МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

ІВАНЧЕНКО ОЛЕГ ВАСИЛЬОВИЧ

УДК 629.039.58:681.518.22

МЕТОДОЛОГІЧНІ ОСНОВИ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ГОТОВНОСТІ ХМАРНИХ СИСТЕМ КРИТИЧНИХ ІНФРАСТРУКТУР

05.13.06 – інформаційні технології

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня доктора технічних наук

Харків – 2021

Дисертацією є кваліфікаційна наукова праця на правах рукопису.

Роботу виконано в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут» Міністерства освіти і науки України.

Науковий консультант: Заслужений винахідник України, лауреат Державної премії в галузі науки і техніки, доктор технічних наук, професор **Харченко Вячеслав Сергійович**, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», завідувач кафедри комп'ютерних систем, мереж і кібербезпеки.

Офіційні опоненти: доктор технічних наук, професор **Мінухін Сергій Володимирович**, Харківський національний економічний університет імені Семена Кузнеця, професор кафедри інформаційних систем;

доктор технічних наук, професор **Заславський Володимир Анатолійович**, Київський національний університет імені Тараса Шевченка, професор кафедри математичної інформатики;

доктор технічних наук, професор **Левикін Віктор Макарович**, Харківський національний університет радіоелектроніки, професор кафедри інформаційних управляючих систем.

Захист відбудеться 13 травня 2021 р. о 15-15 годині на засіданні спеціалізованої вченої ради Д 64.051.09 Харківського національного університету імені В. Н. Каразіна за адресою: 61022, м. Харків, майдан Свободи, 6, ауд. 318.

З дисертацією можна ознайомитись у Центральній науковій бібліотеці Харківського національного університету імені В. Н. Каразіна за адресою: 61022, м. Харків, майдан Свободи, 4.

Автореферат розісланий 09 квітня 2021 р.

Учений секретар
спеціалізованої вченої ради Олена ТОЛСТОЛУЗЬКА

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. 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 критично важливих об'єктів (КВО) міжрегіонального та державного рівня за останні п'ятнадцять років. Для того щоб усунути ці негативні явища виконується комплекс заходів, зокрема: проведення оперативного моніторингу КВО 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. Проте відомі факти аварійного відключення, відмов провідних хмарних провайдерів і кібератак на інформаційні ресурси ХМС 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 значна увага приділена методам оцінювання рівня безпеки критичної енергетичної інфраструктури (КЕІ), аналізу інформаційної і функційної безпеки інформаційно-керуючих систем (ІКС) АЕС – важливої частини КЕІ, а також методам забезпечення гарантоздатності та надійності сервіс-орієнтованих систем. В роботах О. Г. Корченка, С. В. Казимірчук, Б. Б. Ахметова розглянуто процедури оцінювання ризику розподілених систем КІ на основі використання лінгвістичної форми представлення імовірностей негативних подій, деяких суб'єктивних оцінок та нечітко визначених оціночних параметрів. Методи адаптивного управління безпекою КВО на основі ризик-орієнтованого підходу із застосуванням сучасних ІТ розроблено Бєгуном В. В. Методи забезпечення кібербезпеки і категоризації КВО 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 Магларасa, Мітхона Макгерджі, в яких висвітлюються результати вербального та гіпотетичного оцінювання вразливостей і загроз ІКС КІ. Низку досліджень присвячено хмарним інфраструктурам (ХМІ), до складу яких входять різноманітні ХМС з фізичним і віртуальним рівнем реалізації відповідних ІТ і сервісів. Відомі роботи К. Тріведі, Р. Гоша, Ф. Хана висвітлюють проблемні питання, пов'язані з моделюванням поведінки ХМІ в умовах дії негативних факторів, які знижують готовність і рівень безпеки інфраструктури (наприклад, аварія ХМІ AWS в лютому 2017 р.). В цих роботах оцінка готовності ХМІ здійснювалася, враховуючи інформаційно-технічний стан (ІТС) як фізичних (ФМ), так і віртуальних машин (ВМ). Певна частина досліджень, включаючи роботи А. Бєлоглазова, Д. Сілви, присвячена питанням енергоспоживання ХМІ. 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 КІ 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 КЕІ;

– 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 КІ та інформаційної технології тестування регіональних хмарних систем 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.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалася на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» відповідно до державних програм, планів НДР та міжнародних проєктів, а 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.).

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 енергоефекивності 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.

Об'єкт дослідження – процеси оцінювання і забезпечення готовності, функційної та інформаційної безпечності хмарних систем критичних інфраструктур.

Предмет дослідження – 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 ХМС КІ використовувалися методи побудови структурних схем надійності, дерев відмов та атак.

Наукова новизна одержаних 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 надлишковості сервіс-орієнтованих ресурсів (додатків), оперативного моніторингу їхніх інформаційно-технічних станів, що дозволяє забезпечити доступність інтегрованих фізичних (віртуальних) компонентів інфраструктури в умовах негативних впливів;

– інформаційну технологію 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.

Практичне значення одержаних 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 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.); розроблених 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 акціонерному товаристві «Інститут інформаційних технологій» (акт впровадження від 21.10.2020 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.).

Публікації. Основні результати дисертаційної роботи опубліковано в 41

науковій праці, серед яких 2 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).

Особистий внесок здобувача. 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 результатів дисертації. Основні положення й результати дисертаційного дослідження обговорювалися та доповідалися автором 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» (Харків, 2012, 2016, 2018, 2019 рр.); 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.), «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.).

Структура та обсяг дисертації.

Дисертаційна робота складається зі вступу, 7 розділів, висновків, списку використаних джерел та 5 додатків. Обсяг загального тексту дисертації складає 336 сторінок, з них основного тексту 264 сторінки. Робота ілюстрована 145 таблицями, з яких 6 таблиць на 10 окремих сторінках, та 149 рисунками, з яких 3 рисунки на 3 окремих сторінках. Список використаних джерел містить 196 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність, важливість та доцільність дисертаційної роботи; розглянуто існуюче протиріччя; сформульовано наукову проблему, мету й завдання дослідження; охарактеризовано зв'язок з державними програмами та міжнародними проєктами; визначено об'єкт, предмет та методи дослідження, наукову новизну та практичну значущість роботи.

У першому розділі виконано аналіз проблеми забезпечення та оцінювання готовності хмарних систем критичних інфраструктур. Підставою для проведення досліджень послужили 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".

За результатами аналізу встановлено яким чином хмарні системи можуть впливати на функційну та інформаційну безпечність критичних інфраструктур. У якості прикладу було розглянуто ключові фактори ненадійності КЕІ та морської критичної інфраструктури (МКІ). Проведений аналіз систем моніторингу на основі використання хмарних ресурсів відомих провайдерів підтвердив доцільність їхнього застосування для забезпечення функційної та інформаційної безпеки КЕІ та МКІ. Додатково було розглянуто тенденції розвитку концепцій, методів, ІТ оцінювання, забезпечення надійності та безпеки хмарних систем КІ.

Відомо, що найкращу динаміку розвитку підходів 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 в період з 2008 по 2018 роки демонструють провідні хмарні провайдери, а саме Amazon, Google, Microsoft, IBM. 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 аналіз ієрархії властивостей дозволив здійснити вибір показників готовності, надійності та безпеки хмарних систем КІ.

Розділ завершується вибором математичного апарату та обґрунтуванням методології наукових досліджень. Основні результати, які відображено в першому розділі, опубліковано в роботах [1, 16, 17, 22, 38].

У другому розділі наведено основні положення методології забезпечення готовності хмарних систем КІ. Структура методології представлена на рис. 1. Методологія базується на наступних принципах:

1. *Принцип реконфігурування фізичних і кіберактивів, 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.

Процедура реконфігурування здійснюється відповідно до наступної системи вимог і обмежень:

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

де K_{Γ_0} – гранично припустиме значення стаціонарного коефіцієнта готовності (КГ) ХМС КІ; Т – загальний час застосування ХМС КІ за призначенням; τ_M – 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.

2. *Принцип компліментарності*, який на відміну від відомих, передбачає дотримання вимог масованого паралелізму архітектурної побудови КІ. Зокрема, висуваються вимоги забезпечення ефективного функціонування КІ при пріоритеті інфраструктурної надійності та безпеки. Це означає, що в термінах генної інженерії за основу приймається компліментарна побудова молекули ДНК (дезоксирибонуклеїнової кислоти), коли зв'язування відбувається шляхом взаємного тяжіння компонентів: А завжди зв'язується тільки з Т, а Г – з Ц. Тоді, архітектура будь-якої КІ може бути побудована у відповідності з наступними припущеннями: А – це об'єкт управління, наприклад, КЕІ (або окремий її КВО); Т – система забезпечення безпеки та надійності КЕІ (або окремого її КВО); Г – система підтримки прийняття рішень для КЕІ (або КВО); Ц – система управління КЕІ (або КВО).

3. *Принцип оперативного моніторингу інформаційно-технічних станів компонентів КЕІ*, який на відміну від відомих, реалізується на основі застосування систем синхронізованих векторних вимірювань (ССВВ). Використання ССВВ надає можливість за лічені секунди фіксувати негативні явища та оперативно реагувати на них з точки зору мінімізації наслідків.

На основі запропонованої методології (рис. 1), спираючись на зазначені принципи, сформульовано концепцію роботи, яка полягає в побудові хмарних систем КІ як систем високої готовності з недостатньо надійних і безпечних інтегрованих фізичних (віртуальних) компонентів в умовах різноманітних негативних впливів. Згідно концепції негативні впливи представляються у вигляді зловмисних шкідливих впливів та проникнень, на реалізацію яких впливають зовнішні і внутрішні фактори природнього та штучного походження.

Дія зловмисних шкідливих впливів моделюється з застосуванням як стохастичного, так і детерміністського підходів. Узагальнюючи отримані результати аналізу відповідних інфраструктурних активів та відповідних негативних факторів впливу на них, в представленій методології (рис. 1) значна увага приділяється функційній (ФБ) та інформаційній безпечності (ІБ) активів КІ. Відомо, що різноманітні негативні події у вигляді здовмисних шкідливих впливів, відмов, збоїв, дефектів погіршують функційну та інформаційну безпечність критичних інфраструктур. Безумовно це знижує рівень готовності, збільшує ризик негативних впливів на інфраструктурні активи та сприяє виникненню аварій КІ з важкими наслідками. Структурна діаграма ризику негативних впливів на активи критичних інфраструктур представлена на рис. 2.

Застосовуючи рис. 2, була отримана логіко-ймовірнісна модель ризику негативних впливів на активи критичних інфраструктур та здійснено перехід до

оцінної моделі. Отже, для оцінки ризику негативних впливів на активи КІ застосовується співвідношення виду

$$R_{CI} = \left(1 - K_{\Gamma_{CI}}\right) L_{ПНД_{CI}}, \qquad (2)$$

де $K_{\Gamma_{CI}}$ – коефіцієнт готовності критичної інфраструктури з урахуванням негативних впливів на її активи; $L_{ПНД_{CI}}$ – показник причинно-наслідкової декомпозиції (ПНД) негативних впливів на активи КІ, що опосередковано враховує нанесені збитки.

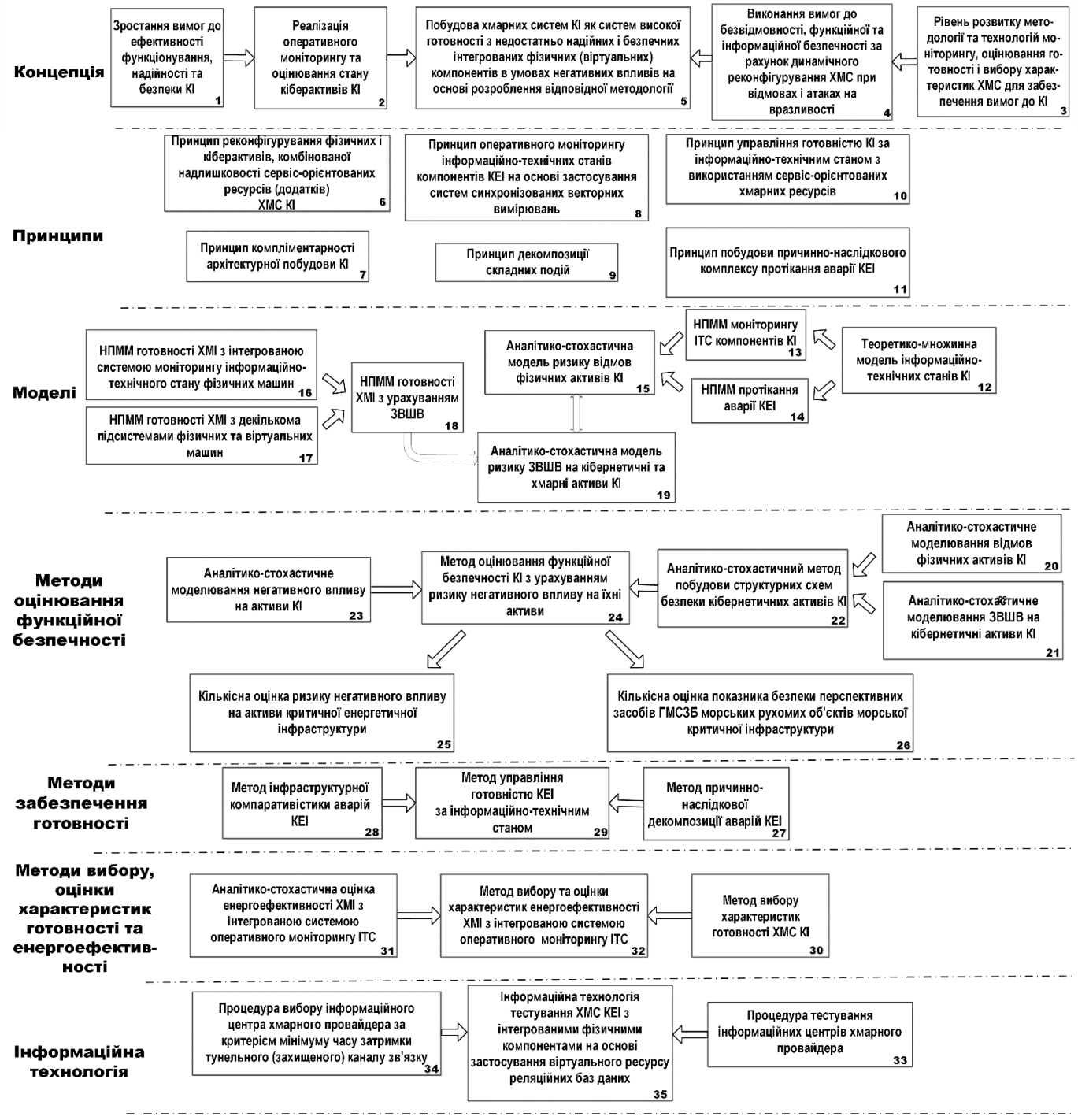


Рис. 1 Методологія забезпечення готовності ХМС критичних інфраструктур

У виразі (2) показник $L_{ПНД_{CI}}$ розраховується як нормована величина на основі певної бізнес-логіки і є безрозмірною величиною. Показник $L_{ПНД_{CI}}$ визначається на основі використання модифікованої алгебри причинно-наслідкових комплексів (ПНК). Приклад щодо розрахунку ризику негативних впливів на активи критичної енергетичної інфрастуктури наведено у розділі п’ять.

