. \tag{5.9}$$

2. Кожному стану F_{ij} та F_{ik} ставиться у відповідність ймовірність p_{ij} та значення показника ПНД L_{ij}. Добуток цих двох величин визначає ступінь

критичності перебування КЕІ в станах F_{ij} та F_{ik}, тобто

$$R_{ij} = p_{ij} L_{ij}. \tag{5.10}$$

У співвідношенні (5.10) складова p_{ij} визначається у відповідності з (4.55) як $p_{ij} = 1 - K_{\Gamma_{ij}}$. Далі результати SF-аналізу згортаються у матриці критичності розмірністю $a \times b$, де a, b – кількість рядків та стовпців, відповідно, які визначаються значеннями ймовірності $P_{ij}(p)$ та важкості наслідків $L_{ij}(l)$. Матриці записуються у вигляді

$$MR_i = \left\| R_{ij}(p,l) \right\|. \tag{5.11}$$

В матриці MR_i (5.11) діагональ критичності, порядок визначення необхідності проведення корегуючих дій визначаються відповідно до вимог, які наведено в роботах [8, 167].

3. Для кожного рядка SF-таблиці компонентної складової інфраструктури S_i визначається ступінь (ймовірність) впливу відповідної відмови (події) та переходу в стан F_{ij} на стану F_{vg} інших компонентних складових КЕІ S_v ($v = 1,...,n, v \neq i, g = 1,...,m_g$). На стан F_{vg} можуть впливати наступні події:

1) відмова (подія) F_{ij} приводить до зміни (зростання або зменшення) ймовірності P_{vg};

2) відмова (подія) F_{ij} приводить до зміни (зростання або зменшення) важкості наслідків L_{wg};

3) відмова (подія) F_{ij} викликає появу нової (неспецифікованої раніше) відмови (події) F_{vmg+1};

4) відмова (подія) F_{ij} приводить до комбінації подій 1–3;

5) відмова (подія) F_{ij} не впливає на стан F_{vg}.

Виходячи з зазначеного, вплив компоненти S_i на компоненту S_v можна описати за допомогою матриці

$$MD_{iv} = \left\| d_{jg}^{iv} \right\|, \tag{5.12}$$

де d_{jg}^{iv} – вектор, який враховує вплив F_{ij} на F_{vg}.

У співвідношенні (5.12) вектор d_{jg}^{iv} визначається як

$$d_{jg}^{iv} = \left\langle \left(x_{jg1}^{iv}, Q_{jg1}^{iv}\right), \left(x_{jg2}^{iv}, Q_{jg2}^{iv}\right), \left(x_{jg3}^{iv}, Q_{jg3}^{iv}\right), \left(x_{jg4}^{iv}, Q_{jg4}^{iv}\right), ... \right\rangle, \tag{5.13}$$

де $x_{jgz}^{iv} = 1(0)$, якщо реалізується (не реалізується) відповідний варіант z впливу F_{ij} на F_{vg}, z = 1,…,5 (одиниці може дорівнюватися тільки одна змінна x_{jgz}^{ik}); L_{jgz}^{iv} – оператор, який характеризує ймовірність та ступінь впливу (якщо $x_{jgz}^{iv} = 0$, то $Q_{jgz}^{iv} = \varnothing$).

Принципи управління безпекою КЕІ можна викласти наступним чином [167]:

1. На підставі розглянутих принципів аналізу пропонується організувати управління КЕІ на всіх можливих рівнях ієрархії з урахуванням впливу множини факторів, включаючи функційну та інформаційну складову забезпечення безпеки. Такий підхід можна реалізувати шляхом переходу до управління готовністю КЕІ за інформаційно-технічним станом.

Під інформаційно-технічним станом (ITS) критичної енергетичної інфраструктури будемо розуміти вектор-функцію виду

$$ITS = F(W, S, R, U, Q), \tag{5.14}$$

де $W = \{W_i\}_{i=1}^{n}$ – множина завдань, які розв’язуються за допомогою КЕІ; $S = \{S_r\}_{r=1}^{k}$ – множина компонентних складових (систем), які входять до складу КЕІ; $R = \{R_d\}_{d=1}^{g}$ – множина режимів експлуатації КЕІ; $U = \{U_h\}_{h=1}^{e}$ – множина стратегій управління готовністю КЕІ; $Q = \{Q_j\}_{j=1}^{m}$ – множина структур КЕІ, враховуючи варіанти реформування (реструктуризації, тощо).

В робот [169] розглянуто питання управління критичними інфраструктурами за їхнім технічним мегастаном. Вважається, що вся сукупність

технічних станів компонентних складових інфраструктури в глобальному сенсі може бути об’єднана в один єдиний мегастан, кількісна оцінка якого визначається та контролюється в процесі експлуатації КЕІ.

2. Управління безпекою КЕІ за її ІТС базується на відомих принципах та стратегіях гнучкого управління готовністю складних систем за їхнім технічним станом [111] і управлінні гарантоздатністю інформаційно-керуючих систем інфраструктури за їхнім інформаційно-технічним станом [170]. В роботі [171] розглянуто концепцію технічного обслуговування компонентних складових КЕІ, орієнтованого на підвищення продуктивності інфраструктури. Концепція базується на застосуванні емпіричної моделі старіння для організації ефективного технічного обслуговування компонентних складових інфраструктури.

Тому фактично отримані в попередніх розділах дисертаційного дослідження результати моделювання доцільно використовувати для обґрунтування стратегій U управління готовністю КЕІ за інформаційно-технічним станом. Виходячи з цього, було запропоновано дві стратегії, а саме: з централізованим управлінням $U_{ЦУ}$ готовністю КЕІ, з децентралізованим управлінням $U_{ДЦУ}$ готовністю КЕІ. При цьому оцінка готовності КЕІ при управлінні за ІТС здійснювалася за результатами аналітико-стохастичного моделювання поведінки інфраструктури.

3. Управління безпекою та іншими властивостями КЕІ повинно здійснюватися в контексті її еволюції, яка обумовлена зміною вимог до систем, характеристик зовнішнього середовища і т.і. Застосування хмарних систем надає широкі можливості щодо вирішення зазначеного завдання і може розглядатися як один з аспектів еволюційного розвитку СУ КЕІ. В роботі [172] розглянута концепція управління готовністю критичних інфраструктур на основі застосування хмарних систем та технологій.

4. Еволюційний характер розвитку КЕІ базується на використанні ефективно працюючої системи оперативного моніторингу ІТС, за допомогою якої можна здійснювати постійний аудит активів та виконувати категоризацію і паспортизацію критично важливих об’єктів інфраструктури за величиною ризику негативного впливу на них.

5.3.2 Еволюційні аспекти управління критичною енергетичною інфраструктурою за інформаційно-технічним станом

Отже, для забезпечення необхідного рівня готовності КЕІ пропонується враховувати еволюційні аспекти розвитку її кібернетичних активів, а також етапи аналітико-стохастичного оцінювання готовності сервіс-орієнтованих хмарних ресурсів, які використовуються в загальному контурі управління інфраструктурою. Для вирішення цієї проблеми було запропоновано перейти до управління готовністю КЕІ за інформаційно-технічним станом, під яким розуміється вектор-функція виду (5.14), яка враховує кількісний склад, структурну побудову, режими експлуатації та стратегії управління готовністю КЕІ.

Для КЕІ від початку створеної як утворення, що еволюціонує, справедливо $T_{ж.ц}^{КВО} \subseteq T_{ж.ц}^{КЕІ}$, де $T_{ж.ц}^{КЕІ}, T_{ж.ц}^{КВО} = \left\{T_i^{КВО}\right\}_i^N$ – тривалість життєвого циклу КЕІ та КВО, відповідно. Якщо КЕІ створена на базі вже існуючих КВО (наприклад, в результаті реформування і т.і.), тоді $T_{ж.ц}^{КЕІ} = \max T_{ж.ц}^{КВО}$. Тоді цілком виправданим буде застосування апарату еволюційного моделювання процесів використання за призначенням КЕІ протягом усього їхнього життєвого циклу.

При розгляді еволюційних аспектів КЕІ будемо виходити з того, що вона розглядається як «система-систем» (system of systems), що має певний запас R-стійкості, тобто здатна до супротиву, парируванню наслідків змін [170]. З практичної точки зору, в першу чергу КЕІ повинна бути стійкою до каскадних відмов. Використання еволюційного підходу, надає можливість розглянути різні за принципами побудови схемні рішення для будь-яких КІ.

Найбільш поширеною є загальна схема побудови (рис. 5.9), що передбачає подальший еволюційний розвиток КІ [168], виходячи з того, що ще на ранніх етапах життєвого циклу (наприклад, на етапах розробки та НДР) компонентні складові зі складу інфраструктури проєктуються з урахуванням їх адаптації до умов, що змінюються в процесі використання за призначенням. Роль та місце макропроцедури управління готовністю КІ за ІТС в структурі еволюційного

розвитку інфраструктури наочно представлено на рис. 5.10. Відповідно до цієї схеми незалежно від шляхів еволюційного розвитку (прогресивного чи регресивного) при наявності ретроспективної інформації (аналоги КВО, КІ) має здійснюватися управління готовністю КІ за інформаційно-технічним станом.

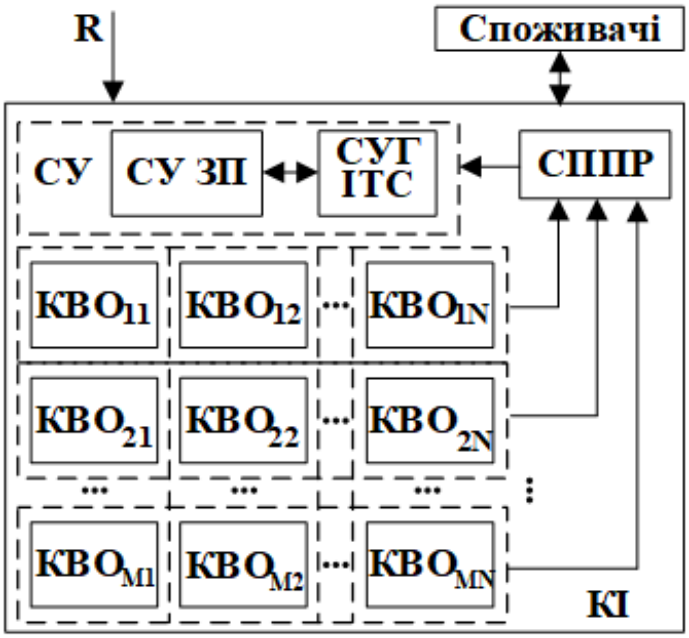


Рис. 5.9 Загальна схема побудови критичної інфраструктури

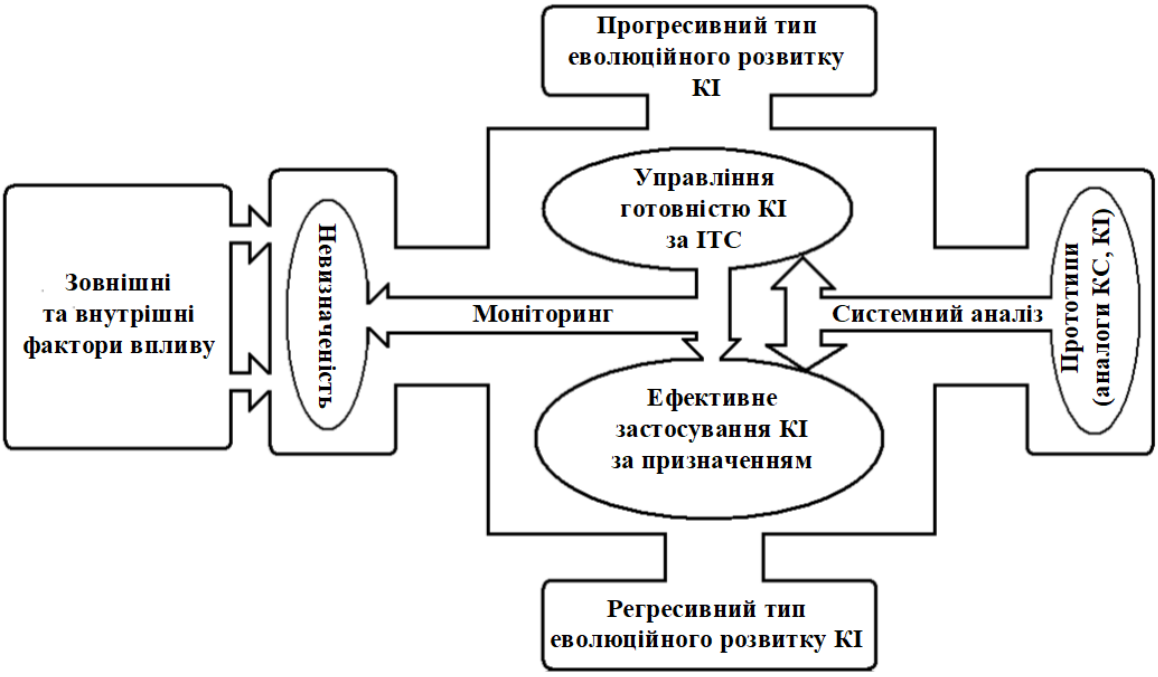


Рис. 5.10 Роль та місце макропроцедури управління готовністю КІ за ІТС в структурі еволюційного розвитку

Разом з тим, еволюційні аспекти розвитку КІ породжують наступні методологічні проблеми:

1) розвиток наукових основ управління готовністю КІ за ІТС (оцінка викликів в сучасному світі; аналіз сучасного стану КІ; моделі та методи управління готовністю КІ за ІТС та ін.);

2) розробка програм управління готовністю КІ за ІТС (моделі, методи контролю (моніторингу) і управління готовністю КІ за ІТС; показники і критерії ефективності управління готовністю КІ за ІТС та ін.);

3) розробка програм проєктування систем контролю і управління готовністю КІ за ІТС (методи синтезу систем контролю і управління готовністю КІ за ІТС; інформаційні технології управління готовністю КІ за ІТС та ін.).

Незважаючи на те, що існує інформаційна невизначеність (рис. 5.10), метою управління готовністю КІ за ІТС є забезпечення ефективної експлуатації інфраструктури незалежно від шляху еволюційного розвитку. Тому до складу системи управління КІ (рис. 5.9) повинні входити система управління застосуванням за призначенням (СУ ЗП) і система управління готовністю за інформаційно-технічним станом (СУГ ІТС). На рівні КВО система управління будується аналогічно, тобто складається з системи використання за призначенням і системи управління технічним станом. Подальші наукові дослідження пов’язані з розробкою методологічних основ і концепції розглянутого наукового напрямку.

Висновки до розділу 5

1. Розглянуто методи забезпечення готовності критичної енергетичної інфраструктури, які засновані на виконанні причинно-наслідкової декомпозиції негативних подій, компаративістичного аналізу та моделюванні процесів протікання аварії інфраструктури. Застосування отриманих причинно-наслідкових комплексів дозволяє структурувати компоненти КЕІ, побудувати відповідні оцінні моделі та визначити рівень функційної безпечності інфраструктури в цілому.

2. Застосування розробленого апарату аналітико-стохастичного

моделювання надало можливість отримати кількісні оцінки коефіцієнта готовності КЕІ для випадків аварії інфраструктури і різноманітних негативних впливів на її кібернетичні активи, підтверджуючи необхідність удосконалення системи моніторингу інформаційно-технічних станів щодо виявлення, пом’якшення дії зловмисних шкідливих впливів на готовність та забезпечення необхідного рівня функційної безпечності інфраструктури.

3. Розроблено апарат логіко-цифрового представлення причинно-наслідкової декомпозиції аварії критичної енергетичної інфраструктури, застосування якого на основі використання операції підсумовування по модулю два дозволяє уніфікувати та спростити процедуру оцінки наслідків аварії КЕІ.

4. В розділі розглянуто метод аналізу на основі модифікованої алгебри причинно-наслідкових комплексів та метод компаративістичного аналізу аварій КЕІ, використання яких дозволить моделювати поведінку критичної енергетичної інфраструктури, враховуючи негативні впливи на її активи та здійснити перехід до стратегій управління готовністю інфраструктури за її інформаційно-технічним станом.

5. Еволюційний характер розвитку критичних інфраструктур базується на відповідних принципах аналізу та управління їхньою безпекою. Застосування ефективно працюючої системи оперативного моніторингу ІТС компонентних складових критичних інфраструктур дозволить проводити постійний аудит їхніх активів та здійснювати категоризацію і паспортизацію критично важливих об’єктів інфраструктури за величиною ризику негативних впливів на них.

Основні положення цього розділу викладені у публікаціях автора [8, 113, 136, 166, 167–169, 171, 172].

РОЗДІЛ 6
МЕТОДИ ВИБОРУ, ОЦІНКИ ХАРАКТЕРИСТИК ГОТОВНОСТІ ТА ЕНЕРГОЕФЕКТИВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР

6.1 Метод вибору характеристик готовності хмарних систем критичних інфраструктур

Забезпечення готовності хмарних систем критичних інфраструктур базується на методології, структура якої зображена на рис. 2.1. Для реалізації основних положень запропонованої методології висунуто концепцію, яка полягає в створенні хмарних систем критичних інфраструктур як систем високої готовності з недостатньо надійних та безпечних інтегрованих фізичних (віртуальних) компонентів в умовах негативних впливів, відмов і атак на їхні вразливості. В цьому сенсі важливо розробити науково-методичний апарат, застосування якого дозволить підвищити готовність та функційну безпечність хмарних систем критичних інфраструктур. Тому в ракурсі виконання завдання відповідно до структури методології, яка зображена на рис. 2.1, необхідно:

– розробити метод вибору характеристик готовності хмарних систем критичної інфраструктури шляхом послідовної реалізації процедур аналітико-стохастичного моделювання поведінки хмарних компонентів з урахуванням зовнішніх та внутрішніх факторів негативного впливу;

– оцінити енергоефективність хмарної інфраструктури шляхом аналітико-стохастичного оцінювання споживаної потужності з урахуванням готовності інтегрованих фізичних та віртуальних компонентів.

З’ясуємо на які особливості архітектурної побудови хмарної інфраструктури [173–175] в першу чергу слід звернути увагу, щоб розв’язати відповідні завдання. Частково нюанси побудови критичних і хмарних інфраструктур з застосуванням систем моніторинга їхніх технічних та інформаційно-технічних станів висвітлено в роботах [109, 32].

6.1.1 Архітектура хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів

Відповідно до класифікаційної схеми, яку зображено на рис. 1.19, необхідним і важливим елементом сучасної критичної інфраструктури є система оперативного моніторингу інформаційно-технічних станів фізичних, кібернетичних та хмарних активів КІ. Результати моделювання поведінки КІ з урахуванням впливу різноманітних відмов компонентних складових свідчать, що саме завдяки застосування системи оперативного моніторингу ІТС вдається підтримувати необхідний рівень готовності інфраструктури в цілому [109, 32].

Слід зазначити, що для більшості видів КІ система моніторингу ІТС повинна використовуватися як повністю автономна. В першу чергу, це стосується КЕІ. Наприклад, однією з причин катастрофи на Саяно-Шушенській ГЕС (Росія, 2009 р.) були відсутність автономного електроживлення системи автоматичного контролю [176] та систематичні порушення працівників служби моніторингу, які не виконували вимоги про регулярний контроль технічного стану основного обладнання [177]. Безумовно вимога атвономності значно підвищує вартість системи моніторингу ІТС, але є цілковито виправданою з точки зору забезпечення готовності та функційної безпечності КІ, що підтверджується результатами аналітико-стохастичного моделювання.

Варто звернути увагу на оперативність виконання моніторингу ІТС компонентних складових ХМІ за умови відповідності архітектурної побудови інфраструктури принципам компліментарності (підрозділ 2.1.3) та оперативного моніторингу (підрозділ 2.1.4). На відміну від КЕІ система оперативного моніторингу інформаційно-технічних станів компонентних складових хмарної інфраструктури будується як інтегрована в середовище ХМІ. Архітектура такої системи моніторингу побудована аналогічно структурі, яка зображена на рис. 2.3. Відповідно до класифікаційної схеми, яка зображена на рис. 3.20, контроль інформаційно-технічних станів фізичних машин хмарної інфраструктури здійснюється зовнішнім контуром інтегрованої системи моніторингу ІТС, а віртуальних машин – за допомогою модулів, виконаних у вигляді моніторів

окремих ВМ.

Тоді, спираючись на результати моделювання, отримані в третьому розділі, необхідно з послідовностей $T_i \in [0, t]$, $i = 1,...,n$ та $\tau_{ктс_j}$, $j = 1,...,m$, які визначають періодичність та тривалість контролю ІТС, відповідно, вибрати таку пару $(T_k, \tau_{ктс_r})$, $k \neq r$, щоб виконувався критерій

$$\Im = \begin{cases} W_{IaaS\ Cloud}(T_k, \tau_{ктс_r}) \geq W_{IaaS\ Cloud_0}; \\ C_{min_0} \leq C_0 \leq C_{max_0}, \end{cases} \quad (6.1)$$

де $W_{IaaS\ Cloud_0}$ – гранично припустиме значення показника готовності ХМІ; $C_0 \in [C_{min_0}; C_{max_0}]$ – граничні витрати необхідні на підтримання необхідного рівня готовності ХМІ.

6.1.2 Аналіз ієрархії властивостей хмарних систем критичних інфраструктур

Для аналізу ієрархії властивостей хмарних систем критичних інфраструктур попередньо необхідно встановити зв’язки між активами КІ. Розглянемо виконання цього завдання на прикладі критичної енергетичної інфраструктури.

Керуючись необхідністю реалізації концепції переходу від типової КЕІ (рис. 4.33) до гібридної кіберенергетичної інфраструктури (рис. 2.10), було запропоновано застосовувати сервіс-орієнтовані хмарні ресурси AWS (рис. 2.7). Для здійснення кардинального переходу до якісно нової кіберенергетичної інфраструктури пропонується спільно використовувати потужний потенціал систем синхронізованих векторних вимірювань та сервісів AWS, які відповідно до спрощеної структурної схеми (рис. 1.18) надають можливість розширити фізичні та утворити хмарні активи критичної енергетичної інфрастукрури. На рис. 6.1 зображено зв’язки між фізичними, кібернетичними та хмарними активами критичної енергетичної інфраструктури.

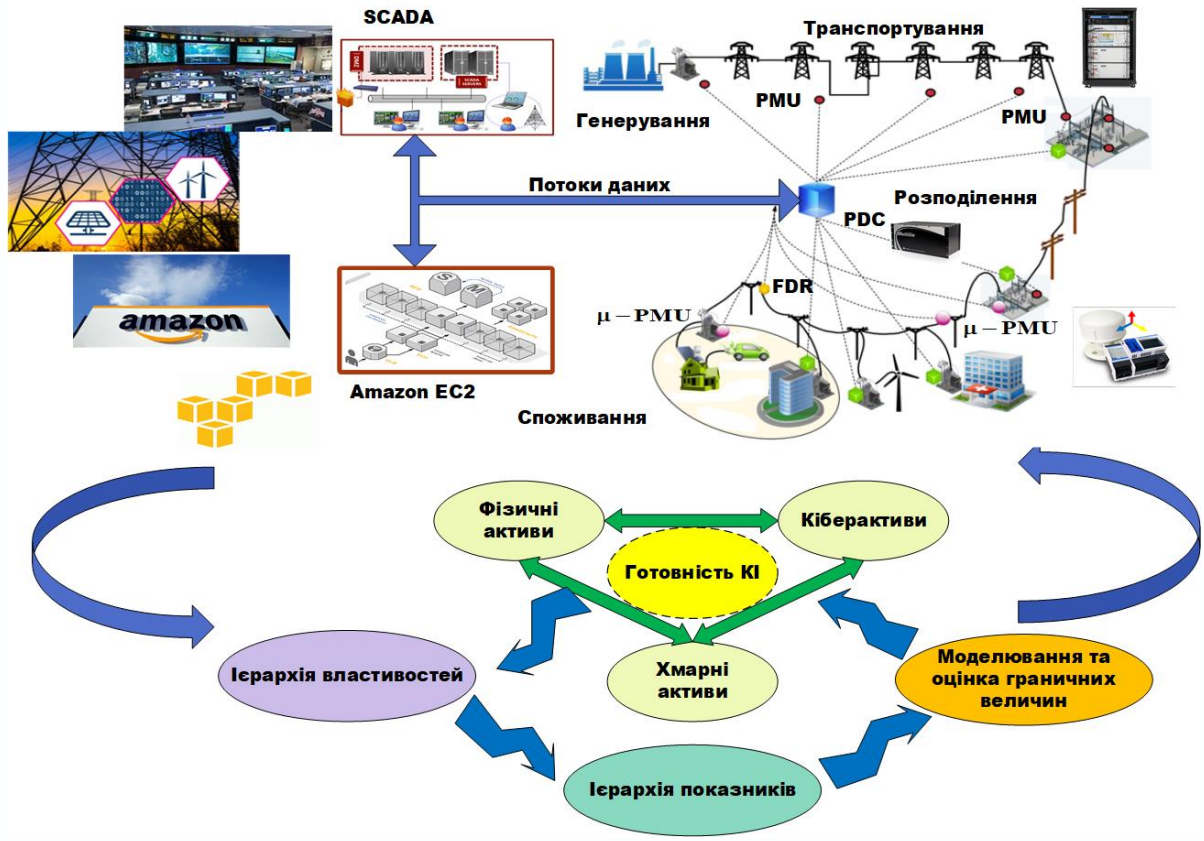


Рис. 6.1 Встановлення зв’язків між активами КЕІ

Отримані результати досліджень підтверджують, що за рахунок застосування додаткових хмарних ресурсів (рис. 6.1), розширюючі обчислювальний потенціал інфраструктури, з’являється можливість посилити моніторингові функції і забезпечити необхідний рівень готовності КЕІ

Розглянувши питання встановлення зв’язків між активами КІ на прикладі критичної енергетичної інфраструктури як перший етап реалізації пропонуємого методу, перейдемо до наступного етапу. Відповідно до рис. 6.1 на наступному етапі встановлюється ієрархія активів КІ. Ця процедура по аналогії з першим етапом теж виконуєься на прикладі критичної енергетичної інфраструктури.

Проведений в першому розділі аналіз свідчить, що важливими для активів КЕІ є наступні властивості: функціональна та інформаційна безпека, продуктивність, готовність, відмовостійкість, надійність, масштабованість, гнучкість управління, контрдії щодо усунення вразливостей програмного забезпечення та інших ЗВШВ. На рис. 6.2 зображено ієрархічну структуру

зазначених властивостей активів КЕІ.

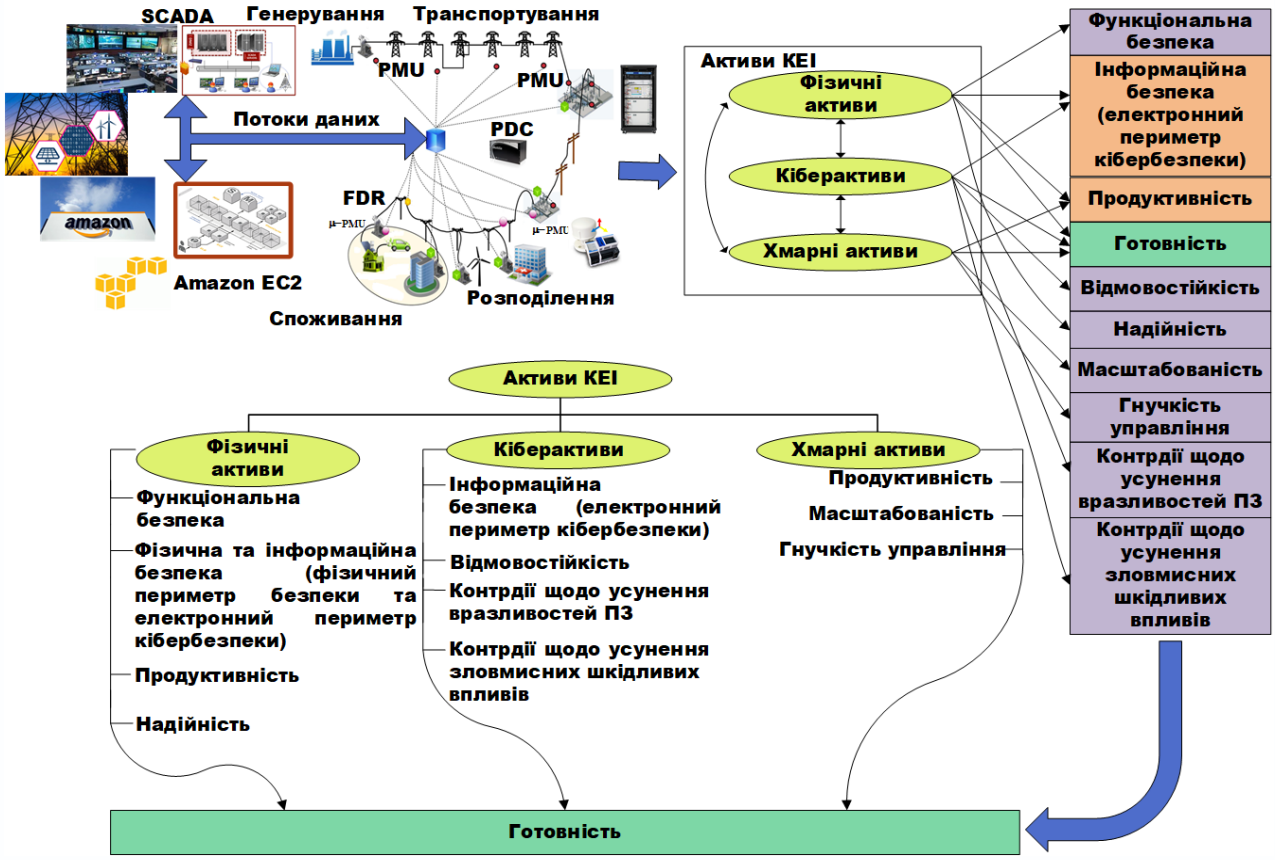


Рис. 6.2 Ієрархічна структура властивостей активів КЕІ

З ієрархічної структури, яка зображена на рис. 6.2, видно, що загальною найбільш важливою властивістю, яка об’єднує та встановлює взаємозалежність між трьома видами активів КЕІ є готовність. Використовуючи ієрархію властивостей активів КЕІ (рис. 6.2), перейдемо до розгляду наступного етапу пропонуємого методу, а саме, розглянемо як здійснюється вибір характеристик готовності хмарних систем критичних інфраструктур.

