DOI: https://doi.org/10.32836/2521-6643-2020.1-59.2
УДК 629.039.58: 681.518.22

О. В. Іванченко, кандидат технічних наук, доцент, доцент кафедри транспортних систем та технологій Університету митної справи та фінансів

АНАЛІТИКО-СТОХАСТИЧНА МОДЕЛЬ ГАРАНТОЗДАТНОСТІ КІБЕРНЕТИЧНИХ ТА ХМАРНИХ АКТИВІВ СИСТЕМИ SCADA КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Аналіз сучасних тенденцій розвитку, застосування за призначенням систем диспетчерського управління та збору даних (SCADA) критичних інфраструктур (КІ) свідчить про необхідність розробки методологічних основ забезпечення гарантоздатності їхніх активів. Підставою для цього є постійно зростаючий рівень загроз кібернетичним активам SCADA, які з метою покращення пропускної спроможності, можливостей щодо створення резервних копій, здатності до аварійного відновлення та швидкодії було доповнено відповідними хмарними обчислювальними системами і технологіями. Використання комплексного підходу щодо вирішення проблеми, пов'язаною з оцінкою рівня готовності, безпеки кібернетичних та хмарних активів SCADA КІ при відмовах і атаках на вразливості розглядається як один з найважливіших науково-дослідницьких чинників в пропонуємій до розгляду статті. Саме тому побудова аналітико-стохастичної моделі гарантоздатності лежить в основі розробляємої процедури оцінювання, яка реалізується у відповідності зі сценаріями зловмисних шкідливих впливів на кібернетичні та фізичні активи системи SCADA КІ.

Ключові слова: *архітектурна реалізація SCADA КІ, кібернетичні та хмарні активи, напівмарковське моделювання.*

Анализ современных тенденций развития, использования по назначению систем диспетчерского управления и сбора данных (SCADA) критических инфраструктур (КИ) свидетельствует о необходимости разработки методологических основ обеспечения гарантоспособности их активов. Основание для этого – возросший уровень угроз кибернетическим активам SCADA, которые с целью улучшения пропускной способности, возможностей по созданию резервных копий, аварийному восстановлению и быстродействию были дополнены соответствующими облачными системами и технологиями. В предлагаемой к рассмотрению статье использование

подхода к решению проблемы, связанной с оценкой уровня готовности, безопасности кибернетических и облачных активов SCADA КИ при отказах и атаках на уязвимости рассматривается как одна из важнейших научно-исследовательских задач. Именно поэтому построение аналитико-стохастической модели гарантоспособности лежит в основе разрабатываемой процедуры оценивания, которая реализуется в соответствии со сценариями злонамеренных вредоносных воздействий на кибернетические и облачные активы системы SCADA КИ.

Ключевые слова: *архитектурная реализация SCADA КИ, кибернетические и облачные активы, полумарковское моделирование.*

Methodological provisions pertaining to necessary a dependability assurance of supervaisory control and data acquisition systems (SCADA) for critical infrastructures is based on analysis of contemporary development trend and operational usage of these systems. At the same time, an increased cyber threats level of the SCADA systems is prooved that developers and service personnel should improve bandwidth, disaster recovery and backup procedures of these systems. The issue can be eliminated by them based on the use of additional cloud systems and technologies. In the proposed paper, usage of a comprehensive approach in order to solve concerns relating to availability, safety of the cyber and cloud assets for SCADA of critical infrastructures is considered as one of the most important scientific task. Which is why the proposed analytical and stochastic dependability models are basis for a developing assessment procedure for SCADA of the critical infastructures, which can be implemented by researchers according to a deliberate malicious impact scenario on assets of SCADA for critical infrastructures. It means that before begin to SCADA system developers and researchers will perform quite deep analysis based on a scientific study. Since how to determine dependability assessment for the SCADA system is an important issue that to be studied. Therefore, developers, service personnel and scientists should work together in order to create effective functioning protection system for cyber and cloud assets of SCADA. In addition, the service personnel should leverage especial cyber protection systems, devices and applications such as, firewalls, password cyberprotection subsystems etc. The author proposes to get more modeling numerical results based on the use of Markov Modeling Process. In fact, the modeling process was carried out in two parts. First part has included a building process of save and secure block diagram for cyber and cloud assets considering different types of deliberate malicious impacts. Second part was being devoted to the implementation Semi-Markov Modeling Process based on the use of overall architecture of the SCADA system.

Keywords: *architectural implementation for SCADA of a critical infrastructure, cyber and cloud assets, Semi-Markov Modeling Process.*

Постановка проблеми. Характерною особливістю сьогодення є постійно зростаючий рівень загроз для систем (об'єктів) критичної інфраструктури (КІ). Зокрема, це стосується компонентів, що утворюють контур управління КІ. Сучасні системи диспетчерського управління та збору даних (SCADA) слід розглядати як один з основних компонентів цього контуру. Тому по відношенню до системи SCADA КІ теж існують певні загрози, які реалізуються через її кібернетичні активи.

Крім того, зростання складності та масштабів завдань для КІ, які вирішуються за допомогою SCADA, викликає необхідність обробки великих обсягів інформації на основі застосування додаткових обчислювальних ресурсів і сервісів. Одним з напрямків вирішення цієї проблеми є використання хмарних обчислювальних систем, які утворюють відповідні активи.

Аналіз відомих загроз і наслідків багатьох негативних подій по відношенню до кібернетичних активів SCADA КІ, а також до хмарних систем відповідних провайдерів свідчить про великий рівень невизначеності, що виникає при урахуванні аспектів готовності, гарантоздатності та кібербезпеки. Для зменшення цієї невизначеності доцільно отримати результати моделювання поведінки кібернетичних та хмарних активів SCADA КІ при негативних шкідливих впливах.

Аналіз останніх досліджень і публікацій. Відомі методи моделювання поведінки складних систем лежать в основі методичного апарату оцінки рівня їхньої готовності та гарантоздатності. Ці методи можуть також бути використані щодо моделювання атак на кібернетичні та хмарні активи системи SCADA КІ. Серед них особливо слід виділити метод дерева відмов (МДВ), який широко застосовується для моделювання поведінки промислових об'єктів під час атак та для розв'язування задач з інженерії надійності [1].

В 90-х роках минулого століття як продовження МДВ було винайдено метод дерева атак [2], який все частіше почав використовуватися для моделювання зловмисних шкідливих впливів (ЗВШВ) в двадцять першому столітті. Моделювання ЗВШВ методом дерева атак здійснювалося з використанням спеціалізованих мов програмування UMLsec [3] та SysMLsec [4].

Важливу роль при моделюванні ЗВШВ грає знання вразливостей та точок докладення атак на кіберактиви. Всі ці аспекти враховуються та аналізуються при визначенні атрибутів дерева атак [5,6].

Наявність хмарних активів в системі управління КІ створює нові загрози функціональній та інформаційній безпеці критичній інфраструктурі в цілому [7]. Необхідно знати місце, роль хмарних активів в загальній архітектурі SCADA та як вони впливають на гарантоздатність системи, інфраструктури в цілому. В цьому контексті важливо встановити баланс між фізичиним, кібернетичними та хмарними активами системи SCADA та визначити їхній рівень готовності. Для розв'язування цієї досить складної задачі слід застосовувати апарат аналітико-стохастичного моделювання кібератак на системи (об'єкти) КІ, який використовувався в роботах [8–10].

Серед загального модельного ряду значну частину складають ймовірнісні моделі надійності програмного забезпечення (ПЗ), яке належить до кібернетичних активів КІ. Системний обзор моделей ПЗ, яке затосовується в системах управління об'єктами атомної енергетики, включаючи марковські моделі, комбінаторні моделі, моделі Байєса, Гоуела-Окумото, представлено в роботі [11]. З цієї точки зору, у дослідників в сфері забезпечення відмовостійкості ПЗ КІ з урахуванням терміну використання програмного забезпечення певний інтерес можуть викликати роботи [12,13].

Відомо, що для оцінки гарантоздатності хмарних активів SCADA КІ застосовуються різноманітні підходи. Наприклад, один з підходів базується на дослідженнях в сфері енергоефективності інформаційних центрів (ІЦ) відповідних хмарних провайдерів. Зокрема, в роботах [14,15] розглядаються моделі енергоспоживання хмарного ІЦ та хмарних систем (ХМС) з урахуванням необхідного обсягу енергії щодо розв'язування конкретних завдань. Теорія масового обслуговування лежить в основі запропонованих моделей.

Досить широке застосування знайшли стохастичні мережі Петрі (СМП) як для моделювання поведінки, так і для оцінки показників ефективності хмарних обчислювальних систем. В роботі [16] моделі на основі застосування СМП використовуються для обчислення деяких метрик продуктивності публічної мобільної хмари.