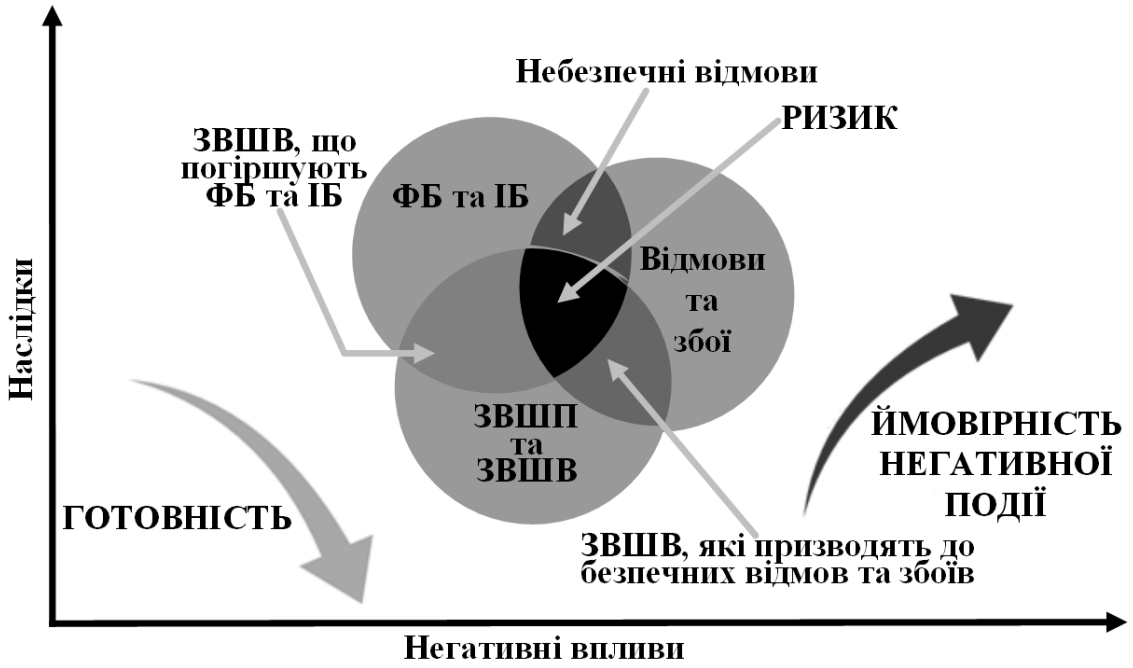


Рис. 2 Структурна діаграма ризику негативних впливів на активи КІ

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 інфрастуруктури.

Основні результати досліджень, які представлено в другому розділі, опубліковано в роботах [1, 25, 28, 29, 31, 32].

У третьому розділі представлено 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.

Загальна методологія оцінювання готовності КІ реалізована шляхом розбудови відповідного модельного ряду. На рис. 3 зображена схема формалізації процесів, які впливають на функціональну та інформаційну безпечності критичної інфраструктури з урахуванням множини її інформаційно-технічних станів $M_{CI} = \left\{ M_{FF}^{PhA}, M_{DMI}^{CbrA}, M_{DMI}^{CldA}, M_{SS}^{CI} \right\}$. Надалі представлена схема використовується для побудови теоретико-множинної моделі ІТС КІ.

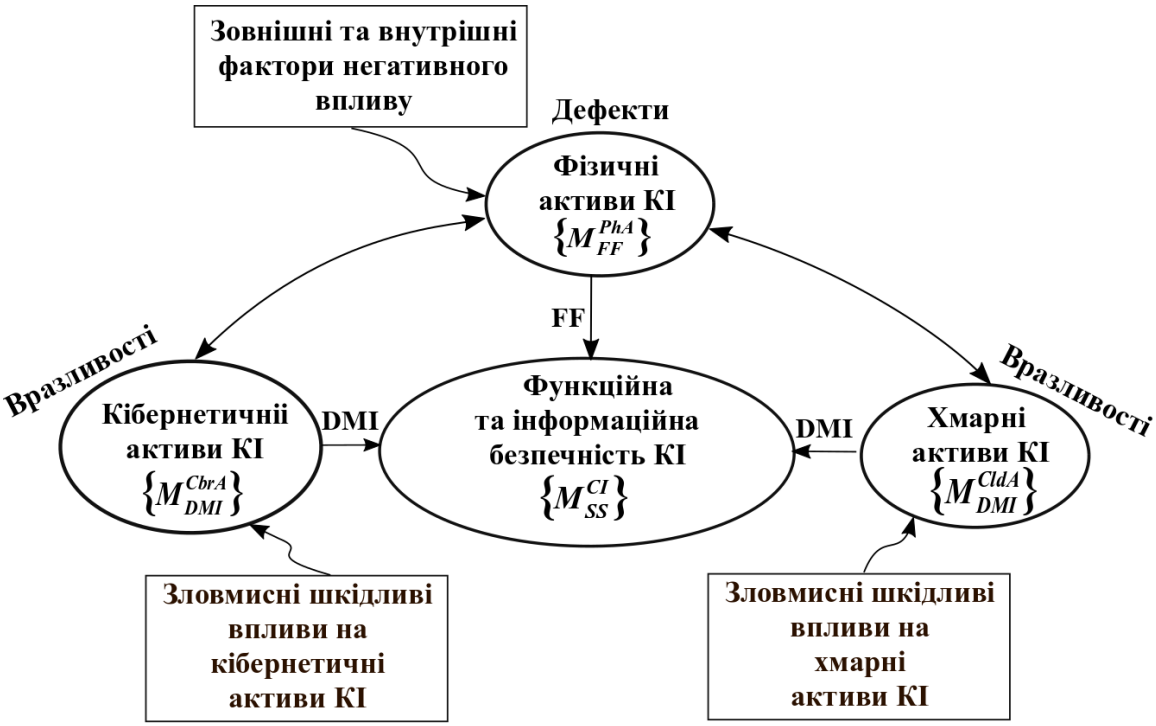


Рис. 3 Схема формалізації процесів, які впливають на ФБ та ІБ КІ

На наступному етапі у відповідності до загальної концепції досліджень було розроблено оцінні моделі надійності КЕІ з системою контролю інформаційно-технічних станів. Подальші розрахунки були реалізовані на основі застосування напівмарковського процесу моделювання (НММ). 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.

Первинно до розгляду була запропонована НПММ моніторингу інформаційно-технічних станів критичної інфраструктури (рис. 4), яка працює в режимі контролю ІТС (скорочено 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 ІТС.

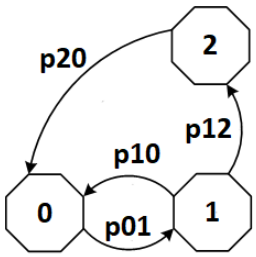


Рис. 4 Граф станів НПММ моніторингу інформаційно-технічних станів

критичної інфраструктури з вірогідним КТС

Результати моделювання для запропонованої НПММ (рис. 4) у вигляді залежності коефіцієнта готовності КІ від середньої наробітки на відмову та середнього часу відновлення для різних значень $\tau_{ктс}$ і фіксованого значення часу застосування за призначенням $T = 5000$ год. зображено на рис. 5.

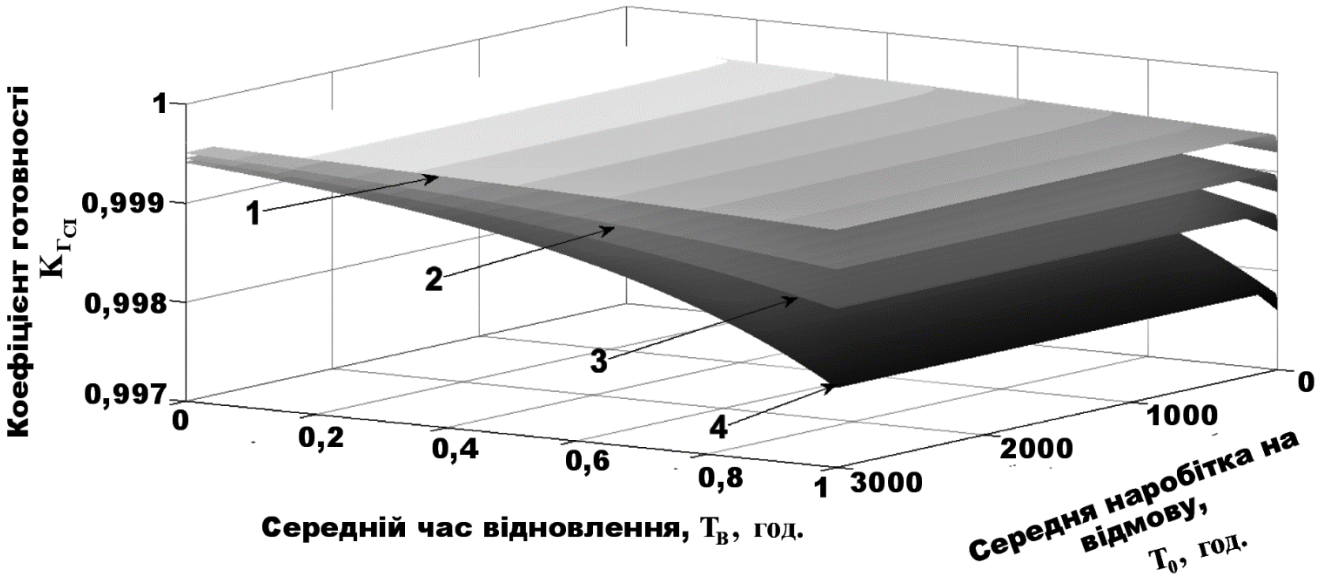


Рис. 5 Кількісні результати моделювання для $T = 5000$ год. за умов: 1) $\tau_{ктс} = 1$ хв. хв.; 2) $\tau_{ктс} = 1{,}5$ хв. хв.; 3) $\tau_{ктс} = 2$ хв.; 4) $\tau_{ктс} = 3$ хв.

Отримані результати моделювання (рис. 5) є занадто оптимістичними, тому що не враховуються негативні ситуації, які пов'язані з наявністю різноманітних вразливостей, помилок обслуговуючого персоналу та прихованих відмов. Реальній дійсності, що складається в сфері застосування КІ, більше відповідає напівмарковська модель моніторингу інформаційно-технічних станів критичної інфраструктури з невірогідним контролем (система А), граф станів якої відображено на рис. 6.

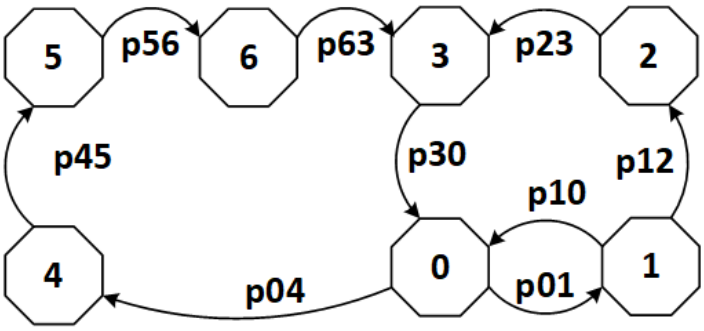


Рис. 6 Граф станів НПММ моніторингу інформаційно-технічних станів критичної інфраструктури з невірогідним контролем

Особливо гостро проблема невірогідного КТС стоїть в сфері застосування КЕІ. Для її усунення пропонується спільно використовувати системи синхронізованих векторних вимірювань (ССВВ) та ХМС.