6.1.3 Аналіз ієрархії та вибір показників готовності хмарних систем критичних інфраструктур

На наступному етапі, використовуючи ієрархію властивостей (рис. 6.2), перейдемо до ієрархії показників готовності хмарних систем критичних інфраструктур. Відповідна процедура встановлення ієрархії показників готовності хмарних систем критичних інфраструктур зображена на рис. 6.3.

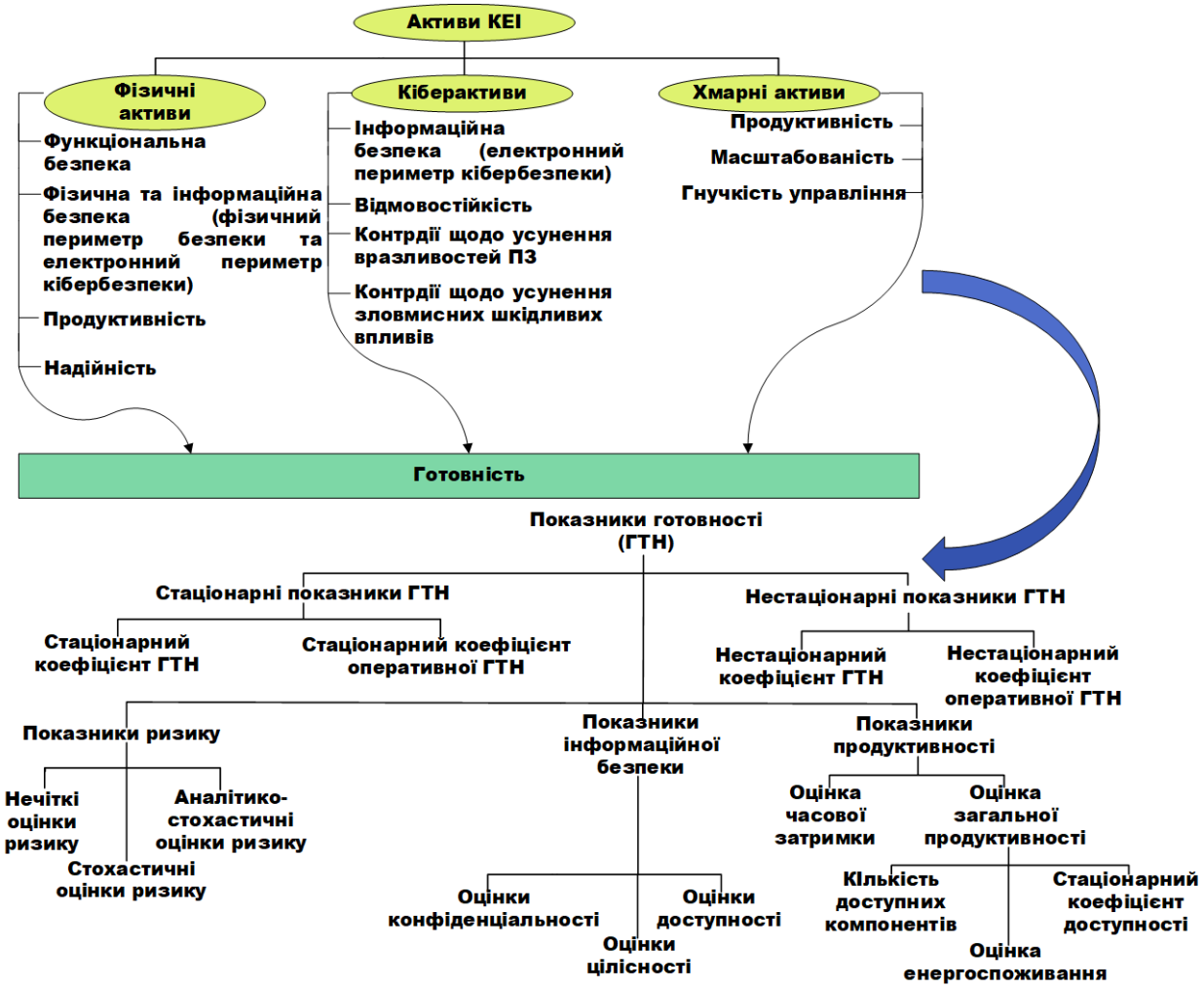


Рис. 6.3 Процедура встановлення ієрархії показників готовності хмарних систем критичної енергетичної інфраструктури

Відповідно до рис. 6.3 показники готовності ХМС КЕІ можна розділити на п’ять груп, а саме: стаціонарні та нестаціонарні показники готовності, показники ризику, показники інформаційної безпеки, показники продуктивності. Для вибору показників готовності хмарних систем згідно з зображеною на рис. 6.3 ієрархією пропонується застосовувати рекомендації, які приводяться в роботах [116, 178, 179], а також враховувати режими функціонування КЕІ. Виходячи з того, що ХМС КЕІ як складова хмарних активів працюють синергічно з інфраструктурою, то будемо вважати, що вони під час застосування за призначенням знаходяться в однакових експлуатаційних режимах. Зважаючи на те, що КЕІ більшу частину часу знаходиться в стаціонарних режимах експлуатації, будемо вважати, що в таких же самих режимах знаходяться та

використовуються за призначенням ХМС. Тому у якості основного показника готовності пропонується застосовувати стаціонарний коефіцієнт готовності (табл. 1.6). Для визначення значень стаціонарного КГ слід застосовувати відомі стохастичні методи оцінювання готовності хмарних систем критичних інфраструктур (табл. 1.5).

6.2 Метод вибору та оцінки характеристик енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів

Метод реалізується в два етапи, а саме:

1) вибір показника енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу ІТС;

2) оцінка характеристик енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу ІТС за результатами аналітико-стохастичного моделювання.

Розглянемо яким чином реалізується перший етап запропонованого методу.

6.2.1 Процедура вибору характеристик енергоефективності хмарної іфраструктури

Теоретичною основою для реалізації процедури є зелений інжиніринг, основні положення якого на підставі аналізу енергоспоживання програмного забезпечення та світового енергоспоживання при розробці інфокомунікаційних технологій розглянуто в роботах [180, 181]. Найбільшої уваги заслуговує робота [60], в якій отримано оцінку продуктивності ХМІ з урахуванням енергоспоживання фізичних машин, що входять до складу інфраструктури. Кількісні оцінки отримано на основі застосування апарату марковського моделювання та стохастичних мереж Петрі [182].

Спираючись на відповідний теоретичний базис та застосовуючи зображену на рис. 6.3 ієрархію показників готовності хмарних систем КЕІ, запропонована наступна процедура вибору характеристик енергоефективності хмарної

інфраструктури:

1) підготовка вхідних даних для виконання аналітико-стохастичного моделювання та оцінки стаціонарного коефіцієнта готовності ХМІ з урахуванням доступності фізичних машин (серверів за типами), які розвератються на базі інфраструктури;

2) аналіз структурної побудови ХМІ з метою визначення кількості підсистем, які включають до свого складу фізичні машини (сервери за типами);

3) вибір енергетичного параметра, який зручно застосовувати для оцінки енергоспоживання фізичних машин (серверів за типами) за той чи інший період часу.

При виконанні третього пункту розглянутої процедури пропонується у якості енергетичного параметру фізичних машин (серверів за типами) хмарної інфраструктури застосовувати споживчу потужність в Ваттах. Місце та роль процедури вибору характеристик енергоефективності хмарної інфраструктури в загальній класифікаційній схемі вибору показників готовності, характеристик надійності та безпеки ХМС КІ зображено на рис. 1.19.

6.2.2 Етапи оцінювання характеристик енергоефективності хмарної інфраструктури

Від процедури вибору перейдемо до розгляду етапів оцінювання характеристик енергоефективності хмарної інфраструктури. Згідно з концепцією зеленого інжинірингу [180, 181] ХМІ повинна будуватися так, щоб заощадити на споживанні електроенергії. Це досить серйозна проблема, виходячи з того, що насьогодні хмарні інформаційні центри споживають 1%, а в 2030 році у кращому випадку будуть споживати 8%, в гіршому випадку – 21% світового енергоспоживання [183]. Тому з метою економії енергоспоживання одна з запропонованих ще в 2014 р. концепцій побудови ХМІ (рис. 1.16) передбачала застосування трьох підсистем ФМ і ВМ та інтегрованої системи моніторингу ІТС (рис. 3.12). В напрямку розвитку зазначеної концепції пропонується оцінювати характеристики енергоефективності ХМІ в три етапи, а саме: а) на першому етапі

застосовується відома з [60] модель продуктивності інфрастуктури з трьома підсистемами ФМ і ВМ для підготовки вхідних даних для подальшого оцінювання; б) на другому етапі будується напівмарковська модель готовності ХМІ з трьома підсистемами ФМ і ВМ та інтегрованою системою моніторингу ІТС; в) на третьому етапі, застосовуючи результати напівмарковського моделювання готовності ХМІ, виконується аналітико-стохастичне оцінювання показників енергоефективності інфраструктури. На рис. 6.4 зображено класифікаційну схему оцінювання енергоефективності ХМІ.

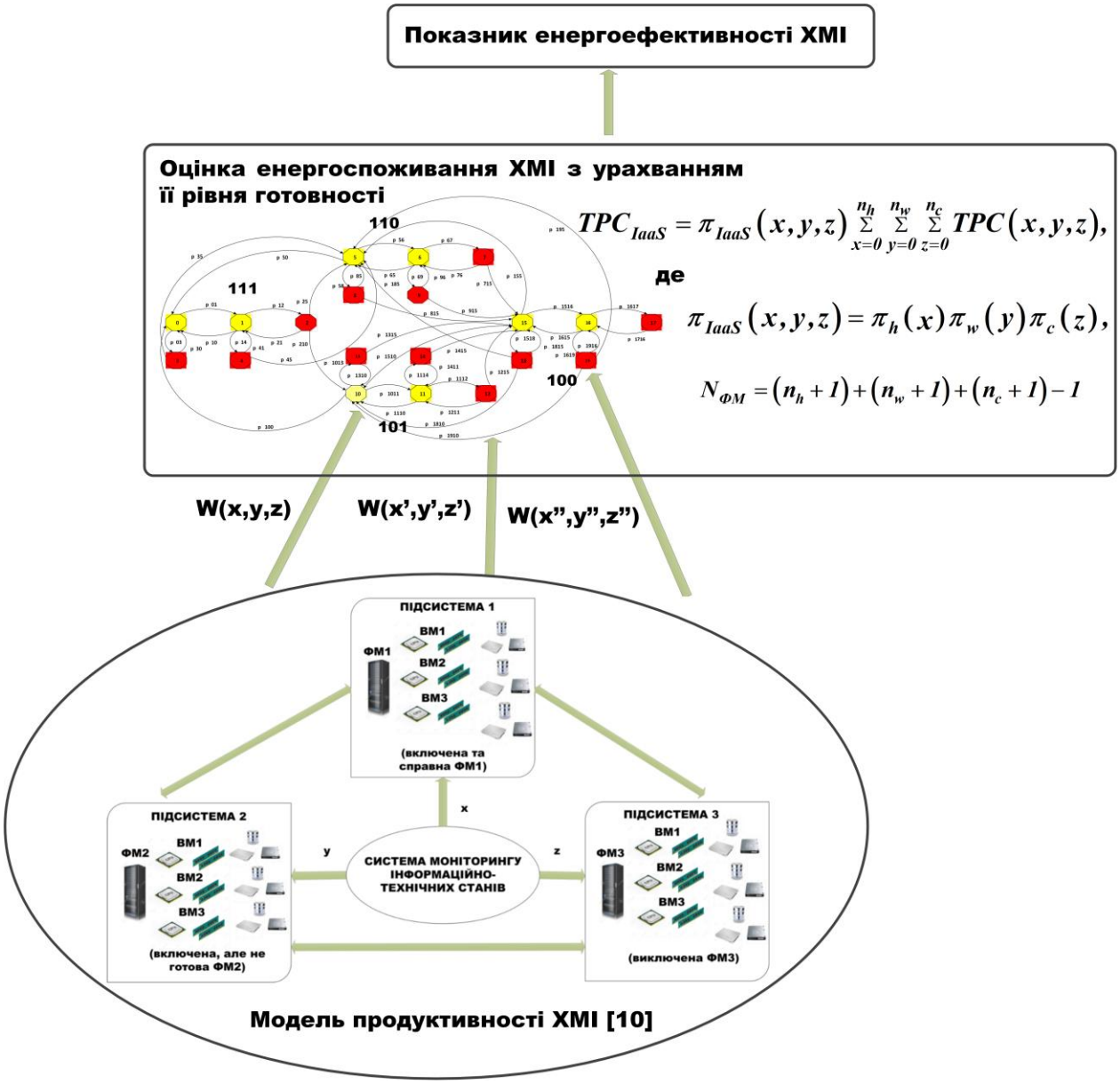


Рис. 6.4 Класифікаційна схема оцінювання енергоефективності ХМІ

Побудуємо відповідні моделі та виконаєм аналітико-стохастичне оцінювання енергоефективності хмарної інфраструктури.

6.2.3 Аналітико-стохастична модель енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів

Для реалізації наступного етапу методу вибору та оцінки характеристик енергоефективності ХМІ у відповідності з класифікаційною схемою, яка зображена на рис. 6.4, будується напівмарковська модель готовності інфраструктури з трьома підсистемами фізичних і віртуальних машин та інтегрованою системою оперативного моніторингу інформаційно-технічних станів (далі, скорочено НПММ готовності ХМІ). Ця напівмарковська модель є продовженням модельного ряду, представленого в роботах [33, 74, 123, 184]. На рис. 6.5 зображено граф станів пропонуємої до розгляду моделі.

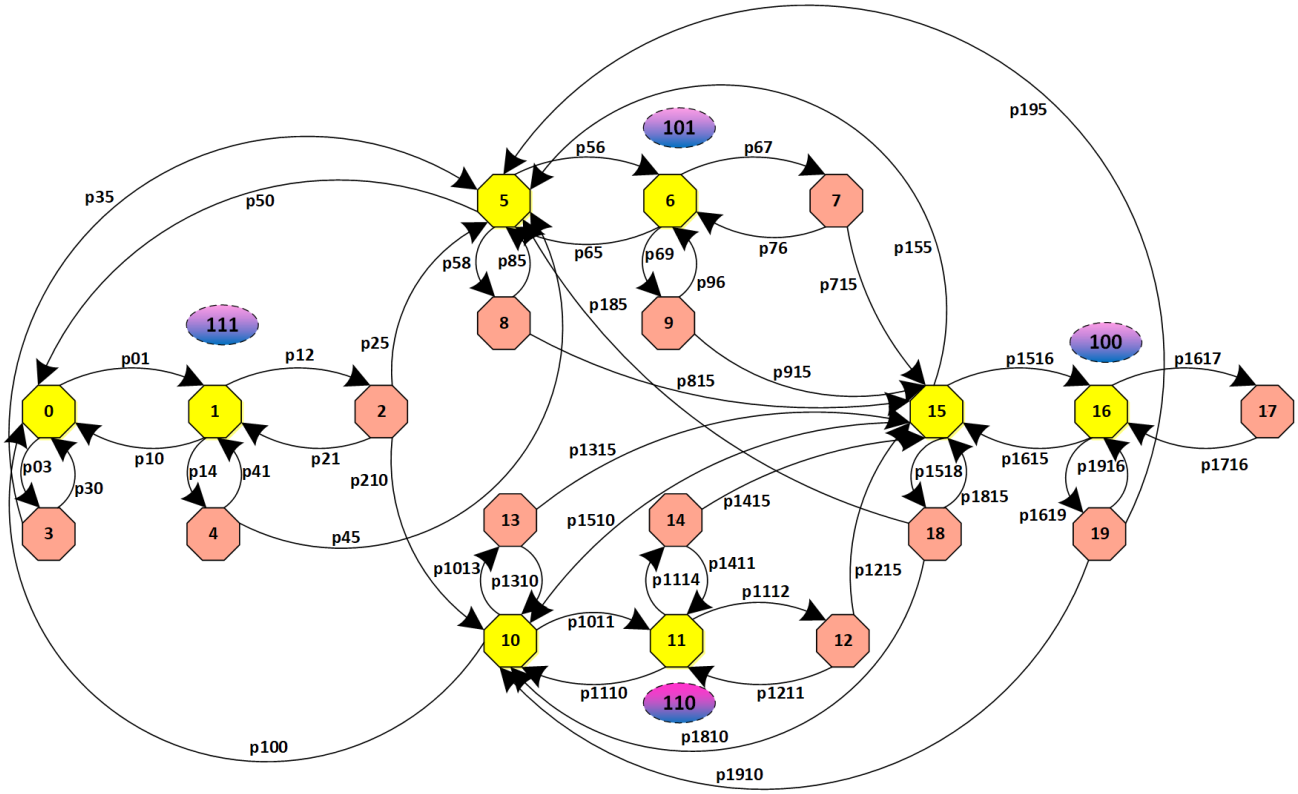


Рис. 6.5 Граф станів НПММ готовності ХМІ з трьома підсистемами ФМ і ВМ та інтегрованою системою оперативного моніторингу ІТС

Фактично на рис. 6.5 зображено граф станів напівмарковської моделі готовності ХМІ, до складу якої входять три фізичні $(n_{PM}=3)$ та шість віртуальних машин $(n_{VM}=6)$ [33]. Згідно з принципом реконфігурування та надлишковості (рис. 2.3) ХМІ вважається працездатною, а її ресурс мінімально доступним, коли відповідно до системи вимог і обмежень (2.2) виконується умова $n_{PM}\geq 1$, $n_{VM}\geq 1$. В противному випадку, коли $n_{PM}=0$, $n_{VM}=0$, ХМІ вважається непрацездатною. Крім того, будемо вважати, що на НПММ (рис. 6.5) розповсюджуються такі ж самі припущення, як і на модель, граф станів, якої зображено на рис. 3.22. Тоді, напівмарковська модель (рис. 6.5) може бути задана наступним чином: $\forall S_i \in S_{A_{IaaS}}$, де $i=\overline{0,19}$, $S_{A_{IaaS}}=\{S_0,S_1,S_5,S_6,S_{10},S_{11},S_{15},S_{16}\}$ $\exists$ $\exists\ \pi_A=\{\pi_0,\pi_1,\pi_5,\pi_6,\pi_{10},\pi_{11},\pi_{15},\pi_{16}\}$ та $\forall S_i \in S_{UA_{IaaS}}$, $S_{UA_{IaaS}}=\{S_2,S_3,S_4,S_7,S_8,S_9,S_{12},$ $S_{13},S_{14},S_{17},S_{18},S_{19}\}$ $\exists$ $\pi_{UA}=\{\pi_2,\pi_3,\pi_4,\pi_7,\pi_8,\pi_9,\pi_{12},\pi_{13},\pi_{14},\pi_{17},\pi_{18},\pi_{19}\}$, $\sum_{i=0}^{19}\pi_i=1$, $S_{A_{IaaS}}\subset S$, $S_{UA_{IaaS}}\subset S$, $S=S_{A_{IaaS}}\cup S_{UA_{IaaS}}$, $S=\{S_0,...,S_{19}\}$, $\forall S_i \to S_k \exists\ Q_{ik}(t)\in |Q_{ij}(t)|$. Елементи матриці $|Q_{ij}(t)|$ задаються $\forall\ S_i \to S_j$, що описують відмови ВМ як

$$Q_{ij}(t)=1-e^{-\lambda_i t}=\mathrm{Exp}(\lambda_i). \tag{6.1}$$

У той же час $\forall\ S_i \to S_j$, де $i\neq k$, елементи матриці $|Q_{ij}(t)|$, що описують процес відновлення ВМ та міграції їхнього ресурсу, записуються у вигляді

$$Q_{ji}(t)=1-(1+\mu_j t)\ e^{-\mu_j t}=\mathrm{Erlang}(2,\mu_j). \tag{6.2}$$

В співвідношеннях (6.1), (6.2) значення інтенсивностей відмов λ_i та інтенсивностей відновлення працездатності ФМ (ВМ) та міграції ресурсу ФМ (ВМ) μ_j задаються наступним чином:

1) λ_1,λ_2 – інтенсивність раптових відмов гарячих та теплих ФМ, відповідно;

2) λ_3,λ_4 – інтенсивність раптових відмов гарячих та теплих ВМ, відповідно;

3) $\lambda_5=\lambda_1+\lambda_2$ – загальна інтенсивність раптових відмов гарячих та теплих ФМ;

4) $\lambda_6 = \lambda_3 + \lambda_4$ – загальна інтенсивність раптових відмов гарячих та теплих ВМ;

5) $\lambda_7 = 0,5\lambda_3$ – інтенсивність раптової відмови останньої працездатної ВМ;

6) μ_1, μ_2 – інтенсивність відновлення і міграціїї ресурсу гарячих та теплих ФМ, відповідно;

7) μ_3, μ_4 – інтенсивність відновлення і міграціїї ресурсу гарячих та теплих ВМ, відповідно.

Діючими є наступні припущення щодо співвідношень:

1) $T_{0_{ФМ}} / T_{0_{ВМ}} \geq 10$, де $T_{0_{ФМ}}$ – середній час наробітки на відмову ФМ; $T_{0_{ВМ}}$ – середній час наробітки на відмову ВМ;

2) $T_{B_{ФМ}} / T_{B_{ВМ}} \geq 2$, де $T_{B_{ФМ}}$ – середній час відновлення працездатності та міграції ресурсу ФМ; $T_{B_{ВМ}}$ – середній час відновлення працездатності та міграції ресурсу ВМ.

Далі реалізується процес напівмарковського моделювання у відповідності до функціональної діаграми, яка зображена на рис. 3.11. Для обчислення стаціонарного коефіцієнта готовності з урахуванням зазначених припущень та функцій розподілу відповідних випадкових величин (6.1), (6.2) застосовуються такі співвідношення:

$$P = \left| p_{ij} \right| = K(\infty), \tag{6.3}$$

$$P_{ij}(\infty) = p_{ij} = \int_0^{\infty} \prod_{\ell \neq i} \left[1 - Q_{i\ell}(\theta) \right] dQ_{ij}(\theta), \tag{6.4}$$

$$\pi_i = \frac{\nu_i h_i}{\sum_{i=0}^{N} \nu_i h_i}, \tag{6.5}$$

$$K_{\Gamma_{IaaS}} = \pi_0 + \pi_1 + \pi_5 + \pi_6 + \pi_{10} + \pi_{11} + \pi_{15} + \pi_{16}, \tag{6.6}$$

де ν_i – стаціонарна ймовірність перебування ХМІ в стані S_i, значення якої визначаються з застосуванням дискретного вкладеного марковського ланцюга [111]; h_i – час перебування ХМІ в стані S_i.

В табл. 6.1 наведено функції розподілу для визначення перехідних імовірностей p_{ij} з застосуванням співвідношень (6.1)–(6.6).

Таблиця 6.1

Функції розподілу для визначення перехідних імовірностей напівмарковського процесу моделювання готовності ХМІ

Перехід для ХМІ	Перехід для ФМ та ВМ	Вид функції розподілу
$0 \to 1$ $\to 3$	$(2,1) \to (1,1)$ $\to (2,0)$	$\mathrm{Exp}(\lambda_3)$ $\mathrm{Exp}(\lambda_1)$
$\to 0$ $1 \to 2$ $\to 4$	$\to (2,1)$ $(1,1) \to (0,1)$ $\to (1,0)$	$\mathrm{Erlang}(2,\mu_3)$ $\mathrm{Exp}(\lambda_3)$ $\mathrm{Exp}(\lambda_1)$
$2 \to 1$ $\to 5(10)$	$(0,1) \to (1,1)$ $\to (2,1)$	$\mathrm{Erlang}(2,\mu_3)$ $\mathrm{Erlang}(2,\mu_1)$
$3 \to 0(5)$	$(2,0) \to (2,1)$	$\mathrm{Erlang}(2,\mu_1)$
$4 \to 1$ $\to 5$	$(1,0) \to (1,1)$ $\to (2,1)$	$\mathrm{Erlang}\ (2,\mu_1)$
$\to 0$ $5 \to 6$ $\to 8$	$\to (2,1)$ $(2,1) \to (1,1)$ $\to (2,0)$	$\mathrm{Erlang}(2,\mu_1)$ $\mathrm{Exp}(\lambda_3)$ $\mathrm{Exp}(\lambda_1)$
$\to 5$ $6 \to 7$ $\to 9$	$\to (2,1)$ $(1,1) \to (0,1)$ $\to (1,0)$	$\mathrm{Erlang}(2,\mu_3)$ $\mathrm{Exp}(\lambda_3)$ $\mathrm{Exp}(\lambda_1)$
$7 \to 6$ $\to 15$	$(0,1) \to (1,1)$ $\to (2,1)$	$\mathrm{Erlang}\ (2,\mu_3)$ $\mathrm{Erlang}\ (2,\mu_1)$
$8 \to 5(15)$	$(2,0) \to (2,1)$	$\mathrm{Erlang}\ (2,\mu_1)$
$9 \to 6$ $\to 15$	$(1,0) \to (1,1)$ $\to (2,1)$	$\mathrm{Erlang}\ (2,\mu_1)$

Продовження таблиці 6.1

Перехід для ХМІ	Перехід для ФМ та ВМ	Вид функції розподілу
$\to 0$ $10 \to 11$ $\to 13$	$\to((2,1))$ $(2,1) \to (1,1)$ $\to (2,0)$	$\mathrm{Erlang}(2,\mu_2)$ $\mathrm{Exp}(\lambda_6)$ $\mathrm{Exp}(\lambda_5)$
$\to 10$ $11 \to 12$ $\to 14$	$\to(2,1)$ $(1,1) \to(0,1)$ $\to(1,0)$	$\mathrm{Erlang}(2,\mu_4)$ $\mathrm{Exp}(\lambda_6)$ $\mathrm{Exp}(\lambda_5)$
$12 \to 11$ $\to 15$	$(0,1) \to(1,1)$ $\to(2,1)$	$\mathrm{Erlang}\ (2,\mu_4)$ $\mathrm{Erlang}\ (2,\mu_2)$
$13 \to 10(15)$	$(2,0) \to (2,1)$	$\mathrm{Erlang}\ (2,\mu_2)$
$13 \to 10(15)$	$(2,0) \to (2,1)$	$\mathrm{Erlang}\ (2,\mu_2)$
$14 \to 11$ $\to 15$	$(1,0) \to(1,1)$ $\to(2,1)$	$\mathrm{Erlang}\ (2,\mu_2)$
$\to 5(10)$ $15 \to 16$ $\to 18$	$\to(2,1)$ $(2,1) \to (1,1)$ $\to(2,0)$	$\mathrm{Erlang}(2,\mu_2)$ $\mathrm{Exp}(\lambda_3)$ $\mathrm{Exp}(\lambda_1)$
$\to 15$ $16 \to 17$ $\to 19$	$\to(2,1)$ $(1,1) \to(0,1)$ $\to(1,0)$	$\mathrm{Erlang}(2,\mu_3)$ $\mathrm{Exp}(\lambda_7)$ $\mathrm{Exp}(\lambda_1)$
$17 \to 16$	$(0,1) \to (1,1)$	$\mathrm{Erlang}(2,\mu_3)$
$18 \to 5(10)$ $\to 15$	$(2,0) \to (2,1)$	$\mathrm{Erlang}(2,\mu_2)$ $\mathrm{Erlang}(2,\mu_1)$
$19 \to 5(10)$ $\to 16$	$(1,0) \to(2,1)$ $\to(1,1)$	$\mathrm{Erlang}(2,\mu_2)$ $\mathrm{Erlang}(2,\mu_1)$

Подальші обчислення рівня готовності ХМІ виконуються з застосуванням алгоритму 6.1. Цей же алгоритм застосовується для оцінки показників енергоефективності ХМІ з трьома підсистемами ФМ і ВМ та інтегрованою системою моніторингу ІТС.

Аналітико-стохастичне оцінювання показників енергоефективності ХМІ реалізується шляхом обчислення моделі, яка враховує енергоспоживання інфраструктури та результати напівмарковського моделювання процесів зміни її

рівня готовності (алгоритм 6.1). З цією метою застосовувалися відомі рівняння для визначення показника енергоспоживання TPC_{IaaS} хмарної інфраструктури [60], а саме:

$$N_{ФМ} = (n_h + 1) + (n_w + 1) + (n_c + 1) - 1, \tag{6.7}$$

$$TPC_{IaaS} = \pi_{IaaS}(x, y, z) \sum_{x=0}^{n_h} \sum_{y=0}^{n_w} \sum_{z=0}^{n_c} TPC(x, y, z), \tag{6.8}$$

де $N_{ФМ}$ – загальна кількість працездатних та споживаючих електроенергію ФМ; $TPC(x, y, z)$ – показник енергоспоживання (в Ваттах) *x* гарячих, *y* теплих, *z* холодних працездатних фізичних машин ХМІ; $\pi_{IaaS}(x, y, z)$ – ймовірність складної події, яка полягає в тому, що в будь-який момент часу користувачі ХМІ мають в своєму розпорядженні *x* гарячих, *y* теплих, *z* холодних працездатних (з доступним ресурсом) фізичних машин.