Мета статті. Виходячи з зазначеного, актуальною задачею є створення науково-методичного апарату моделювання поведінки системи SCADA КІ з урахуванням негативного впливу на її активи. Фактично мета статті полягає

в розробці аналітико-стохастичної моделі готовності кібернетичних та хмарних активів SCADA КІ при відмовах і атаках на їхні вразливості. Оцінка готовності SCADA КІ, яка враховує ЗВШВ на відповідні активи може бути використана для спільного забезпечення гарантоздатності хмарних систем і критичних інфраструктур, оперативного моніторингу, оцінювання стану, захисту фізичних і кібернетичних активів при відмовах і атаках на вразливості.

Виклад основного матеріалу. Як наочний приклад розглянемо процес функціонування SCADA у складі системи управління критичної енергетичної інфраструктури (КЕІ). На рис. 1 представлено компоненти КЕІ, які визначають основні функції енергетичної інфраструктури. Система SCADA відповідає за якісне виконання трьох функцій КЕІ, а саме: транспортування, розподілення, споживання.

Спираючись на загальну концепцію забезпечення гарантоздатності SCADA КІ, розглянемо методологічні основи ризик-аналізу негативного впливу на активи критичної енергетичної інфраструктури. Таксономію методу оцінювання функціональної безпеки КЕІ з урахуванням ризику негативного впливу на її активи, до складу яких входять фізичні (ФА), кібернетичні (КА) та хмарні (ХМА) активи, зображено на рис. 2. На думку автора, аналогічний підхід, інструментарій реалізації якого описано в роботі [17], можна застосовувати для оцінювання гарантоздатності системи SCADA КІ за умови дії зловмисних шкідливих впливів на її активи.

У ракурсі визначення перспектив подальшого розвитку розглянемо можливість спільного застосування SCADA КЕІ та ХМС, які водночас утворюють відповідні активи, тобто ХМА. Наприклад, в роботі [18] розглянуто можливість створення хмарно-орієнтованої мікросервісної платформи SCADA щодо покращення виконання функцій по збору, зберіганню, аналізу, обробці, відображенню інформації та відповідні переваги такої архітектурної реалізації при розв’язуванні завдань по віддаленому аварійному відновленню, створенню резервних копій і еластичному управлінню обчислювальним навантаженням.

Рис. 1. Основні компоненти критичної енергетичної інфрастуктури [19]

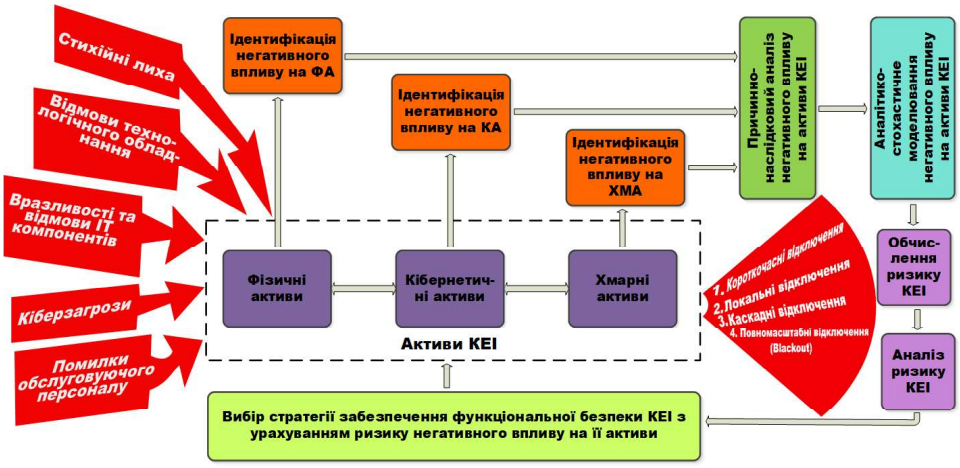

Рис. 2. Таксономія методу оцінювання функціональної безпеки КЕІ з урахуванням ризику негативного впливу на її активи

Важливим аспектом застосування за призначенням в структурі системи управління КЕІ є розподілення функцій енергоінфраструктури між фізичними, кібернетичними та хмарними активами SCADA. До вирішення цієї задачі необхідно підійти комплексно, враховуючи розширення функцій SCADA КЕІ щодо аварійного відновлення, резервного копіювання та зберігання інформації за рахунок застосування ХМС. Залучення активів системи SCADA щодо виконання основних функцій КЕІ представлено в табл. 1.

Таблиця 1.

Залучення активів системи SCADA щодо виконання основних функцій КЕІ

Функції КЕІ	Активи SCADA КЕІ		
	ФА	КА	ХМА
Транспортування	+	+	–
Розподілення	+	+	+
Споживання	–	+	+

В табл. 2 представлено результати порівняльного аналізу можливостей різних типів активів хмарних систем, критичної енергетичної інфраструктури та системи SCADA з ХМС, яка входить до контуру управління КЕІ щодо виконання аварійного відновлення, резервного копіювання та зберігання інформації. На підставі виконаного аналізу розширюються можливості щодо побудови аналітико-стохастичної моделі готовності кібернетичних та хмарних активів SCADA КІ, яка враховує як різноманітні відмови, так і ЗВШВ.

Таблиця 2.

Аналіз можливостей активів КЕІ, ХМС та SCADA

Типи активів систем та інфраструктур		Функції відновлення та зберігання інформації		
		Аварійне відновлення	Резервне копіювання	Зберігання інформації
КЕІ	ФА	–	–	–
	КА	–	+	+
ХМС	ФА	–	+	–
	КА	+	+	+
SCADA КЕІ з ХМС	ФА	–	+	–
	КА	+	+	+

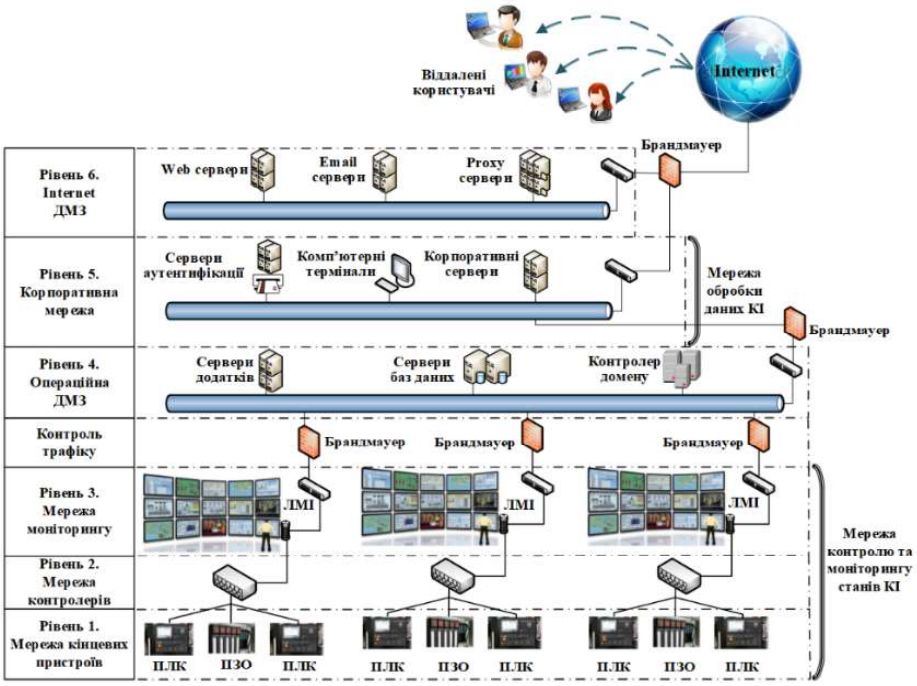

Рис. 3. Архітектура ФА та КА системи SCADA КІ для мережевого рівня їхньої реалізації [20]

Розглянемо яким чином можна побудувати пропонуєму модель на основі архітектурної реалізації об'єкта дослідження. На рис. 3 представлена архітектура фізичних та кібернетичних активів системи SCADA КІ для мережевого рівня їхньої реалізації. Будемо вважати, що на систему SCADA КІ, архітектура якої представлена на рис. 3, здійснюється атака за певним сценарієм з використанням ЗВШВ на її фізичні та кібернетичні активи. Припустимо, що у відповідності зі сценарієм, враховуючи результати відомого досвіду ЗВШВ на ФА та КА національної критичної енергоінфраструктури [21], атака реалізується в декілька етапів, а саме:

1) на першому етапі здійснюється цільовий фішинг (ЦФ);

2) на другому етапі можливе розкриття інформації (РЗІ) внаслідок здійснення ЦФ;

3) на третьому етапі система може бути цілковито скомпрометована за рахунок фальсифікації (ФСФ) та підміни інформації (ПДМ).

На рис. 4–8 зображено діаграми зловмисних шкідливих впливів на ФА та КА системи SCADA КІ, які реалізуються згідно описаного сценарію.