Застосування додаткових модулів ССВВ та відповідних хмарних сервісів AWS надає можливість перетворити існуючу систему моніторингу інформаційно-технічних станів критичних інфраструктур (рис. 6) (система А) в більш сучасну систему оперативного моніторингу (система Б) з вірогідним КТС. 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 НПММ 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 НПММ системи L. Для системи А, перші дві нотації $S_{A_i},Q_{A_{ij}}(t)$ відповідної граматики доповнюються наступними чотирма нотаціями:

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

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

Друга напівмарковська модель описує роботу системи Б і є логічним продовженням першої моделі. Перші дві нотації $S_{Б_i},Q_{Б_{ij}}(t)$ записуються у відповідності до графу станів, зображеному на рис. 7. Решта нотацій граматики Б записується у вигляді

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

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

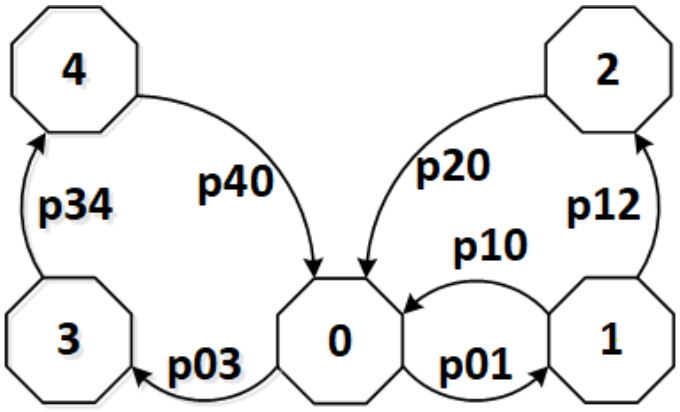


Рис. 7 Граф станів напівмарковської моделі моніторингу інформаційно-технічних станів критичної інфраструктури з вірогідним контролем

Результати порівняльного аналізу системи оперативного моніторингу інформаційно-технічних станів критичної інфраструктури з вірогідним контролем (система Б) над існуючою системою моніторингу ІТС КІ з невірогідним КТС (система А) представлено в таблиці 1. Отримані результати свідчать про безумовну перевагу системи Б над системою А. Виграш в значеннях коефіцієнта готовності складає понад 37 %.

Таблиця 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 (система А)	Система оперативного моніторингу ІТС КІ з вірогідним КТС (система 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

Розглянемо яким чином виконується моделювання поведінки та оцінювання готовності хмарної інфраструктури, до складу якої входять ХМС, що розгортаються у вигляді фізичних і віртуальних машин. Після аналізу відомих методів перевагу було надано методу напівмарковського моделювання на основі використання вкладених марковських ланцюгів (ВМЛ), який включає наступні кроки: а) аналіз класифікаційної схеми забезпечення готовності ХМІ з декількома підсистемами ФМ і ВМ; б) аналіз характеристик, режимів функціонування та основних властивостей ХМІ; в) формалізоване визначення, характеристика основних станів та побудова відповідної моделі готовності ХМІ; г) реалізація методу напівмарковського моделювання у відповідності з діаграмою, яка зображена на рис. 8. Особливість моделей, реалізуємих відповідно до запропонованого методу, полягає в урахуванні вироджених станів компонентів інфраструктури.

Впродовж процесу розроблення моделей відповідно до запропонованого методу (рис. 8) було враховано можливості щодо створення сучасної інтегрованої системи моніторингу (СІНТЕМ) інформаційно-технічних станів ХМС на основі розгортання мереж мікросервісів і віртуальних моніторів (рис. 9). 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.

Узагальнені результати моделювання у вигляді граничних показників надійності хмарної інфраструктури з вірогідним контролем інформаційно-технічних станів фізичних та віртуальних машин приведено в таблиці 2.

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.

Основні результати третього розділу опубліковано в роботах [2, 3, 10, 13, 14, 16, 19, 24–26, 28, 29, 37, 39]

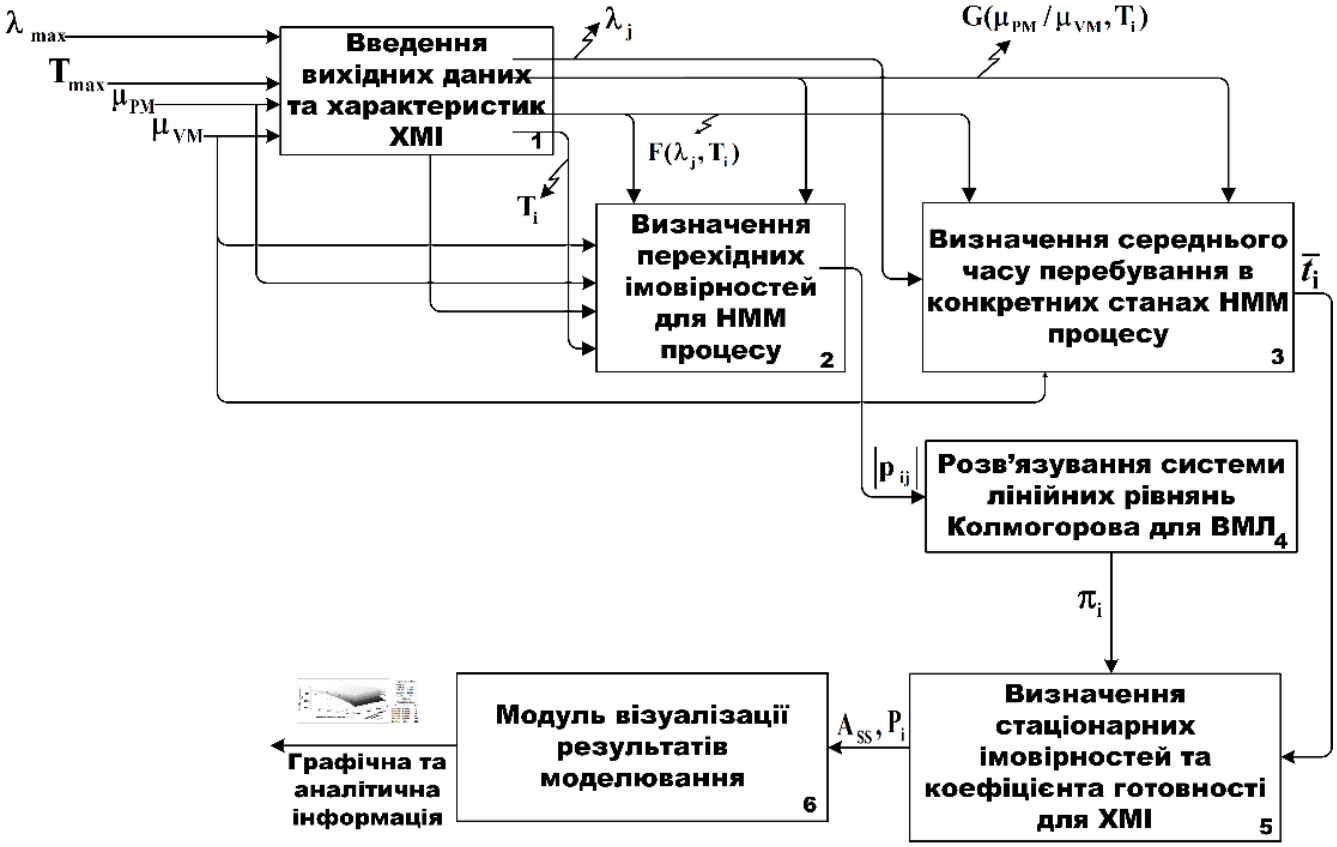


Рис. 8 Діаграма реалізації методу НММ готовності ХМІ

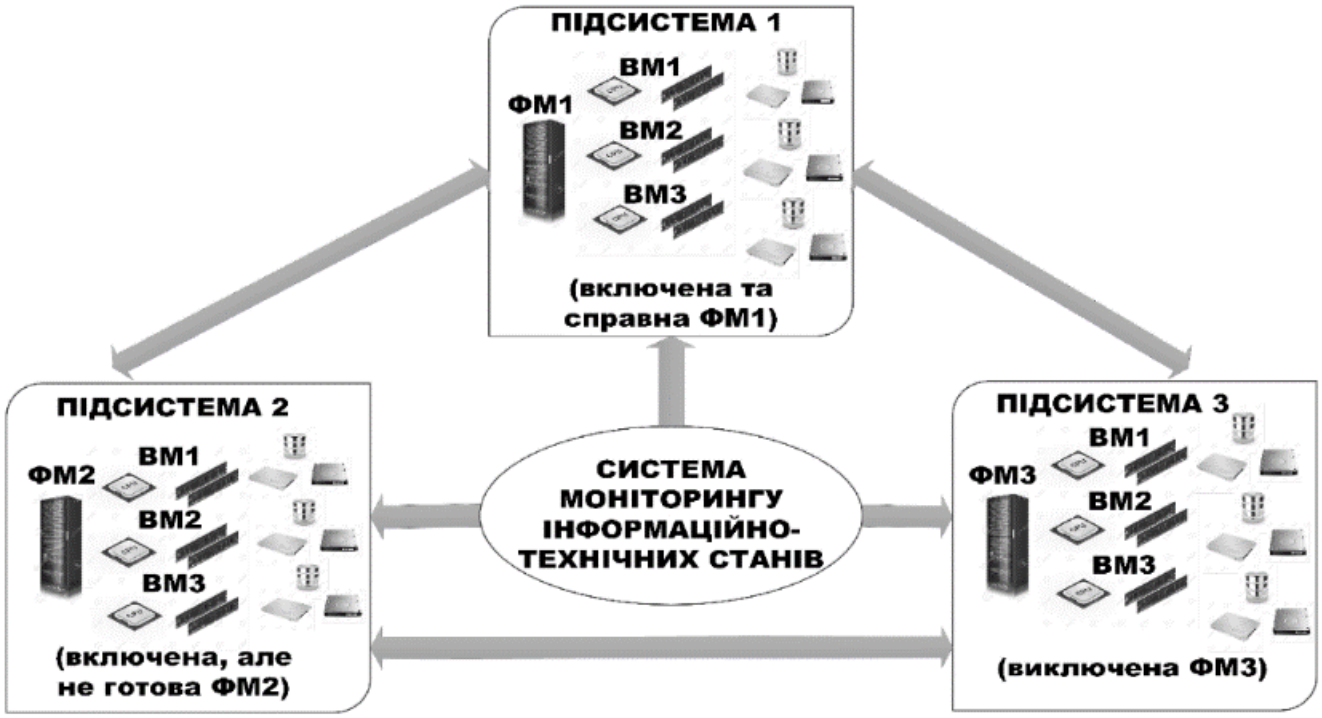


Рис. 9 Спрощена структурна схема хмарної інфраструктури з трьома підсистемам фізичних та віртуальних машин і СІНТЕМ ІТС

Таблиця 2

Граничні величини показників надійності ХМІ з КТС ФМ та ВМ

Коефіцієнт готовності	Показники надійності	
	Середня наробітка на відмову, год.	Інтенсивність відновлення, 1/год.
0,99	2380	4
	2083	5
	1667	8
	1562	10
	1316	20
	1219	30
	1110	40
	1020	50

У четвертому розділі 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. Для розв'язування завдань визначення рівня функційної безпечності КІ було запропоновано аналітико-стохастичний метод (АСТМ) побудови структурних схем безпеки (ССБ), схема алгоритму реалізації якого зображена на рис. 10.

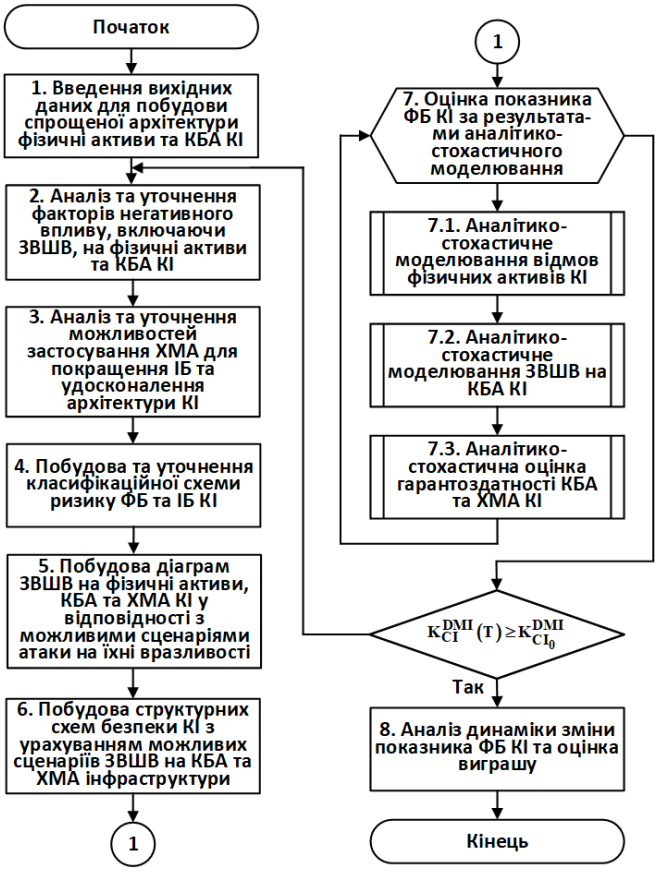


Рис. 10 Схема алгоритму реалізації АСТМ побудови структурних схем безпеки кібернетичних активів КІ

Розглянемо деякі теоретичні засади щодо реалізації пропонуємого методу, за допомогою яких можна на формальному рівні описати етапи реалізації атаки на кібернетичні та хмарні активи критичної енергоінфраструктури. Припустимо, що на активи інформаційно-керуючої системи типу SCADA, яка використовується в контурі управління КЕІ, за певним сценарієм здійснюється атака з використанням ЗВШВ, яка реалізується в декілька етапів, а саме: а) на першому етапі здійснюється цільовий фішинг (ЦФ); б) на другому етапі внаслідок ЦФ розкривається інформація (РЗІ); в) на третьому етапі за рахунок фальсифікації (ФСФ) та підміни інформації (ПДМ) здійснюється компрометація системи. Аналіз відомого досвіду свідчить, що спостерігається чітка послідовність виконання визначених етапів та залежність наступних етапів кібератаки від попередніх. Як правило, атака починається з того, що зловмисниками за рахунок ЦФ здійснюється розкриття інформації. Ця обставина надає змогу поетапно реалізувати кібератаку, спрощена діаграма, якої зображена на рис. 11.