Алгоритм 1: ГОТОВНІСТЬ (ДОСТУПНІСТЬ) ХМАРНОЇ ІНФРАСТРУКТУРИ $\left(K_{\Gamma_{IaaS}}(T) = \{\pi_1, \pi_2, ..., \pi_m\}\right)$

1 Обчислення інтервалу моделювання $K_{\Gamma_{IaaS}}(T)$ як $T = \sum_{i=1}^{n} t_i$

2 Введення вхідних даних та характеристик ХМІ λ_{max}, λ_{step}, t_{min}, t_{step}, μ_j

3 **for** *i=1 to n* **do**

4 $\lambda_i = \lambda_{max} - i \cdot \lambda_{step}$

5 **for** *j = 1 to m* **do**

6 $T_j = t_{min} + j \cdot t_{step}$;

7 $h_j = F(\lambda_i, \mu_j)$;

8 $p_{ij} = G(\lambda_i, \mu_j, T_j)$;

9 $\nu_i = L(h_j, p_{ij})$;

10 $\xi_i = \nu_i \cdot p_{ij}$;

11 $\eta_i = \sum_{i \in S} \nu_i \cdot p_{ij}$;

12 $\pi_i = \xi_i / \eta_i$;

13 $\pi_{i(\ell)}(t) = \sum_{\ell \in S_A} \pi_\ell$;

14 **end**

15 **end**

16 **return** $K_{\Gamma_{IaaS}}(T) = \pi_{i(\ell)}(t)$; **mesh** ($t, \lambda_i, K_{\Gamma_{IaaS}}(T)$); **visualization** $K_{\Gamma_{IaaS}}(\lambda_i, T)$

У співвідношенні (6.8) значення ймовірності $\pi_{IaaS}(x,y,z)$ можна визначити за допомогою співвідношення [60]

$$\pi_{IaaS}(x,y,z)=\pi_h(x)\pi_w(y)\pi_c(z), \tag{6.9}$$

де $\pi_h(x)$ – стаціонарна ймовірність наявності *x* гарячих ПРС ФМ; $\pi_w(y)$ – стаціонарна ймовірність наявності *y* теплих ПРС ФМ; $\pi_c(z)$ – стаціонарна ймовірність наявності *z* холодних ПРС ФМ.

Складові співвідношення (6.9) визначаються за результатами напівмарквоського моделювання (рис. 6.5). На відміну від відомого показника енергоспоживання хмарної інфраструктури, пропонуємий до застосування показник $ТРС_{IaaS}$ (6.7) не є постійною величиною на інтервалі часу $T\in[0,t]$, а представляє собою функціональну залежність від комплексного показника готовності ХМІ.

При обчисленні показника $ТРС_{IaaS}$ враховується енергоспоживання трьох ФМ, які позначаються індексом (111), тобто розрахунки ведуться для однієї гарячої, однієї теплої і однієї холодної фізичних машин. Слід пам’ятати, що холодна ФМ електроенергію не споживає. Крім того, вважається, що робота всіх шести віртуальних машин між собою синхронізована. Проте, враховуючи співвідношення $ТРС_{ВМ} \square ТРС_{ФМ}$, при розрахунках показника енергоспоживання $ТРС_{IaaS}$ хмарної інфраструктури в цілому, енергоспоживанням віртуальних машин можна знехтувати. Характеристика станів НПММ готовності ХМІ з урахуванням енергоспоживання фізичних машин наведена в табл. 6.2.

Таблиця 6.2

Характеристика станів напівмарковської моделі готовності ХМІ

Індекс енергоспоживання	Характеристика енергоспоживання ФМ	Підмножина станів НПММ готовності
(111)	Гаряча та тепла ФМ споживають електроенергію; холодна ФМ електроенергію не споживає	S_0,S_1,S_2,S_3,S_4

Продовження таблиці 6.2

Індекс енергоспоживання	Характеристика енергоспоживання ФМ	Підмножина станів НПММ готовності
(101)	Гаряча ФМ споживає електроенергію; тепла та холодна ФМ електроенергію не споживають	S_5, S_6, S_7, S_8, S_9
(110)	Гаряча та тепла ФМ споживають електроенергію; холодна ФМ електроенергію не споживає	$S_{10}, S_{11}, S_{12}, S_{13}, S_{14}$
(100)	Гаряча ФМ споживає електроенергію; тепла та холодна ФМ електроенергію не споживають	$S_{15}, S_{16}, S_{17}, S_{18}, S_{19}$

У якості прикладу визначим значення показника $ТРС_{IaaS}$ хмарної інфраструктури за три місяці застосування її за призначенням, коли деякі вхідні дані змінюються в певному діапазоні (табл. 6.3) , інші – приймають фіксовані значення. На рис. 6.6 зображено кількісні результати моделювання залежності $K_{\Gamma_{IaaS}}(\lambda_1, T)$. Крім того, на рис. 6.7, 6.8 зображено результати обчислення показника енергоспоживання хмарної інфраструктури $ТРС_{IaaS}$ для конкретного типу серверних систем (тобто фізичних машин), які входять до складу інфраструктури. Обчислення (рис. 6.7, 6.8) виконано для різних варіантів завантаження серверних систем ХМІ [60].

Таблиця 6.3

Вхідні дані для обчислення напівмарковської моделі готовності ХМІ

Інтенсивність відмов гарячих ФМ, 1/год.	Інтенсивність відновлення/міграції ресурсу гарячих ФМ, 1/год.	Інтенсивність відмов гарячих ВМ, 1/год.	Інтенсивність відновлення/міграції ресурсу гарячих ВМ, 1/год.
$\lambda_{1_{min}} = 2 \cdot 10^{-5}$, $\lambda_{1_{max}} = 1 \cdot 10^{-4}$	$\mu_{1_{min}} = 4;5;8;10$, $\mu_{1_{max}} = 20;30;40;50$	$\frac{\lambda_1}{\lambda_3} \geq 10$	$\frac{\mu_3}{\mu_1} \geq 2$

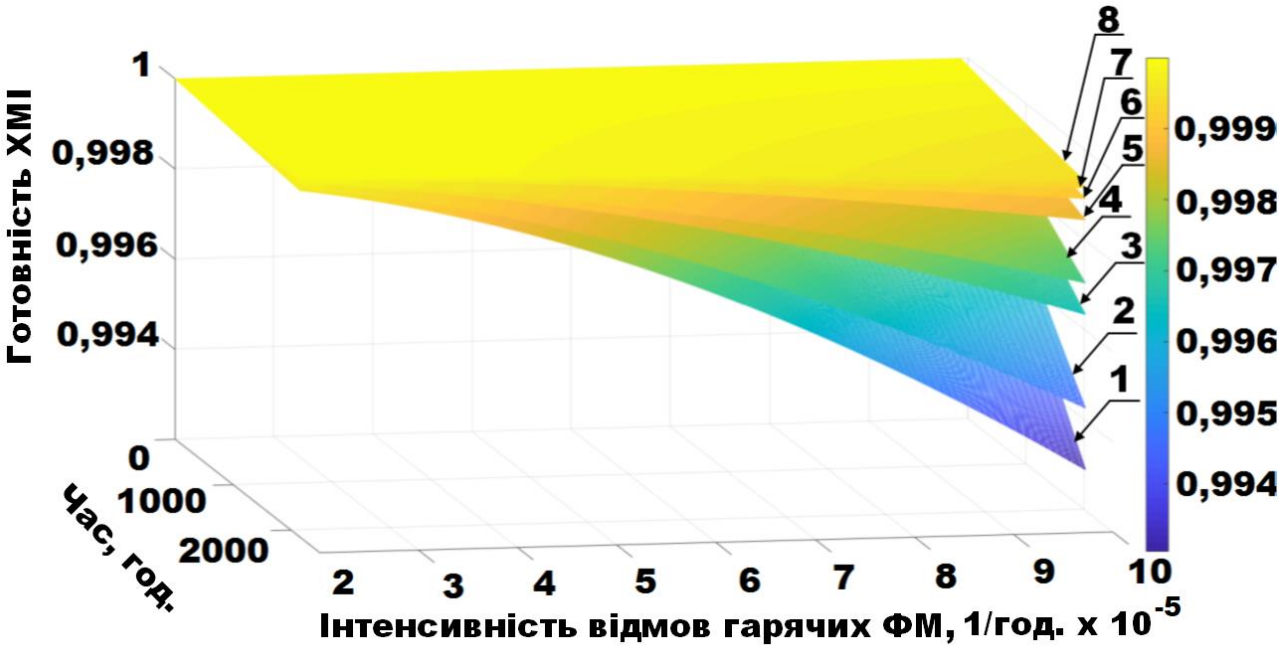


Рис 6.6 Функціональна залежність $K_{\Gamma_{IaaS}}(\lambda_1, T)$ для: 1 – $\mu_1 = 4$ 1/год.; 2 – $\mu_1 = 5$ 1/год.; 3 – $\mu_1 = 8$ 1/год.; 4 – $\mu_1 = 10$ 1/год.; 5 – $\mu_1 = 20$ 1/год.; 6 – $\mu_1 = 30$ 1/год.; 7 – $\mu_1 = 40$ 1/год.; 8 – $\mu_1 = 50$ 1/год.

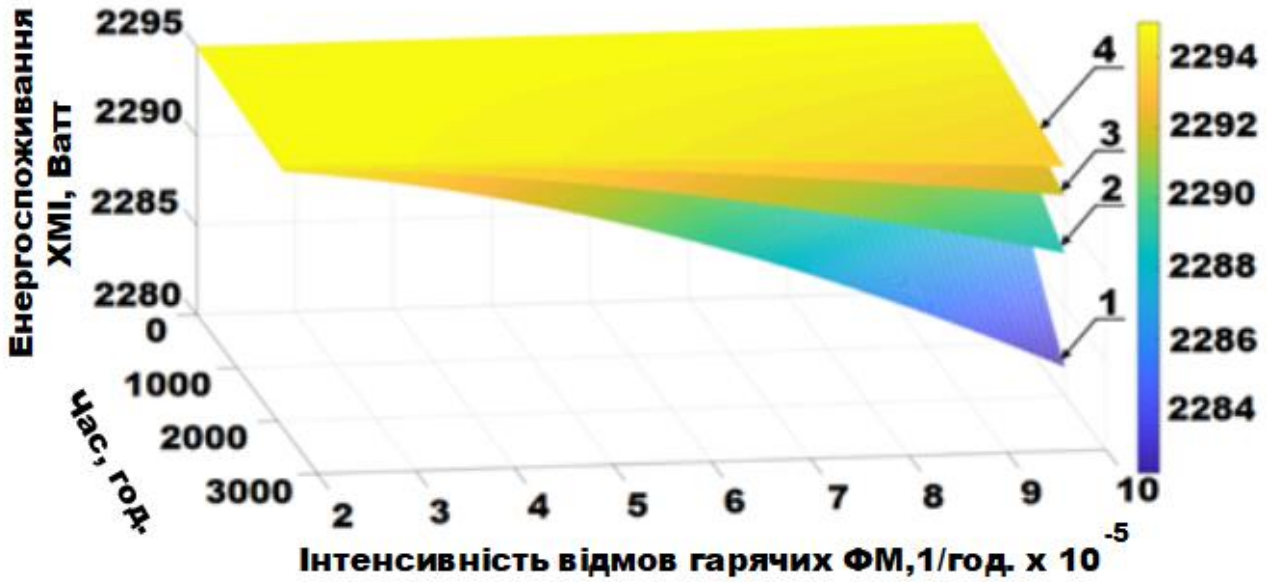


Рис. 6.7 Енергоспоживання ХМІ з серверною системою Hewlett Packard Enterprise ProLiant ML350 Gen10 для 100% завантаження, коли: 1 – $\mu_1 = 5$ 1/год.; 2 – $\mu_1 = 10$ 1/ год.; 3 – $\mu_1 = 20$ 1/ год.; 4 – $\mu_1 = 40$ 1/ год.

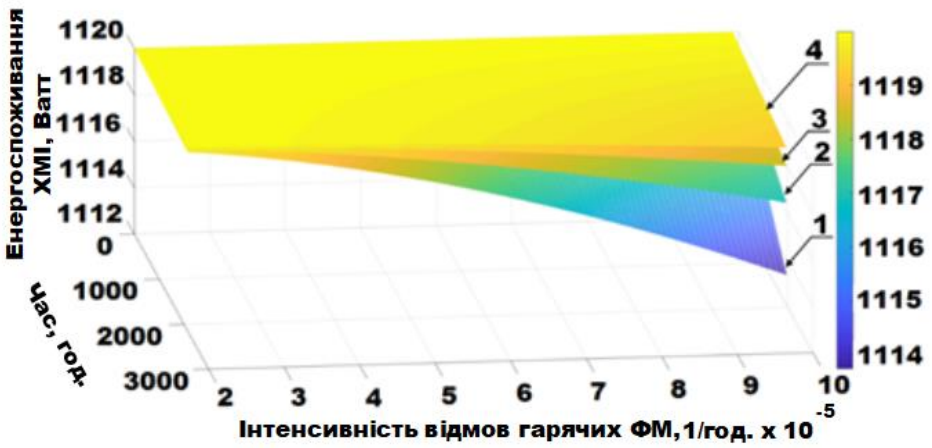


Рис. 6.8 Енергоспоживання XMI з серверною системою Hewlett Packard Enterprise ProLiant ML350 Gen10 для 50% завантаження, коли: 1 $-\mu_1 = 5$ 1/год.; 2 $-\mu_1 = 10$ 1/ год.; 3 $-\mu_1 = 20$ 1/ год.; 4 $-\mu_1 = 40$ 1/ год.

Пропонується у якості додаткового показника енергоефективності XMI розглядати відношення між *Продуктивністю Z* (кількістю обчислювальних операцій в секунду, відома з [185] величина) та *Потужністю* TPC_{IaaS} (енергоспоживанням) інфраструктури. На рис. 6.9–6.12 зображено залежність Z/TPC_{IaaS} від часу застосування за призначенням та інтенсивністю відмов гарячих ФМ для відповідних серверних систем [185] з урахуванням їхнього завантаження.

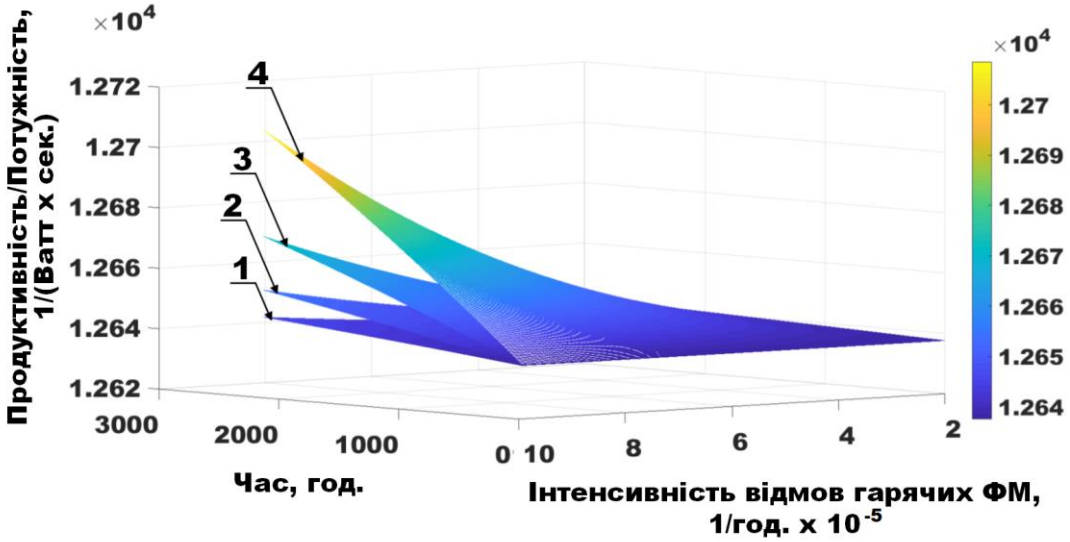


Рис. 6.9 Залежність Продуктивність/Потужність для серверної системи Hewlett Packard Enterprise ProLiant ML350 Gen10 для 50% завантаження, коли: 1 $-\mu_1 = 5$ 1/год.; 2 $-\mu_1 = 10$ 1/ год.; 3 $-\mu_1 = 20$ 1/ год.; 4 $-\mu_1 = 40$ 1/ год.

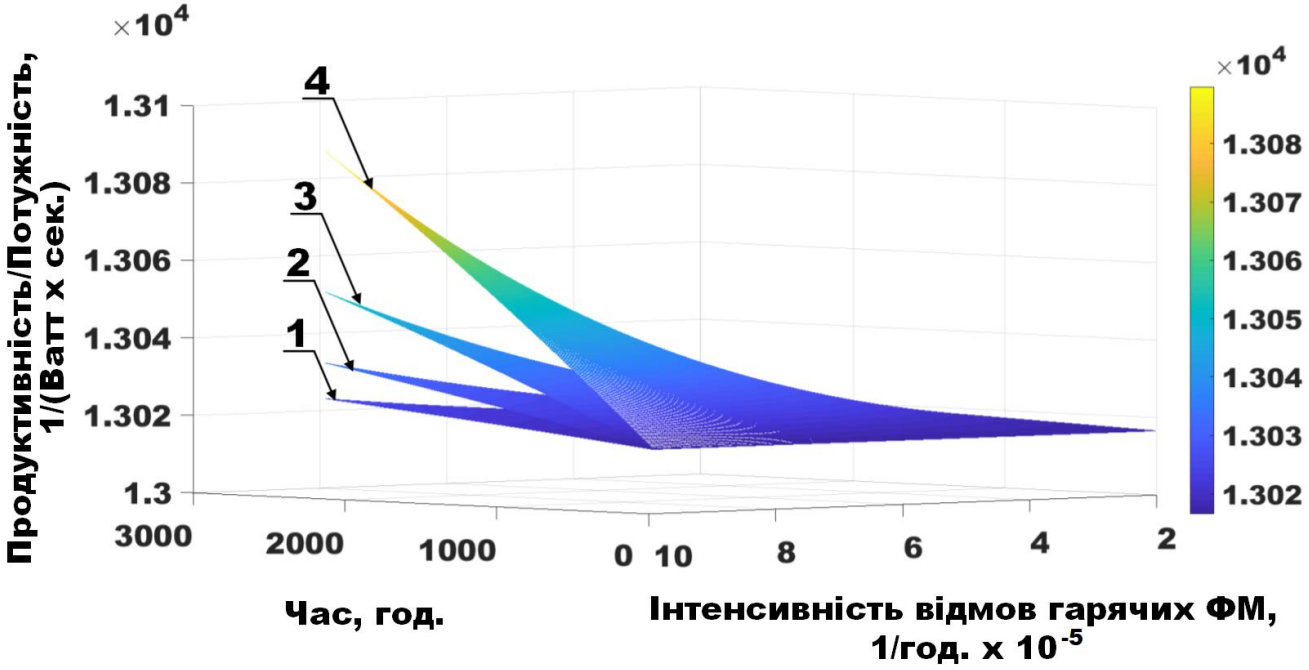


Рис. 6.10 Залежність *Продуктивність/Потужність* для серверної системи Hewlett Packard Enterprise ProLiant ML350 Gen10 для 100% завантаження, коли: $1-\mu_1=5$ 1/год.; $2-\mu_1=10$ 1/ год.; $3-\mu_1=20$ 1/ год.; $4-\mu_1=40$ 1/ год.

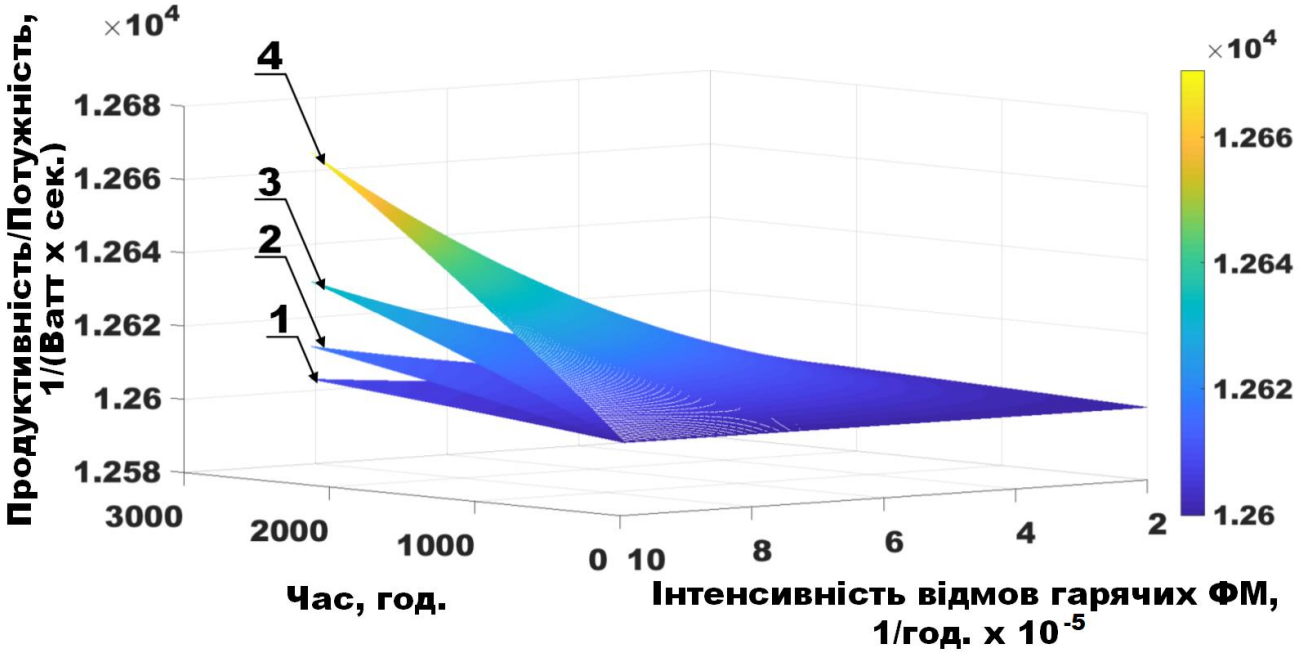


Рис. 6.11 Залежність *Продуктивність/Потужність* для серверної системи Dell Inc. PowerEdge R940 для 50% завантаження, коли: $1-\mu_1=5$ 1/год.; $2-\mu_1=10$ 1/ год.; $3-\mu_1=20$ 1/ год.; $4-\mu_1=40$ 1/ год.

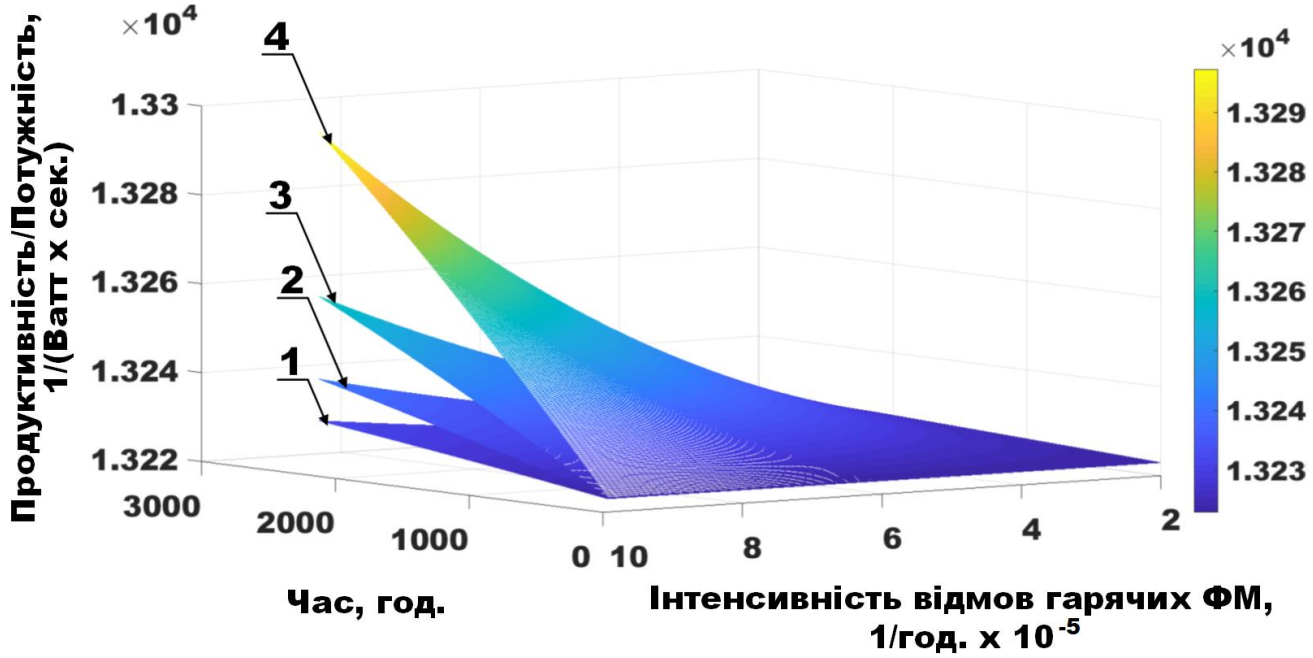


Рис. 6.12 Залежність *Продуктивність/Потужність* для серверної системи Dell Inc. PowerEdge R940 для 100% завантаження, коли: 1 – $\mu_1 = 5$ 1/год.; 2 – $\mu_1 = 10$ 1/ год.; 3 – $\mu_1 = 20$ 1/ год.; 4 – $\mu_1 = 40$ 1/ год.

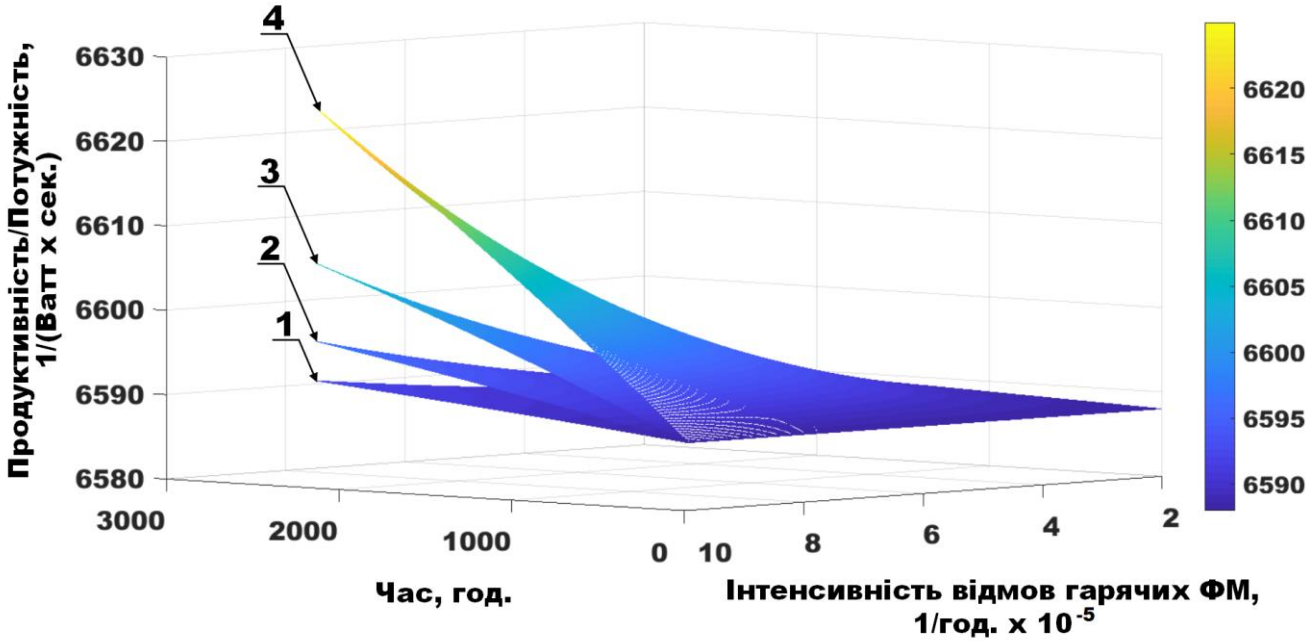


Рис. 6.13 Залежність *Продуктивність/Потужність* для серверної системи Quanta Grid T42S–2U для 50% завантаження, коли: 1–$\mu_1 = 5$ 1/год.; 2–$\mu_1 = 10$ 1/год.; 3 – $\mu_1 = 20$ 1/ год.; 4 – $\mu_1 = 40$ 1/ год.

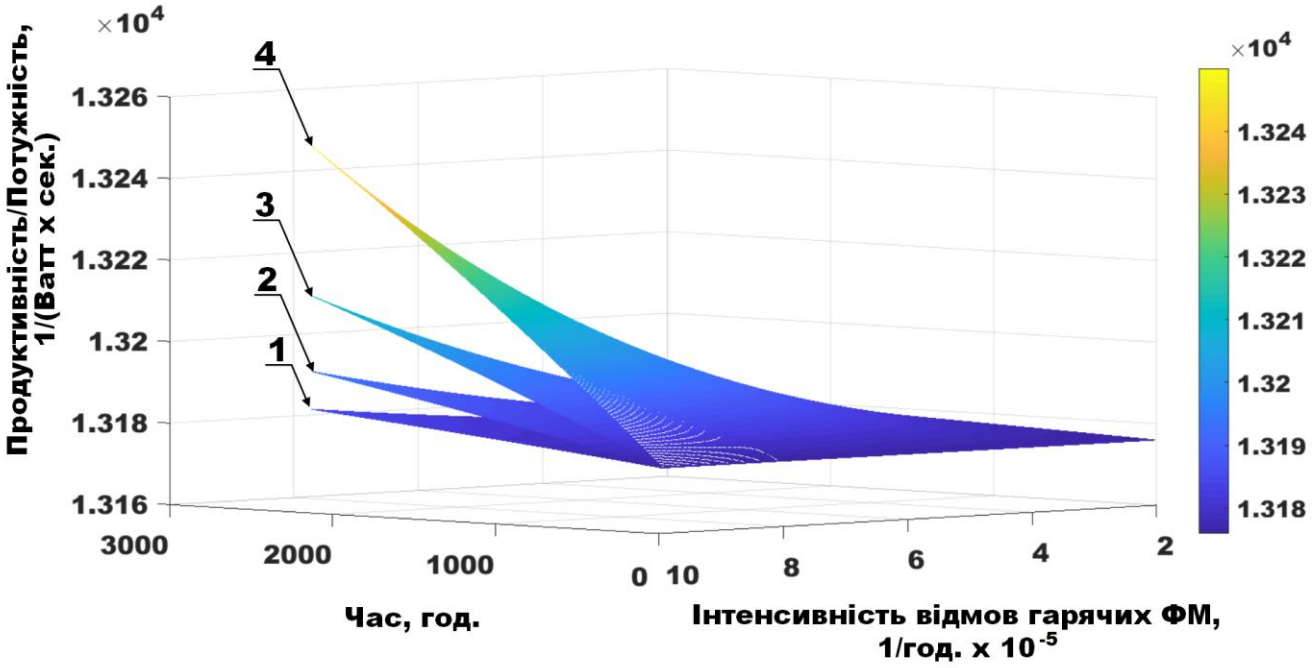


Рис. 6.14 Залежність *Продуктивність/Потужність* для серверної системи Quanta Grid T42S–2U для 100% завантаження, коли: 1 $-\mu_1 = 5$ 1/год.; 2 $-\mu_1 = 10$ 1/ год.; 3 $-\mu_1 = 20$ 1/ год.; 4 $-\mu_1 = 40$ 1/ год.