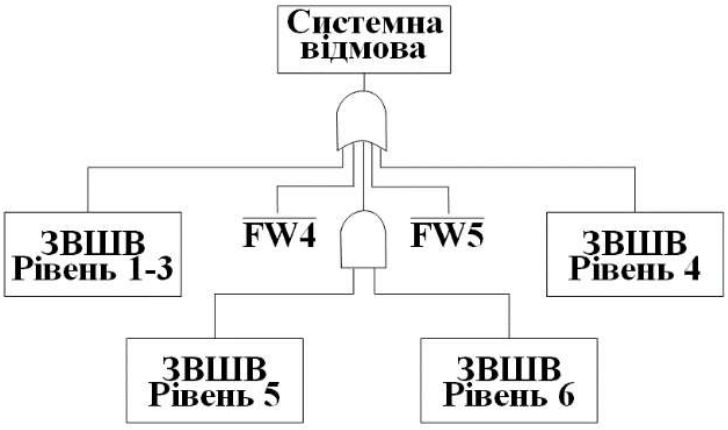

Рис. 4. Діаграма ЗВШВ на ФА та КА системи SCADA КІ

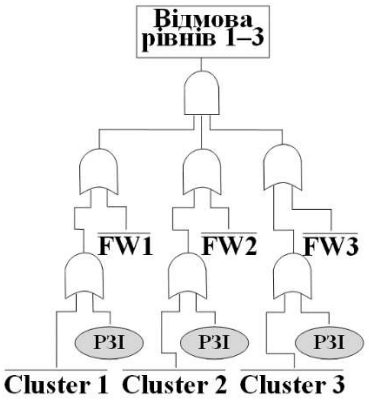

Рис. 5. Діаграма ЗВШВ на перший, другий та третій мережеві рівні SCADA КІ

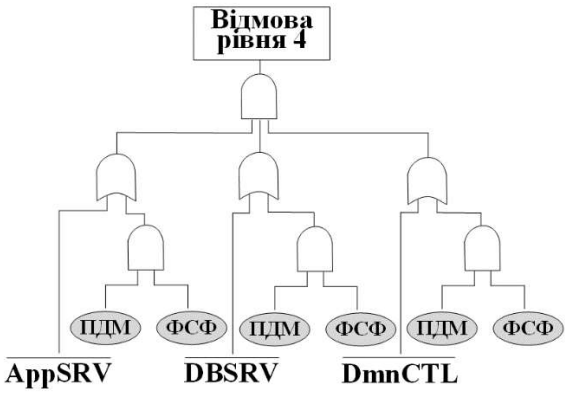

Рис. 6. Діаграма ЗВШВ на четвертий мережевий рівень SCADA КІ

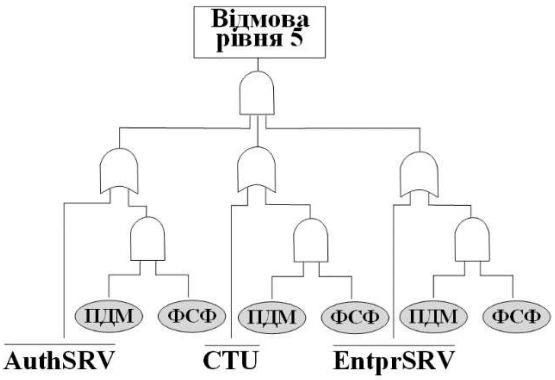

Рис. 7. Діаграма ЗВШВ на п’ятий мережевий рівень SCADA КІ

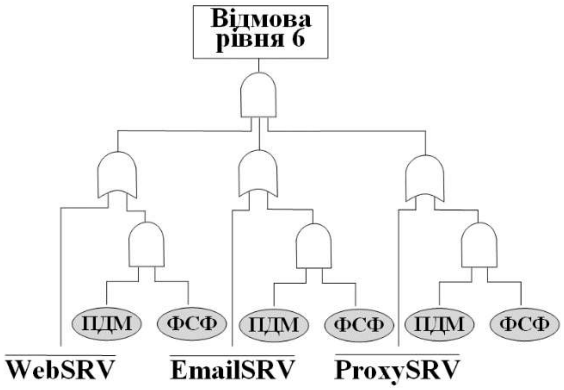

Рис. 8. Діаграма ЗВШВ на шостий мережевий рівень SCADA КІ

Всього передбачається розглянути п’ять можливих сценаріїв здійснення ЗВШВ. Відповідно на рис. 5–8 відображено діаграми для першого сценарію. Характеристика видів ЗВШВ представлена в табл. 3. Загальний аналіз наслідків ЗВШВ на активи системи SCADA КІ з урахуванням зазначених сценаріїв (рис. 4–12) виконано в табл. 4.

Згідно рис. 5, 9–12 перший, другий, третій кластери, відповідно позначені як Clusters 1–3, утворюються шляхом об’єднання елементів мережі контролю та оперативного моніторингу станів КІ (рис. 3) системи SCADA. Для подальшої розбудови аналітико-стохастичної моделі та отримання результатів моделювання необхідно розглянути чотири важливих припущення, які стосуються узгодженості сценаріїв реалізації ЗВШВ з архітектурною побудовою активів системи SCADA КІ і урахуванням відповідних мережевих рівнів, а саме:

1) перший сценарій ЗВШВ реалізується для архітектури системи SCADA КІ, яка представлена на рис. 3;

2) другий, третій, четвертий, п’ятий сценарії ЗВШВ реалізуються для перспективної архітектури фізичних, кібернетичних та хмарних активів системи SCADA КІ, яку відображено на рис. 13;

3) функції АВД та РКП дозволяють повністю усунути наслідки ЗВШВ;

4) ХМС відносяться до відмовостійких систем з четвертим рівнем готовності по шкалі HAL (High Availability Level), тобто їхній коефіцієнт готовності не менше ніж 0,9999 [22].