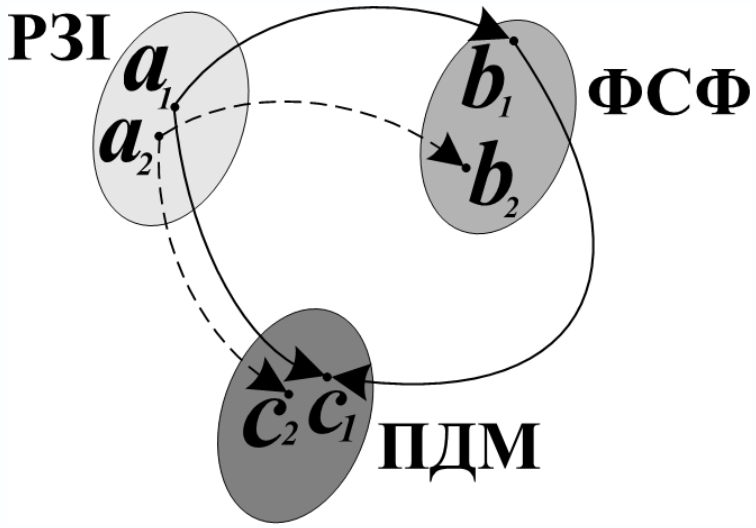


Рис. 11 Спрощена діаграма етапів реалізації кібератаки

У той же час, спираючись на відомий досвід кібератак на активи системи SCADA КЕІ, треба розуміти, що без виконання початкового етапу РЗІ наступні етапи фальсифікації та підміни інформації реалізувати майже неможливо. В таблиці 3 наведено формалізми на основі бінарних відношень, які описують етапи реалізації атаки на кібернетичні активи (КБА) системи SCADA КЕІ з урахуванням вказаних аспектів.

Таблиця 3

Бінарні відношення, які описують етапи реалізації атаки на КБА системи SCADA КІ

Етапи реалізації атаки на КБА	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	$\delta \subset A \times C \longleftrightarrow \delta = \{(a,c) \mid a \in \delta, c \in \delta\}$

Відповідно до таблиці 3 між елементами $a \in \mathrm{A}$, $b \in \mathrm{B}$ та $c \in \mathrm{C}$ існують бінарні відношення, де $\mathrm{A} = \underset{\mathrm{i}\in\mathrm{I}}{\cup} a_{\mathrm{i}}$, $\mathrm{B} = \underset{\mathrm{j}\in\mathrm{J}}{\cup} b_{\mathrm{j}}$, $\mathrm{C} = \underset{\mathrm{r}\in\mathrm{R}}{\cup} c_{\mathrm{r}}$ є відповідними множинами елементів. Наприклад, запис $\exists\, \rho \subset \mathrm{A} \times \mathrm{B}$ означає, що існує функція ρ, яка деякому елементу a_{i} з множини A ставить у відповідність елемент b_{j} з множини B та задається як декартів добуток $\mathrm{A} \times \mathrm{B} = \{(a,b) | a \in \mathrm{A}, b \in \mathrm{B}\}$, тобто бінарне відношення $\rho \subset \mathrm{A} \times \mathrm{B}$ множин A та B розглядається як підмножина декартівого добутку $\mathrm{A} \times \mathrm{B}$. Аналогічно можна задати бінарне відношення $\sigma \subset \mathrm{B} \times \mathrm{C}$ множин B та C. Отже, застосовуючи діаграму етапів реалізації кібератаки (рис. 11), визначення трьох рівнів успішності атаки на КБА та формалізми, які наведено в таблиці 3, спробуємо сформулювати і довести 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. 11 переходи РЗІ $\longrightarrow$ ФСФ, ФСФ $\longrightarrow$ ПДМ та РЗІ $\longrightarrow$ ПДВ (позначені суцільною лінією) між собою поєднані. Тоді, застосовуючи формалізми таблиці 3, отримаємо добуток бінарних відношень ρ та σ у вигляді

$$\rho \circ \sigma = \underset{(a,b)}{\mathrm{C}}\, \underset{c}{\mathrm{V}} (a,b) \in \rho \wedge (b,c) \in \sigma = (a,c), \tag{3}$$

де $\underset{(a,b)}{\mathrm{C}}$ – класифікатор або символ абстракції по змінним a та b; $\underset{c}{\mathrm{V}}$ – квантор існування по змінній c.

Співвідношення (3) можна записати у вигляді 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. 11 переходи РЗІ $\longrightarrow$ ФСФ та РЗІ $\longrightarrow$ ПДВ (позначені пунктирною лінією) між собою не поєднуються, що підтверджує не виконання умови транзитивності. Тоді, застосовуючи формалізми таблиці 3, отримаємо добуток бінарних відношень ρ та δ у вигляді

$$\rho \Delta \delta = \underset{(a,(b,c))}{\mathrm{C}} (a,b) \in \rho \wedge (a,c) \in \delta \neq \rho \circ \delta. \tag{4}$$

Співвідношення (4) свідчить, що умова транзитивності бінарних відношень не виконується. ■

Розроблений метод (рис. 10) використано для отримання оцінки функційної безпечності активів системи SCADA критичної енергетичної інфраструктури, структурна схема активів якої представлена на рис. 12. У якості комплексного показника гарантоздатності (ГРТЗ) активів системи SCADA критичної енергетичної інфраструктури використано стаціонарний коефіцієнт готовності, який відповідно до структурної схеми безпеки (рис. 13) розраховується як

$$\mathrm{K}_{\mathrm{SCADA}}^{\mathrm{DMI}} = \mathrm{K}_{\mathrm{SCADA}_1}^{\mathrm{DMI}} \mathrm{K}_{\mathrm{SCADA}_2}^{\mathrm{DMI}} \mathrm{K}_{\mathrm{SCADA}_3}^{\mathrm{DMI}} \mathrm{A}_{\mathrm{FW}_4} \mathrm{A}_{\mathrm{FW}_5}, \tag{5}$$

де $K^{DMI}_{SCADA_1}$ – КГ першого, другого, третього кластерів SCADA КЕІ; $K^{DMI}_{SCADA_2}$ – КГ четвертого мережевого рівня SCADA КЕІ; $K^{DMI}_{SCADA_3}$ – КГ п’ятого та шостого мережевих рівнів SCADA КЕІ; A_{FW_4}, A_{FW_5} – КГ четвертого та п’ятого брандмауерів, відповідно.

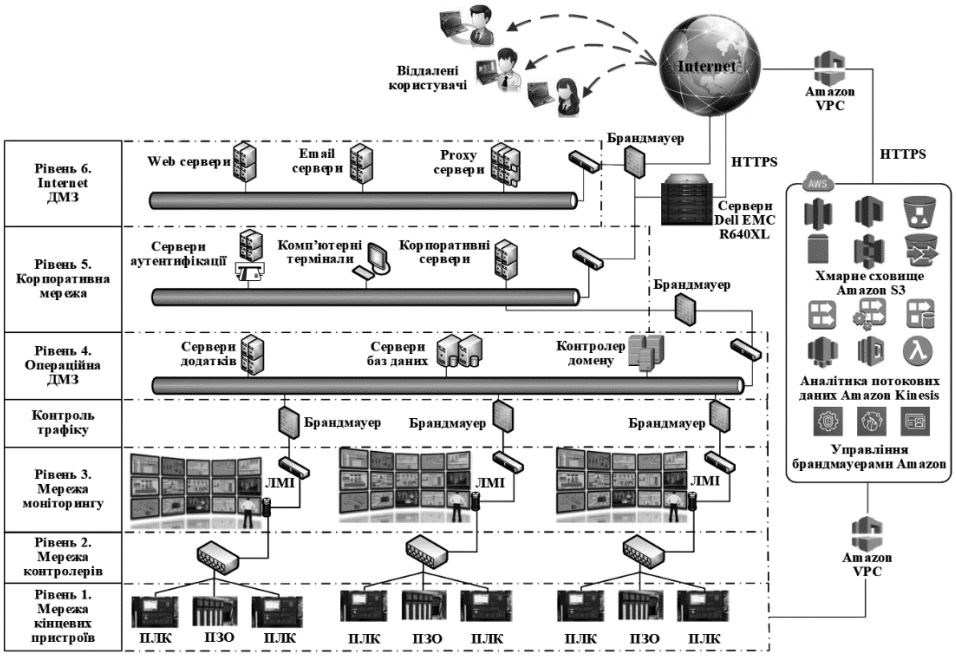


Рис. 12 Структурна схема активів системи SCADA КЕІ

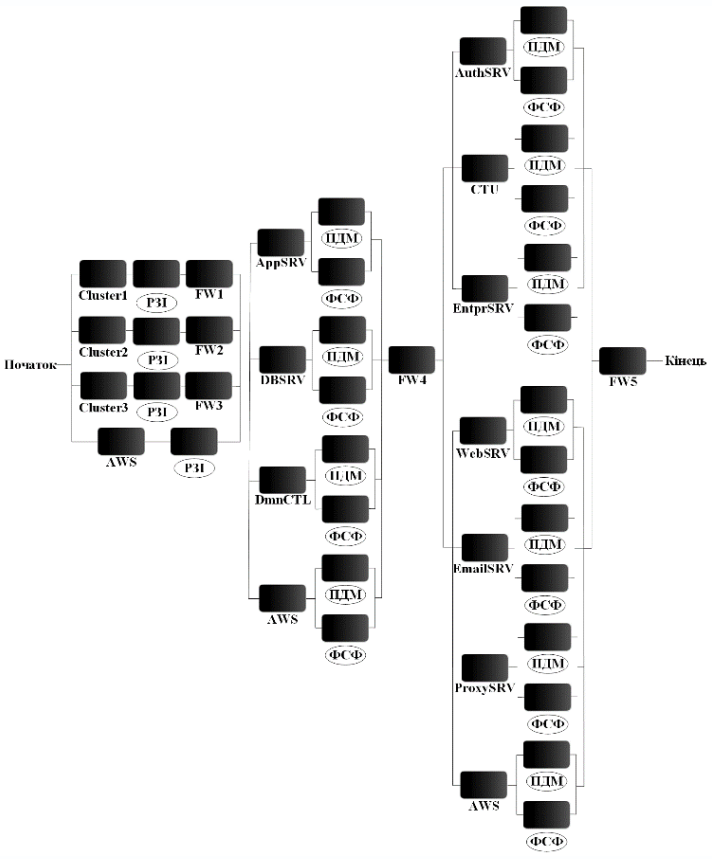


Рис. 13 Структурна схема безпеки активів системи SCADA КЕІ

На рис. 14, 15 зображено графічні залежності для отриманих НПММ зловмисного шкідливого впливу на активи SCADA КЕІ, коли здійснюються РЗІ, ФСФ та ПДМ.

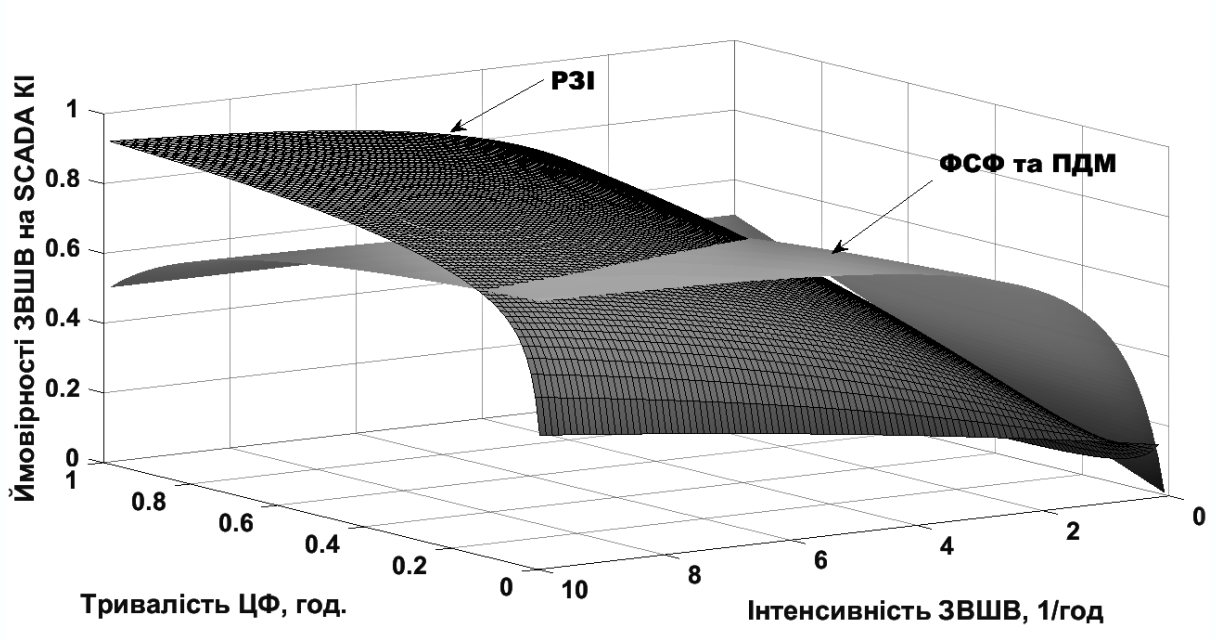


Рис. 14 Залежності ймовірності реалізації ЗВШВ у вигляді РЗІ, ФСФ та ПДМ для активів системи SCADA КІ