Узагальнені результати моделювання у вигляді порівняльної характеристики конфігурації ХМІ для двох типів серверних систем зведені в окрему табл. 6.4. Обчислення виконувалися за дії припущення, що обидва типи серверів задовільняють вимогам користувачів.

Таблиця 6.4

Порівняльна характеристика результатів моделювання для двох типів серверних систем, що входять до складу ХМІ

Продуктивність		Потужність		Співвідношення між продуктивністю та потужністю з урахуванням рівня готовності (доступності)
Робоче навантаження	Обсяг навантаження	Середня споживча потужність без урахування рівня готовності (доступності), Вт	Середня споживча потужність з урахуванням рівня готовності (доступності), Вт	
для п’яти серверів Hewlett Packard Enterprise ProLiant ML350 Gen10				
100%	29003230	2295	2289	12638
50%	14578560	1120	1117	13017

Продовження таблиці 6.4

Продуктивність		Потужність		Співвідношення між продуктивністю та потужністю з урахуванням рівня готовності (доступності)
Робоче навантаження	Обсяг навантаження	Середня споживча потужність без урахування рівня готовності (доступності), Вт	Середня споживча потужність з урахуванням рівня готовності (доступності), Вт	
для п’яти серверів Dell Inc. PowerEdge R940				
100%	57644020	4575	4562	12600
50%	28892060	2185	2179	13223

Кількісні результати моделювання, які наведено в табл. 6.4, отримано за умови, що хмарна інфраструктура розгортається на основі саме розглянутих серверних систем, які надають користувачам відповідний хостинг. Порівняльна характеристика отриманих результатів моделювання для серверів Hewlett Packard Enterprise ProLiant ML350 Gen10 та Dell Inc. PowerEdge R940 (табл. 6.3) свідчить, що за показником середньої споживчої потужності (в Ваттах) з урахуванням рівня готовності (доступності) кращими є серверні системи Hewlett Packard Enterprise ProLiant ML350 Gen10.

Висновки до розділу 6

1. Розроблено метод вибору характеристик готовності хмарних систем критичних інфраструктур, який базується на результатах аналізу властивостей та аналітико-стохастичному моделюванні процесів зміни інформаційно-технічних станів фізичних і віртуальних машин, що входять до складу ХМС КІ.

2. Ключову роль в оцінюванні рівня готовності хмарних систем критичних інфраструктур грає інтегрована система оперативного моніторингу інформаційно-технічних станів, на основі застосування якої виконується відновлення працездатності та реалізується процес міграції обчислювальних ресурсів фізичних і віртуальних машин ХМС КІ.

3. Виконано аналіз ієрархії властивостей хмарних систем критичних інфраструктур. За результатами аналізу на прикладі критичної енергетичної інфрастуктури встановлено, що найбільш важливою властивістю, яка об’єднує та встановлює взаємозалежність між фізичними, кібернетичними та хмарними активами КЕІ є готовність.

4. Розроблено метод вибору та оцінки характеристик енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів, який реалізується в два етапи, а саме, здійснюється напівмарковське моделювання та визначається рівень готовності ХМІ; за даними моделювання з використанням кількісних оцінок готовності визначається показник енергоефективності інфраструктури.

5. У якості прикладу шляхом визначення величини співвідношення між продуктивністю виконання обчислювальних операцій і розрахованим з урахуванням готовності (доступності) ресурсу значенням показника енергоефективності двох серверних систем визначено кращу, яка задовольняє вимогам зеленого інжинірингу та може бути застосована для формування конфігурації хмарної інфраструктури.

Основні результати шостого розділу опубліковано в роботах [109, 32, 116, 33, 74, 123, 184].

РОЗДІЛ 7
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ТЕСТУВАННЯ ХМАРНИХ СИСТЕМ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

7.1 Розробка методу вибору інформаційного центру хмарного провайдера

Насьогодні використання хмарних ресурсів і сервісів в контурі управління критичними інфраструктурами значно розширює їхні можливості щодо оперативного та якісного виконання завдань застосування за призначенням. Хмарні системи надають можливість отримати широкий спектр послуг, включаючи створення резервного контуру управління критичними інфраструктурами, виконання функцій по збору, обробці, аналізу та зберіганню великих обсягів даних і т.і. Наприклад, використання потужного хмарного ресурсу в сфері застосування КЕІ надає можливість створити сервіси, які в перспективі могли б розв’язувати завдання щодо оцінювання, контролю та забезпечення готовності інфраструктури [127].

Якісні послуги в інтересах забезпечення готовності КЕІ можуть надаватися найпотужнішим хмарним провайдером AWS [69, 94, 95], що підтверджується результатами аналізу продуктивності мережі, яка спільно працює з хмарним сховищем Amazon S3 [186]. Як правило, сервіси AWS та інших потужних хмарних провайдерів (Google, Microsoft, IBM, Apple) надаються через постійно функціонуючу мережу інформаційних центрів, що працюють по всьому світі. Тому важливим завданням є вибір конкретного інформаційного центру хмарного провайдера через підключення до якого будуть надаватися відповідні послуги. Згідно з процедурою встановлення ієрархії показників готовності хмарних систем КЕІ (рис. 6.3) для розв’язування зазначеного завдання цілковито обгрунтованим є використання критерію мінімуму часу затримки тунельного (захищеного) каналу зв’язку, який застосовується в контурі управління інфраструктурою.

Виходячи з зазначеного, розглянемо метод вибору інформаційного центру хмарного провайдера, який включає такі етапи:

1) оцінка часу затримки інформаційних даних між системою оперативного моніторингу КЕІ та інтегрованими фізичними (віртуальними) компонентами ХМС;

2) тестування та вибір інформаційного центра хмарного провайдера за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв'язку.

Розглянемо перший етап реалізації пропонуємого методу.

7.1.1 Оцінка часу затримки інформаційних даних між системою оперативного моніторингу критичної енергетичної інфраструктури та інтегрованими фізичними (віртуальними) компонентами хмарних систем

Відповідно до структури методології (рис. 2.1) та концепції (рис. 2.2) забезпечення готовності ХМС КІ, основні етапи реалізації яких щодо питань отримання експериментальних даних та результатів аналітико-стохастичного моделювання розглянуто в роботах [8, 32, 76, 102, 123, 187], необхідно розробити інформаційну технологію тестування регіональних ХМС з інтегрованими фізичними компонентами з метою вибору інформаційного центру конкретного хмарного провайдера.

Відомий досвід свідчить, що оцінювання часу затримки інформаційних потоків даних виконується в експериментальному порядку. Тому на початковому етапі планувався експеримент, який був реалізується за певним сценарієм. Можливі сценарії проведення експериментів по тестуванню хмарних систем різних провайдерів розглянуто в [188]; по створенню інноваційних хмарних сервісів з застосуванням баз даних і оцінці їхньої продуктивності, включаючи оцінку часу затримки, розглянуто в [189].

Як результат, для проведення експерименту пропонується застосовувати прймально-передавальну систему, до складу якої входять три модулі, а саме: модуль моделювання та аналізу даних (ММАД), модуль передачі даних (МПД), модуль прийому та ретрансляції даних (МПРД). Відповідно до спрощеної схеми проведення експерименту, яка відображена на рис. 7.1, модулі утворюють контур обміну потоками даних зі зворотнім зв'язком. Модуль ММАД виконує основні функції, які стосуються формування сигналу, його обробки, аналізу та визначення

часу затримки інформаційних даних.

Рис. 7.1 Спрощена схема проведення експерименту

Приймаючи до уваги схему експерименту (рис. 7.1) було розроблено хмарний симулятор, який функціонує в двох основних режимах, а саме, в режимі off-line та в режимі on-line. На рис. 7.2 зображено структурну схему функціонування симулятора в режимі off-line. Характерною особливістю обох зазначених режимів є застосування віртуальних реляційних баз даних (ВРБД), які виконують наступні важливі функції:

1) запис інформації у вигляді потоків даних, що курсують в каналі зв’язку;

2) запис параметрів, що фіксуються засобами реєстрації даних, розроблених на основі використання спеціальних тригерів.

Необхідно відзначити, що в режимі off-line симулятор може використовуватися досить різноманітно. Наприклад, за потреби можна тренувати обслуговуючий персонал щодо виконання функціональних обов’язків як в штатних звичайних, так і в не штатних екстремальних ситуаціях. В той же час, в режимі off-line може здійснюватися аналіз записаного трафіку щодо виявлення аномалій, які пов’язані з порушеннями інформаційної та функціональної безпеки.

В табл. 7.1 виконано порівняльний аналіз режимів функціонування хмарного симулятора.

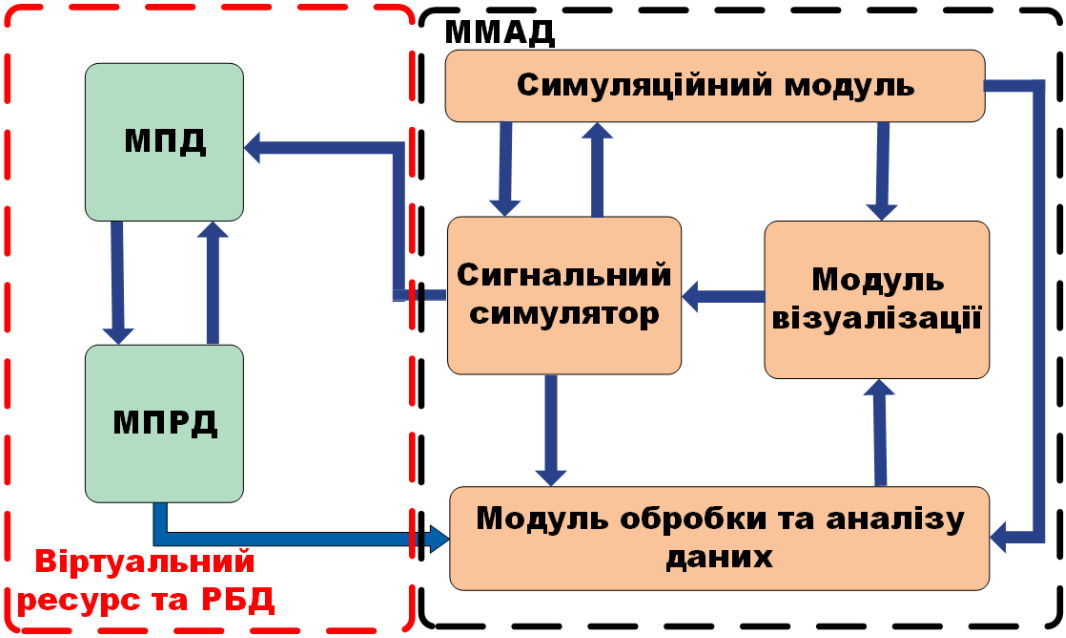


Рис. 7.2 – Структурна схема функціонування хмарного симулятора в режимі off-line

Таблиця 7.1

Порівняльний аналіз режимів функціонування хмарного симулятора

Режим функціонування симулятора	Режими функціонування модулів симулятора	Характеристика зовнішніх пристроїв, які підключені до симулятора
off-line (рис. 7.1–7.2)	ММАД, МПД, МПРД – включені та мають спільний канал зв'язку	Робота зовнішніх пристроїв повністю симулюється відповідним віртуальним ресурсом, який розвертається на внутрішньому сервері
on-line (рис. 7.4–7.5)	ММАД, МПД – включені та мають спільний канал зв'язку з зовнішніми пристроями; МПРД – виключений	У якості зовнішніх пристроїв (тобто пристроїв, що є джерелами потоків даних) можуть застосовуватися інформаційні центри хмарних провайдерів, системи ССВВ, мікро-ССВВ, фазові концентратори даних. Всі зазначені компоненти повністю або частково належать до активів КЕІ

Відповідно до рис. 7.2 робота симуляційного модуля в режимі реального часу синхронізована з сигнальним симулятором, що дозволяє за допомогою спеціальних тригерів фіксувати момент передачі та прийому потоків даних і визначати час затримки, що обчислюється за допомогою наступного співвідношення:

$$\Delta t = t_{timestamp_returning} - t_{timestamp_sending}, \tag{7.1}$$

де $t_{timestamp_sending}$ – час передачі потоків даних; $t_{timestamp_returning}$ – час прийому потоків даних.

Значення Δt (7.1) записуються до віртуальної реляційної бази даних, що працює в режимі “клієнт–сервер”. Залежність часу затримки (7.1) від кількості ітерацій модельованого потоку даних та узагальнені (згруповані) результати аналізу Δt за умов функціонування хмарного симулятора в режимі off-line, відображено на рис. 7.3 та рис. 7.4. За допомогою рис. 7.4 визначається максимальна і мінімальна кількість загрупованих значень, що є корисним з точки зору визначення щільності розподілу і решти чисельних характеристик.

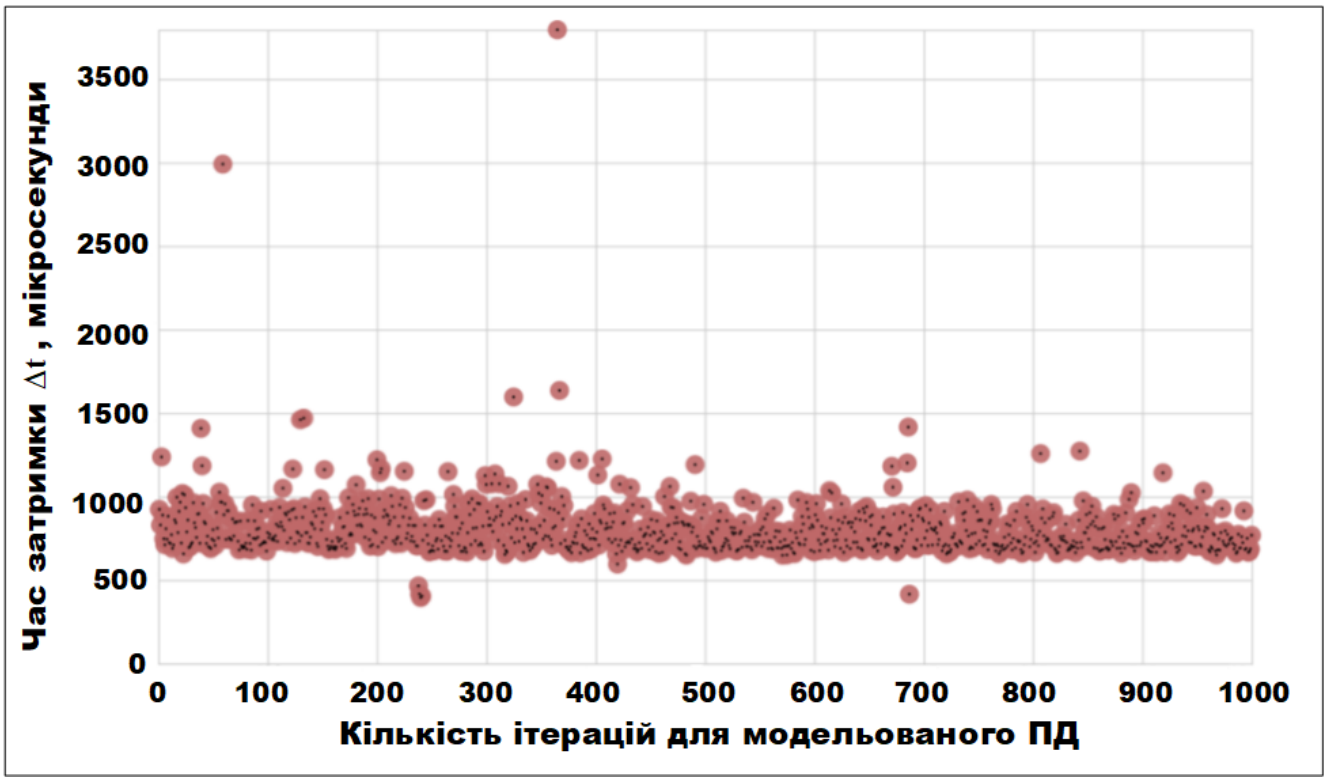


Рис. 7.3 Залежність часу затримки від кількості ітерацій модельованого потоку даних

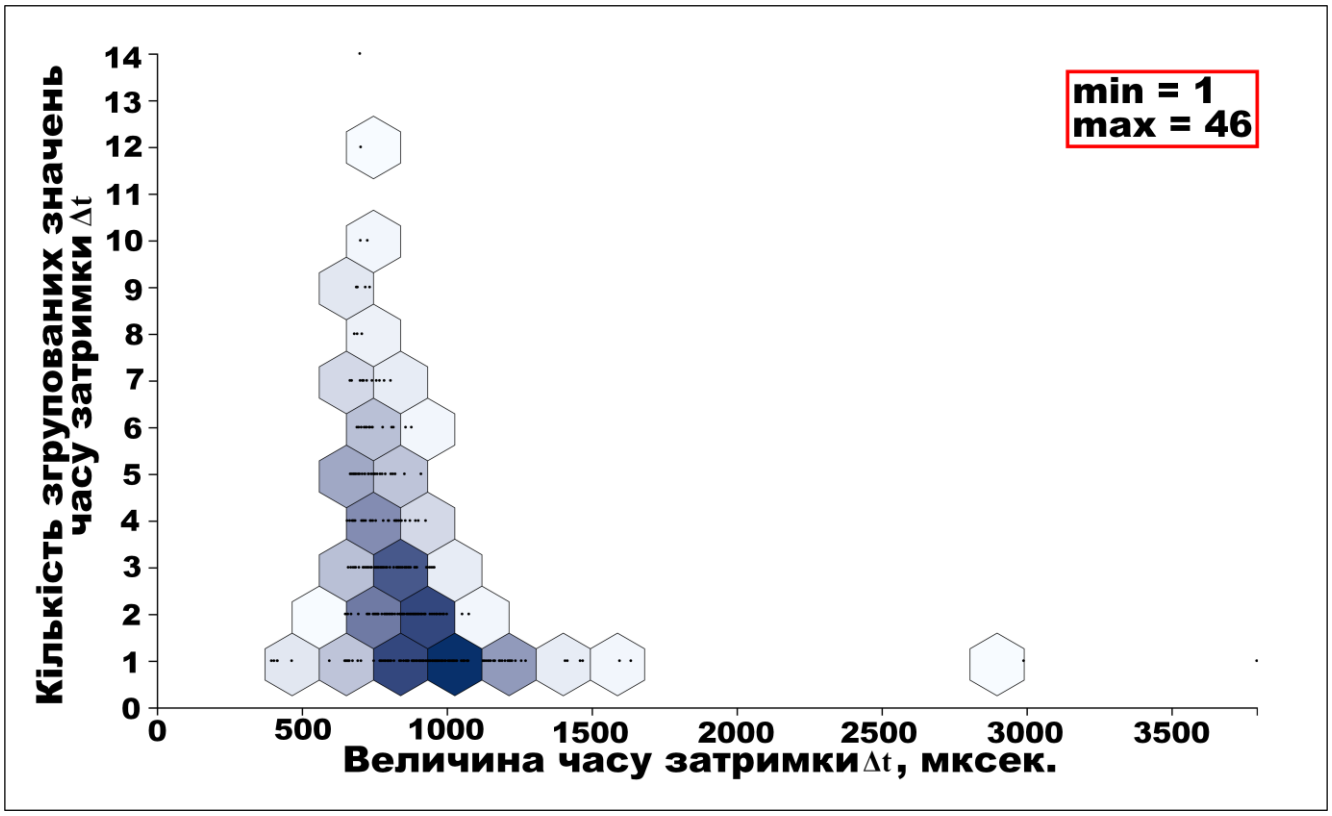


Рис. 7.4 Узагальнені (згруповані) результати аналізу часу затримки Δt

Відповідно до рис. 7.3 та рис. 7.4 встановлено, що величина часу затримки Δt змінюється в інтервалі від 595 до 1076 мікросекунд. Отримані таким чином дані (рис. 7.3) в прикладному аспекті можуть застосовуватися для налаштування та калібрування хмарного симулятора при його функціонуванні в режимі off-line.

7.1.2 Процедура тестування інформаційного центру хмарного провайдера

Розглянемо яким чином реалізується процедура тестування інформаційного центру відповідного провайдера після виконання налаштування та калібрування хмарного симулятора в режимі off-line (рис. 7.1–7.4).

На рис. 7.5 зображено спрощену схему проведення експерименту, на основі якого реалізується процедура тестування інформаційного центру (ІЦ) відповідного хмарного провайдера (ХМП). В тривіальному сенсі згідно з загальною концепцією забезпечення готовності ХМС це означає, що попередньо при створенні хмарних активів будь-якої критичної інфраструктури необхідно переконатися в наявності надійного захищеного (тунельного) каналу зв’язку з ІЦ ХМП. З цією метою модуль МПРД відключається, а замість нього підключається

ІЦ ХМП. Слід зазначити, що надійний захищений від дії ЗВШВ тунельний канал зв'язку для забезпечення ефективного безпечного функціонування системи оперативного моніторингу інформаційно-технічних станів компонентів КЕІ на основі застосування модулів ССВВ у вигляді розгорнутої та агрегованої мережі VPN може надаватися хмарним провайдером AWS.

Рис. 7.5 Спрощена схема проведення експерименту для тестування ІЦ ХМП

Фактично процедура реалізується в три етапи:

1) хмарний симулятор переводиться в режим on-line, тобто відключається модуль МПРД і замість нього підключається ІЦ ХМП;

2) формується передаваємий в напрямку ІЦ ХМП сигнал заданої структури;

3) приймається, обробляється та реєструється сигнал від ІЦ ХМП.

На рис. 7.6 зображено структурну схему функціонування симулятора в режимі on-line.

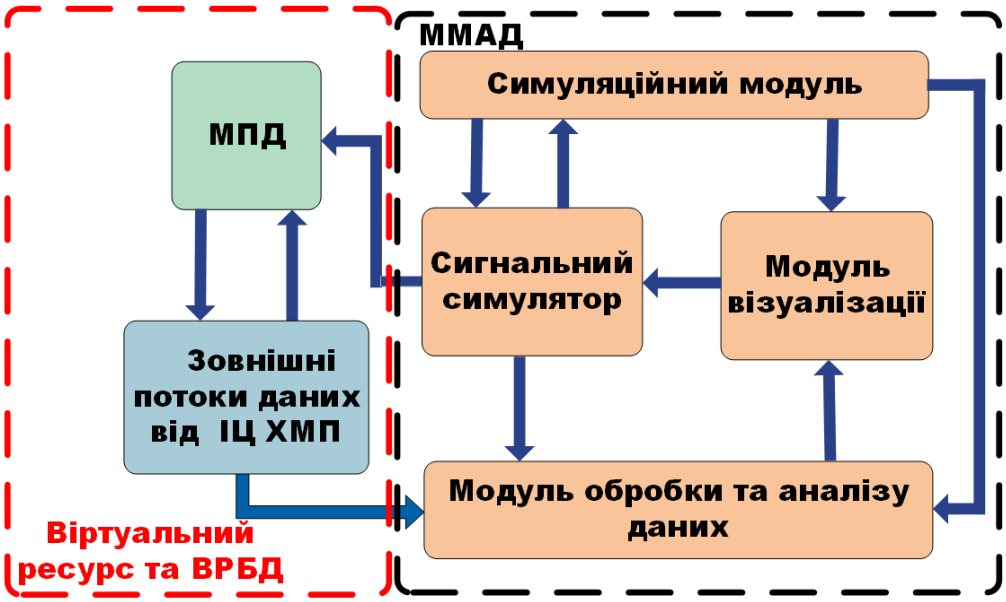


Рис. 7.6 Структурна схема функціонування хмарного симулятора в режимі on-line

Для успішної реалізації зазначеної процедури важливе значення має етап формування сигналу заданої структури. Наприклад, при виборі ІЦ ХМП для забезпечення ефективного застосування за призначенням системи оперативного моніторингу інформаційно-технічних станів компонентів КЕІ, яка функціонує на основі спільного використання модулів ССВВ [190] та фазових концентраторів [191], на виході сигнального симулятора необхідно сформувати оцифрований масштабований сигнал $x(t)$, який за своїми параметрами відповідає діапазону аналогових вихідних напруг і фаз зазначених пристроїв. В роботах [192, 193] розглянуто розв'язування цієї досить складної задачі за допомогою системи комп'ютерної математики Matlab/Simulink. В створеному хмарному симуляторі для формування вихідного сигналу у вигляді потоку даних аналогічним чином застосовується система Matlab/Simulink (рис. 7.6).

Потік даних в запропонованому хмарному симуляторі формується у вигляді послідовності гармонічних сигналів $X = \{x_1(t), x_2(t), ..., x_n(t)\}$, яку отримують з найпростішого гармонічного сигналу [194]

$$x(t) = A\cos(\omega t + \varphi). \tag{7.2}$$

Послідовність X отримують, застосувавши дискретне перетворення Фур'є для $x(t)$ і виконавши зсув по фазі для $x_k(t)$, де $k = \overline{1,n}$. Тоді, відповідно до [195] можна записати

$$X = \frac{2}{M}\sum_{i=0}^{M-1} x_i e^{-\frac{j2\pi i}{M}} = X_c - jX_s, \tag{7.3}$$

де

$$X_c = \frac{2}{M}\sum_{i=0}^{M-1} x_i \cos\left(\frac{2\pi i}{M}\right), \tag{7.4}$$

$$X_s = \frac{2}{M}\sum_{i=0}^{M-1} x_i \sin\left(\frac{2\pi i}{M}\right). \tag{7.5}$$

Враховуючи (7.3)–(7.5), у відповідності з [195] складова (M-1) гармонічного сигналу $x(t)$ (7.2) записується як

$$X^{M-1} = X_c^{M-1} - jX_s^{M-1} = X(\cos\varphi + j\sin\varphi) = Xe^{j\varphi}. \tag{7.6}$$

Відомо, що для компонентів КЕІ найбільш інформативним параметром щодо виникнення негативних подій є фаза. Тому відповідно до рис. 2.5, 2.6 у випадку зміни фази φ, яка є найбільш інформативним для КЕІ параметром, по величині фазового зсуву $\Delta\varphi$ двох гармонічних сигналів можна встановити момент виникнення аномалії (рис. 2.6), попередити її та уникнути негативних наслідків. Фазовий зсув визначається зі співвідношення [194] $\Delta\varphi = |\varphi_1 - \varphi_2|$, де φ_1, φ_2 – початкові фази двох гармонічних сигналів.

Далі, потоки даних через МПД розповсюджуються до ІЦ ХМП. Моменти розповсюдження сигналу від сигнального симулятора та повернення після проходження ІЦ ХМП реєструються і згідно співвідношення (7.1) визначається їхній час затримки Δt. Отримавши статистичну інформацію від декількох ІЦ ХМП, можна у відповідності з висунутим критерієм мінімуму часу затримки визначити кращий інформаційний центр, який буде відповідати вимогам щодо оперативного розв’язування відповідних завдань по забезпеченню готовності КЕІ.

7.1.3 Процедура вибору інформаційного центру хмарного провайдера за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв’язку

Відповідно до рис. 7.5, 7.6, використовуючи розглянутий метод та розроблену інформаційну технологію, у якості прикладу було проведено тестування дев’яти реально існуючих регіональних сервіс-орієнтованих ресурсів, які розгорнуто в різних країнах світу, та одного штучно створеного локального віртуального ресурсу місцевого рівня (рис. 7.3, рис. 7.4) в режимі “клієнт–сервер”. А саме, сформована послідовність гармонічних коливань, які в математичній формі описуються співвідношеннями (7.2)–(7.6) та з виходу сигнального симулятора поступають в модуль передачі даних, де посилюються і передаються до відповідних абонентів. Результати тестування абонентів (в мікросекундах) у вигляді коробчастої діаграми зображено на рис. 7.7 та рис. 7.8. Тестовані абоненти (рис. 7.7, рис. 7.8) розташовані зліва направо.