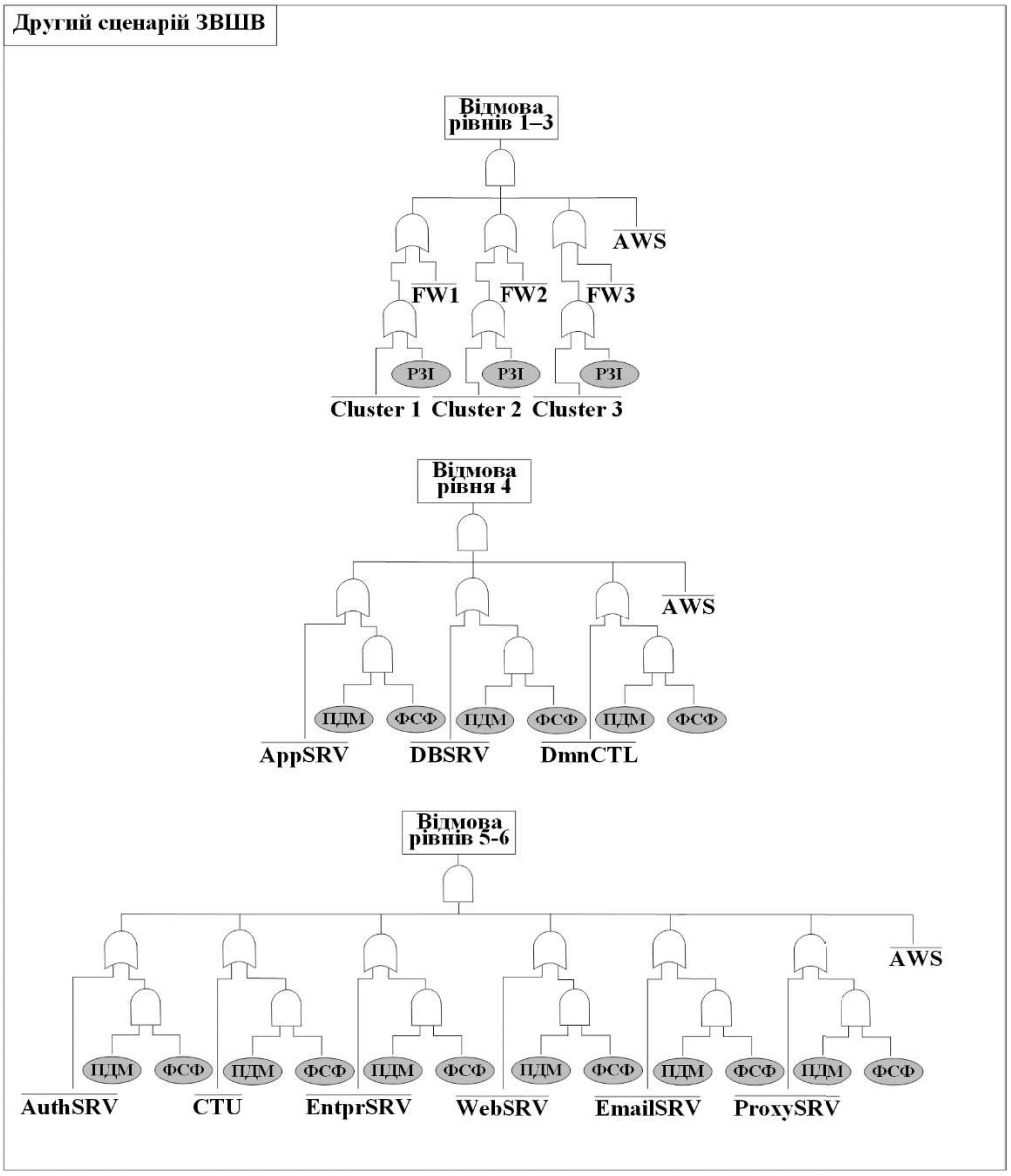

Рис. 9. Другий сценарій ЗВШВ на активи систми SCADA КІ

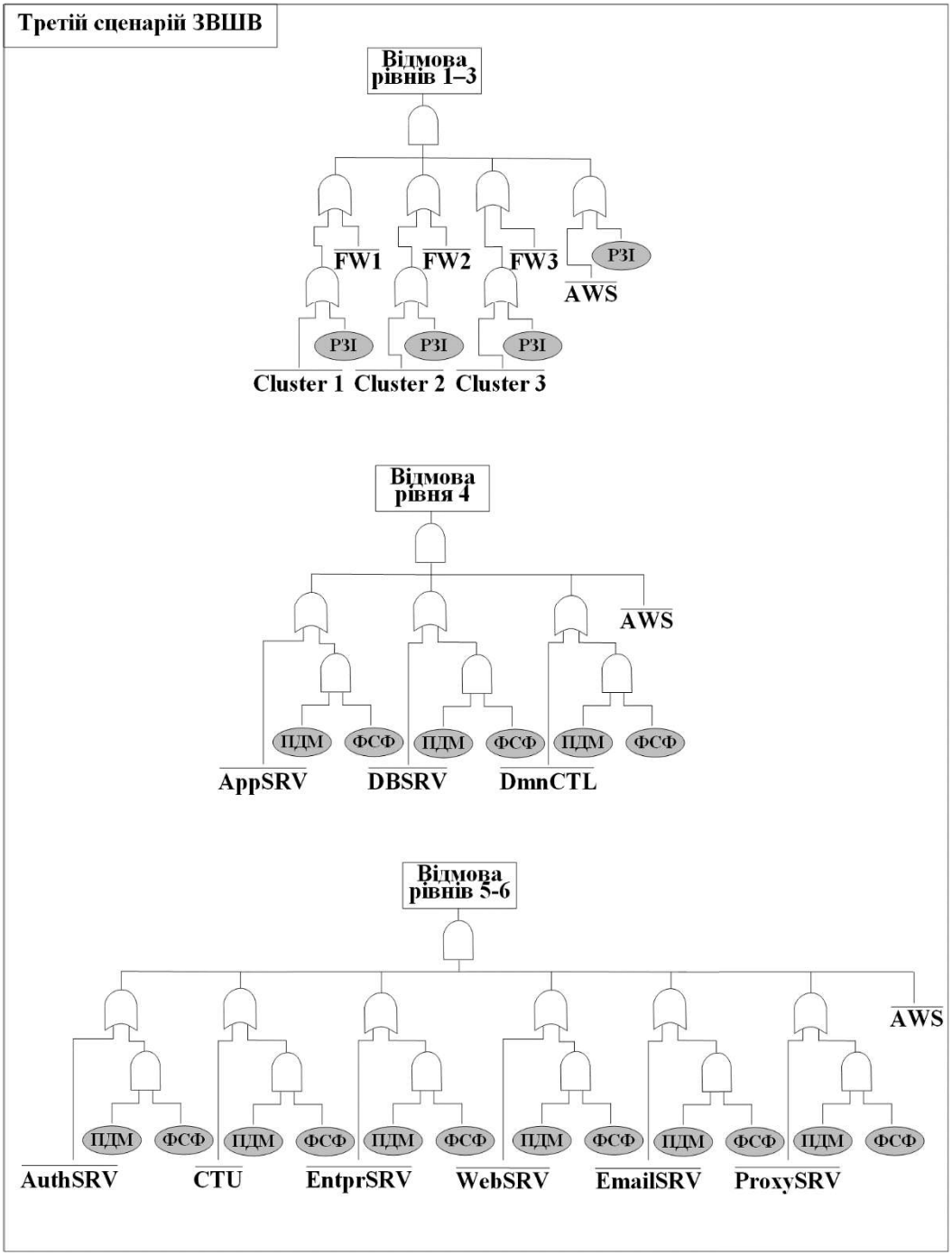

Рис. 10. Третій сценарій ЗВШВ на активи систми SCADA КІ

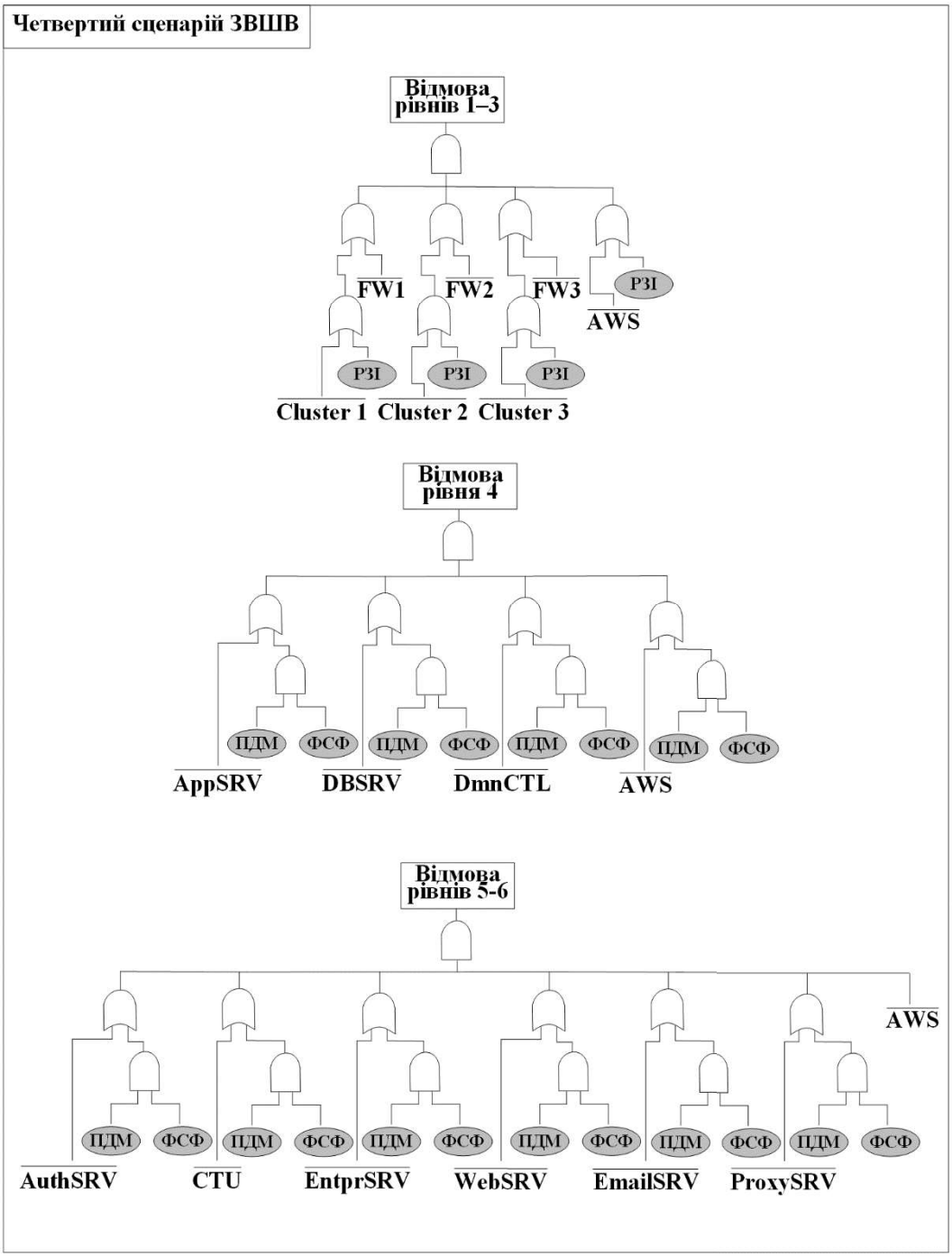

Рис. 11. Четвертий сценарій ЗВШВ на активи систми SCADA КІ

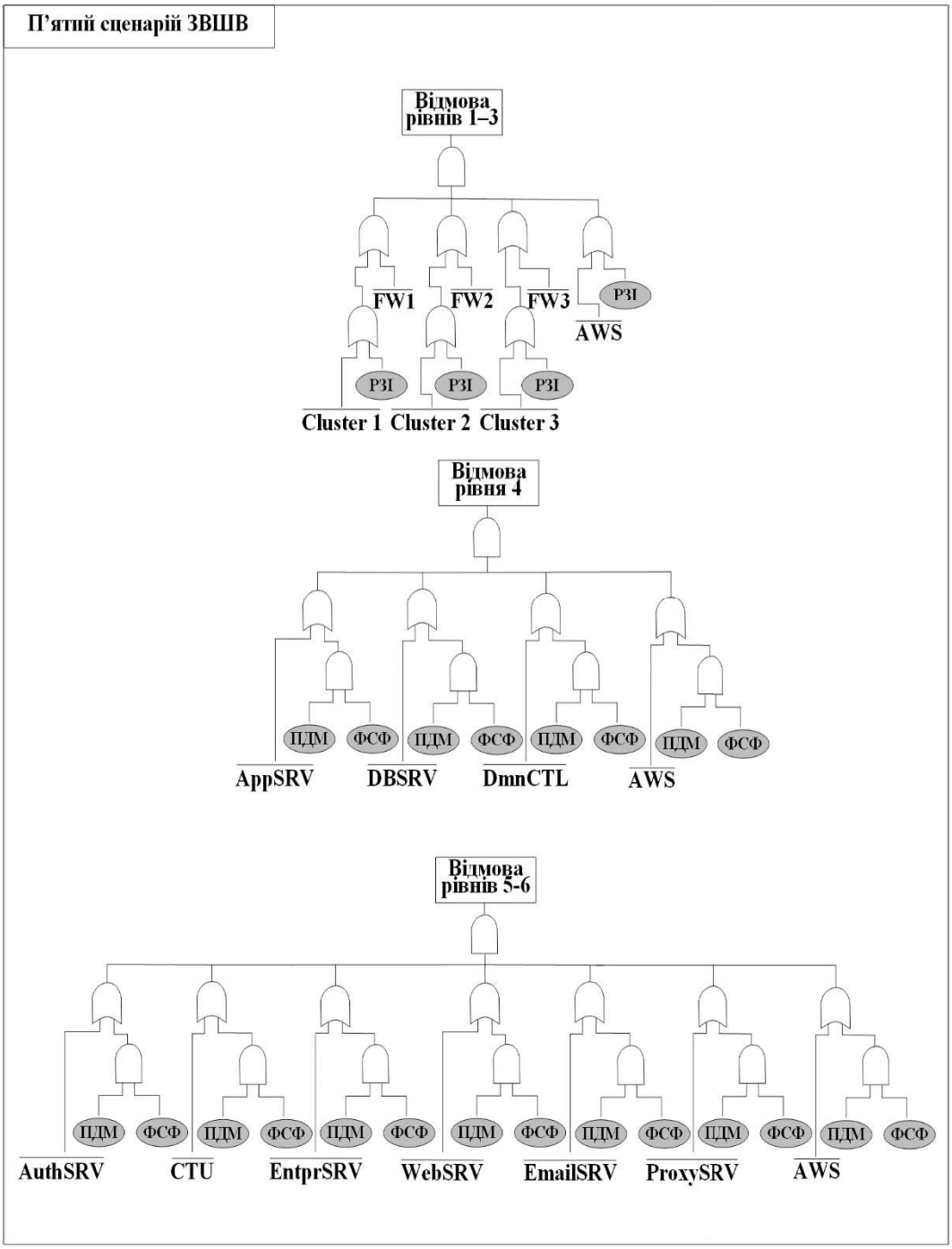

Рис. 12. П'ятий сценарій ЗВШВ на активи систми SCADA КІ

Таблиця 3.

Характеристика видів ЗВШВ на активи системи SCADA КІ

Вид ЗВШВ	Загальна характеристика
Розкриття інформації (РЗІ)	1. Здійснюється ЦФ шляхом збору, обробки та аналізу службової інформації корпоративних мереж КІ, включаючи моніторинг інформації, яка курсує у вхідних каскадах мережевих рівнів системи SCADA. 2. Виконується ЦФ електронної пошти керівників підрозділів КІ. 3. Здійснюється крадіжка облікових даних для доступу до системи SCADA КІ.
Фальсифікація інформації (ФСФ)	1. За результатами ЦФ здійснюється всебічне вивчення системи SCADA, тобто вивчаються структурна побудова, програмне та апаратне забезпечення, навантаження і тому інше. 2. Розробка та впровадження вбудованого шкідливого програмного забезпечення для управління обладнанням компонентів КІ. 3. Викривлення інформації, яка курсує в інфокомунікаційних системах мережевого рівня SCADA КІ.
Підміна інформації (ПДМ)	1. Проникнення в серверні системи мережевого рівня SCADA КІ. 2. Інформація управління викривляється та повністю замінюється неправдивою інформацією. 3. Повна компрометація системи за рахунок доступу до інформаційного ресурсу. 4. Команди управління обслуговуючого персоналу системи SCADA замінюються на шкідливі команди зловмисників за рахунок чого здійснюється синхронізоване дистанційне відключення компонентів КІ. 5. Комплексні зловмисні шкідливі впливи, які реалізуються у вигляді: віддаленого відключення резервних блоків живлення пунктів управління компонентами КІ; одночасних фейкових телефонних дзвінків, які відволікають та ускладнюють роботу операторів та обслуговуючого персоналу системи SCADA КІ; розгортання бот мережі, що знищує дані необхідні для управління обладнанням.

Таблиця 4.

Загальний аналіз наслідків ЗВШВ на активи системи SCADA КІ

Номер сценарія ЗВШВ	Вид ЗВШВ	Компоненти, на які направлена дія ЗВШВ	Наслідки ЗВШВ	Рівень успішності ЗВШВ
1	2	3	4	5
Перший	РЗІ	Програмовані логічні контролери (ПЛК), протиаварійне захисне обладнання (ПЗО), сенсорні модулі (ССРМ), людино-машинні інтерфейси (ЛМІ), які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу SCADA КІ	Отримання доступу до інформаційного ресурсу системи SCADA КІ	Високий