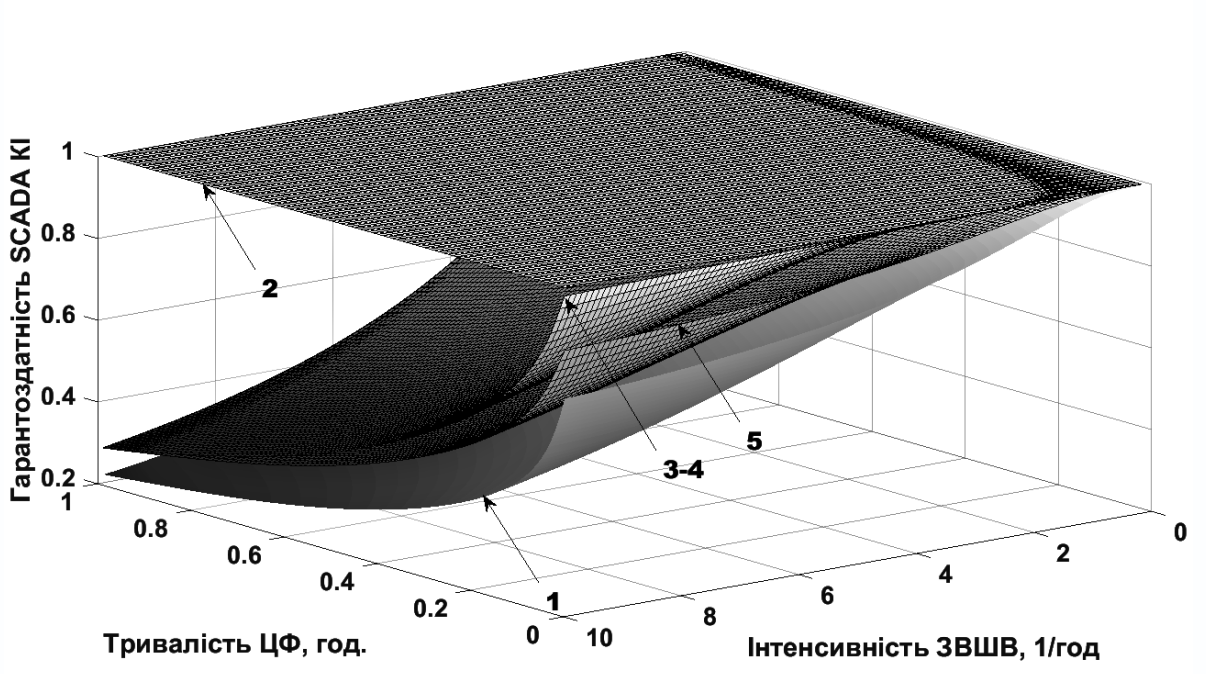


Рис. 15 Комплексний показник гарантоздатності активів системи SCADA КІ для п’ятьох сценаріїв атак за умови, що на зміну ключів витрачається 3 хв.

Оцінка виграшу обчислювалася у вигляді абсолютної різниці між значеннями стаціонарного коефіцієнта неготовності (КНГ) для відповідних пар сценаріїв атак з застосуванням наступного співвідношення:

$$\Delta_{SCADA} = \left| \overline{K}^{DMI}_{SCADA_{k,h}} - \overline{K}^{DMI}_{SCADA_{2,h}} \right|, \qquad (6)$$

де k=1,3,4,5 – номери відповідних сценаріїв ЗВШВ; h – номер зрізу КНГ, для якого виконується обчислення; $\overline{K}^{DMI}_{SCADA_{2,h}}$ – значення h-го зрізу КНГ для другого сценарію кібератаки.

Динаміку зміни величини КНГ для кібернетичних та хмарних активів SCADA КІ відображено в таблиці 4.

Таблиця 4

Динаміка зміни величини коефіцієнта неготовності системи SCADA КІ з урахуванням ЗВШВ на кібернетичні та хмарні активи

Порівняльна комбінація сценаріїв ЗВШВ	Загальні параметри ЗВШВ		Тривалість процедури “зміни ключів”, хв.	Зменшення значень КНГ, %
	Тривалість ЦФ, хв.	Максимальна інтенсивність ЗВШВ, 1/год.		
1	2	3	4	5
(2;1) (2;3) (2;5) (3;1) (3;5)	3	10	30	34,9 8,7 20,8 26,2 12,1%
(2;1) (2;3) (2;5) (3;1) (3;5)	6	10	3	49,5 25 34,6 24,5 9,5

Наступним кроком було оцінювання функційної безпечності КЕІ з урахуванням ризику негативних впливів на її активи згідно методу, діаграма реалізації якого представлена на рис. 16. У якості наочного прикладу розглядався сценарій протікання відомої аварії КЕІ з каскадними відключеннями компонентних складових. Кількісна оцінка ризику отримана відповідно до співвідношення (2), складові якого визначалися за допомогою апарату: 1) причинно-наслідкового аналізу негативного впливу на активи КЕІ, тобто обчислювався показник ПНД $L_{ПНД_{CEI}}$ інфраструктури; 2) аналітико-стохастичного моделювання негативного впливу на активи КЕІ, тобто за результатами напівмарковського моделювання обчислювався $K_{Г_{CEI}}$ інфраструктури.

На рис. 17 зображено результати кількісної оцінки ризику аварії КЕІ $R_{CEI}(\lambda_1,\lambda_2)$ в залежності від інтенсивностей відмов компонентних складових інфраструктури та помилок обслуговуючого персоналу (ОП). Аналіз результатів моделювання (рис. 17) надав змогу здійснити вибір стратегії забезпечення функційної безпечності КЕІ. Зокрема, перевага була надана стратегії управління готовністю КЕІ за інформаційно-технічним станом (основні положення відповідного методу розглянуто в наступному розділі роботи).

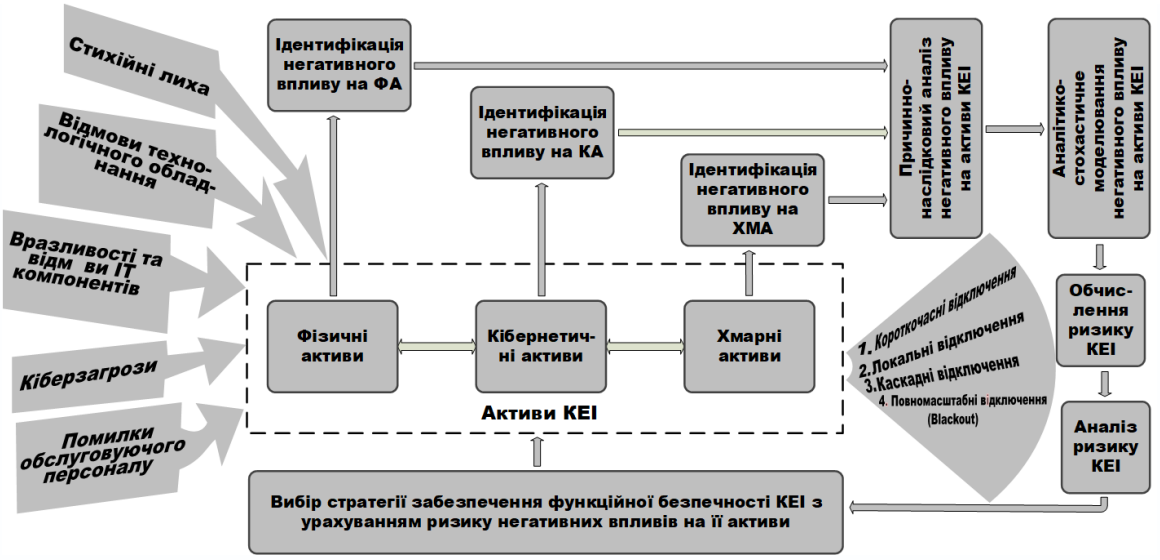


Рис. 16 Діаграма реалізації методу оцінювання функційної безпечності КЕІ з урахуванням ризику негативних впливів на її активи

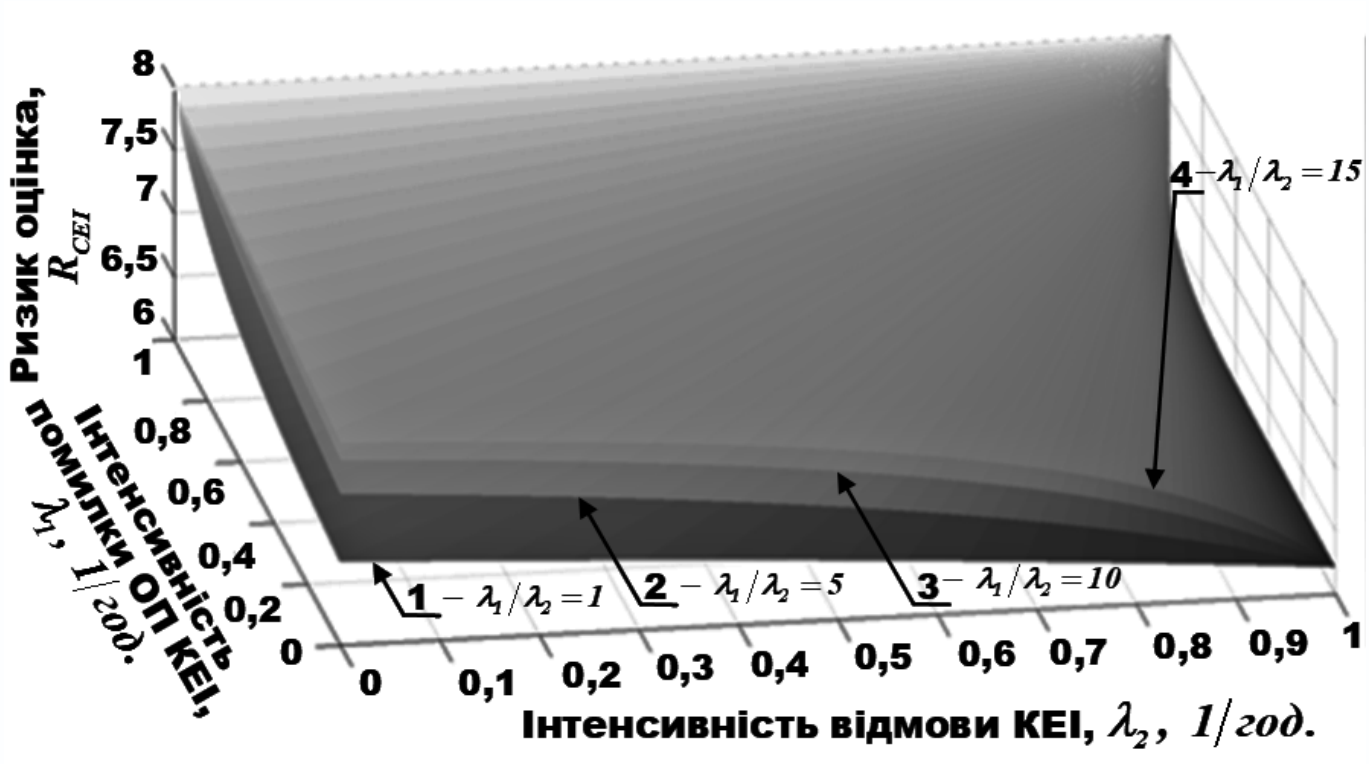


Рис. 17 Аналітико-стохастична оцінка ризику аварії КЕІ

Наступний блок розробленої методології (рис. 1) присвячено кількісній оцінці показника безпеки перспективних засобів Глобальної морської системи зв’язку та забезпечення безпеки мореплавства (ГМСЗБ, GMDSS) морських рухомих об’єктів (МРО) морської критичної інфраструктури (МКІ). Серед перспективних засобів ГМСЗБ слід відзначити бездротові сенсорні мережі (БДСМ або WSN) та ХМС. Роль та місце БДСМ, ХМС та радіотелекомунікаційних засобів як перспективних засобів ГМЗСБ МРО МКІ відображено на відповідній функціональній схемі (рис. 18).

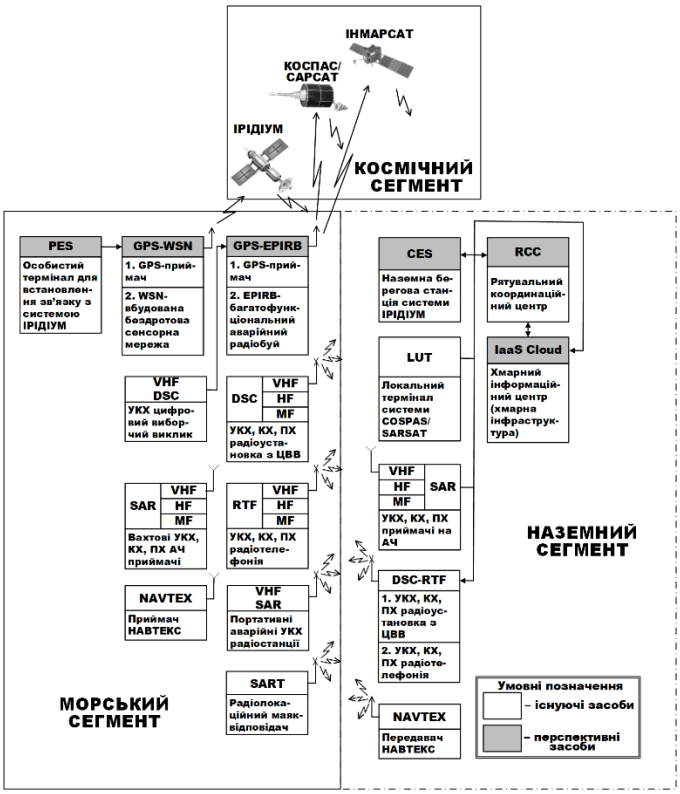


Рис. 18 Функціональна схема застосування перспективних засобів ГМСЗБ морських рухомих об’єктів МКІ

На наступному етапі будується діаграма впливу ризик-факторів на сегменти Глобальної морської системи зв’язку та забезпечення безпеки мореплавства (рис. 19) і схема алгоритму реалізації атаки на засоби ГМСЗБ (рис. 20).