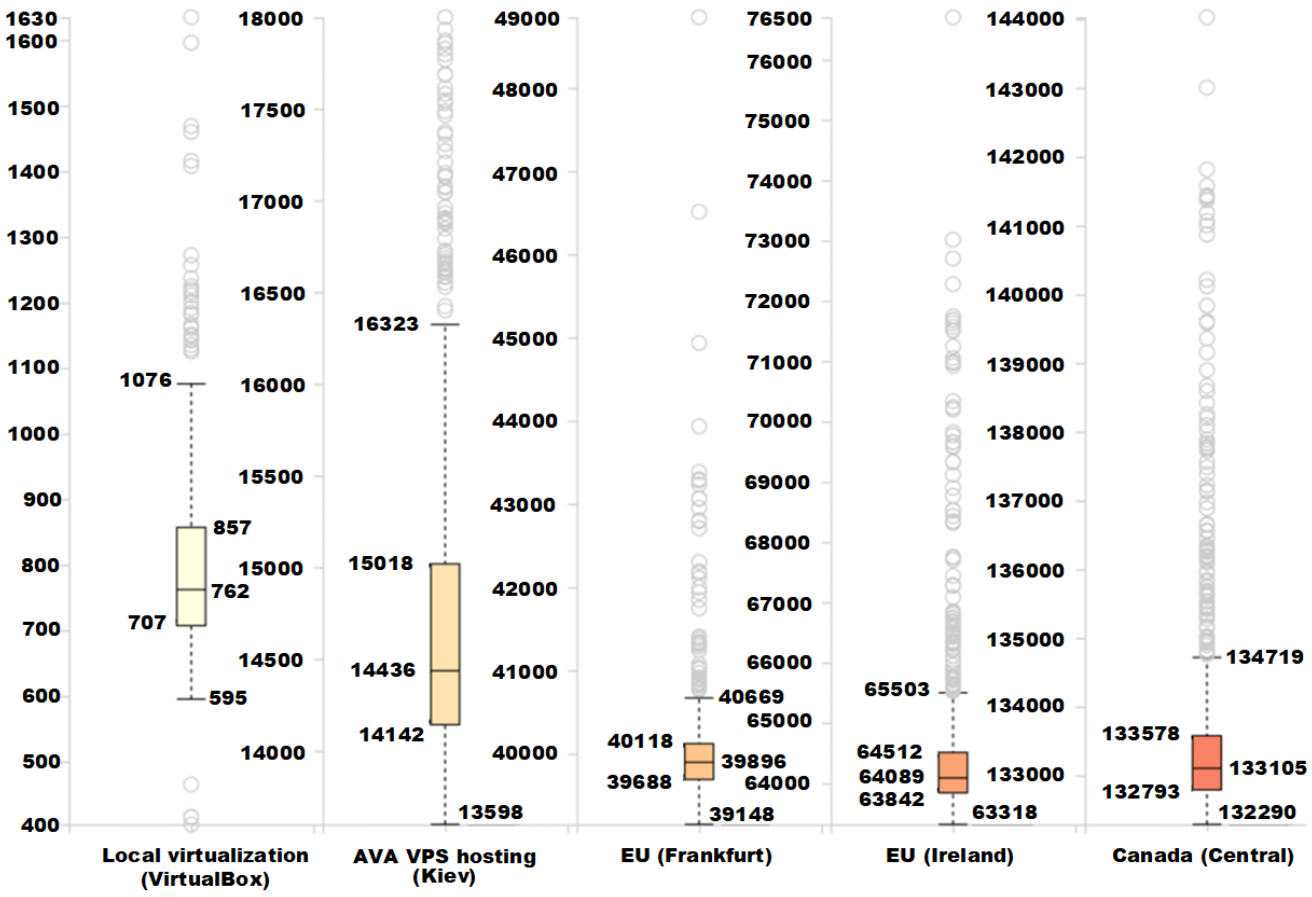


Рис. 7.7 Результати тестування (мкс) локального віртуального сервісу (Virtual Box), AVA VPS хостінгу (м. Київ) та трьох ІЦ ХМП Amazon EC2

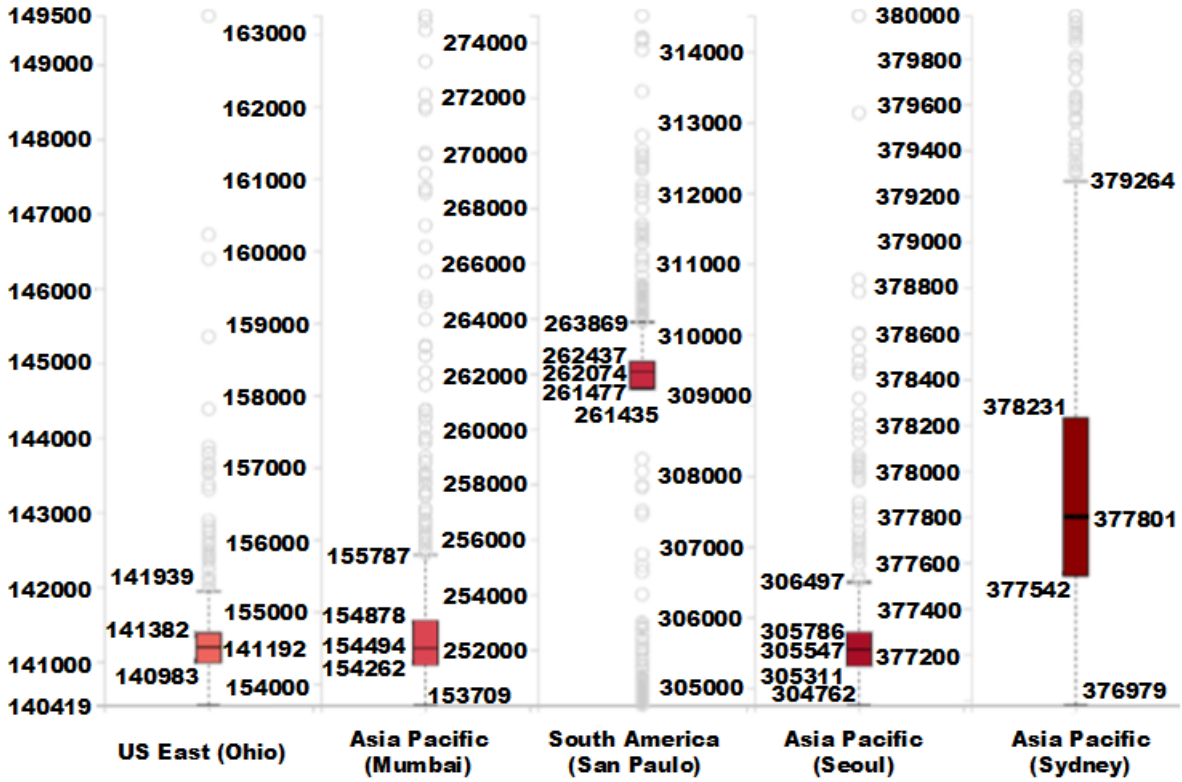


Рис. 7.8 Результати тестування (мкс) п’яти ІЦ ХМП Amazon EC2

На наступному етапі реалізації запропонованої процедури розв’язувалося завдання щодо вибору інформаційного центру хмарного провайдера за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв’язку. Відповідний критерій записується у вигляді

$$\Im = \begin{cases} K_{Г_{ІЦ}}(T) \geq K_{Г_0}; \\ \Delta t \longrightarrow \min; \\ C_{\min_0} \leq C_0 \leq C_{\max_0}; \end{cases} \tag{7.7}$$

де $K_{Г_{ІЦ}}(T)$ – стаціонарний коефіцієнт готовності інформаційного центру хмарного провайдера за час застосування за призначенням T; $K_{Г_0}$ – гранично припустиме значення стаціонарного коефіцієнта готовності інформаційного центру хмарного провайдера; $C_0 \in \left[C_{\min_0}; C_{\max_0}\right]$ – граничні витрати необхідні на підтримання необхідного рівня готовності інформаційного центру хмарного провайдера.

Порівняльний аналіз результатів тестування сервіс-орієнтованих систем (рис. 7.7, рис. 7.8) наведено в табл. 7.2.

Таблиця 7.2

Порівняльний аналіз результатів тестування сервіс-орієнтованих систем

№	Розташування (географічне положення)	Мінімальне значення, мкс.	Нижній квартиль, мкс.	Медіана, мкс.	Верхній квартиль, мкс.	Максимальне значення, мкс.
1	Local virtualization (VirtualBox)	595	707	762	857	1 076
2	Ava VPS hosting (Kiev)	13 598	14 142	14 436	15 018	16 323

Продовження таблиці 7.2

№	Розташування (географічне положення)	Мінімальне значення, мкс.	Нижній квартиль, мкс.	Медіана, мкс.	Верхній квартиль, мкс.	Максимальне значення, мкс.
Amazon Elastic Compute Cloud (Amazon EC2)						
3	EU (Frankfurt)	39 148	39 688	39 896	40 118	40 669
4	EU (Ireland)	63 318	63 842	64 089	64 512	65 503
5	Canada (Central)	132 290	132 793	133 105	133 578	134 719
6	US East (Ohio)	140 419	140 983	141 192	141 382	141 939
7	Asia Pacific (Mumbai)	153 709	154 262	154 494	154 878	155 787
8	South America (San Paulo)	261 435	261 477	262 074	162 437	263 869
9	Asia Pacific (Seoul)	304 762	305 311	305 547	305 786	306 497
10	Asia Pacific (Sydney)	376 979	377 542	377 801	378 231	379 264

Отже, у разі виконання вимог щодо рівня готовності можна стверджувати, що на регіональному рівні доцільно використовувати сервіс-орієнтований ресурс Ava VPS hosting (м. Київ), для якого час затримки складає біля 16,3 мілісекунди; серед досліджуваних сервіс-орієнтованих ресурсів ХМПР за результатами тестування відповідно до критерію (7.7) найкращим є ІЦ Amazon EC2, який розташовано у Франкфурті (Німеччина) з часом затримки 40,7 мілісекунди.

Отримані значення часу затримки є цілковито прийнятливими для розв’язування завдань управління енергопотоками в сфері застосування критичної енергетичної інфраструктури. Це пов`язано з тим, що КЕІ є досить інерційною системою, що прослідковується при управлінні енергопотоками, коли час

відпрацювання регулюючих команд може складати до двох хвилин.

7.2 Інформаційна технологія тестування хмарних систем критичної енергетичної інфраструктури з інтегрованими фізичними компонентами на основі використання віртуального ресурсу реляційних баз даних

Результати експерименту надали можливість сформулювати деякі положення науково-прикладного характеру і розробити відповідну інформаційну технологію.

Запропонована інформаційна технологія являє собою сукупність програмно-апаратних засобів та відповідного методу, комплексне застосування яких надає можливість здійснити вибір інформаційного центру хмарного провайдера у відповідності з критерієм мінімуму часу затримки тунельного (захищеного) каналу зв’язку. Інформаційна технологія (рис. 7.9) виконує послідовність функцій, наведених нижче.

А1. Аналіз та візуалізація вхідних даних. У якості вхідних даних розглядається інформація про зовнішні об’єкти дослідження, а саме: вихідні дані системи синхронізованих векторних вимірювань; вихідні дані компонентів, що утворюють хмарні та кібернетичні активи критичної енергетичної інфраструктури і т.і. Розглядається та підлягає аналізу структура вихідних сигналів зовнішніх об’єктів дослідження, їхні параметри, пропускна спроможність, тощо. Розрізняють три типи потоків даних, які поступають на вхід симулятора: потоки даних від зовнішнього об’єкту дослідження; потоки даних, які формуються в режимі off-line симулятора; потоки даних, які формуються в режимі on-line симулятора.

Вихідними даними є інформація про особливості побудови та функціонування об’єкту дослідження. По результатам аналізу вхідних даних формуються команди на виконання аналізу майбутньої тестової системи (інфраструктури); формування та візуалізацію варіантів розвитку подій; планування експерименту, який буде проводитися за певним сценарієм. У якості вихідної інформації фігурує також інформація про час затримки тунельного (захищеного) каналу зв’язку та прийомо-передачі відповідного інформаційного

центру конкретного хмарного провайдера.

А2. Визначення та аналіз тестованої системи або інфраструктури. За результатами реалізації зазначеної функції визначається профіль об’єкта, тобто визначається його ресурсне навантаження, кількість інформаційних каналів, пропускна спроможність, тощо.

А3. Формування та візуалізація множини варіантів розвитку подій. Використовуючи інформацію про профіль об’єкта дослідження та керуючись методами логічного аналізу, дедукції та індукції, на виході модуля формується множина можливих варіантів розвитку подій.

А4. Планування експерименту, який реалізується за певним сценарієм. Застосовуючи методи планування експерименту до множини можливих варіантів розвитку подій, будується план експерименту, визначаються умови, терміни та послідовність його проведення. Згідно плану на першому етапі проведення експерименту включається режим off-line, який реалізується відповідно до схеми, зображеної на рис. 7.10.

А5. При включенні режиму off-line виконується налаштування та калібрування сигнального симулятора з застосуванням інтегрованих засобів вимірювання з відомими характеристиками точності. Відповідно до рис. 7.10 генерується імітаційний потік даних, який використовується для калібрування приймально-передавального каналу зв’язку та налаштування засобів вимірювання. Після налаштування сигнальний симулятор застосовується для розв’язування завдань за призначенням.

А6. Виконується розгортання РБД та налаштування пристроїв реєстрації параметрів. Для виконання цієї функції застосовуються програмовані тригери, за допомогою яких фіксуються моменти передачі та прийому потоків даних і визначається час затримки згідно співвідношення (7.1).

А7. Розмикається внутрішній контур, який виконує функції А5, А6, та підключається зовнішній приймально-передавальний канал зв’язку, що застосовується для обробки інформаційних ПД від ІЦ конкретного хмарного провайдера.

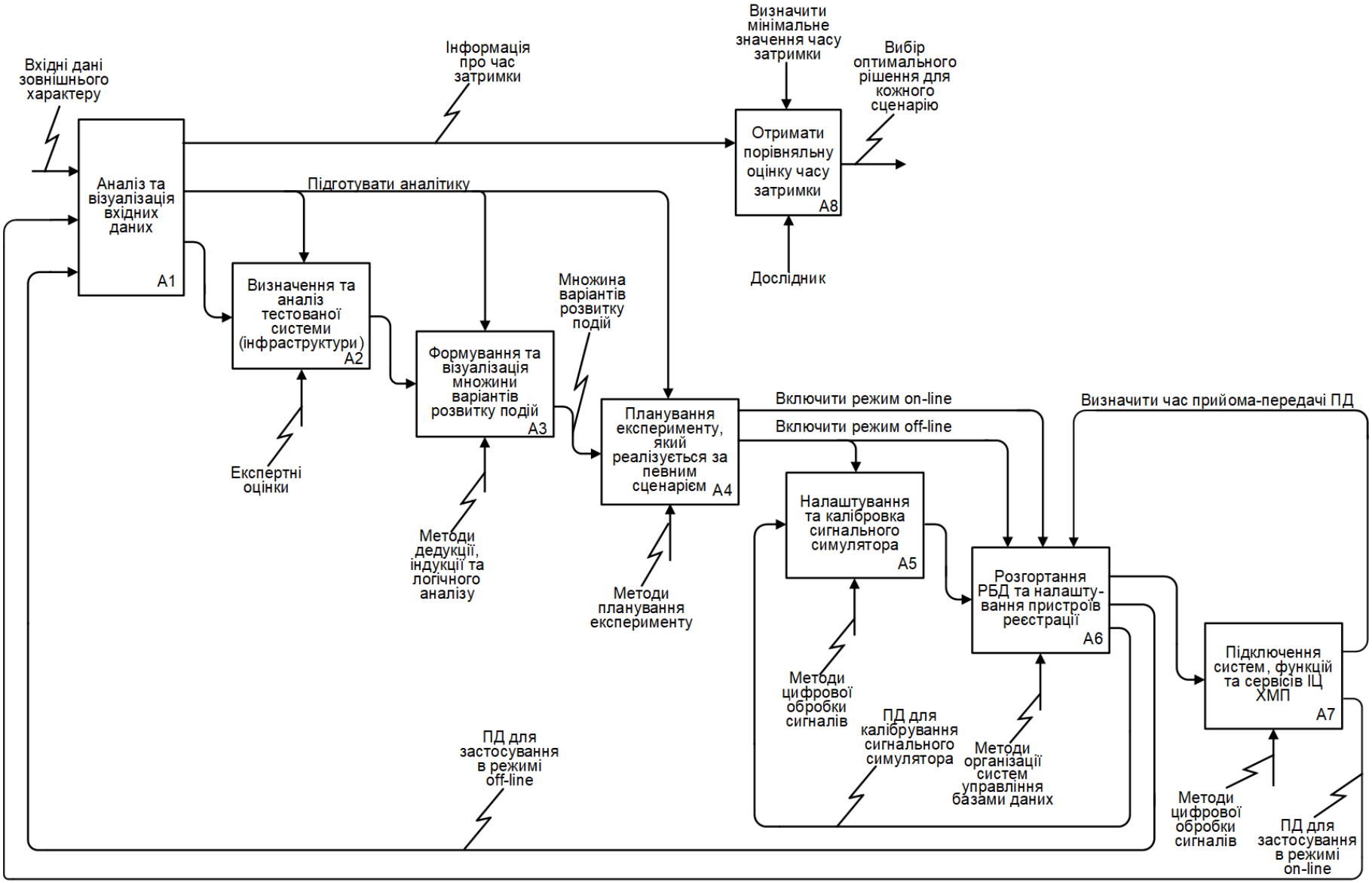


Рисунок 7.9 – Інформаційна технологія тестування хмарних систем КЕІ (IDEF0-діаграма)

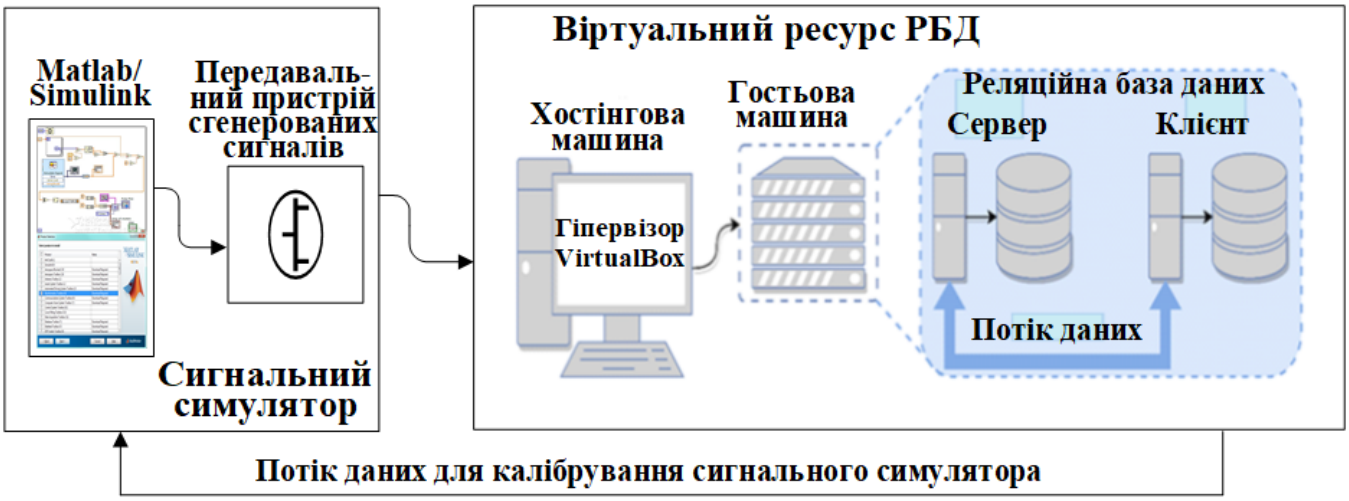


Рисунок 7.10 – Схема реалізації режиму off-line хмарного симулятора

На рис. 7.10 зображено структурні елементи сигнального симулятора та віртуальні ресурси реляційних баз даних. Згідно зображеної схеми стає зрозуміло як утворюється внутрішній контур, який використовується для виконання операцій налаштування та калібрування сигнального симулятора. При розв’язуванні цього завдання доцільно використовувати цифрові пристрої вимірювання з попередньо відомими та обчислюваємими характеристиками. Наприклад, в роботі [196] розглянуто математичну модель цифрового засобу вимірювання з двохланцюговим аналого-цифровим перетворювачем послідовних приближень. Запропонована модель може бути використана для обчислення метрологічних характеристик інтегрованих засобів вимірювання.

Після чого інформація у вигляді потоку даних записується та зберігається у реляційній базі даних. В такому форматі ця інформація використовується за призначенням, включаючи інформацію для визначення часу затримки потока даних в каналі зв’язку. Загальна схема взаємодії двох баз даних в режимі “клієнт–сервер” зображена на рис. 7.11. Відповідно до рис. 7.11, РБД мають два об’єднаних з’єднання та три тригери, що забезпечують конвеєр обміну потоками даних. Варто зазначити, що коли тригери спрацьовують, виникає можливість зберегти поточну позначку часу та записати її.

Нижче наведено SQL скрипти процесу взаємодії двох РБД. Подальше

оцінювання часу затримки здійснюється відповідно до рис. 7.2 з використанням співвідношення (7.1). Результати оцінювання зображено на рис. 7.3 та рис. 7.4. За рахунок реалізації функцій А4–А6 симулятор фактично налаштований на роботу з зовнішнім контуром, тобто з хмарними системами або з системою синхронізованих векторних вимірювань.

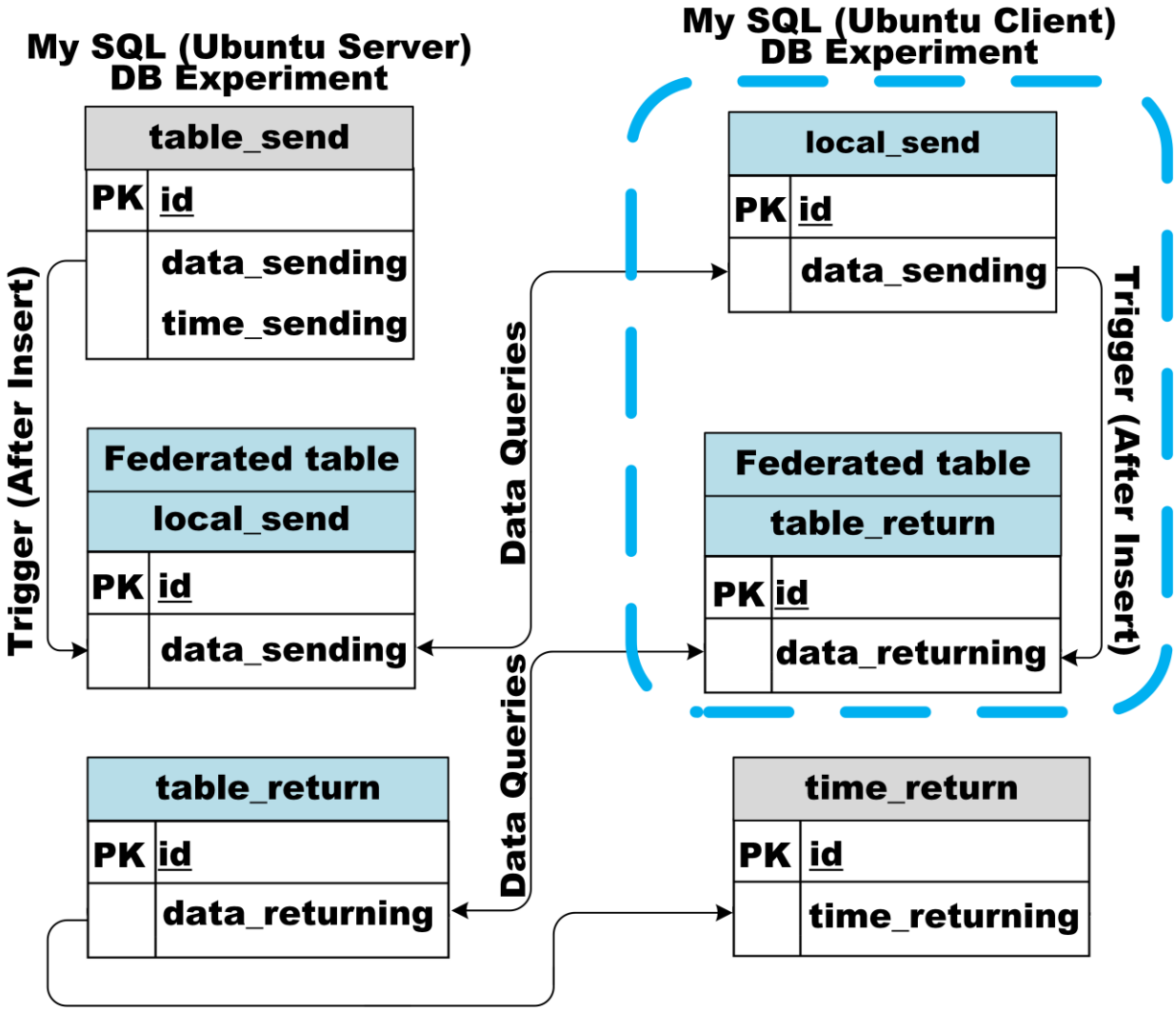


Рисунок 7.11 – Загальна схема взаємодії двох реляційних баз даних

А7. Підключення систем, функцій та сервісів ІЦ ХМП. Фактично це означає, що ПД з виходу симулятора поступає в ІЦ відповідного провайдера, де за допомогою впроваджених методів цифрової обробки сигналів, виконується їхнє перетворення, запис та ретрансляція у зворотньому напрямку. Отриманий таким чином потік даних в режимі on-line повертається до симулятора де фіксується його

час прибуття, здійснюється обробка та виконується порівняльний аналіз за критерієм мінімуму часу затримки.

SQL Script

```
create database Experiment;
use Experiment;

create server link_to_client foreign data wrapper mysql options (user 'user', password
'user', host '10.0.2.11', database 'Experiment');

create table table_send (id int PRIMARY KEY, data_sending double, time_sending time(6));
create table time_return (id int PRIMARY KEY, time_returning time(6));
create table table_return (id int PRIMARY KEY, data_returning double);

create table local_send (id int PRIMARY KEY, data_sending double) engine=federated
connection='link_to_client';

delimiter /
create trigger table_send after insert on table_send for each row
begin
insert into local_send (id, data_sending) values(new.id, new.data_sending);
end; /
delimiter ;

create trigger table_return after insert on table_return for each row insert into
time_returning (id, time_returning) values(new.id, curtime(6));

delimiter /
CREATE PROCEDURE create_data(x int)
BEGIN
  DECLARE i INT default 1;
  WHILE i <= x DO
    insert into table_send(id, data_sending, time_sending) values(i, data_stream,
curtime(6));
    SET i = i + 1;
  END WHILE;
```

У разі виконання критерія мінімуму часу затримки тунельного (захищеного) приймально-передавального каналу зв’язку інформаційний центр конкретного хмарного провайдера визнається як той, що максимально задовільняє вирішальному правилу (7.7) і в умовах сьогодення може застосовуватися для створення хмарних активів існуючої критичної енергетичної інфраструктури; а в перспективі також може бути використаним в контурі управління SmartGrid інфраструктури (рис. 2.7 та рис. 2.10).

7.3 Систематизація та аналіз результатів впровадження

В межах виконаного дисертаційного дослідження було систематизовано результати практичного впровадження запропонованих моделей, методів та інформаційної технології. Сформульовано висновки та рекомендації.

Зокрема, за результатами впровадження інформаційної технології на підприємствах «НВП Радій», «НВП Радікс», Товариства з обмеженою відповідальністю «Радіо Інформаційні Технології» та у Приватному акціонерному товаристві «Інститут інформаційних технологій» встановлено, що на регіональному рівні доцільно використовувати сервіс-орієнтований ресурс AVA VPS hosting (м. Київ); серед досліджуваних сервіс-орієнтованих ресурсів ХМПР за результатами тестування відповідно до критерію (7.7) найкращим є ІЦ Amazon EC2, який розташовано у Франкфурті (Німеччина).

Висновки до розділу 7

1. Показано, що для забезпечення готовності хмарних активів критичних інфраструктур необхідно розробити метод вибору інформаційного центру хмарного провайдера.

2. Встановлено, що в прикладному аспекті для вибору інформаційного центру хмарного провайдера доцільно застосовувати сигнальний симулятор, налаштування та калібрування якого може здійснюватися на основі використання віртуального ресурсу реляційних баз даних, розгорнутих за допомогою програмного продукту VirtualBox. Відповідно до рис. 7.3 та рис. 7.4 встановлено, що величина часу затримки Δt для зазначеного ресурсу змінюється в інтервалі від 595 до 1076 мікросекунд.

3. Розроблено процедуру вибору інформаційного центру хмарного провайдера за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв’язку, яка реалізується за допомогою запропонованого симулятора сигналів, що працює в режимі on-line.

4. Проведно тестування десяти сервіс-орієнтовавних ресурсів регіонального рівня за критерієм мінімуму часу затримки між системою оперативного моніторингу критичної енергетичної інфраструктури та інтегрованими фізичними (віртуальними) компонентами хмарних систем. За результатами тестування встановлено кращі хмарні системи регіонального та європейського рівня.

5. Розроблено інформаційну технологію, яка визначає час затримки

інформаційних потоків даних з застосуванням віртуального ресурсу реляційних баз даних, що дозволяє здійснити оптимальний вибір інформаційного центру відповідного хмарного провайдера за критерієм мінімуму часу затримки.

Основні положення цього розділу викладені у публікаціях автора [8, 32, 76, 102, 123, 127, 187, 196].

ВИСНОВКИ

У дисертаційній роботі сформульовано та розв’язано актуальну науково-прикладну проблему створення методології та розробки технології спільного забезпечення готовності хмарних систем і критичних інфраструктур при відмовах і атаках на вразливості.

1. На основі проведеного аналізу негативних факторів впливу, тенденцій розвитку було сформульовано основні положення методології оцінювання та забезпечення готовності хмарних систем критичних інфраструктур. Подальше застосування розглянутої методології на прикладі критичної енергетичної інфраструктури дозволить підвищити функціональність, інформативність контуру її управління та здійснити еволюційний перехід до гібридної кіберенергетичної інфрастуруктури.

2. Розроблено методи забезпечення готовності критичної енергетичної інфраструктури, які засновані на використанні алгебри причинно-наслідкових комплексів, компаративістичного аналізу та моделюванні процесів протікання аварії інфраструктури. За допомогою використання запропонованих методів вирішуються завдання по оцінюванню ризиків та надаються пропозиції щодо зменшення ризиків КЕІ шляхом забезпечення готовності інфраструктури; виконуються заходи по категоризації критично важливих об’єктів інфраструктури за величиною ризику негативного впливу на них.

3. Розроблено напівмарковські моделі готовності хмарної інфраструктури з декількома підсистемами фізичних, віртуальних машин та інтегрованої системою оперативного моніторингу їхнього інформаційно-технічного стану, що дозволяє враховувати негативні фактори зовнішнього та внутрішнього впливу на їхню безпеку, відмови і атаки на вразливості. Запропонований метод напівмарковського моделювання надав змогу отримати граничні величини показників готовності критичних інфраструктур, фактично відтворюючи їхню поведінку в різноманітних

умовах, включаючи дію зловмисних шкідливих впливів. Приріст величини коефіцієнта готовності становить 37%.

4. Розроблено інформаційну технологію тестування хмарних систем з інтегрованими фізичними компонентами, за допомогою якої здійснюється вибір інформаційного центру відповідного хмарного провайдера за критерієм мінімуму часу затримки та з урахуванням необхідного рівня готовності хмарної інфраструктури. Отримані результати підтверджують універсальний та комплексний характер отриманої інформаційної технології, що надає можливість здійснювати обмін інформацією в контурі управління критичних інфраструктур з застосуванням сервіс-орієнтованих ресурсів. За результатами досліджень встановлено, що при тестуванні хмарних систем Amazon EC2 час затримки експериментального потоку даних не перевищує 0,4 секунди. Отриманий результат є прийнятним з точки зору забезпечення ефективного функціонування контуру управління КІ на основі використання ресурсу ХМС.