	ФСФ	Серверні (СРВС) та інфокомунікаційні системи (ІКС), контролери доменів (КНТД), комп'ютерні термінали (КМПТ) четвертого, п'ятого, шостого мережевих рівнів SCADA КІ	Викривлення даних контуру управління КІ з застосуванням інформаційного ресурсу системи SCADA КІ	
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів SCADA КІ	Компрометація системи, заміна вірогідних даних неправдивими, застосування зловмисниками кібернетичних активів SCADA для відключення компонентів КІ з блокуванням дій обслуговуючого персоналу	

Продовження таблиці 4.

1	2	3	4	5
Другий	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу SCADA КІ	Наслідки ЗВШВ оперативно усунуто за рахунок підключення ХМС (Amazon Web Services), створення додаткового резервного контуру у вигляді ХМА для всіх шести мережевих рівнів SCADA КІ та реалізації функцій аварійного відновлення (АВД) і резервного копіювання (РКП)	Низький
	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів SCADA КІ		
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів SCADA КІ		
Третій	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу, частково хмарні системи AWS (ХМА) SCADA КІ	Отримання доступу до інформаційного ресурсу та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	Середній
	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів SCADA КІ	Наслідки ЗВШВ усунено за рахунок застосування ХМА системи SCADA КІ та реалізації функцій АВД і РКП	
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів SCADA КІ		

Продовження таблиці 4.

1	2	3	4	5
Четвертий	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу, частково хмарні системи AWS (ХМА) SCADA КІ	Отримання доступу до інформаційного ресурсу та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	Середній
	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів, частково хмарні системи AWS (ХМА) SCADA КІ	Викривлення даних контуру управління КІ з застосуванням інформаційного ресурсу КА та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п'ятого, шостого мережевих рівнів, частково хмарні системи AWS (ХМА) SCADA КІ	Компрометація систем четвертого мережевого рівня та ХМА SCADA КІ. Для п'ятого та шостого мережевих рівнів SCADA КІ наслідки ЗВШВ оперативно усунуто за рахунок застосування ХМА та реалізації функцій АВД і РКП	
П'ятий	РЗІ	ПЛК, ПЗО, ССРМ, ЛМІ, які утворюють перший, другий, третій кластери мережі контролю та оперативного моніторингу, хмарні системи AWS (ХМА) SCADA КІ	Отримання доступу до інформаційного ресурсу та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	Високий

Продовження таблиці 4.