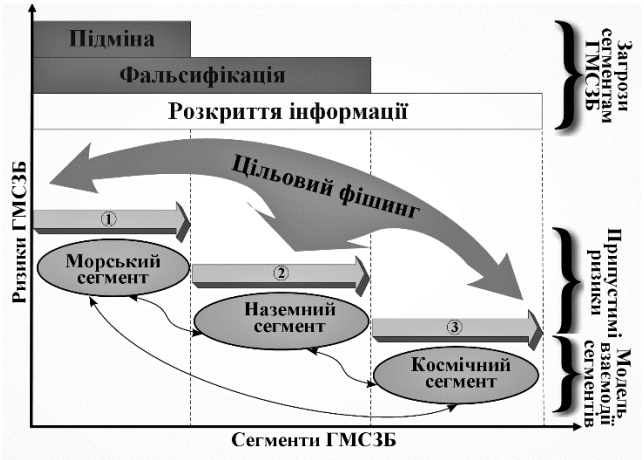


Рис. 19 Діаграма впливу ризик-факторів на сегменти ГМСЗБ

Далі, враховуючи можливий сценарій атаки CA_k, були побудовані діаграма системної відмови SF_k, діаграма ЗВШВ $DMI_k(ID, TI, SI)$ з урахуванням ризик-факторів (рис. 19) по виконанню трьох негативних дій, тобто РЗІ, ФСФ та ПДМ. Паралельно було отримано теоретико-множинну модель $Availability_{ГМСЗБ}$ та здійснено перехід до опорної моделі $A_{ГМСЗБ}$ для визначення коефіцієнта готовності системи ГМСЗБ.

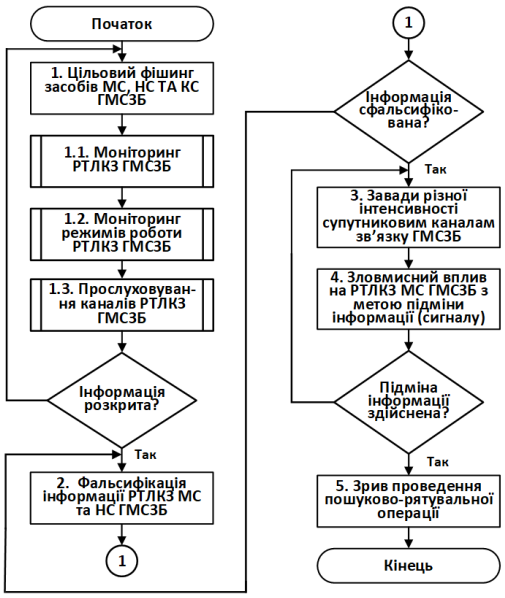


Рис. 20 Схема алгоритму реалізації атаки на засоби ГМСЗБ

Керуючись основними положеннями відповідного методу (рис. 9) та попередньо отриманим модельним рядом $W_{ГМСЗБ} = \langle CA_k, SF_k, DMI_k(ID, TI, SI), Availability_{ГМСЗБ}, A_{ГМСЗБ} \rangle$, було побудовано ССБ ГМСЗБ, яка зображена на рис. 21.

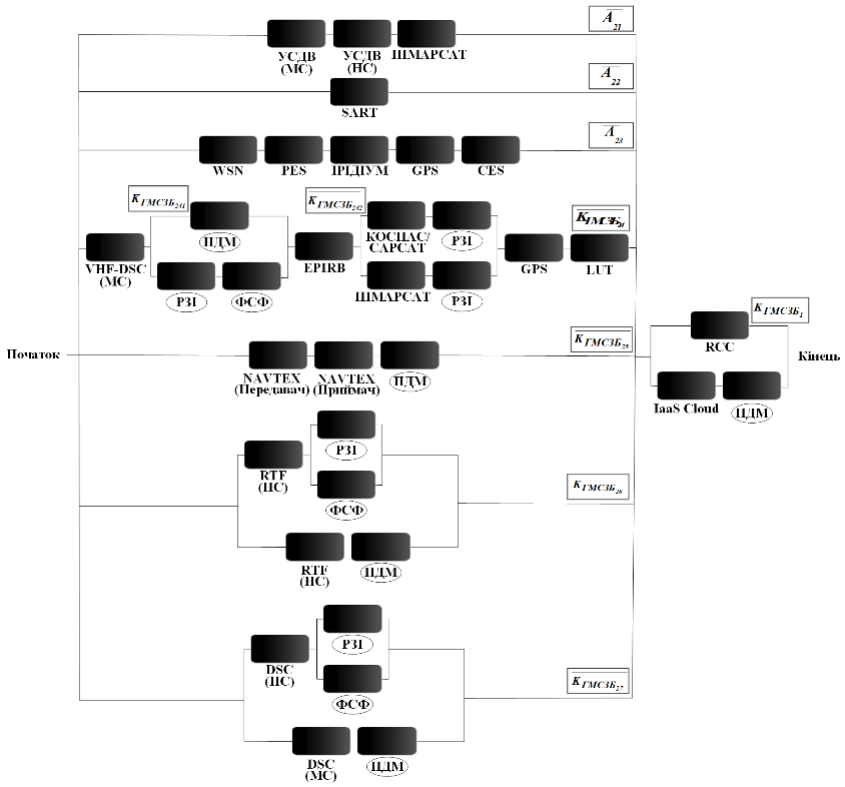
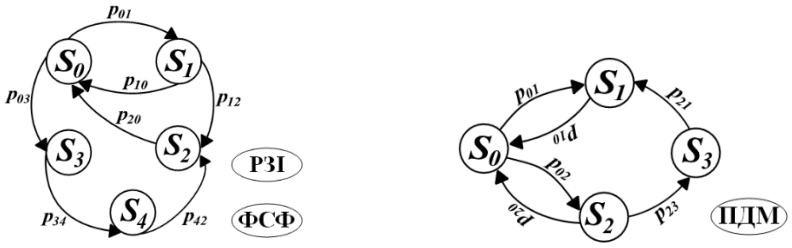


Рис. 21 Структурна схема безпеки засобів ГМСЗБ

На рис. 22 приведено графи станів напівмарковських моделей ЗВШВ на засоби ГМСЗБ, які використовувалися для визначення імовірностей виконання дій по розкриттю, фальсифікації та підміні інформації. Аналогічні моделі застосовувалися для отримання оціночних залежностей (див. рис. 14, 15).



а) б)

Рис. 22 Моделі ЗВШВ на засоби ГМСЗБ: а) для РЗІ та ФСФ; б) для ПДФ

На рис. 23, 24 відображено результати дослідження кількісної оцінки показника безпеки (ПБ) перспективних засобів ГМСЗБ у порівнянні з існуючими.

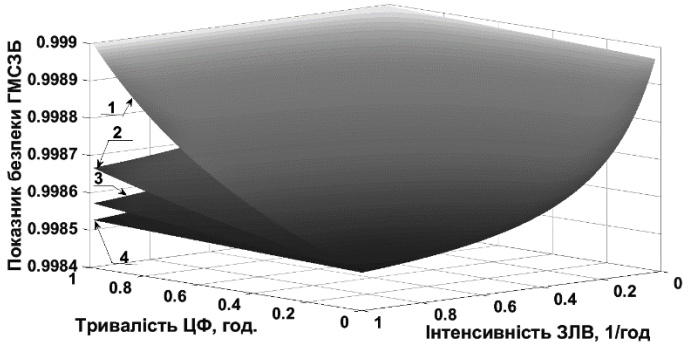


Рис. 23 Різниця між ПБ перспективних та існуючих засобів ГМСЗБ: 1 – $\gamma_{DMI}/\gamma_{tp}=1$; 2 – $\gamma_{DMI}/\gamma_{tp}=2$; 3 – $\gamma_{DMI}/\gamma_{tp}=4$; 4 – $\gamma_{DMI}/\gamma_{tp}=10$

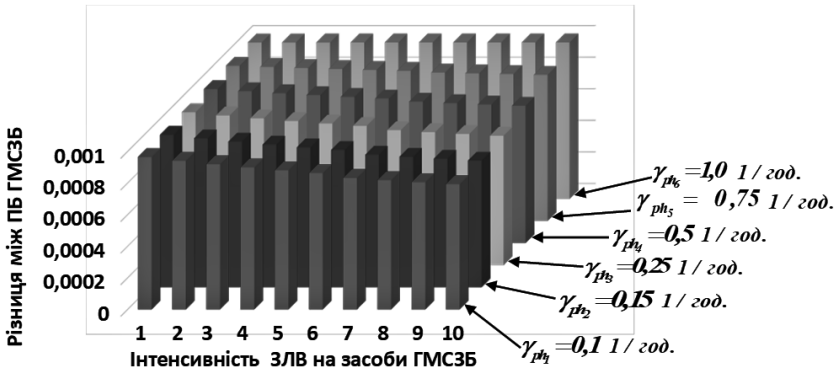


Рис. 24 Різниця між ПБ перспективних та існуючих засобів ГМСЗБ з урахуванням інтенсивності цільового фішингу та інших ЗВШВ

Таким чином, результати досліджень представлені в четвертому розділі підтверджують доцільність використання хмарних систем для покращення функційної безпечності КІ з урахуванням ризиків негативного впливу на активи відповідних інфраструктур. У той же час, кількісні результати аналітико-стохастичного моделювання та оцінювання з визначенням показника гарантоздатності системи SCADA критичної енергетичної інфраструктури за умови застосування ХМС надає можливість отримати виграш від 8,7% до 49,5% (таблиця 4), що сприяє покращенню її готовності. Варіант використання БДСМ та додаткових

хмарних активів як перспективних засобів для ГМСЗБ МРО МКІ також надає можливість покращити рівень функційної та інформаційної безпечності Глобальної морської системи зв'язку та забезпечення безпеки мореплавства.

Основні результати четвертого розділу опубліковано в роботах [4–6, 11, 15, 21, 27, 30, 33, 35, 36, 38, 41].

У п'ятому розділі наведено методи забезпечення готовності КЕІ, які засновані на використанні алгебри ПНК, компаративістичного аналізу та моделюванні процесів протікання аварії інфраструктури. Фактично мета розробки відповідних методів полягає в кількісному оцінюванні та зменшенні ризику КЕІ з урахуванням негативного впливу на фізичні і кібернетичні активи інфраструктури.

Відомо, що аварії КЕІ приводять до великих економічних втрат і тяжких наслідків. В той же час зручний інструментарій для аналізу цих складних негативних подій з оцінкою ризику для КЕІ відсутній. Тому відповідно до запропонованої методології розроблено метод ПНД та метод компаративістичного аналізу (КМПА) аварій КЕІ. На рис. 25 зображено схему алгоритму реалізації етапів обох методів.

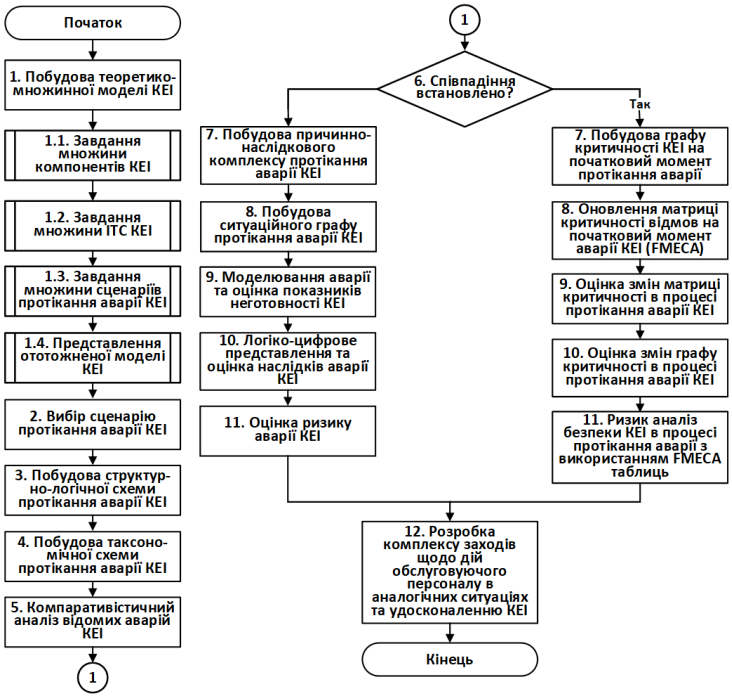


Рис. 25 Схема алгоритму реалізації етапів методів причинно-наслідкової декомпозиції та компаративістичного аналізу аварій КЕІ

Метод компаративістичного аналізу реалізується у формі перехресного аналізу (ПРХА) інформації про відомі аварії критичних енергетичних інфраструктур, тобто у певній послідовності задаються питання, які стосуються аварійної та передаварійної ситуацій. Результати ПРХА оформлюються у вигляді таблиці, за допомогою якої встановлюються співпадіння або їхня відсутність. За умови наявності співпадіння реалізується гілка (рис. 25) 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 аварій КЕІ. На рис. 26 відображено схему ПНК протікання першого етапу однієї з найбільших аварій об'єднаної КЕІ США та Канади (Blackout), яка відбулася в серпні 2003 року.