5. Удосконалено метод оцінювання функційної безпечності критичних інфраструктур за рахунок використання процедур аналітико-стохастичного моделювання, причинно-наслідкового аналізу та кількісного оцінювання ризику негативного впливу на активи КІ. Метод апробовано для оцінювання показників гарантоздатності інформаційно-керуючої системи типу SCADA КЕІ та перспективних засобів Глобальної морської системи зв’язку та забезпечення безпеки мореплавства МРО МКІ. Отримані кількісні результати моделювання для системи SCADA КЕІ за умови застосування ХМС свідчать про покращення її готовності, а виграш у цьому випадку складає від 8,7% до 49,5%. Варіант використання бездротових сенсорних мереж та додаткових хмарних активів як перспективних засобів для системи ГМСЗБ морських рухомих об’єктів морської критичної інфраструктури надає можливість покращити рівень її функційної та інформаційної безпечності.

6. Удосконалено метод оцінки енергоефективності хмарної інфраструктури з урахуванням готовності фізичних та віртуальних машин зі складу інфраструктури.

Застосування методу дозволило знизити енергоспоживання серверних систем, які входять до складу інфраструктури, та покращити архітектурну побудову ХМІ за рахунок використання інтегрованої системи моніторингу її інформаційно-технічних станів. Середня споживча потужність серверних систем ХМІ завдяки застосуванню методу знизилась, про що свідчать результати досліджень, які представлено в таблиці 4.

7. Удосконалено метод вибору характеристик хмарних систем критичної інфраструктури на основі реалізації процедур аналітико-стохастичного моделювання процесів зміни характеристик готовності хмарних компонентів з оперативною системою моніторингу інформаційно-технічних станів, яка реалізується за допомогою використання систем синхронізованих векторних вимірювань та додаткових хмарних ресурсів (систем). Застосування цих ресурсів (систем) дозволило отримати оцінки граничних величин характеристик готовності КІ і підвищити їхню надійність, функційну та інформаційну безпечність. Кількісні результати дослідження, що підтверджують цей висновок, приведені в таблиці 2.

8. Дістав подальшого розвитку метод моделювання та оцінки готовності критичної інфраструктури з урахуванням еволюційних аспектів її управління за інформаційно-технічним станом на основі застосування запропонованих методів причинно-наслідкової декомпозиції та компаративістичного аналізу, а також шляхом реалізації відповідних етапів аналітико-стохастичного оцінювання готовності сервіс-орієнтованих хмарних ресурсів, які використовуються в загальному контурі управління інфраструктурою. Застосування цих моделей та методів дозволить перейти до стратегій управління готовністю інфраструктури за інформаційно-технічним станом та підвищити ефективність її застосування за призначенням.

9. Систематизовано результати використання розроблених науково-методичного апарату та інформаційної технології в діяльності науково-промислових підприємств, закладів вищої освіти, виконанні міжнародних проєктів, що підтверджено відповідними актами впровадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mission-Critical Cloud Computing for Critical Infrastructures / T. Gamage, D. Anderson, D. Bakken, K. Birman, A. Bose, C. Hauser, K. Maheshwari // Smart Grids: Clouds, Communications, Open Source, and Automation. 2014. P. 1–15. doi:10.1201/b16908-1.

2. Running smart grid control software on cloud computing architectures / K. Birman, L. Ganesh, R. Van Renesse // Workshop Computational Needs for the Next Generation Electric Grid, Cornell University, April, 2011, Ithaca, USA. P. 1–33.

3. Smart Generation and Transmission With Coherent, Real-Time Data / D. Bakken, A. Bose, C. Hauser, D. Whitehead, G. Zweigle // Proceedings of the IEEE, Washington, June, 2011, Washington, USA. P. 928–951.

4. Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions / L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi, A. Dejamkhooy, R. Bayindir, M. Iranpour // 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, Odisha, July 29–31, 2020, Keonjhar, Odisha, India. P. 1–8.

5. Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region [Electronic resource].

URL : https://aws.amazon.com/ru/message/41926/ (date of request 12.10.2020).

6. Amazon S3 outage a Fukushima moment for cloud computing [Electronic resource]. URL : https://www.theserverside.com/opinion/Amazon-S3-outage-a-Fukushima-moment-for-cloud-computing (date of request 12.10.2020).

7. The NIST Definition of Cloud Computing [Electronic resource]. URL : http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf (date of request 12.10.2020).

8. Иванченко О. В. Модели надёжности и живучести энергетических систем. Принципы и модели управления критической энергетической инфраструктурой по техническому мегасостоянию // Безопасность критических инфраструктур:

математические и инженерные методы анализа и обеспечения : кол. монографія / за заг. ред. В. С. Харченка. Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. Розділ 10. С. 311–359.

9. Candle in the Wind? Energy System Resilience to Natural Shocks [Electronic resource].
URL : http://documents1.worldbank.org/curated/en/951761560795137447/pdf/Candle-in-The-Wind-Energy-System-Resilience-to-Natural-Shocks.pdf (date of request 20.10.2020).

10. Yailymova H., Zaslavskyi V., Yang H. Models and methods in creative computing: Diversity and type-variety principle in development of innovation solutions. In 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017 11th International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC). Exeter, UK, 2017. P. 454-461.

11. Zaslavskyi V., Pasichna M. Optimization Techniques for Modelling Energy Generation Portfolios in Ukraine and the EU: Comparative Analysis. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing. Springer, Cham, 2019. Vol. 761. P. 545–555.

12. Zaslavskyi V., Pasichna M. Type Variety Principle and the Algorithm of Strategic Planning of Diversified Portfolio of Electricity Generation Sources. Advances in Intelligent Systems and Computing. Springer, Cham, 2018. Vol. 582. P.474–485.

13. Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [Electronic resource] / P. Fairley // IEEE Spectrum. 2016. Vol. 53, no. 5. pp. 11–13.

URL : https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7459104 (date of request 20.10.2020).

14. Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems / C. Ten, K. Yamashita, Z. Yang, A. Vasilakos, A. Ginter // IEEE Transactions on Smart Grid. 2018. Vol. 9, no. 5, P. 4405–4425. doi:

10.1109/TSG.2017.2656068.

15. Cyber-Attack against Ukrainian Critical Infrastructure [Electronic resource]. URL : https://www.eenews.net/assets/2016/07/19/document_ew_02.pdf (date of request 20.10.2020).

16. Cybersecurity for Energy Delivery Systems [Electronic resource]. URL:https://cred-c.org/sites/default/files/slides/04_Featured-Presentation_CREDC-IW2016_Conway%2C%20Tim.pdf (date of request 20.10.2020).

17. Скляр В. В. Методологія та інформаційні технології забезпечення функціональної безпеки інформаційно-управляючих систем : дис. д-ра техн. наук : 05.13.06 : захищена 06.06.11 : затв. 30.08.11 / Скляр Володимир Володимирович. – Х., 2011. – 324 с.

18. Класифікації морських суден [Електронний ресурс]. URL : https://navy.mil.gov.ua/en/klasifikatsiji-morskikh-suden (дата звернення 23.10.2020).

19. Cyber-Attacks Against the Autonomous Ship / G. Kavallieratos, S. Katsikas, V. Gkioulos // Computer Security. SECPRE 2018, CyberICPS 2018. 2019. Vol. 11387. P. 20–36. doi.org/10.1007/978-3-030-12786-2_2.

20. Иванченко О. В., Каряка А. В., Маврин С. А., Филимонов И. Л. Оценка уровня надёжности телекоммуникационных систем морских подвижных объектов для их технического обслуживания по состоянию // Радіоелектронні і комп’ютерні системи. 2008. Вип. 6 (33). С. 128–133.

21. A Security Evaluation of AIS Automated Identification System / M. Balduzzi, A. Pasta, K. Wilhoit // Computer Security Applications Conference : Proc. of the 30th Intern. Conf., New Orleans, December 8–12, 2014, New Orleans, USA. P. 436–445.

22. Cyber threat to ships – real but manageable [Electronic resource]. URL : https://library.e.abb.com/public/b9d267b4767c582f85257ca1003280e9/106_Cyber_threat_to_ships_real_but_manageable.pdf (date of request 25.10.2020).

23. A critical analysis of security vulnerabilities and counter measures in a smart ship system [Electronic resource].

URL : https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1209&context=ism (date of

request 25.10.2020).

24. Levykin V., Ievlanov M., Neumyvakina O. Developing the models of patterns in the design of requirements to an information system at the knowledge level // Eastern-European Journal of Enterprise Technologies. 2017. Vol 5., no. 2 (89). P. 19–26.

25. Levykin V., Chala O. Development of a method of probabilistic inference of sequences of business process activities to support business process management // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 5, no. 3 (95). P. 16–24.

26. Levykin V., Chala O. Method of determining weights of temporal rules in markov logic network for building knowledge base in information control system // EUREKA : Physics and Engineering. 2018. Vol. 5. P. 3–10.

27. Synchrophasors: How They are Making the Electric Grid Smarter [Electronic resource]. URL:https://www.youtube.com/watch?v=uylGQ9ntLd0&list=PLP2qkC5pxHqEEatgzoTVVdzKvQucJzY_q (date of request 29.10.2020).

28. Wide Area Monitoring System [Electronic resource]. URL : https://www.youtube.com/watch?v=7dp8CFEF-aw (date of request 29.10.2020).

29. Synchrophasor Technology Applications [Electronic resource]. URL : https://www.youtube.com/watch?v=3SLk6WGCXX8 (date of request 29.10.2020).

30. The Evaluation of Phasor Measurement Units and Their Dynamic Behavior Analysis / H. Liu, T. Bi, Q. Yang // IEEE Transactions on Instrumentation and Measurement. 2013. Vol. 62, no. 6, P. 1479–1485. doi: 10.1109/TIM.2013.2242611.

31. Implementation Techniques for Frequency Phasor Estimation in Phasor Measurement Units (PMUs) / A. Jain, A. Bhardwaj, S. Kumar, S. Bhullar // 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU). 2018. P. 1–6. doi: 10.1109/IoT-SIU.2018.8519907.

32. Иванченко О. В., Харченко В. С. Полумарковская модель готовности облачной инфраструктуры с интегрированной системой мониторинга технического состояния // Радіоелектронні і комп’ютерні системи. 2016. № 5 (79). С. 15–19.

33. Semi-Markov Availability Model for Infrastructure as a Service Cloud

Considering Energy Performance / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, I. Blindyuk, K. Smoktii // Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control. 2019. Vol. 171. P. 141–159. doi:10.1007/978-3-030-00253-4_7.

34. 2018 Security Research [Electronic resource]. URL : https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf (data of request 30.10.2020).

35. Cloud Computing and Security – A Natural Match [Electronic resource]. URL : https://trustedcomputinggroup.org/wp-content/uploads/Cloud-Computing-and-Security-Whitepaper_July29.2010.pdf (data of request 30.10.2020).

36. COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes [Electronic resource]. URL : https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/ (data of request 30.10.2020).

37. CyVolve. State of Cybersecurity Report [Electronic resource]. URL : https://www.cyvolve.com/downloads/CyVolve-State-of-Cybersecurity-Report-2020.pdf (data of request 31.11.2020).

38. Top cybersecurity facts, figures and statistics for 2020 [Electronic resource]. URL : https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html (data of request 30.10.2020).

39. AWS Security Hub Partners [Electronic resource]. URL : https://aws.amazon.com/ru/security-hub/partners/ (data of request 30.10.2020).

40. Cloud Security Guarding for AWS [Electronic resource]. URL : https://www.barracuda.com/resource/ref_architectures/cloudsolutionguardianAWS (data of request 31.10.2020).

41. AWS Security with Check Point CloudGuard [Electronic resource]. URL : https://www.checkpoint.com/solutions/amazon-aws-security/ (data of request 31.10.2020).

42. Cloud Security and Analytics [Electronic resource]. URL : https://www.ibm.com/security/security-intelligence/qradar/securing-the-cloud (data of request 31.10.2020).

43. Mission Cloud for AWS Security Hub [Electronic resource]. URL : https://www.skyhighnetworks.com/mvision-cloud-for-amazon-web-services-aws-security-hub/ (data of request 31.10.2020).

44. Stay afloat using AWS Security Hub and Splunk to find, fix and prevent security leaks [Electronic resource]. URL : https://www.splunk.com/en_us/form/stay-afloat-using-aws-security-hub.html (data of request 31.10.2020).

45. Delivering intelligent threat detection and response on Amazon Web Services [Electronic resource]. URL : https://www.vectra.ai/partners/aws (data of request 31.10.2020).

46. CloudGuard Cloud Security Posture Management [Electronic resource]. URL : https://www.checkpoint.com/downloads/products/cloudguard-CSPM-cloud-security-platform-product-brief.pdf (data of request 01.11.2020).

47. Power-up the security blanket [Electronic resource]. URL : https://www.wartsila.com/insights/article/power-up-the-security-blanket (data of request 02.11.2020).

48. Infographic: History of IIoT Cyber-Attacks and How to Avoid Them [Electronic resource].

URL : https://www.engineering.com/IOT/ArticleID/13353/Infographic-History-of-IIoT-Cyber-Attacks-and-How-to-Avoid-Them.aspx (data of request 02.11.2020).

49. Cyber Immunity, a holistic view for Industrial Control Systems [Electronic resource].

URL : https://electricenergyonline.com/energy/magazine/1180/article/Security-Sessions-Cyber-Immunity-A-Holistic-View-for-Industrial-Control-Systems.htm (data of request 02.11.2020).

50. Харченко В. С. Гарантоздатні системи та багатоверсійні обчислення, аспекти еволюції // Радіоелектронні і комп’ютерні системи. 2009. № 7 (41). С. 46–59.

51. Industrial Internet of Things Security for the Transportation Infrastructure / B. Pretorius, B. van Niekerk // Journal of Information Warfare. 2020. Vol. 19, no. 3. P. 50–67.

52. Maritime Cybersecurity – Shift Happens [Electronic resource]. URL : https://www.wartsila.com/insights/webinar/details_maritime-cybersecurity (data of request 03.11.2020).

53. Cyber Security Challenges for the Maritime Industry [Electronic resource]. URL : https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/ (data of request 03.11.2020).

54. SHARPE at the age of twenty-two / K. Trivedi, R. Sahner // SIGMETRICS Performance Evaluation Review. 2009. Vol. 36, no 4, P. 52–57.

55. HAIL : A high-availability and integrity layer for cloud storage / K. Bowers, A. Juels, A. Oprea // CCS ’09 : 16th ACM Conference on Computer and Communication Security, Chicago Illinois, November, 2009, Chicago Illinois, USA. P. 187–198.

56. QoS-aware scheduling in heterogeneous datacenters with paragon / C. Delimitrou, C. Kozyrakis // ACM Transactions on Computer Systems (TOCS). 2013. Vol. 31, no. 4, P. 12.

57. HCloud : Resource-efficient provisioning in shared cloud systems / C. Delimitrou, C. Kozyrakis // ACM Sigplan Notices. 2016. Vol. 51, no. 4. P. 473–488.

58. Bolt : I know what you did last summer ... in the cloud / C. Delimitrou, C. Kozyrakis // ACM SIGARCH Computer Architecture News. 2017. Vol. 45, no. 1. P. 599–613.

59. Иванченко О. В., Харченко В. С. Анализ стохастических методов метамоделирования и оценивания готовности облачных инфраструктур // Радіоелектронні і комп’ютерні системи. 2016. № 6 (80). С. 6–11.

60. Stochastic Model Driven Capacity Planning for an Infrastructure-as-a-Service Cloud / R. Ghosh, F. Longo, R. Xia, Vijay K. Naik, K. Trivedi // IEEE Transactions On Services Computing. 2013. Vol. 7, no. 4. P. 667–680.

61. Power-hierarchy of dependability-model types / M. Malhotra, K. Trivedi // IEEE Transactions on Reliability. 1994. Vol. 43, no. 3. P. 493–502.

62. A scalable availability model for Infrastructure-as-a-Service cloud / F. Longo, R. Ghosh, V. K. Naik, K. Trivedi // 2011 IEEE/IFIP 41st International Conference on

Dependable Systems & Networks (DSN), Hong Kong, 27–30 June, 2011, Hong Kong, China. P. 335–346.

63. Quantifying software performance, reliability and security: An architecture-based approach [Text] / V. Sharma, K. Trivedi // Journal of Systems and Software. 2007. Vol. 80, no. 4. P. 493–509.

64. Queueing networks and Markov chains: modeling and performance evaluation with computer science applications / G. Bolch, S. Greiner, H. De Meer, K. Trivedi. [New Jersey] : John Wiley & Sons, 2006. 878 p.

65. A hidden semi-Markov model with missing data and multiple observation sequences for mobility tracking / S.-Z. Yu, H. Kobayashi // Signal Processing. 2003. Vol. 83, no. 2. P. 235–250.

66. Sensitivity Analysis of Server Virtualized System Availability / R. Matos, P. Maciel, F. Machida, D. Kim, K. Trivedi // Transactions on Reliability. 2012. Vol. 61, no. 4. P. 994–1006.

67. Modeling user-perceived reliability based on user behavior graphs / D. Wang, K. Trivedi // International Journal of Reliability, Quality and Safety Engineering. 2009. Vol. 16, no. 4. P. 303–329.

68. Combining performance and availability analysis in practice / K. Trivedi, E. Andrade, F. Machida // Advances in Computers. 2012. Vol. 84. P. 1–38.

69. Amazon S3 [Electronic resource]. URL : https://aws.amazon.com/ru/s3/ (date of request 29.11.2020).

70. Харыбин А. В. Анализ требований к функциональной безопасности современных ИУС критического применения и их структурных элементов в различных условиях эксплуатации // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : кол. монографія / за заг. ред. В. С. Харченка. Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. Підрозділ 13.1. С. 410–413.

71. Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies / A. Sundararajan, T. Khan, A. Moghadasi, A.

Sarwat // Journal of Modern Power Systems and Clean Energy. 2019. Vol. 7, no. 3. P. 449–467.

72. Evolution of von Neumann's paradigm: Dependable and green computing / V. Kharchenko, A. Gorbenko // East-West Design & Test Symposium (EWDTS 2013), Rostov-on-Don, September 27–30, 2013, Rostov-on-Don, Russia. P. 1–6.

73. Stochastic Model Driven Capacity Planning for an Infrastructure-as-a-Service Cloud / R. Ghosh, F. Longo, R. Xia, Vijay K. Naik, K. Trivedi // IEEE Transactions On Services Computing. 2013. Vol. 7, no. 4. P. 667–680.

74. Semi-Markov availability model for infrastructure as a service cloud considering hidden failures of physical machines / O. Ivanchenko, V. Kharchenko, Y. Ponochovnyi, I. Blindyuk, K. Smoktii // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 13th Intern. Conf., Kyiv, May 15–18, 2017, Kyiv, Ukraine. Vol. 1844. P. 634–644.

75. Semi-Markov availability model considering deliberate malicious impacts on an Infrastructure-as-a-Service Cloud / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii // 2018 IEEE 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) : Proc. of the 14th Intern. Conf., Lviv–Slavske, February 20–24, 2018, Lviv–Slavske, Ukraine. P. 570–573.

76. Semi-Markov's models for availability assessment of an Infrastructure as a Service Cloud with multiple pools of physical and virtual machines / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) : Proc. of the 14th Intern. Conf., Kyiv, May 24–27, 2018, Kyiv, Ukraine. P. 98–102.

77. NIST Cloud Computing Reference Architecture / R. Bohn, J. Messina, F. Liu, J. Tong, J. Mao // 2011 IEEE World Congress on Services, Washington, July 4–9, 2011, Washington, USA. P. 594–596.

78. Scalable Analytics for IaaS Cloud Availability / R. Ghosh, F. Longo, F. Frattini, S. Russo K. Trivedi // IEEE Transactions on Cloud Computing. 2014. Vol. 2, no. 1.

P. 57–70.

79. Sensitivity Analysis of Server Virtualized System Availability / R. Matos, P. Maciel, F. Machida, D. Kim, K. Trivedi // IEEE Transactions on Reliability. 2012. Vol. 61, no. 4. P. 994–1006.

80. Molecular computation of solutions to combinatorial problems / L. Adleman // Science. 1994. Vol. 266, no. 5187. P. 1021–1024.

81. Сахабутдинова А. Р. Небиологическое применение молекул ДНК / А. Р. Сахабутдинова, К. И. Михайленеко, Р. Р. Гарафутдинов, О. Ю. Кирьянов, М. А. Сагитова, А. М. Сагитов, А. В. Чемерис // Биомика. 2019. Т. 11, № 3. С. 344–377.

82. Паун Г., Розенберг Г., Саломаа А. ДНК–компьютер. Новая парадигма вычислений. М. : Мир, 2004. 528 с.

83. Phasor measurement unit : A revolution in power system / S. Kumar Singh // International Research Journal of Engineering and Technology (IRJET). 2018. Vol. 5, no. 9. P. 177–182.

84. A survey on smart grid technologies and applications / G. Dileep // Renewable Energy. 2020. Vol. 146. P. 2589–2625.

85. Мокеев А. В., Бовыкин В. Н., Хромцов Е. И., Миклашевич А. В., Попов А. И., Родионов А. В. Применение технологии синхронизированных векторных измерений для управления, защиты и автоматики // Релейщик. 2019. № 3 (35). С. 32–37.

86. Sniffing out grid attacks / P. Fairley // IEEE Spectrum. 2016. Vol. 53, no. 9. P. 13–15.

87. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations [Electronic resource]. URL : https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Full_Final_Report.pdf#search=Final%20Report%2C%20Blackout%2C%202003 (date of request 15.12.2020).

88. Role of Phasor Measurement Unit in Wide Area Monitoring and Control [Electronic resource]. URL : https://www.erlphase.com/downloads/application_notes/Roles_of_PMUs_in_Wide_Area_Monitoring_and_Control.pdf (date of request 15.12.2020).

89. Smart Grid communication applications: measurement equipment and networks architecture for data and energy flow / T. Atmaja, D. Andriani, R. Darussalam // Journal of Mechatronics, Electrical Power, and Vehicular Technology. 2019. Vol. 10, no. 2. P. 73–84.

90. GridCloud : Infrastructure for Cloud-Based Wide Area Monitoring of Bulk Electric Power Grids / D. Anderson, T. Gkountouvas, M. Meng et al. // IEEE Transactions on Smart Grid. 2019. Vol. 10, no. P. 2170–2179.

91. GridControl : A Software Platform to Support the Smart Grid [Electronic resource] URL : http://www.cs.cornell.edu/projects/gridcontrol/index.html (date of request 17.12.2020).

92. Adding a Hardwar Virtual Private Gateway to Your VPC [Electronic resource].
URL: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html (date of request 17.12.2020).

93. Amazon S3 [Electronic resource]. URL : https://aws.amazon.com/ru/s3/ (date of request 17.12.2020).

94. Amazon EC2: безопасные масштабируемые вычисления для виртуальной поддержки любой нагрузки [Електронний ресурс]. URL : https://aws.amazon.com/ru/ec2/ (дата звернення 17.12.2020).

95. Amazon Kinesis: простой сбор, обработка и анализ видеопотоков и потоковых данных в режиме реального времени [Електронний ресурс]. URL : https://aws.amazon.com/ru/kinesis/ (дата звернення 17.12.2020).

96. Vulnerability and security in a changing power system [Electronic resource]. URL: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2598690/TR+A7278.pdf?sequence=2 (date of request

18.12.2020).

97. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies / G. Kjølle, I. Utne, O. Gjerde // Reliability Engineering & System Safety. 2012. Vol. 105. P. 80–89.

98. HAZOP–Local approach in the Mexican oil and gas industry / M. Pérez-Marín, M. Rodríguez-Toral // Journal of Loss Prevention in the Process Industries. 2013. Vol. 26, no. 5. P. 936–940.

99. Харченко В. С., Иванченко О. В., Мащенко Е. Н. Методология FMECA: новая парадигма анализа видов и последствий отказов критических инфраструктур // Автоматизація : проблеми, ідеї, рішення : матеріали Міжнар. наук.-техн. конф., м. Севастополь, 6–10 верес. 2010 р. Севастополь, 2010. С. 142–145.

100. CASE-оценка критических программных систем : безопасность / Під ред. Харченка В. С. Міністерство освіти та науки України, Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», 2012. – 302 с.

101. Скатков А. В., Иванченко О. В. Цикломатическая сложность моделей компонентов критических инфраструктур // Інформаційні технології та інформаційна безпека в науці, техніці та навчанні : ІНФОТЕХ–2011 : матеріали Міжнар. наук.-практ. конф., м. Севастополь, 5–10 верес. 2011 р. Севастополь, 2011. С. 102–103.

102. Иванченко О. В. Аналитико-стохастические модели надёжности и безопасности критических энергетических инфраструктур // Информационные технологии для критических инфраструктур : кол. монографія / за заг. ред. О. В. Скаткова. Севастополь : Севастопольський національний техн. ун-т, 2012. Глава 3. С. 89–124.

103. Іванченко О. В. Теоретико-множинна модель кібератаки системи корпоративного управління // Математичні проблеми технічної механіки та прикладної математики : матеріали Міжнар. наук. конф., м. Дніпро–Кам’янське, 2–5 груд. 2019 р. , Дніпро, Кам’янське, Україна. Дніпро : Університет митної справи та фінансів, 2019. Дніпро–Кам’янське, 2019. С. 65–66.

104. Software Reliability and Testing Time Allocation: An Architecture-Based Approach / R. Pietrantuon, S. Russo, K. Trivedi // IEEE Transactions on Software Engineering. 2010. Vol. 36, no. 3. P. 323–337.

105. Optimal Allocation of Test Resources for Software Reliability Growth Modeling in Software Development / M. Lyu, S. Rangarajan, A. P. A. van Moorsel // IEEE Transactions on Reliability. 2002. Vol. 51, no. 2. P. 183–192.

106. Efficient allocation of testing resources for software module testing based on the hyper-geometric distribution software reliability growth model / Rong-Huei Hou, Sy-Yen Kuo, Yi-Ping Chang // 7th International Symposium on Software Reliability Engineering : Proc. of ISSRE'96, White Plains, 30 Oct.–2 Nov., 1996, White Plains, NY, USA. P. 289–298.

107. Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment / M. Ceriotti, L. Mottola, G. Picco et al. // 2009 International Conference on Information Processing in Sensor Networks, San Francisco, April 13–16, 2009, San Francisco, CA, USA. P. 277–288.

108. Automated Generation of Performance and Dependability Models for the Assessment of Wireless Sensor Networks / C. Martino, M. Cinque, D. Cotroneo // IEEE Transactions on Computers. 2012. Vol. 61, no. 6. P. 870–884.

109. Иванченко О. В. Полумарковские модели мониторинга информационно-технического состояния критических инфраструктур // Радіоелектронні і комп'ютерні системи. 2012. № 7 (59). С. 219–224.

110. Иванченко О. В., Паткаускас А. В., Маврин С. А., Корощенко Н. Н. Обобщённый критерий синтеза адаптивной системы технического диагностирования сложных промышленных объектов // Радіоелектронні і комп'ютерні системи. 2009. № 7 (41). С. 127–135.

111. Волков Л. И. Управление эксплуатацией летательных комплексов. М. : Высшая школа, 1981. 368 с.

112. Understanding failures in international safety-critical infrastructures: a comparison of European and North American power failures [Electronic resource]. URL:

http://www.dcs.gla.ac.uk/~johnson/papers/Blackout_Comparison/Johnson_Power_Infrastructure.pdf (data of request 20.12.2020).

113. Иванченко О. В., Харченко В. С., Бирюков Д. Ю. Полумарковская модель протекания аварии критической инфраструктуры // Радіоелектронні і комп'ютерні системи. 2013. № 5 (64). С. 45–51.

114. Скатков А. В., Воронин Д.Ю. Комплементарное управление критическими инфраструктурами на основе концепции потенциал// Информационные технологии для критических инфраструктур : кол. монографія / за заг. ред. О. В. Скаткова. Севастополь : Севастопольський національний техн. ун-т, 2012. Глава 1. С. 10–18.

115. Иванченко О. В., Бочарова В. В., Владимирова Е. С., Фомина А. Б. Модели надёжности и безопасности критических энергетических инфраструктур // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. Севастополь, 2011. Вип. 4 (8). С. 109–119.

116. Иванченко О. В., Бочарова В. В. Обоснование предельных величин показателей надёжности критических энергетических инфраструктур // Радіоелектронні і комп'ютерні системи. 2012. № 5 (57). С. 197–201.

117. Comparison of level-crossing times for Markov and semi-Markov processes / F. Ferreira, A. Pacheco // Statistics & Probability Letters. 2007. Vol. 77, no. 2. P. 151–157.

118. Numerical bounds for semi-Markovian quantities and application to reliability / S. Mercier // Methodology and Computing in Applied Probability. 2008. Vol. 10, no. 2. P. 179–198.

119. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся ВТУЗОВ. Москва : Наука, 1986. 544 с.

120. Иванченко О. В., Буланый А. П., Прокопенко Р. А. Обобщенный критерий управления конфигурацией инфраструктуры как сервиса облачных вычислений // Вісник Академії митної служби України. 2015. № 1 (53). С. 43–55.

121. A scalable availability model for Infrastructure-as-a-Service cloud / F. Longo,

R. Ghosh, V. Naik, K. Trivedi // 2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN), Hong Kong, June 27–30, 2011, Hong Kong, China. P. 335–346.

122. End-to-End Performability Analysis for Infrastructure-as-a-Service Cloud: An Interacting Stochastic Models Approach / R. Ghosh, K. Trivedi, V. Naik, D. Kim // 2010 IEEE 16th Pacific Rim International Symposium on Dependable Computing, Tokyo, December 13–15, 2010, Tokyo, Japan. P. 125–132.

123. Semi-Markov availability model of an infrastructure as a service cloud with multiple pools / O. Ivanchenko, V. Kharchenko // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 12th Intern. Conf., Kyiv, June 21–24, 2016, Kyiv, Ukraine. Vol. 1614. P. 349–360.

124. (26) Scalable Analytics for IaaS Cloud Availability / R. Ghosh, F. Longo, F. Frattini, S. Russo, K. Trivedi // IEEE Transactions on Cloud Computing. 2014. Vol. 2, no. 1. P. 57–70.

125. Острейковский В. А. Теория надёжности. М. : Высшая школа, 2003. 463 с.

126. 2018 Security Research [Electronic resource]. URL: https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf (data of request 22.12.2020).

127. Availability as a cloud service for control system of critical energy infrastructure / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii, Y. Ponochovnyi // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 14th Intern. Conf., Kyiv, May 14–17, 2018, Kyiv, Ukraine. Vol. 2104. P. 571–582.