1	2	3	4	5
П’ятий	ФСФ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів, хмарні активи SCADA КІ	Викривлення даних контуру управління КІ з застосуванням інформаційного ресурсу КА та ХМА системи SCADA КІ, реалізація функцій АВД і РКП неможлива	Високий
	ПДМ	СРВС та ІКС, КНТД, КМПТ четвертого, п’ятого, шостого мережевих рівнів, хмарні системи AWS (ХМА) SCADA КІ	Компрометація системи, заміна вірогідних даних неправдивими, застосування зловмисниками кібернетичних та хмарних активів SCADA для відключення компонентів КІ з блокуванням дій обслуговуючого персоналу, реалізація функцій АВД і РКП неможлива	

Відповідно до рис. 4–8 ймовірність складної події, яка полягає в неготовності активів системи SCADA КІ за результатами реалізації першого сценарію ЗВШВ, можна записати наступним чином [23]:

$$UnAvailability = P\left(\Phi\left(X\right)=0\right) = P\left\{UA_{1-3_j} \cup UA_{4_j} \cup \left[UA_{5_j} \cap UA_{6_j}\right] \cup \right.$$
$$\left. \cup \overline{FW4} \cup \overline{FW5}\right\}, \quad (1)$$

$$UA_{1-3_1} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$
$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\}, \quad (2)$$

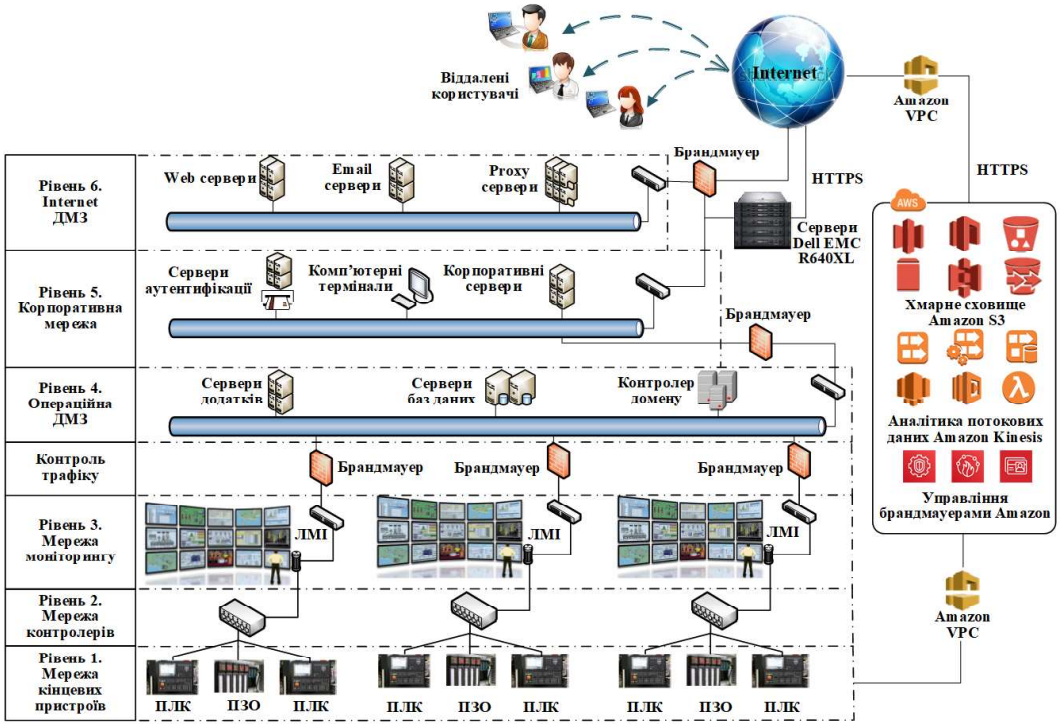

Рис. 13. Архітектура ФА, КА та ХМА системи SCADA КІ для мережевого рівня їхньої реалізації

$$UA_{4_1} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\}, \quad (3)$$

$$UA_{5_1} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\}, \quad (4)$$

$$UA_{6_1} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{\mathrm{Pr}oxySRV} \cup \left[TI \cap SI\right]\right\}, \quad (5)$$

де *ID* – подія, яка полягає в реалізації ЗВШВ у вигляді РЗІ; *TI* – подія, яка полягає в реалізації ЗВШВ у вигляді ФСФ; *SI* – подія, яка полягає в реалізації ЗВШВ у вигляді ПДМ; *j* – номер відповідного сценарію ЗВШВ.

Аналогічна подія для другого сценарію ЗВШВ згідно рис. 9 може бути записана у вигляді

$$UA_{1-3_2} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$
$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\} \cap \overline{AWS}, \quad (6)$$

$$UA_{4_2} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (7)$$

$$UA_{5_2} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (8)$$

$$UA_{6_2} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{\mathrm{Pr}\, oxySRV} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}. \quad (9)$$

У той же час ймовірність складної події згідно рис. 10, яка полягає в неготовності активів системи SCADA КІ за результатами реалізації третього сценарію ЗВШВ, можна записати як

$$UA_{1-3_3} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$
$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\} \cap \left\{\overline{AWS} \cup ID\right\}, \quad (10)$$

$$UA_{4_3} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (11)$$

$$UA_{5_3} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (12)$$

$$UA_{6_3} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{\mathrm{Pr}\, oxySRV} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}. \quad (13)$$

Для четвертого сценарію, який реалізується у відповідності з рис. 11, ймовірність складної події, що полягає в неготовності системи SCADA КІ за результатами дії ЗВШВ, записується наступним чином:

$$UA_{1-3_4} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$
$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\} \cap \left\{\overline{AWS} \cup ID\right\}, \quad (14)$$
$$UA_{4_4} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (15)$$
$$UA_{5_4} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{AWS} \cup \left[TI \cap SI\right]\right\}, \quad (16)$$
$$UA_{6_4} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{\mathrm{Pr}oxySRV} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}. \quad (17)$$

Відповідно до рис. 12 ймовірність складної події, яка полягає в неготовності активів системи SCADA КІ за результатами реалізації п'ятого сценарію ЗВШВ, можна визначити як

$$UA_{1-3_4} = \left\{\left[\overline{Cluster1} \cup ID\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup ID\right] \cup \overline{FW2}\right\} \cap$$
$$\cap \left\{\left[\overline{Cluster3} \cup ID\right] \cup \overline{FW3}\right\} \cap \left\{\overline{AWS} \cup ID\right\}, \quad (18)$$
$$UA_{4_4} = \left\{\overline{AppSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{DBSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{DmnCTL} \cup \left[TI \cap SI\right]\right\} \cap \overline{AWS}, \quad (19)$$
$$UA_{5_4} = \left\{\overline{AuthSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{CTU} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{EntprSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{AWS} \cup \left[TI \cap SI\right]\right\}, \quad (20)$$
$$UA_{6_4} = \left\{\overline{WebSRV} \cup \left[TI \cap SI\right]\right\} \cap \left\{\overline{EmailSRV} \cup \left[TI \cap SI\right]\right\} \cap$$
$$\cap \left\{\overline{\mathrm{Pr}oxySRV} \cup \left[TI \cap SI\right]\right\} \cap \cap \left\{\overline{AWS} \cup \left[TI \cap SI\right]\right\}. \quad (21)$$

Керуючись пропозиціями, описаними в [23,24], та застосовуючи отримані вирази (1)–(21), перейдемо від діаграм ЗВШВ на активи системи SCADA КІ (рис. 4–12) до її структурних схем безпеки (ССБ), які представлено на рис. 14–18.