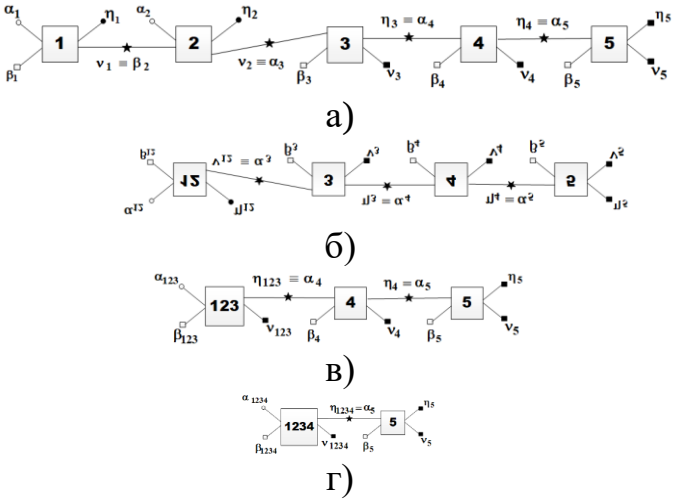


Рис. 26 Схема протікання першого етапу аварії KEI (Blackout): а) загальна схема ПНК; б) згортка 1-ої та 2-ої ланок ПНК; в) згортка 1-ої, 2-ої та 3-ої ланок ПНК; г) згортка 1-ої, 2-ої, 3-ої та 4-ої ланок ПНК

Користуючись схемою протікання першого етапу аварії KEI (рис. 26), була записана наступна послідовність логічних переходів: 1) $\beta_1 \to \nu_1 \equiv \beta_2 \to \nu_2 \equiv \alpha_3 \to \eta_3 \equiv \alpha_4 \to \eta_4 \equiv \alpha_5 \to \eta_5$ – ПНК1; 2) $\alpha_1 \to \eta_1$, $\alpha_2 \to \eta_2$ – причинно-наслідкові ланки (ПНЛ1, ПНЛ2); 3) $\beta_3 \to \nu_3$, $\beta_4 \to \nu_4$, $\beta_5 \to \nu_5$ – умовні ланки (УЛ3–УЛ5). Далі у відповідності до отриманих послідовностей логічних переходів будується ситуаційний граф, який використовується для переходу до аналітико-стохастичного моделювання відповідних негативних подій, які формально описуються за допомогою модифікованого ПНК. Схема трансформації ситуаційного графу в графи станів модельного ряду для аварії KEI відображена на рис. 27. Для отримання відповідної оцінки використовувалися напівмарковські моделі.

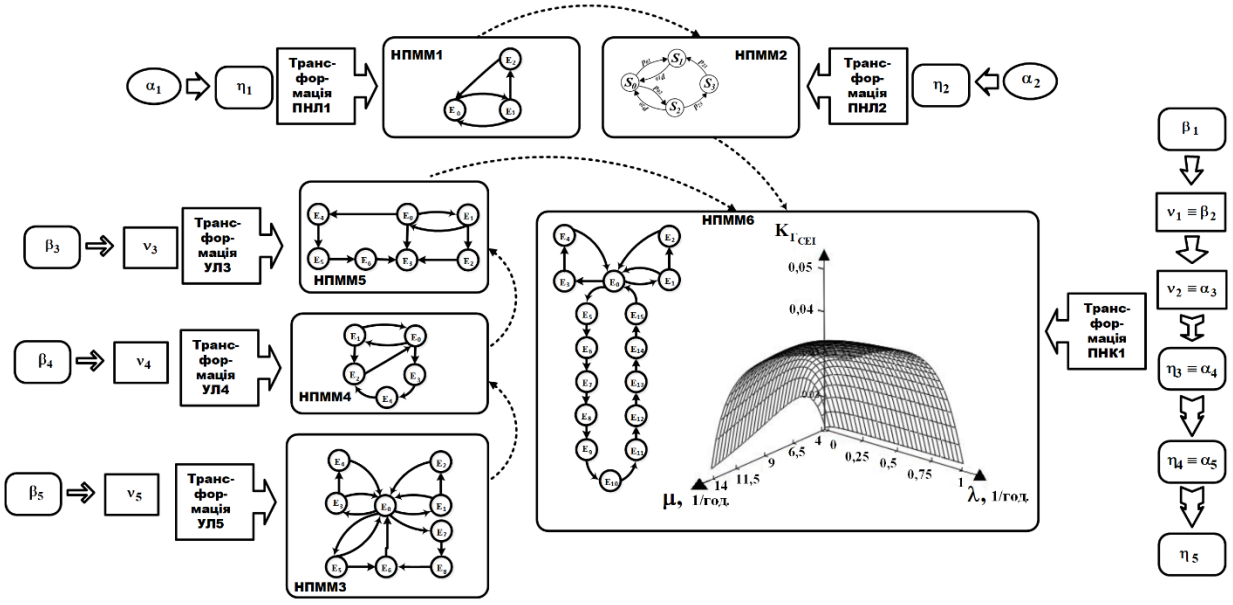


Рис. 27 Схема трансформації ситуаційного графа в графи станів модельного ряду для аварії KEI

Оскільки результати КМПА свідчать, що аварія КЕІ представляє собою складну подію А, яка протікає у вигляді послідовності негативних подій A_i, де $i=1,...,N$, то справедливим є твердження

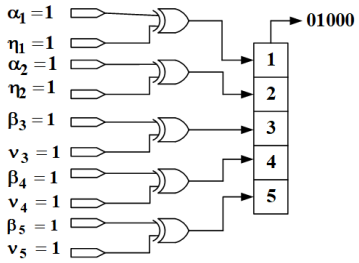
$$P(A)=P\left[\bigcap_{s=1}^{N}\left\{A^s\right\}\right]=\prod_{s=1}^{N}P(A_s). \qquad (7)$$

Враховуючи співвідношення (7), загальна оцінка КГ КЕІ може бути записана у вигляді

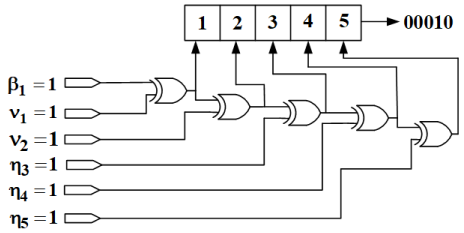
$$K_{\Gamma_{CEI}}=\prod_{j=1}^{m}K_{\Gamma_j}, \qquad (8)$$

де $j=1,...,m$ – сукупність КВО зі складу КЕІ, що знаходяться під впливом s-ої послідовності негативних подій; K_{Γ_j} – стаціонарний коефіцієнт готовності j-го КВО зі складу КЕІ.

На рис. 28 зображено схему реалізації логіко-цифрового представлення (ЛЦП) результатів причинно-наслідкової декомпозиції аварії КЕІ, яка модифікована на основі операції додавання по модулю два XOR та відтворює попередні операції (рис. 26, 27). Оцінка ризику аварії КЕІ з урахуванням результатів аналітико-стохастичного моделювання та ЛЦП (оцінка XOR) отримана відповідно до співвідношення (2) і представлена на рис. 17.



а)



б)

Рис. 28 Схеми ЛЦП ПНД аварії КЕІ: а) для ПНЛ1, 2 та УЛ3–УЛ5; б) для ПНК1

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. Керуючись загальними принципами аналізу та забезпечення безпеки критичної енергетичної інфраструктури, під інформаційно-технічним станом (ITS) інфраструктури будемо розуміти вектор-функцію виду

$$ITS=F(W,S,R,U,Q),$$

де $W=\left\{W_i\right\}_{i=1}^{n}$ – множина завдань, які розв'язуються за допомогою КЕІ; $S=\left\{S_r\right\}_{r=1}^{k}$ – множина компонентних складових (систем), які входять до складу КЕІ; $R=\left\{R_d\right\}_{d=1}^{g}$ – множина режимів експлуатації КЕІ; $U=\left\{U_h\right\}_{h=1}^{e}$ – множина стратегій

управління готовністю КЕІ; $Q = \left\{ Q_j \right\}_{j=1}^{m}$ – множина структур КЕІ, враховуючи варіанти реформування (реструктуризації, тощо).

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 $T_{ж.ц}^{КЕІ} = \max T_{ж.ц}^{КВО}$.

Тому фактично отримані результати моделювання (рис. 17, 27) доцільно використовувати для обґрунтування стратегій U управління готовністю КЕІ за ІТС. Виходячи з цього, було запропоновано дві стратегії, а саме: з централізованим управлінням $U_{ЦУ}$ готовністю КІ, з децентралізованим управлінням $U_{ДЦУ}$ готовністю КІ. При цьому оцінка готовності КІ при управлінні за ІТС здійснювалася за результатами аналітико-стохастичного моделювання поведінки інфраструктури.

Результати досліджень, які представлені в п’ятому розділі, надають можливість отримати кількісні оцінки коефіцієнта готовності КЕІ для випадків аварії інфраструктури і різноманітних негативних впливів на її кібернетичні активи; підтверджують необхідність удосконалення системи моніторингу ІТС щодо виявлення, пом’якшення дії зловмисних впливів на готовність та забезпечення необхідного рівня функційної безпечності інфраструктури.

До того ж 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 ІТС. Наявність ефективно працюючої системи оперативного моніторингу ІТС дозволить проводити постійний аудит активів будь-яких КІ і здійснювати категоризацію та паспортизацію їхніх критично важливих об’єктів за величиною ризику негативного впливу.

Основні результати п’ятого розділу опубліковано в роботах [1, 7–9, 11, 12, 23, 40].

У шостому розділі наведено методи вибору, оцінки характеристик готовності та енергоефективності хмарних систем критичних інфраструктур за результатами аналітико-стохастичного моделювання процесів зміни ІТС фізичних і віртуальних машин, що входять до складу ХМС.

При розробці методу вибору характеристик готовності ХМС КІ враховувалися зв’язки між активами інфраструктури та можливості щодо створення інтегрованої системи оперативного моніторингу ІТС. Як результат запропоновано метод вибору, оцінки та забезпечення характеристик готовності хмарних систем КІ. У якості прикладу була розглянута процедура встановлення ієрархії показників забезпечення готовності КЕІ. Відповідно до отриманої ієрархії оцінка енергоспоживання розглядалася як одна з найважливіших, що впливає на готовність КІ. Тому наступний науковий результат отримано як метод оцінки енергоефективності ХМІ з урахуванням готовності її ФМ та ВМ. На рис. 29 представлено граф станів напівмарковської моделі готовності ХМІ з трьома підсистемами фізичних та

віртуальних машин, яка була використана для отримання оцінок енергоспоживання інфраструктури.

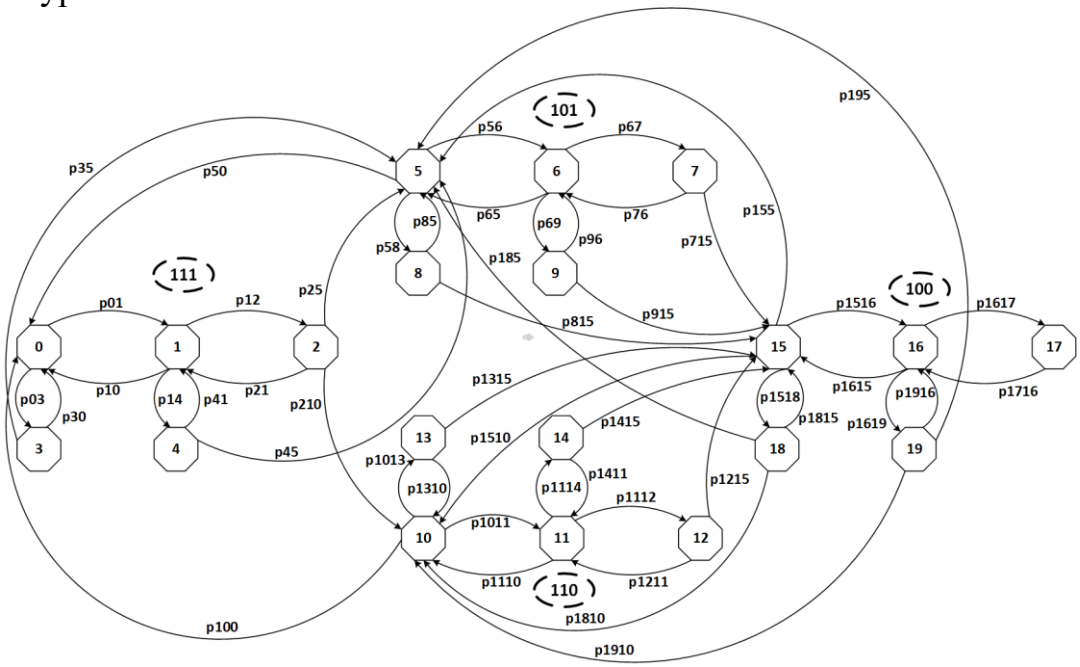


Рис. 29 Граф станів напівмарковської моделі готовності ХМІ з трьома підсистемами фізичних та віртуальних машин

Відповідно до рис. 28 НПММ інфраструктури задавалася наступним чином: $\forall S_i \in S_{A_{IaaS}}$, $S_{A_{IaaS}} = \{S_0, S_1, S_5, S_6, S_{10}, S_{11}, S_{15}, S_{16}\}$ $\exists$ $\pi_A = \{\pi_0, \pi_1, \pi_5, \pi_6, \pi_{10}, \pi_{11}, \pi_{15}, \pi_{16}\}$, $\sum_{i=0}^{N} \pi_i = 1$, де N=19 та $\forall S_j \in S_{UA_{IaaS}}$, $S_{UA_{IaaS}} = \{S_2, S_3, S_4, S_7, S_8, S_9, S_{12}, S_{13}, S_{14}, S_{17}, S_{18}, S_{19}\}$ $\exists$ $\exists$ $\pi_{UA} = \{\pi_2, \pi_3, \pi_4, \pi_7, \pi_8, \pi_9, \pi_{12}, \pi_{13}, \pi_{14}, \pi_{17}, \pi_{18}, \pi_{19}\}$, $S_{A_{IaaS}} \subset S$, $S_{UA_{IaaS}} \subset S$, $S_{A_{IaaS}} \cup \cup S_{UA_{IaaS}} = S$, тоді $\forall S_i \to S_k$ $\exists$ $Q_{ik}(t) \in |Q_{ij}(t)|$. Тоді, згідно методу напівмарковського моделювання готовності ХМІ, діаграма реалізації якого представлена на рис. 8, КГ інфраструктури визначається як

$$K_{\Gamma_{IaaS}} = \pi_0 + \pi_1 + \pi_5 + \pi_6 + \pi_{10} + \pi_{11} + \pi_{15} + \pi_{16}. \quad (9)$$

На наступному етапі на основі використання напівмарковської моделі готовності (рис. 29) визначається показник енергоспоживання інфраструктури TPC_{IaaS}. Розрахунки виконуються за допомогою такого співвідношення:

$$TPC_{IaaS} = K_{\Gamma_{IaaS}} \sum_{x=0}^{n_h} \sum_{y=0}^{n_w} \sum_{z=0}^{n_c} TPC(x, y, z), \quad (10)$$

де n_h, n_w, n_c – кількість фізичних машин гарячої, теплої та холодної підсистем ХМІ; $TPC(x, y, z)$ – енергоспоживання фізичних машин гарячої, теплої та холодної підсистем ХМІ.