128. Іванченко О. В. Аналітико-стохастична модель готовності системи SCADA критичної інфраструктури // 20th International Scientific and Practical Conference on Perspective Directions for the Development of Science and Practice : Proc. of the 20th Intern. Conf., Athens, June 8–9, 2020, Athens, Greece. P. 166–170.

129. Іванченко О. В. Аналітико-стохастична модель зловмисного шкідливого впливу на кібернетичні активи системи SCADA критичної інфраструктури // 21st

International Scientific and Practical Conference on Current Trends in the Development of Science and Practice : Proc. of the 21st Intern. and Pract. Conf., Haifa, 15–16 June, 2020, Haifa, Israel. P. 125–130.

130. Смоктий О. Д., Смоктий К. В., Иванченко О. В. Анализ механизма и последствий воздействия DDoS-атак на эталонную модель взаимодействия открытых систем OSI // Системи управління, навігації та зв’язку. 2017. № 1 (41). С. 33–37.

131. Иванченко О. В., Солдатенко Е. С., Владимирова Е. С. Архитектурный подход к оценке надежности программного обеспечения системы управления критической инфраструктуры // Системи обробки інформації. 2014. № 1 (117). С. 173–179.

132. Іванченко О. В. Аналітико-стохастичний метод побудови структурних схем безпеки кібернетичних активів системи SCADA критичної інфраструктури // Системи та технології. 2019. № 1 (57). С. 81–106.

133. Іванченко О. В. Аналітико-стохастична модель гарантоздатності кібернетичних та хмарних активів системи SCADA критичної інфраструктури // Системи та технології. 2020. № 1 (59). С. 14–59.

134. Іванченко О. В. Оцінювання рівня безпеки системи SCADA критичної інфраструктури з урахуванням доступності кібернетичних та хмарних активів // Системи та технології. 2019. № 2 (58). С. 5–32.

135. Иванченко О. В., Харченко В. С. Причинно-следственная декомпозиция аварий и инцидентов критических инфраструктур // Проблемы критических ситуаций в точной механике и управлении : материалы Всерос. научн. конф. с междунар. участием, г. Саратов, 25–27 сент. 2013 г. Саратов, 2013. С. 59–63.

136. Иванченко О. В., Харченко В. С. Метод причинно-следственной декомпозиции аварий и инцидентов критических инфраструктур // Радіоелектронні і комп’ютерні системи. 2014. № 5 (69). С. 12–17.

137. Risk assessment of critical energy infrastructure considering physical and cyber assets: Methodology and models / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak,

S. Konovalenko // 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) : Proc. of the 4th Intern. Symp., Lviv, September 20 –21, 2018, Lviv, Ukraine. P. 225–228.

138. Dependability Assessment for SCADA System Considering Usage of Cloud Resources / O. Ivanchenko, V. Kharchenko, E. Brezhnev, Y. Ponochovnyi, B. Moroz, L. Kabak // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT) : Proc. of the 11th Intern. Conf., Kyiv, May 14–18, 2020, Kyiv, Ukraine. P. 13–17.

139. Ukraine cyber-induced power outage : Analysis and practical mitigation strategies / D. Whitehead, K. Owens, D. Gammel, J. Smith // 2017 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, April 3–6, 2017, College Station, TX, USA. P. 1–8.

140. Analysis of the Cyber Attack on the Ukrainian Power Grid [Electronic resource] URL : https://pdf4pro.com/amp/view/tlp-white-analysis-of-the-cyber-attack-on-the-ukrainian-57c2eb.html (data of request 23.12.2020).

141. Vulnerability Assessment of Cybersecurity for SCADA Systems / C. Ten, C. Liu, G. Manimaran // IEEE Transactions on Power Systems. 2008. Vol. 23, no. 4. P. 1836–1846.

142. SCADA systems : challenges for forensic investigators / I. Ahmed, S. Obermeier, M. Naedele, G. Richard // Computer. 2012. Vol. 45, no. 12. P. 44–51.

143. Харченко В. С. Гарантоздатні системи та багатоверсійні обчислення, аспекти еволюції // Радіоелектронні і комп’ютерні системи. 2009. № 7(41). С. 46–59.

144. Dell EMC PowerEdge R640. Technical Guide [Electronic resource]. URL : https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/us/PowerEdge-R640-Technical-Guide.pdf (data of request 23.12.2020).

145. Риге Ж. Бинарные отношения, замыкания, соответствия Галуа // Кибернетический сборник : сб. переводов. Москва : Иностранная литература, 1963.

Вып. 7. С. 129–185.

146. Вагнер В. В. Теория отношений и алгебра частичных отображений // Теория полугрупп и её приложения : сб. статей. Саратов, 1965. Вып. 1. С. 3–178.

147. Жотиков В. Г. Обобщенные группы Вагнера и их приложения в геометрии и физике // Гиперкомплексные числа в геометрии и физике. 2009. Т. 6, № 2(12). С. 32–48.

148. Cybersecurity for Energy Delivery Systems [Electronic resource]. URL : https://cred-c.org/sites/default/files/slides/04_Featured-Presentation_CREDC-IW2016_Conway%2C%20Tim.pdf (date of request 24.12.2020).

149. (24) Твердохлебов В. А. Контроль и диагноз сложных систем методами теории бинарных отношений. Саратов : Изд-во Сарат. Ун-та, 1967. 30 с.

150. Харыбин А. В. Анализ требований к функциональной безопасности современных ИУС критического применения и их структурных элементов в различных условиях эксплуатации // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : кол. монографія / за заг. ред. В. С. Харченка. Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. Підрозділ 13.1. С. 410–413.

151. Sensitivity analysis of a hierarchical model of mobile cloud computing / R. Matos, J. Araujo, D. Oliveira, P. Maciel, K. Trivedi // Simulation Modelling Practice and Theory. 2015. Vol. 50. P. 151–164.

152. Распределённые критические системы и инфраструктуры : практикум / О. В. Иванченко, В. С. Ловягин, Е. Н. Мащенко, А. В. Скатков, В. И. Шевченко. Харьков : Национальный аэрокосмический университет имени Н. Е. Жуковского «ХАИ», 2013. 179 с.

153. Distributed Coordination and Optimisation of Network-Aware Electricity Prosumers [Electronic resource]. URL: https://openresearch-repository.anu.edu.au/bitstream/1885/110027/1/Scott%20Thesis%202016.pdf (data of request 26.12.2020).

154. Systemic Failure on a Grand Scale: The 14 August 2003 North American

Blackout [Electronic resource].
URL : https://agupubs.onlinelibrary.wiley.com/doi/epdf/10.1029/2003SW000027 (data of request 24.12.2020).

155. Принцип причинно-следственной декомпозиции динамических систем : монография / А. Ф. Резчиков, В. А. Твердохлебов. Саратов: ООО Издательский Центр «Наука», 2013. 56 с.

156. Гаршин А. Ю., Иванченко О. В., Мащенко Е. Н. Методика оценки уровня опасности морской критической инфраструктуры // Системи озброєння і військова техніка. 2010. № 3 (23). С. 107–109.

157. Global Maritime Distress and Safety System (GMDSS) [Electronic resource].
URL:https://www.researchgate.net/publication/336737300_Global_Maritime_Distress_and_Safety_System_GMDSS_Next_Generation (data of request 24.12.2020).

158. Cyber-Attacks Against the Autonomous Ship / G. Kavallieratos, S. Katsikas, V. Gkioulos // Computer Security. 2019. Vol. 11387. P. 20–36. doi.org/10.1007/978-3-030-12786-2_2.

159. Представление автоматных отображений геометрическими структурами : монография / В. А. Твердохлебов, А. С. Епифанов. Саратов : ООО Издательский Центр «Наука», 2013. 204 с.

160. Резчиков А. Ф., Твердохлебов В. А. Причинно-следственные комплексы как модели сложных человеко-машинных систем // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : кол. монографія / за заг. ред. В. С. Харченка. Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. Розділ 1. С. 17–58.

161. Systemic Failure on a Grand Scale : The 14 August 2003 North American Blackout [Electronic resource].
URL : https://agupubs.onlinelibrary.wiley.com/doi/epdf/10.1029/2003SW000027 (data of request 24.12.2020).

162. Understanding failures in international safety-critical infrastructures: a

comparison of European and North American power failures [Electronic resource] URL : http://www.dcs.gla.ac.uk/~johnson/papers/Blackout_Comparison/Johnson_Power_Infrastructure.pdf (data of request 24.12.2020).

163. Establishing public policy as a primary cause of engineering failures in National Infrastructures [Electronic resource]. URL:http://www.dcs.gla.ac.uk/~johnson/papers/Public_Policy/Chris_W_Johnson_US_Blackout.pdf (data of request 25.12.2020).

164. Иванченко О. В., Скатков А. В. Проблемы обеспечения безопасности и надёжности энергетических инфраструктур // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : кол. монографія / за заг. ред. В. С. Харченка. Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. Розділ 9. С. 284–310.

165. Распределённые критические системы и инфраструктуры : практикум / О. В. Иванченко, В. С. Ловягин, Е. Н. Мащенко, А. В. Скатков, В. И. Шевченко. Харьков : Национальный аэрокосмический университет имени Н. Е. Жуковского «ХАИ», 2013. 179 с.

166. Мащенко Е. Н., Иванченко О. В., Смахашева Н. В. Аналитико-стохастическая модель управления техническим состоянием изделий критического применения // Радіоелектронні і комп’ютерні системи. 2010. № 7 (48). С. 30–34.

167. Иванченко О. В., Харченко В. С., Одарущенко О. Н. Принципы анализа и управления безопасностью критических инфраструктур // Вісник Хмельницького національного університету. 2010. № 5 (170). С. 218–221.

168. Яцек Я. Ф., Иванченко О. В., Войтюк А. В., Степанов В. А. Комплексный подход к управлению критическими инфраструктурами по техническому мегасостоянию // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. Севастополь, 2010. Вип. 4 (4). С. 91–99.

169. Management of critical infrastructures based on technical megastate [Electronic resource] / O. Ivanchenko, V. Kharchenko, A. Skatkov // An International Journal. Information and Security. 2012. Vol. 28, no. 1. pp. 37–51. URL :

http://defencemanagement.org/system/files/28.03_Ivanchenko_Kharchenko_Skatkov.pdf (date of request 16.12.2020).

170. Харченко В. С. Гарантоздатні системи та багатоверсійні обчислення, аспекти еволюції // Радіоелектронні і комп'ютерні системи. 2009. № 7(41). С. 46–59.

171. Иванченко О. В., Ловягин В. С. Техническое обслуживание компонентной составляющей критических инфраструктур // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. Севастополь, 2011. Вип. 1 (5). С. 253–259.

172. Иванченко О. В., Харченко В. С., Смоктий К. В., Смоктий О. Д. Концепция управления готовностью критических инфраструктур на основе применения облачных информационных технологий // Системи та технології. 2016. № 1 (55). С. 5–23.

173. Minukhin S., Brynza N., Sitnikov D. Analyzing Performance of Apache Spark MLlib with Multinode Clusters on Azure HDInsight: Spark-Perf Case Study // Advances in Intelligent Systems and Computing. 2021. Vol. 1246. P. 114–134.

174. Minukhin S., Fedko V., Gnusov Y. Enhancing the performance of distributed big data processing systems using Hadoop and Polybase // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 4, no. 2 (94). P. 16–28.

175. Minukhin S., Novikov M., Brynza N., Sitnikov D. Experimental research of optimizing the Apache Spark tuning: RDD vs Data Frames. In: CMIS–2020 Computer Modeling and Intelligent Systems. Zaporizhzhia, Ukraine, 2020. P. 409–425.

176. Авария на Саяно-Шушенской ГЭС: шесть лет со дня катастрофы [Електронний ресурс]. URL : https://tass.ru/proisshestviya/1382685 (дата звернення 17.12.2020).

177. Итоговый доклад парламентской комиссии по расследованию обстоятельств, связанных с возникновением чрезвычайной ситуации техногенного характера на Саяно-Шушенской ГЭС 17 августа 2009 года [Електронний ресурс].
URL : http://council.gov.ru/media/files/41d44f243eed7779e852.pdf (дата звернення

17.12.2020).

178. Modeling user-perceived reliability based on user behavior graphs / D. Wang, K. Trivedi // International Journal of Reliability, Quality and Safety Engineering. 2009. Vol. 16, no. 4. P. 303–329.

179. Шубинский И. Б. Структурная надежность информационных систем. Методы анализа. Москва : «Журнал Надежность», 2012. 216 с.

180. Including Software Aspects in Green IT: How to Create Awareness for Green Software Issues / E. Kern, A. Guldner, S. Naumann // Green IT Engineering Social, Business and Industrial Applications. Studies in Systems, Decision and Control. 2019. Vol. 171. P. 3–20. doi.org/10.1007/978-3-030-00253-4_1.

181. Trends in worldwide ICT electricity consumption from 2007 to 2012 / W. Van Heddeghem, S. Lambert, B. Lannoo, D. Colle, M. Pickavet, P. Demeester // Computer Communications. 2014. Vol. 50. P. 64–76.

182. Modeling and performance analysis of large scale IaaS clouds / R. Ghosh, F. Longo, V. Naik, K. Trivedi // Future generation computer systems. 2013. Vol. 29, no. 5. P. 1216–1234.

183. Як «хмари» можуть поставити «зеленій» енергетиці підніжку [Електронний ресурс]. URL : https://techtoday.in.ua/reviews/yak-hmary-mozhut-postavyty-zelenij-energetyczi-pidnizhku-128365.html (дата звернення 18.12.2020).

184. Иванченко О. В., Смоктий К. В., Харченко В. С., Блындюк И. В. Стохастическая модель надежности инфраструктуры как сервиса облачных вычислений // Вісник Академії митної служби України. 2014. № 2 (52). С. 50–68

185. Fourth Quarter 2017 SPECpower_ssj2008 Results [Electronic resource]. URL : http://www.spec.org/power_ ssj2008/results/res2017q4/ (date of request 20.12.2020).

186. On the Network Performance of Amazon S3 Cloud-Storage Service / V. Persico, A. Montieri, A. Pescapè // 2016 5th IEEE International Conference on Cloud Networking (Cloudnet), Pisa, October 3–5, 2016, Pisa, Italy. P. 113–118.

187. Іванченко О. В. Методологічні основи та засоби оцінювання і

моніторингу характеристик гарантоздатної хмарної інфраструктури критичних енергетичних систем // Актуальні проблеми економіки, управління та фінансів : матеріали Міжнар. наук.-практ. конф., м. Дніпро, 19 квіт. 2019 р. Дніпро, 2019. С. 329–330.

188. Characterizing Cloud-to-User Latency as Perceived by AWS and Azure Users Spread over the Globe / F. Palumbo, G. Aceto, A. Botta, D. Ciuonzo, V. Persico, A. Pescape // 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, December 9–13, 2019, Waikoloa, HI, USA. P. 1-6.

189. On the Performance of Cloud Services and Databases for Industrial IoT Scalable Applications [Electronic resource].
URL : https://search.proquest.com/openview/3ff5ac101c4373a49883649589edb477/1?pq-origsite=gscholar&cbl=2032404 (date of request 10.01.2021).

190. DISTIL: Design and implementation of a scalable synchrophasor data processing system / M. Andersen, S. Kumar, C. Brooks, A. von Meier, D. Culler // 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, November 2–5, 2015, Miami, USA. P. 271–277.

191. Low-cost implementation and characterization of an active phasor data concentrator / P. Castello, C. Muscas, P. Pegoraro, S. Sulis //ACTA IMEKO. 2019. Vol. 8, no. 2. P. 21–27.

192. Precision Micro-Synchrophasors for Distribution Systems: A Summary of Applications / A. von Meier, E. Stewart, A. McEachern, M. Andersen, L. Mehrmanesh // IEEE Transactions on Smart Grid. 2017. Vol. 8, no. 6. P. 2926–2936.

193. A MATLAB-based PMU simulator / D. Dotta, J. Chow, L. Vanfretti, M. Almas, M. Agostini // 2013 IEEE Power & Energy Society General Meeting, Vancouver, July 21–25, 2013, Vancouver, Canada. P. 1–5.

194. ДСТУ 3592–97. Сигнали радіотехнінчі вимірювальні. Терміни та визначення. Київ, 1997. 23 с.

195. Development of DFT based MATLAB and LABVIEW Models for Phasor Measurements / A. Jain, M. Verma // International Journal of Information and Electronics

Engineering. 2016. Vol. 6, no. 6. P. 331–336.

196. Иванченко О. В., Кривонос М. В., Бирюков Д. Ю. Математическая модель цифрового средства измерения с двухзвенным аналого-цифровым преобразователем последовательных приближений // Вісник СевНТУ. Серія «Інформатика, електроніка, зв’язок». 2011. Вип. 114. С. 90–94.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. Иванченко О. В. Модели надёжности и живучести энергетических систем. Принципы и модели управления критической энергетической инфраструктурой по техническому мегасостоянию // Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : кол. монографія / Харків : Нац. аэрокосм. ун-т “Харьк. авиац. ин-т”, 2011. С. 311–336.

2. Иванченко О. В. Аналитико-стохастические модели надёжности и безопасности критических энергетических инфраструктур // Информационные технологии для критических инфраструктур : кол. монографія Севастополь : Севастопольський національний техн. ун-т, 2012. С. 89–124.

Наукові праці, в яких опубліковані основні наукові результати дисертації:

3. Иванченко О. В. Полумарковские модели мониторинга информационно-технического состояния критических инфраструктур // Радіоелектронні і комп’ютерні системи. 2012. № 7 (59). С. 219–224.

4. Іванченко О. В. Аналітико-стохастичний метод побудови структурних схем безпеки кібернетичних активів системи SCADA критичної інфраструктури // Системи та технології. 2019. № 1 (57). С. 81–106.

5. Іванченко О. В. Оцінювання рівня безпеки системи SCADA критичної інфраструктури з урахуванням доступності кібернетичних та хмарних активів // Системи та технології. 2019. № 2 (58). С. 5–32.

6. Іванченко О. В. Аналітико-стохастична модель гарантоздатності кібернетичних та хмарних активів системи SCADA критичної інфраструктури // Системи та технології. 2020. № 1 (59). С. 14–59.

7. Яцек Я. Ф., Иванченко О. В., Войтюк А. В., Степанов В. А. Комплексный подход к управлению критическими инфраструктурами по техническому

мегасостоянию // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. Севастополь, 2010. Вип. 4 (4). С. 91–99 *(Особистий внесок здобувача: розроблено двохрівневі моделі управління готовністю критичних інфраструктур за технічним мегастаном)*.

8. Иванченко О. В., Харченко В. С., Одарущенко О. Н. Принципы анализа и управления безопасностью критических инфраструктур // Вісник Хмельницького національного університету. 2010. № 5 (170). С. 218–221 *(Особистий внесок здобувача: сформульовано окремі принципи аналізу безпеки критичних інфраструктур)*.

9. Мащенко Е. Н., Иванченко О. В., Смахашева Н. В. Аналитико-стохастическая модель управления техническим состоянием изделий критического применения // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 30–34 *(Особистий внесок здобувача: запропоновано концепцію управління технічним станом виробів критичного призначення)*.

10. Иванченко О. В., Харченко В. С., Бирюков Д. Ю. Полумарковская модель протекания аварии критической инфраструктуры // Радіоелектронні і комп'ютерні системи. 2013. № 5 (64). С. 45–51 *(Особистий внесок здобувача: побудовано та виконано обчислення напівмарковської моделі протікання аварії критичної енергетичної інфраструктури)*.

11. Иванченко О. В., Харченко В. С. Метод причинно-следственной декомпозиции аварий и инцидентов критических инфраструктур // Радіоелектронні і комп'ютерні системи. 2014. № 5 (69). С. 12–17 *(Особистий внесок здобувача: розроблено основні положення методу причинно-наслідкової декомпозиції та виконано аналітико-стохастичне моделювання аварії критичної енергетичної інфраструктури)*.

12. Иванченко О. В., Ловягин В. С. Техническое обслуживание компонентной составляющей критических инфраструктур // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. 2011. Вип. 1 (5). С. 253–259 *(Особистий внесок здобувача: сформульовано окремі положення концепції*

технічного обслуговування компонентної складової критичної інфраструктури за станом).

13. Иванченко О. В., Бочарова В. В., Владимирова Е. С., Фомина А. Б. Модели надёжности и безопасности критических инфраструктур // Севастополь. Академія Військово-Морських Сил імені П. С. Нахімова : зб. наук. пр. 2011. Вип. 4 (8). С. 109–119 *(Особистий внесок здобувача: виконано аналіз властивостей, що визначають якість застосування критичної енергетичної інфраструктури за призначенням; розроблено причинно-наслідкову модель протікання аварії критичної енергетичної інфраструктури)*.

14. Иванченко О. В., Бочарова В. В. Обоснование предельных величин показателей надёжности критических энергетических инфраструктур // Радіоелектронні і комп'ютерні системи. 2012. № 5 (57). С. 197–201*(Особистий внесок здобувача: розроблено марковську модель протікання аварії та визначено граничні величини показників надійності критичної енергетичної інфраструктури)*.

15. Иванченко О. В., Солдатенко Е. С., Владимирова Е. С. Архитектурный подход к оценке надежности программного обеспечения системы управления критической инфраструктуры // Системи обробки інформації. 2014. № 1 (117). С. 173–179 *(Особистий внесок здобувача: виконано оцінювання рівня надійності системи управління інфраструктурою з урахуванням безвідмвності програмного забезпечення критичного додатку)*.

16. Иванченко О. В., Харченко В. С. Полумарковская модель готовности облачной инфраструктуры с интегрированной системой мониторинга технического состояния // Радіоелектронні і комп'ютерні системи. 2016. № 5 (79). С. 15–19 *(Особистий внесок здобувача: побудовано та обчислено напівмарковську модель готовності хмарної інфраструктури з контролем технічного стану фізичних машин)*.

17. Иванченко О. В., Харченко В. С. Анализ стохастических методов метамоделирования и оценивания готовности облачных инфраструктур // Радіоелектронні і комп'ютерні системи. 2016. № 6 (80). С. 6–11 *(Особистий внесок*

здобувача: розроблено концептуальні положення щодо побудови та обчислення метамоделі готовності хмарної інфраструктури).

18. Иванченко О. В., Смоктий К. В., Харченко В. С., Блындюк И. В. Стохастическая модель надежности инфраструктуры как сервиса облачных вычислений // Вісник Академії митної служби України. 2014. № 2 (52). С. 50–68 *(Особистий внесок здобувача: побудовано та обчислено напівмарковську модель готовності хмарної інфраструктури з трьома підсистемами фізичних машин)*.

19. Иванченко О. В., Буланый А. П., Прокопенко Р. А. Обобщенный критерий управления конфигурацией инфраструктуры как сервиса облачных вычислений // Вісник Академії митної служби України. 2015. № 1 (53). С. 43–55 *(Особистий внесок здобувача: розроблено таксономічну схему управління конфігурацією хмарної інфраструктури)*.

20. Иванченко О. В., Кривонос М. В., Бирюков Д. Ю. Математическая модель цифрового средства измерения с двухзвенным аналого-цифровым преобразователем последовательных приближений // Вісник СевНТУ. Серія «Інформатика, електроніка, зв'язок». 2011. Вип. 114. С. 90–94 *(Особистий внесок здобувача: побудовано математичну модель цифрового засобу вимірювання з двохланцюговим аналого-цифровим пристроєм послідовного приближення)*.

21. Гаршин А. Ю., Иванченко О. В., Мащенко Е. Н. Методика оценки уровня опасности морской критической инфраструктуры // Системи озброєння і військова техніка. 2010. № 3 (23). С. 107–109 *(Особистий внесок здобувача: запропоновано визначення морської критичної інфраструктури)*.

Наукові праці, в яких опубліковані основні наукові результати дисертації у зарубіжних спеціалізованих виданнях:

22. Ivanchenko O., Kharchenko V., Moroz B., Kabak L. , Blindyuk I., Smoktii K. Semi-Markov Availability Model for Infrastructure as a Service Cloud Considering Energy Performance // Green IT Engineering: Social, Business and Industrial

Applications. Studies in Systems, Decision and Control. 2019. Vol. 171. P. 141–159. (***Scopus***) *(Особистий внесок здобувача: побудувано та обчислено стохастичну модель енергоефективності хмарної інфраструктури з трьома підсистемами фізичних та віртуальних машин).*

23. Ivanchenko O., Kharchenko V., Skatkov A. Management of critical infrastructures based on technical megastate // An International Journal. Information and Security. 2012. Vol. 28, no. 1. P. 37–51 *(Особистий внесок здобувача: сформульовано концепцію управління критичними інфраструктурами за технічним мегастаном).*

Наукові праці, які засвідчують апробацію матеріалів дисертації:

24. Semi-Markov availability model of an infrastructure as a service cloud with multiple pools / O. Ivanchenko, V. Kharchenko // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 12th Intern. Conf., June 21–24, Kyiv, 2016. Vol. 1614. P. 349–360 (***Scopus***) *(Особистий внесок здобувача: сформульовано принципи реконфігурування, надлишковості сервіс-орієнтованих ресурсів).*

25. Semi-Markov availability model for infrastructure as a service cloud considering hidden failures of physical machines / O. Ivanchenko, V. Kharchenko, Y. Ponochovnyi, I. Blindyuk, K. Smoktii // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 13th Intern. Conf., May 15–18, Kyiv, 2017. Vol. 1844. P. 634–644 (***Scopus***) *(Особистий внесок здобувача: сформульовано принципи оперативного моніторингу інформаційно-технічних станів хмарних систем).*

26. Availability as a cloud service for control system of critical energy infrastructure / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii, Y. Ponochovnyi // ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : Proc. of the 14th Intern. Conf., May 14–17, Kyiv, 2018. Vol. 2104. P. 571–582 (***Scopus***) *(Особистий внесок здобувача:*

сформульовано принципи побудови хмарної платформи для оцінки рівня готовності критичної енергетичної інфраструктури).

27. Risk assessment of critical energy infrastructure considering physical and cyber assets: Methodology and models / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, S. Konovalenko // 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) : Proc. of the 4th Intern. Symp., September 20 –21, Lviv, 2018. P. 225–228 (***Web of Science***) *(Особистий внесок здобувача: отримано оцінку ризику негативного впливу на фізичні та кібернетичні активи критичної енергетичної інфраструктури).*

28. Semi-Markov availability model considering deliberate malicious impacts on an Infrastructure-as-a-Service Cloud / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii // 2018 IEEE 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) : Proc. of the 14th Intern. Conf., February 20–24, Lviv–Slavske, 2018. P. 570–573 (***Web of Science***) *(Особистий внесок здобувача: побудовано та обчислено модель готовності хмарної інфраструктури з урахуванням зловмисного шкідливого впливу).*

29. Semi-Markov's models for availability assessment of an Infrastructure as a Service Cloud with multiple pools of physical and virtual machines / O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) : Proc. of the 14th Intern. Conf., May 24–27, Kyiv, 2018. P. 98–102 ***(Scopus)*** *(Особистий внесок здобувача: побудовано та обчислено модель готовності хмарної інфраструктури з декількома підсистемами фізичних та віртуальних машин).*

30. Dependability Assessment for SCADA System Considering Usage of Cloud Resources / O. Ivanchenko, V. Kharchenko, E. Brezhnev, Y. Ponochovnyi, B. Moroz, L. Kabak // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT) : Proc. of the 11th Intern. Conf., May 14–18, Kyiv, 2020.

P. 13–17 (***Scopus***) *(Особистий внесок здобувача: виконано оцінювання рівня гарантоздатності системи диспетчерського контролю та збору даних)*.

31. Харченко В. С., Иванченко О. В., Мащенко Е. Н. Методология FMECA: новая парадигма анализа видов и последствий отказов критических инфраструктур // Автоматизація: проблеми, ідеї, рішення : матеріали Міжнар. наук.-техн. конф., 6–10 верес. 2010 р. Севастополь, 2010. С. 142–145 Принципи аналізу та управління безпекою критичної енергетичної інфраструктури *(Особистий внесок здобувача: сформульовано принцип компліментарності побудови критичних інфраструктур)*.

32. Скатков А. В., Иванченко О. В. Цикломатическая сложность моделей компонентов критических инфраструктур // Інформаційні технології та інформаційна безпека в науці, техніці та навчанні : ІНФОТЕХ–2011 : матеріали Міжнар. наук.-практ. конф., 5–10 верес. 2011 р. Севастополь, 2011. С. 102–103 *(Особистий внесок здобувача: введено визначення цикломатичної складності для моделей функціонування компонентів критичних інфраструктур цикломатичної складності для моделей функціонування компонентів критичних інфраструктур)*.

33. Иванченко О. В., Харченко В. С. Причинно-следственная декомпозиция аварий и инцидентов критических инфраструктур // Проблемы критических ситуаций в точной механике и управлении : материалы Всерос. научн. конф. с междунар. участием, 25–27 сент. 2013 г. Саратов, 2013. С. 59–63 *(Особистий внесок здобувача: сформульовано принцип побудови причинно-наслідкового комплексу протікання аварії критичної енергетичної інфраструктури)*.

34. Іванченко О. В. Методологічні основи та засоби оцінювання і моніторингу характеристик гарантоздатної хмарної інфраструктури критичних енергетичних систем // Актуальні проблеми економіки, управління та фінансів : матеріали Міжнар. наук.-практ. конф., 19 квіт. 2019 р. Дніпро, 2019. С. 329–330.

35. Іванченко О. В. Аналітико-стохастична модель готовності системи SCADA критичної інфраструктури // 20th International Scientific and Practical Conference on

Perspective Directions for the Development of Science and Practice : Proc. of the 20th Intern. Conf., Athens, June 8–9, 2020, Athens, Greece. P. 166–170.

36. Іванченко О. В. Аналітико-стохастична модель зловмисного шкідливого впливу на кібернетичні активи системи SCADA критичної інфраструктури // 21st International Scientific and Practical Conference on Current Trends in the Development of Science and Practice : Proc. of the 21st Intern. and Pract. Conf., Haifa, 15–16 June, 2020, Haifa, Israel. P. 125–130.