У співвідношенні (10) складова $K_{\Gamma_{IaaS}}$ розраховується за допомогою співвідношення (9). Порівняльну характеристику результатів моделювання для двох типів серверних систем, на основі яких розгортається хмарна інфраструктура і отримується відповідний хостинг, наведено в таблиці 5.

Таблиця 5

Порівняльна характеристика результатів моделювання для двох типів серверних систем, що входять до складу ХМІ

Продуктивність		Потужність		Співвідношення між продуктивністю та потужністю без урахування 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% 50%	29003230 14578560	2295 1120	2289 1117	12638 13017
для п’яти серверів Dell Inc. PowerEdge R940				
100% 50%	57644020 28892060	4575 2185	4562 2179	12600 13223

Результати, які відображено в шостому розділі, мають важливе науково-прикладне значення з точки зору покращення показників енергоефективності ХМІ і можуть бути використані для обґрунтування їхніх граничних значень. Розв’язування цієї проблеми здійснювалося шляхом вибору відповідних показників готовності та енергоспоживання ХМІ з декількома підсистемами фізичних та віртуальних машин.

Основні результати шостого розділу опубліковано в роботах [3, 14, 16, 18, 22, 24, 25].

У сьомому розділі розглянуто ІТ тестування регіональних ХМС з інтегрованими фізичними компонентами з метою вибору інформаційного центру (ІЦ) відповідного хмарного провайдера (ХМПР). Створена ІТ тестування реалізована у вигляді наступних кроків: 1) планування експерименту щодо оцінювання часу затримки потоків даних; 2) розробка процедури тестування інформаційних центрів ХМПР; 3) вибір ІЦ ХМПР за критерієм мінімуму часу затримки тунельного (захищеного) каналу зв’язку. При плануванні експерименту використовується приймально-передавальна система, яка складається з трьох модулів, а саме: модуля моделювання та аналізу даних (ММД), модуля передачі даних (МПД), модуля прийому та ретрансляції даних (МПРД). Відповідно до спрощеної схеми проведення експерименту, яка відображена на рис. 30, модулі утворюють контур обміну потоками даних зі зворотнім зв’язком.

Рис. 30 Спрощена схема проведення експерименту

Для моделювання даних розроблено хмарний симулятор, за допомогою якого отримано експериментальні дані щодо часу затримки генеруємого потоку даних (ПД) від штучно створеного віртуального ресурсу, що імітує функціонування хмари. Час затримки визначався з використанням наступного співвідношення:

$$\Delta t = t_{timestamp\_returning} - t_{timestamp\_sending}, \quad (11)$$

де $t_{timestamp\_sending}$ – час передачі ПД; $t_{timestamp\_returning}$ – час прийому ПД.

Значення Δt у відповідності зі співвідношенням (11) записувалися до віртуальної реляційної бази даних, що працювала в режимі “клієнт–сервер”. Результати оцінювання часу затримки відповідних ПД відображено на рис. 31.

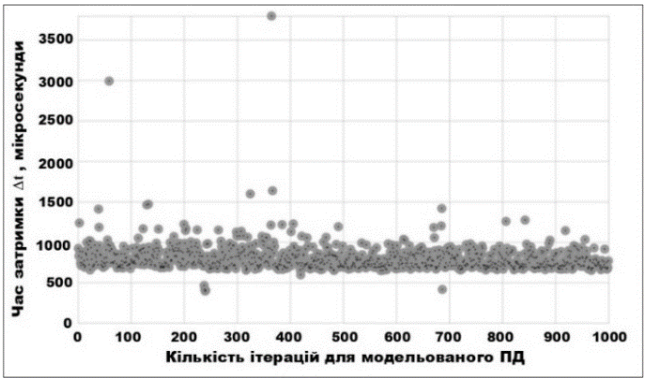


Рис. 31 Залежність часу затримки від кількості ітерацій модельованого ПД

Відповідно до рис. 31 встановлено, що величина часу затримки Δt змінюється в інтервалі від 595 мкс. до 1076 мкс. На рис. 32 представлено результати тестування (мкс.) сервіс-орієнтованих ресурсів в режимі “клієнт–сервер”, отриманих з застосуванням запропонованої ІТ.

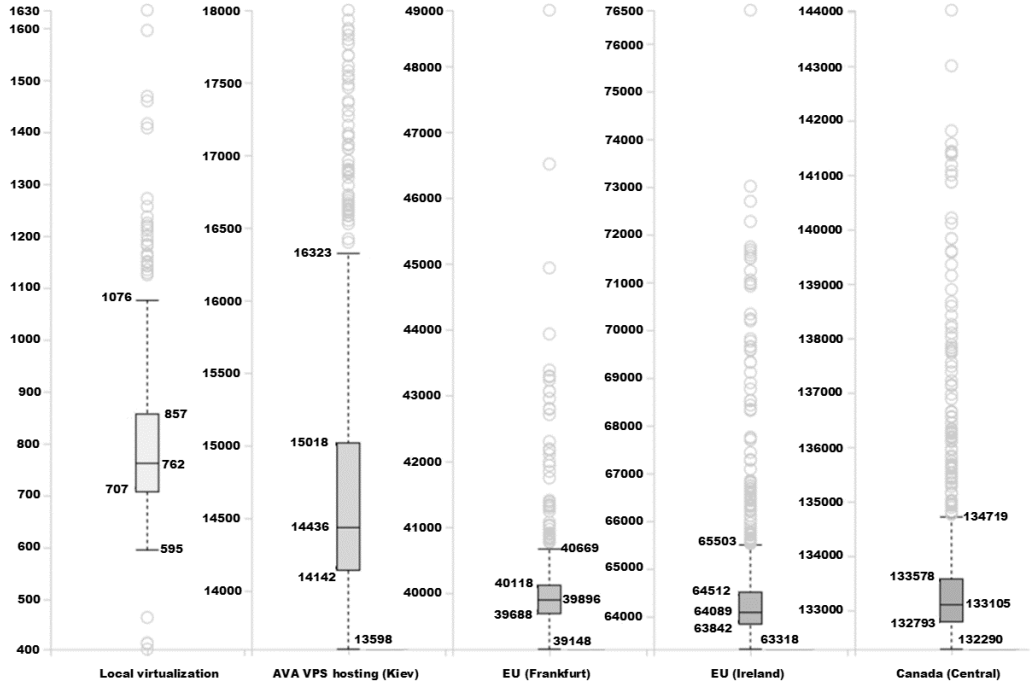


Рис. 32 Результати тестування локального віртуального сервісу (Virtual Box), AVA VPS хостінгу (м. Київ) та трьох ІЦ Amazon EC2 (мкс.)

Таблиця 6

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
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

Далі завдання вирішувалося у відповідності з критерієм мінімуму часу затримки тунельного (захищеного) каналу зв'язку, який записується у вигляді

$$\Im = \begin{cases} K_{\Gamma_{ЩІ}}(T) \geq K_{\Gamma_0}; \\ \Delta t \longrightarrow \min; \\ C_{\min_0} \leq C_0 \leq C_{\max_0}; \end{cases} \qquad (12)$$

де $K_{\Gamma_{ЩІ}}(T)$ – коефіцієнт готовності ІЦ конкретного ХМПР за час застосування за призначенням Т.

Підводячи підсумки, можна відзначити, що 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», 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 (12) найкращим є ІЦ Amazon EC2, який розташовано у Франкфурті (Німеччина).

Таким чином, матеріали досліджень, які представлено в сьомому розділі, надали можливість визначити і підтвердити практичну цінність отриманих наукових результатів щодо забезпечення готовності ХМС КІ. Універсальний характер розробленої ІТ дозволяє застосовувати її для комплексного вирішування завдань щодо тестування та вибору найкращих сервіс-орієнтованих ресурсів в першу чергу для КЕІ. Подальші перспективи використання запропонованої ІТ пов'язані з дослідженнями щодо створення сучасної кіберенергетичної інфраструктури.

Основні результати сьомого розділу опубліковано в роботах [1, 2, 16, 20, 24, 26, 29, 34].

ВИСНОВКИ

У дисертаційному дослідженні розв’язана актуальна науково-прикладна проблема, яка дозволяє усунути протиріччя між існуючою методологічною базою щодо оцінювання готовності КІ та тенденціями розвитку методів, технологій, вибору відповідних характеристик сервіс-орієнтованих хмарних ресурсів (систем) для забезпечення функційної безпечності інфраструктур. Зокрема, за результатами проведених досліджень можна зробити наступні висновки.

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 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)*.

АНОТАЦІЯ

Іванченко О. В. Методологічні основи та інформаційна технологія забезпечення готовності хмарних систем критичних інфраструктур. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології. – 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.

Дисертаційна робота присвячена вирішенню важливої науково-прикладної проблеми усунення протиріччя між існуючою методологічною базою щодо оцінювання готовності критичних інфраструктур та тенденціями розвитку методів, технологій, вибору відповідних характеристик сервіс-орієнтованих хмарних ресурсів (систем) для забезпечення функційної безпечності інфраструктур.

Основу дисертаційного дослідження складають методи оцінювання та забезпечення готовності хмарних систем критичних інфраструктур при відмовах і атаках на вразливості. У якості математичного апарату застосовувалися підходи щодо побудови аналітико-стохастичних, напівмарковських моделей поведінки хмарних систем критичних інфраструктур під час негативного впливу на їхні активи.

Запропонована методологія дозволить підвищити функційну та інформаційну безпечність критичних інфраструктур з урахуванням ризику негативного впливу на їхні фізичні та кібернетичні активи. Застосування хмарних систем у контурі управління та моніторингу інформаційно-технічних станів критичних інфраструктур покращить їхню готовність. Практичне значення одержаних результатів полягає в тому, що розроблені методи, моделі є підґрунтям для створення та імплементації інформаційної технології тестування регіональних інформаційних центрів хмарного провайдера. Впровадження запропонованих методів, моделей, інформаційної технології дозволить створювати гарантоздатні хмарні системи критичних інфраструктур з недостатньо надійних, безпечних інтегрованих фізичних (віртуальних) компонентів в умовах негативних впливів та виконувати категоризацію критично важливих об'єктів за рівнем ризику негативного впливу.

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

ABSTRACT

Ivanchenko O. V. Methodological foundations and information technology for availability assurance of cloud systems of critical infrastructures. – Manuscript.

Thesis for a Doctor Degree of Technical Sciences in specialty 05.13.06 – Information technologies. – National Aerospace University "Kharkiv Aviation Institute of the Ministry of Education and Science of Ukraine; V. N. Karazin Kharkiv National University of the Ministry of Education and Science of Ukraine. – Kharkiv, 2021.

The thesis research deals with solution of an important scientific and applied issue pertaining to eliminating the contradiction between the existing methodological base for assessing the availability of critical infrastructures and trends in the development of methods, technologies, and selection of the appropriate characteristics for service-oriented cloud resources (systems) in order to ensure the safety of the infrastructures.

The first section comprehensively covers a problem of ensuring and estimation of availability level for cloud systems of the critical infrastructures. 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. 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. 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. 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 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. This method can be used in order to evaluate and formulate recommendations for reducing the risk of negative events for the critical infrastructure.

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 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. 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 methods of assessment, ensuring the availability of cloud systems of critical infrastructures in case of failures and attacks on vulnerabilities are basis of the thesis research. As a mathematical toolkit was used to construct analytical and stochastic models, Semi-Markov models of the behavior of cloud systems of critical infrastructures during a negative impact on their assets.

The proposed methodology will improve the safety and security of critical infrastructures, taking into account the risk of negative impact on their physical and cybernetic assets. The usage of cloud systems in the control and monitoring loop of information and technical states of critical infrastructures will improve their availability, too. The practical significance of the obtained results lies in the fact that the developed methods and models are the basis for the creation and implementation of an testing information technology for regional information centers of a concrete cloud provider. The introduction of the proposed methods, models and information technology is based on the use of modern monitoring tools will make it possible to create reliable cloud systems of critical infrastructures from insufficiently reliable integrated physical (virtual) components in conditions of negative impacts and can as well help performing the categorize procedure for the critical objects considering the level of risk for negative impact.

Key words: cloud systems, critical infrastructures, analytical and stochastic modeling process, semi-Markov models, risk for negative impacts, testing information technology.

Підписано до друку 05.03.2021.
Формат 60 х 90/16. Друк ризографічний.
Гарнітура Times New Roman
Зам. 2632/2021. Ум. Вид. арк. 0.9.
Тираж 100 прим. Ціна договірна.

Надруковано ФОП Видавець А.Б.
м. Харків, вул. Видавнича, 3001, офіс 1001.
Свідоцтво про державну реєстрацію ВОО № 12345 від 18.12.2017.