37. Іванченко О. В. Теоретико-множинна модель кібератаки системи корпоративного управління // Математичні проблеми технічної механіки та прикладної математики : матеріали Міжнар. наук. конф., 2–5 груд. 2019 р. Дніпро : Університет митної справи та фінансів. Дніпро–Кам'янське, 2019. С. 65–66.

Наукові праці, які додатково відображають наукові результати дисертації:

38. Иванченко О. В., Каряка А. В., Маврин С. А., Филимонов И. Л. Оценка уровня надёжности телекоммуникационных систем морских подвижных объектов для их технического обслуживания по состоянию // Радіоелектронні і комп'ютерні системи. 2008. Вип. 6 (33). С. 128–133 *(Особистий внесок здобувача: побудовано та обчислено моделі надійності морських рухомих об'єктів критичної інфраструктури для їхнього технічного обслуговування за станом)*.

39. Иванченко О. В., Паткаускас А. В., Маврин С. А., Корощенко Н. Н. Обобщённый критерий синтеза адаптивной системы технического диагностирования сложных промышленных объектов // Радіоелектронні і комп'ютерні системи. 2009. № 7 (41). С. 127–135 *(Особистий внесок здобувача: сформульовано критерій синтезу системи технічного діагностування критично важливих об'єктів)*.

40. Иванченко О. В., Харченко В. С., Смоктий К. В., Смоктий О. Д. Концепция управления готовностью критических инфраструктур на основе применения облачных информационных технологий // Системи та технології. 2016. № 1 (55).

С. 5–23 *(Особистий внесок здобувача: сформульовано концепцію та розроблено критерій управління готовністю критичних інфраструктур на основі застосування хмарних систем)*.

41. Смоктий О. Д., Смоктий К. В., Иванченко О. В. Анализ механизма и последствий воздействия DDoS-атак на эталонную модель взаимодействия открытых систем OSI // Системи управління, навігації та зв’язку. 2017. № 1 (41). С. 33–37 *(Особистий внесок здобувача: виконано аналіз механізму впливу DDoS-атак на програмне забезпечення критичних інфраструктур)*.

ДОДАТОК Б

АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ

ЗАТВЕРДЖУЮ
Директор СКТБ
Інститута технічної механіки
Національної академії наук України
член.-кореспондент НАН України
доктор технічних наук, професор
А,П.Алпатов
"11" 07 2020 р.

АКТ ВПРОВАДЖЕННЯ
наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему "Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур", виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови – начальника відділу СКТБ Компанійця В.І., та членів комісії с.н.с., ІТМ, к.т.н., Фокова О.А.,наук.співробітника ІТМ, к.т.н. Палія О.С., провідного інженера ІТМ Авдєєва А.М.., встановила, що результати наукових досліджень к.т.н., доцента Іванченка О.В., а саме: метод оцінювання функційної безпечності критичної інфраструктури за рахунок використання процедур аналітико-стохастичного моделювання та причинно-наслідкового аналізу ризиків з урахуванням негативного впливу на фізичні та кібернетичні активи а також метод моделювання та оцінювання готовності критичної інфраструктури, які враховують еволюційні аспекти управління реалізацією відповідних систем за інформаційно-технічним станом та базуються на аналітико-стохастичному оцінюванні сервіс-орієнтованих хмарних ресурсів в контурі управління та дозволяють підвищити точність оцінки наслідків аварій були використані у процесі розробки техніко-економічного обгрунтування космічної програми України щодо оцінювання ризику окремих її компонентів у процесі реалізації комплексу заходів по забезпеченню її функційної надійності.

Впровадження результатів дисертаційного дослідження дозволило зробити оцінки критичних ризиків реалізації компонентів Програми відповідно рівню їх негативного впливу на можливості надійної реалізації урядової концепції Космічної програми України.

Голова комісії Компанієць В.І.
Члени комісії Фоков О.А.
Палій О.С.
Авдєєв А.М.

ЗАТВЕРДЖУЮ

Генеральний директор ТОВ "РІТ"

Каменський Сергій Олександрович

м. Харків, 10.09.2020р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему "Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур", виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови – *генерального директора Каменського С.О.* та членів – *начальника виробництва Потапенко О.В., керівника відділу розробки ПЗ Коваля В.П.* встановила, що отримані Іванченком О.В. наукові результати, а саме:

1) метод оцінки енергоефективності хмарної інфраструктури з інтегрованою системою оперативного моніторингу інформаційно-технічних станів фізичних та віртуальних машин;

2) інформаційна технологія тестування хмарних систем критичної інфраструктури з інтегрованими фізичними компонентами на основі застосування віртуального ресурсу реляційних баз даних,

були використані при оцінюванні продуктивності функціонування інформаційних центрів хмарних провайдерів, а саме:

– під час проектування резервного контуру управління критичної інфраструктури з застосуванням симулятора інформаційного потоку даних від системи синхронізованих векторних вимірювань;

– для оцінки швидкодії інфокомунікаційних каналів хмарного забезпечення динамічної системи моніторингу технічних параметрів та інформаційно-технічних станів компонентів критичної інфраструктури.

Впровадження результатів дисертаційного дослідження зумовило:

– підвищення точності аналітико-стохастичного оцінювання показників готовності компонентів критичної інфраструктури (на 8%) за рахунок збільшення обсягів інформації, яка обробляється за допомогою хмарних сервісів, що значно розширило функціональність системи синхронізованих векторних вимірювань та знизило вартість її підсистеми обробки даних з урахуванням витрат на енергоспоживання;

– підвищення точності оцінювання швидкодії (на 5%) сервіс-орієнтованих ресурсів інформаційного забезпечення перспективної динамічної системи моніторингу технічних параметрів та інформаційно-технічних станів компонентів критичної інфраструктури, яка застосовується в резервному контурі управління інфраструктурою.

Голова комісії _____ / Каменський С.О.

Члени комісії _____ / Потапенко О.В

_____ / Коваль В.П.

Україна
Товариство з обмеженою відповідальністю
«Радіо Інформаційні Технології»
№31641603
Місто Харків

ЗАТВЕРДЖУЮ
Виконавчий директор
АТ «Інститут інформаційних технологій»
В. Д. Кравченко
"21" жовтня 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему "Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур", виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови – головного конструктора АТ «Інститут інформаційних технологій» доктора технічних наук професора Горбенка І. Д. та членів комісії – начальника відділу к.т.н. Бобуха В. А., наукового співробітника к.т.н. Єсіна М.В. встановила, що отримані Іванченком О. В. наукові результати, а саме:

1) метод компаративістичного аналізу аварій критичної інфраструктури, який базується на застосуванні модифікованої алгебри причинно-наслідкових комплексів, їхньому логіко-цифровому представленні та агрегатуванні у вигляді структурно-логічних схем і аналітико-стохастичних моделей протікання аварій, що дозволяє оцінювати і формулювати рекомендації щодо зменшення їх ризиків;

2) метод моделювання та оцінювання готовності критичної інфраструктури, який враховує еволюційні аспекти її управління за інформаційно-технічним станом, базується на аналітико-стохастичному оцінюванні сервіс-орієнтованих хмарних ресурсів в контурі управління та дозволяє підвищити точність оцінки наслідків аварій інфраструктури,

були використані для оцінювання ризиків критично важливих об'єктів підприємства, а саме:

– під час розробки основних положень методики категоризації критично важливих об'єктів за рівнем ризику негативного впливу на них в процесі виконання НДР «Гармонія»;

– для виконання категоризації та паспортизації критично важливих об'єктів за рівнем ризику негативного впливу в процесі виконання НДР «Гармонія»;

Впровадження результатів дисертаційного дослідження дозволило:

– систематизувати інформацію щодо загроз, вразливостей для кібернетичних активів критично важливих об'єктів та можливих сценаріїв атаки на них.

Голова комісії І. Д. Горбенко

Члени комісії В. А. Бобух
М. В. Єсіна

ЗАТВЕРДЖУЮ

Генеральний директор
ПАТ «НВП «Радій»»
кандидат технічних наук,
Лауреат Державної премії
України в галузі науки та
техніки

О.А. Сіора

«29» 09 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему "Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур", виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови комісії – генерального конструктора ПАТ «НВП "Радій"» кандидата технічних наук Токарєва В.І. та членів комісії начальників відділів конструкторського бюро АСУ ТП кандидатів технічних наук Головира В.О., Бєлого Ю.О. встановила, що результати наукових досліджень к.т.н., доцента Іванченка О.В., а саме:

– метод оцінювання функційної безпечності критичної енергетичної інфраструктури з урахуванням негативних впливів на її фізичні та кібернетичні активи;

– аналітико-стохастичні моделі гарантоздатності кібернетичних та хмарних активів критичної енергетичної інфраструктури;

– напівмарковська модель моніторингу інформаційно-технічних станів компонентів критичної енергетичної інфраструктури;

– напівмарковська модель протікання аварії критичної енергетичної інфраструктури з системою контролю інформаційно-технічних станів її компонентних складових;

– метод причинно-наслідкової декомпозиції та компаративістики аварій критичної енергетичної інфраструктури;

– метод моделювання та оцінки готовності критичної енергетичної інфраструктури, який враховує еволюційні аспекти її управління за технічним мегастаном з застосуванням додаткових хмарних сервісів,

було використано для розробки процедури оцінювання ризику систем критичної енергетичної інфраструктури, що розширює можливості реалізації відповідних організаційно-технічних заходів по забезпеченню функційної безпечності інфраструктури.

Впровадження результатів дисертаційного дослідження дозволило перейти до створення технології для категорування систем критичної енергетичної інфраструктури за рівнем ризику негативного впливу на її активи і забезпечити розв'язування однієї з найважливіших науково-технічних задач згідно урядової концепції по створенню державної системи захисту критичної інфраструктури.

Голова комісії Токарєв В.І.

Члени комісії Головир В.О.

Бєлий Ю.О.

ЗАТВЕРДЖУЮ

Директор

ТОВ «НВП «Радікс»

Андрашов А. О.

«16» 09 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему "Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур", виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови комісії – директора ТОВ «НВП «Радікс» Андрашова Антона Олександровича, членів комісії - провідного наукового співробітника к.т.н. доцента Одарущенка Олега Миколайовича, старшого наукового співробітника к.т.н. доцента Стрюка Олексія Юрійовича, наукового співробітника Божко Віктора Івановича встановила, що результати наукових досліджень к.т.н., доцента Іванченка Олега Васильовича, а саме:

– аналітико-стохастичний метод побудови структурних схем безпеки фізичних та кібернетичних активів критичної енергетичної інфраструктури;

– аналітико-стохастична модель ризику відмов фізичних та кібернетичних активів критичної енергетичної інфраструктури;

– метод вибору характеристик сервіс-орієнтованих ресурсів критичної енергетичної інфраструктури шляхом послідовної реалізації процедур аналітико-стохастичного моделювання процесів зміни рівня готовності хмарних компонентів;

– напівмарковська модель готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних машин;

– напівмарковська модель готовності хмарної інфраструктури з декількома підсистемами фізичних та віртуальних машин;

– метод оцінки енергоефективності хмарної інфраструктури шляхом аналітико-стохастичного оцінювання споживаної потужності за результатами напівмарковського моделювання процесів зміни рівня готовності інтегрованих фізичних та віртуальних компонентів,

було використано в процесі розробки нормативних документів по оцінюванню рівня готовності та функційної безпечності критичної енергетичної інфраструктури; при виконанні ризик-аналізу міні платформи для розумних енергетичних мереж та тестового стенду для перевірки параметрів енергозабезпечення підприємства.

Впровадження результатів дисертаційного дослідження сприяло відпрацюванню комплексу заходів щодо реалізації процедур аварійного відновлення та резервного копіювання інформаційних ресурсів, які є важливими для безпеки компонентів критичної енергетичної інфраструктури.

Голова комісії А.О. Андрашов

Члени комісії О.М. Одарущенко

О.Ю. Стрюк

В.І. Божко

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» д.т.н., професор

_____ В.М. Павленко

"3" грудня 2019 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему "Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур", виконаної на здобуття наукового ступеня доктора технічних наук, в навчальному процесі та при виконанні міжнародних проектів

Комісія у складі голови – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій, к.т.н. Одокієнка О.В., членів – к.т.н., доцента Боярчука А.В., к.т.н., доцента Ілляшенка О.О., встановила, що результати наукових досліджень Іванченка Олега Васильовича, а саме:

– метод компаративістичного аналізу аварій критичної енергетичної інфраструктури з застосуванням алгебри причинно-наслідкових комплексів та їхнього логіко-цифрового представлення;

– метод моделювання та оцінки готовності критичної інфраструктури (КІ), який враховує еволюційні аспекти її управління по технічному мегастану та етапи аналітико-стохастичного оцінювання готовності сервіс-орієнтованих хмарних ресурсів, що використовуються в контурі управління КІ;

– метод оцінки енергоефективності хмарної інфраструктури шляхом аналітико-стохастичного оцінювання споживаної потужності за результатами напівмарковського моделювання процесів зміни рівня готовності інтегрованих фізичних та віртуальних машин;

– напівмарковські моделі готовності хмарної інфраструктури з інтегрованою системою моніторингу інформаційно-технічних станів фізичних та віртуальних машин,

реалізовані в навчальному процесі та в роботах, що пов'язані з міжнародною співпрацею Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» у вигляді:

1) лекцій та практичних занять з методів оцінювання та забезпечення готовності хмарних систем критичних інфраструктур у навчальних дисциплінах «Надійність та відмовостійкість комп'ютерних систем», «Інженерія програмного забезпечення. Частина друга», «Теорія та технології критичного комп'ютингу»;

2) матеріалів проектів за програмами Європейського Союзу TEMPUS:

– SAFEGUARD 158886-TEMPUS-1-2009-1-UK-TEMPUS-JPCR «Національна мережа центрів інноваційної університетсько-індустріальної кооперації з інженерії безпеки» (2010-2013 рр.), зокрема, навчально-методичного забезпечення курсу «Розподілені критичні системи та інфраструктури»;

– TEMPUS-GREENCO (Green Computing and Communication) 530270-TEMPUS-1-2012-UK-TEMPUS-JPCR (2012-2015 рр.), зокрема, навчально-методичного забезпечення курсу «Основи зеленої IT-інженерії. Моделювання хмарних систем»;

– TEMPUS-SEREIN (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains) 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR (2013-2016 рр.), зокрема, навчально-методичного забезпечення курсу «Безпечний та резіл'єнтний комп'ютинг в гуманітарній та промисловій сферах. Частина перша. Основи безпечного та резіл'єнтного комп'ютингу».

Встановлено, що отримані результати наукових досліджень дозволили підвищити фундаментальність, наочність та практичну спрямованість навчального процесу; сприяли покращенню міжнародних зв'язків університету у галузі підготовки фахівців і міжнародного наукового співробітництва та якості виконання проектів.

Голова комісії О.В. Одокієнко

Члени комісії А.В. Боярчук

О.О. Ілляшенко

"3" грудня 2019 р.

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного аерокосмічного
університету ім. М.Є. Жуковського
«Харківський авіаційний інститут»
д.т.н., с.н.с.

_____ В.В. Павліков
“ 13 ” грудня 2019 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Іванченка Олега Васильовича на тему “Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур”, виконаної на здобуття наукового ступеня доктора технічних наук, в наукових проектах унииверситету

Комісія у складі голови – декана факультету радіоелектроніки, комп’ютерних систем та інфокомунікацій, к.т.н. Одокієнка О.В., членів – к.т.н., професора Фурманова К.К., к.т.н., професора Орєхова О.О., встановила, що результати наукових досліджень Іванченка Олега Васильовича, а саме:

1) методи оцінювання та вибору характеристик хмарних систем критичних інфраструктур в умовах негативних впливів;

2) метод оцінки готовності хмарної інфраструктури на основі застосування програмного інструментарію напівмарковського моделювання та стохастичної оцінки за результатами моніторингу її інформаційно-технічних станів та обсягів енергоспоживання;

3) моделі готовності хмарної інфраструктури з декількома підсистемами фізичних машин та інтегрованою системою моніторингу інформаційно-технічних станів,

реалізовані у вигляді науково-теоретичних положень у наукових проектах, які виконувалися за держзамовленням:

– Методологічні засади та технології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ» ДР №0119U100979, 2019-2021рр.);

– Методологія сталого розвитку та інформаційні технології зеленого комп’ютингну та комунікацій (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ» ДР № 0118U003822, 2018-2020рр.);

– Наукові основи, методи та засоби зеленого комп'ютингу та комунікацій (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ» ДР № 0115U000996, 2015-2017рр.).

Практичне значення результатів дослідження, отриманих автором при виконання проектів, полягає в тому, що вони:

– дозволяють підвищити повноту оцінки готовності (доступності) хмарної інфраструктури з декількома підсистемами фізичних машин, яка застосовується в контурі управління критичних інфраструктур;

– забезпечують зменшення енергоспоживання хмарної інфраструктури при забезпеченні вимог до готовності;

– є основою щодо створення гарантоздатних сервіс-орієнтованих хмарних технологій, які можуть бути застосовані для розширення функціональності та динамічного діапазону в сучасних інформаційно-управляючих системах критичних інфраструктур.

Голова комісії О.В. Одокієнко

Члени комісії К.К. Фурманов

Є.О. Орєхов

"15" грудня 2019 р.

ДОДАТОК В

МОДЕЛЬ ГОТОВНОСТІ ХМАРНОЇ ІНФРАСТРУКТУРИ З ТРЬОМА ФІЗИЧНИМИ МАШИНАМИ

$$K_{\Gamma}(t) = \pi_0(t) + \pi_2(t) + \pi_3(t) + \pi_5(t), \tag{В.1}$$

$$\pi_0(t) = P_0 \frac{\overline{t_0}}{U},\ \pi_2(t) = P_2 \frac{\overline{t_2}}{U},\ \pi_3(t) = P_3 \frac{\overline{t_3}}{U}, \tag{В.2}$$

$$\pi_5(t) = P_5 \frac{\overline{t_5}}{U},\quad U = \sum_{i=0}^{7} P_i \bar{t}_i, \tag{В.3}$$

$$P_0 = P_1 = \frac{\alpha\beta}{2\alpha\beta + \xi_1 + \xi_2 + \xi_3[\beta + \eta]}, \tag{В.4}$$

$$P_2 = P_0 \frac{\xi_1}{\alpha\beta},\ P_3 = P_0 \frac{\xi_2}{\alpha\beta},\ P_4 = P_0 \frac{\xi_3}{\alpha\beta}, \tag{В.5}$$

$$P_5 = P_0 \frac{p_{20}\xi_3}{\alpha\beta},\ P_6 = P_0 \frac{p_{45}p_{56}\xi_3}{\alpha\beta},\ P_7 = 1 - \sum_{i=0}^{6} \pi_i, \tag{В.6}$$

де

$$\beta = 1 - p_{56}(p_{65} + p_{67}),\ \alpha = \beta(1 - p_{24}p_{42}) - p_{34}(p_{43} + p_{45}p_{53}) - p_{24}p_{45}p_{52},$$

$$\xi_3 = p_{13}p_{34} + p_{12}p_{24}\beta,\ \xi_2 = p_{45}p_{53}\xi_3 + \beta(\alpha p_{13} + p_{43}\xi_3),\ \xi_1 = \beta(\alpha p_{12} + p_{42}\xi_3) + p_{45}p_{52}\xi_3,$$

$$\eta = p_{20}(1 + p_{56}(1 + p_{67})),\ p_{10} = e^{-2\gamma\tau_c},\ p_{42} = p_{43} = p_{65} = e^{-\lambda\tau_c},$$

$$p_{12} = \frac{1}{2}\left(1 - e^{-2\gamma T}\right),\ p_{13} = 1 - p_{10} - p_{12},\ p_{24} = p_{34} = (1 + \mu_1 T)e^{-\mu_1 T},$$

$$p_{20} = p_{30} = 1 - p_{24},\ p_{45} = 1 - p_{42} - p_{43},\ p_{52} = \frac{1}{2}\left[1 - \left(1 + \mu_2^2 T^2 + 2\mu_2 T\right)e^{-2\mu_2 T}\right],$$

$$p_{56} = \left[(1 + \mu_2 T)e^{-\mu_2 T}\right]^2,\ p_{67} = 1 - p_{65},\ p_{53} = 1 - p_{52} - p_{56},$$

$$\bar{t}_0 = T,\ \bar{t}_1 = \frac{1}{2\gamma}\left(1 - e^{-2\gamma\tau_c}\right),\ \bar{t}_2 = \bar{t}_3 = \bar{t}_7 = \frac{2}{\mu_1},\ \bar{t}_4 = \bar{t}_6 = \frac{1}{\gamma}\left(1 - e^{-\gamma\tau_c}\right),$$

$$\bar{t}_{51} = 1 - e^{-2\mu_2 T},\ \bar{t}_{52} = 1 - (1 + 2\mu_2 T)e^{-2\mu_2 T},\ \bar{t}_{53} = \frac{1 - \left[1 + 2\mu_2 T(1 + T)\right]e^{-2\mu_2 T}}{2},$$

$$\bar{t}_5 = \frac{1}{2\mu_2}\left(\bar{t}_{51} + \bar{t}_{52} + \bar{t}_{53}\right).$$

ДОДАТОК Г

МОДЕЛЬ ГОТОВНОСТІ ХМАРНОЇ ІНФРАСТРУКТУРИ З ТРЬОМА ПІДСИСТЕМА ФІЗИЧНИХ ТА ВІРТУАЛЬНИХ МАШИН І КОНТРОЛЕМ ІНФОРМАЦІЙНО-ТЕХНІЧНИХ СТАНІВ

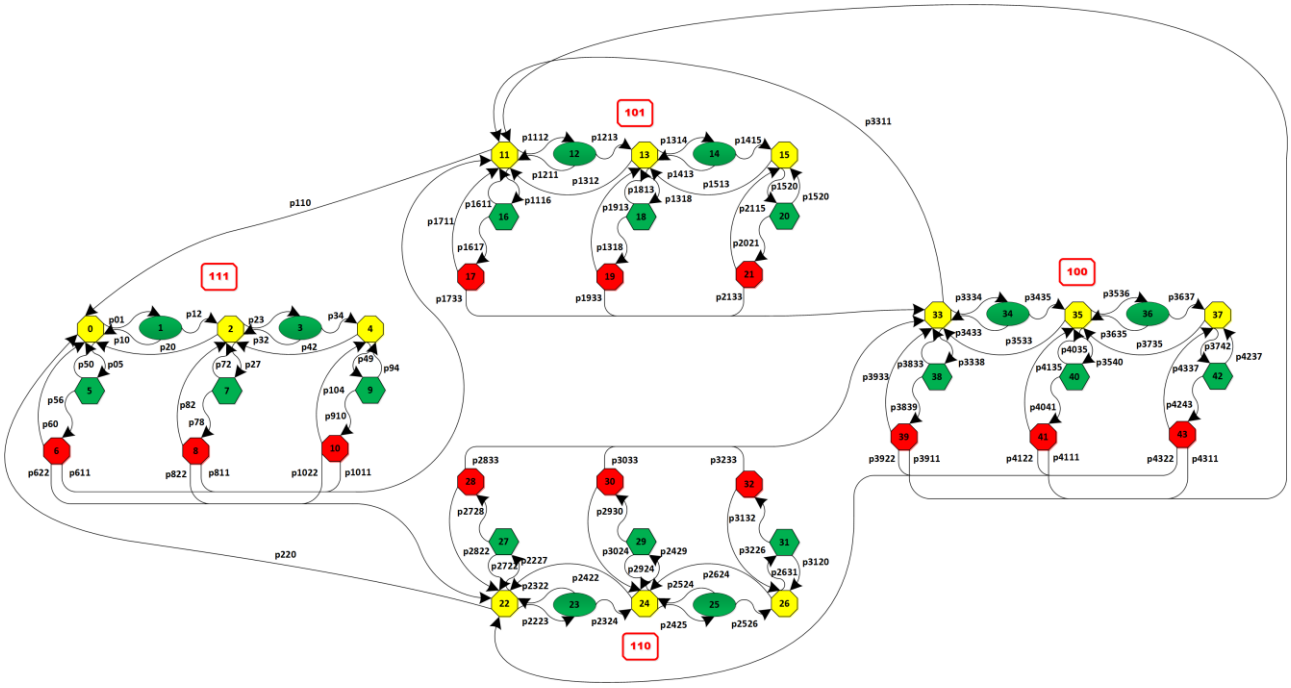


Рис. Г.1 Граф станів НПММ готовності ХМІ з трьома підсистемами фізичних та віртуальних машин і контролем їхнього ІТС

Відповідно до рис. Г.1 інформаційно-технічні стани, в яких ХМІ перебуває в стані контроля ІТС, утворюють множину $S_{ктс} = \{S_1, S_3, S_5, S_7, S_9, S_{12}, S_{14}, S_{16}, S_{18}, S_{20}, S_{23}, S_{25}, S_{27}, S_{29}, S_{31}, S_{34}, S_{36}, S_{38}, S_{40}, S_{42}\}$ таку, що $\forall S_i \in S_{ктс}\ \exists\ S_i \longrightarrow S_j$, для яких

$$Q_{ij}(t) = \begin{cases} 0, t < T, \\ 1, t \geq T. \end{cases} \qquad (Г.1)$$

Відповідно $\forall S_j \in S_{ктс}\ \exists\ S_j \longrightarrow S_i$, для яких

$$Q_{ji}(t) = \begin{cases} 0, t < \tau_{ктс}, \\ 1, t \geq \tau_{ктс}. \end{cases} \qquad (Г.2)$$

В виразах (Е.1), (Е.2) складові означають Т – період проведення контроля ІТС, $\tau_{ктс}$ – тривалість проведення контроля ІТС фізичних та віртуальних машин.

Для станів, що утворюють множину $S_F = \{S_6, S_8, S_{10}, S_{17}, S_{19}, S_{21}, S_{28}, S_{30}, S_{32},$

$S_{39}, S_{41}, S_{43}\}$ $\forall S_j \in S_{ктс}\ \exists\ S_j \longrightarrow S_k$, $S_k \in S_F$ елементи матриці $\left|Q_{ij}(t)\right|$ можна записати як

$$Q_{jk}(t) = 1 - e^{-\lambda_k t} = \mathrm{Exp}(\lambda_k), \qquad (Г.3)$$

де λ_k – інтенсивність відмов ФМ або ВМ.

Для решти переходів $S_k \longrightarrow S_i$ елементи матриці $\left|Q_{ij}(t)\right|$ можна записати у вигляді

$$Q_{ki}(t) = 1 - (1 + \mu_k t)e^{-\mu_k t} = \mathrm{Erlang}(2, \mu_k), \qquad (Г.4)$$

де μ_k – інтенсивність відновлень працездатності ФМ або ВМ.

З урахуванням умови нормування $\sum_{i=0}^{43} \pi_i = 1$ стаціонарний коефіцієнт готовності обчислюється з застосуванням такого співвідношення:

$$K_{\Gamma_{IaaS}} = \pi_0 + \pi_2 + \pi_4 + \pi_{11} + \pi_{13} + \pi_{15} + \pi_{22} + \pi_{24} + +\pi_{26} + \pi_{33} + \pi_{35} + \pi_{37}. \qquad (Г.5)$$

Складові співвідношення (Г.5) обчислюються з застосуванням відомого апарату напівмарковського моделювання.

ДОДАТОК Д

АНАЛІЗ ЗЛОВМИСНИХ ШКІДЛИВИХ ВПЛИВІВ НА АКТИВИ СИСТЕМИ SCADA КЕІ

Таблиця Д.1

Аналіз наслідків ЗВШВ на активи системи SCADA КЕІ

Номер сценарію ЗВШВ	Вид ЗВШВ	Компоненти, на які направлена дія ЗВШВ	Наслідки ЗВШВ	Рівень успішності ЗВШВ
Перший	РЗІ	Програмовані логічні контролери (ПЛК), протиаварійне захисне обладнання (ПЗО), сенсорні модулі (ССРМ), людино-машинні інтерфейси (ЛМІ), які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу SCADA КІ	Отримання доступу до інформаційного ресурсу системи SCADA КІ	Високий
	ФСФ	Серверні (СРВС) та інфокомунікаційні системи (ІКС), контролери доменів (КНТД), комп’ютерні термінали (КМПТ) четвертого, п’ятого, шостого мережевих рівнів SCADA КІ	Викривлення даних контуру управління КІ з застосуванням інформаційного ресурсу системи SCADA КІ	
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів SCADA КІ	Компрометація системи, заміна вірогідних даних неправдивими, застосування зловмисниками кібернетичних активів SCADA для відключення компонентів КІ з блокуванням дій обслуговуючого персоналу	

Продовження таблиці Д.1

Номер сценарію ЗВШВ	Вид ЗВШВ	Компоненти, на які направлена дія ЗВШВ	Наслідки ЗВШВ	Рівень успішності ЗВШВ
Другий	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу SCADA КІ	Наслідки ЗВШВ оперативно усунуто за рахунок підключення ХМС (Amazon Web Services), створення додаткового резервного контуру у вигляді ХМА для всіх шести мережевих рівнів SCADA КІ та реалізації функцій аварійного відновлення (АВД) і резервного копіювання (РКП)	Низький
	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів SCADA КІ		
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів SCADA КІ		
Третій	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу, частково хмарні системи AWS (ХМА) SCADA КІ	Отримання доступу до інформаційного ресурсу та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	Середній
	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів SCADA КІ	Наслідки ЗВШВ усунено за рахунок застосування ХМА системи SCADA КІ та реалізації функцій АВД і РКП	
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів SCADA КІ		

Продовження таблиці Д.1

Номер сценарію ЗВШВ	Вид ЗВШВ	Компоненти, на які направлена дія ЗВШВ	Наслідки ЗВШВ	Рівень успішності ЗВШВ	
Четвертий	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу, частково хмарні системи AWS (ХМА) SCADA КІ	Отримання доступу до інформаційного ресурсу та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	Середній	
	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів, частково хмарні системи AWS (ХМА) SCADA КІ	Викривлення даних контуру управління КІ з застосуванням інформаційного ресурсу КА та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива		
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів, частково хмарні системи AWS (ХМА) SCADA КІ	Компрометація систем четвертого мережевого рівня та ХМА SCADA КІ. Для п’ятого та шостого мережевих рівнів SCADA КІ наслідки ЗВШВ оперативно усунуто за рахунок застосування ХМА та реалізації функцій АВД і РКП		