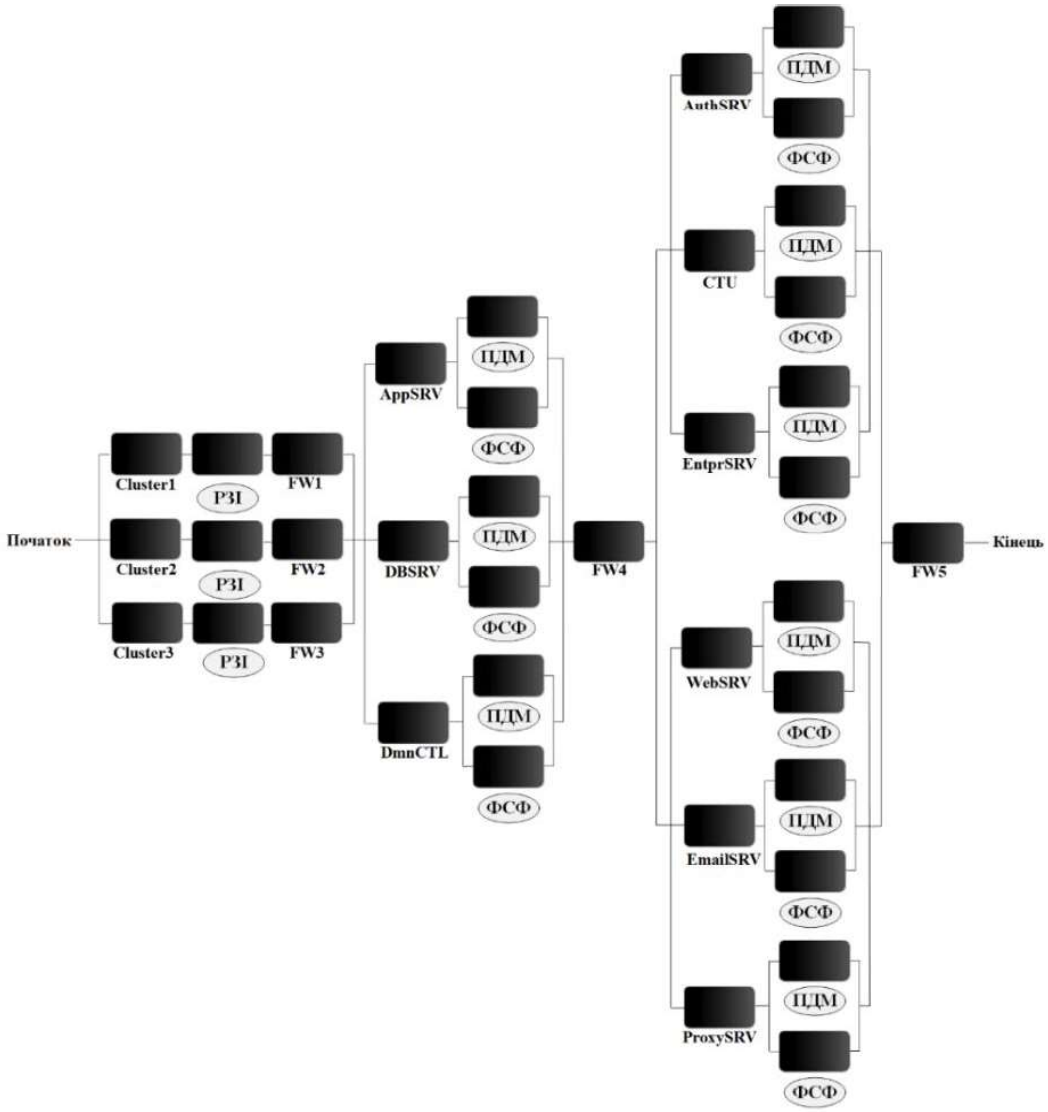

Рис. 14. ССБ системи SCADA КІ для першого сценарію ЗВШВ

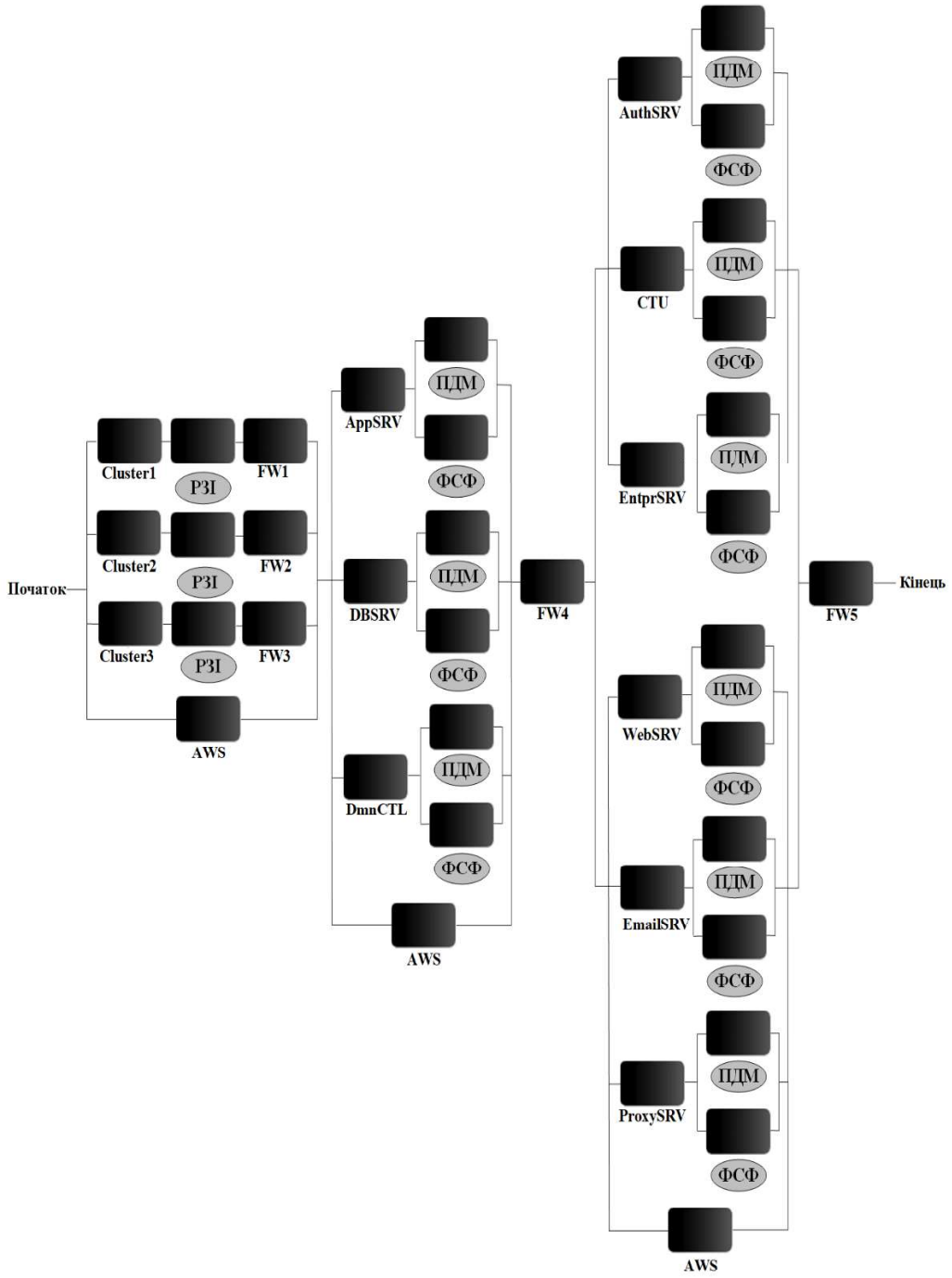

Рис. 15. ССБ системи SCADA КІ для другого сценарію ЗВШВ

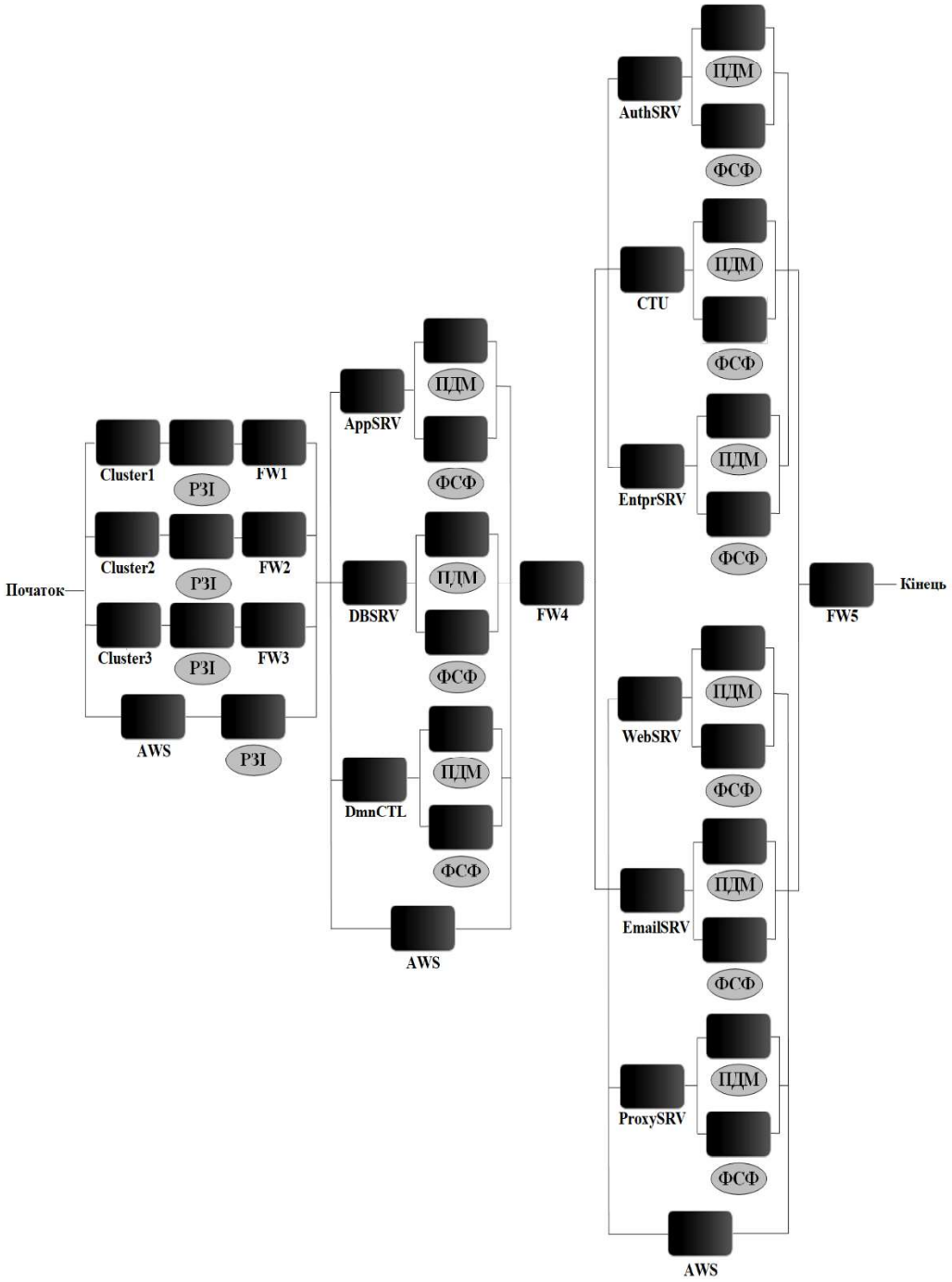

Рис. 16. ССБ системи SCADA КІ для третього сценарію ЗВШВ

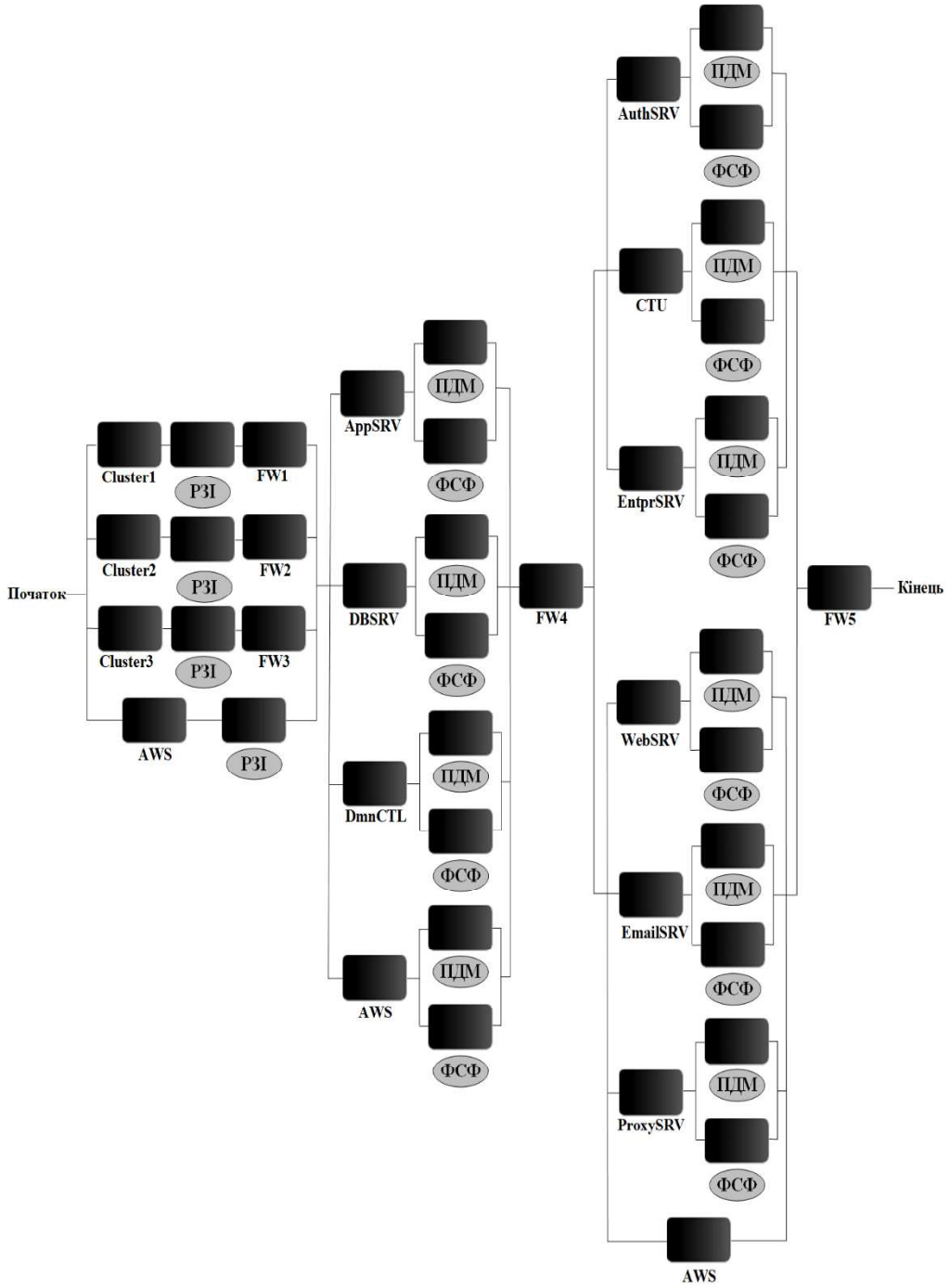

Рис. 17. ССБ системи SCADA КІ для четвертого сценарію ЗВШВ

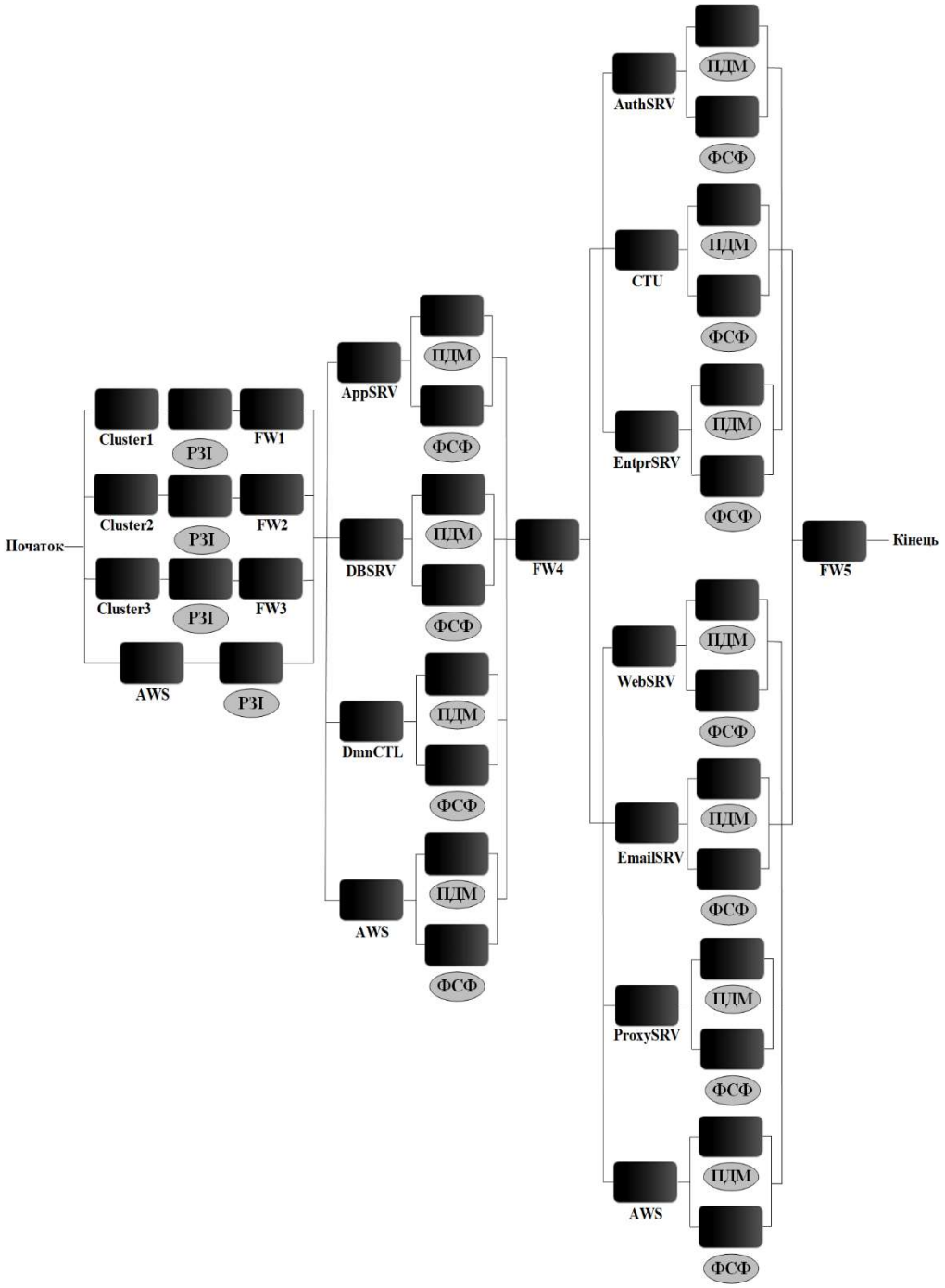

Рис. 18. ССБ системи SCADA KI для п’ятого сценарію ЗВШВ

У якості комплексного показника гарантоздатності (ГРТЗ) активів системи SCADA КІ пропонується застосовувати стаціонарний коефіцієнт готовності (СКГ), обгрунтування доцільності використання якого представлено в роботах [18,23–25]. В загальному вигляді, враховуючи приведені варіанти архітектурної реалізації (рис. 3,4), значення СКГ системи SCADA КІ за умови дії ЗВШВ визначається згідно наступного співвідношення:

$$K_{SCADA}^{DMI} = K_{SCADA_1}^{DMI} K_{SCADA_2}^{DMI} K_{SCADA_3}^{DMI} A_{FW_4} A_{FW_5}, \quad (22)$$

де $K_{SCADA_1}^{DMI}$ – СКГ першого, другого, третього кластерів SCADA КІ; $K_{SCADA_2}^{DMI}$ – СКГ четвертого мережевого рівня SCADA КІ; $K_{SCADA_3}^{DMI}$ – СКГ п'ятого та шостого мережевих рівнів SCADA КІ; A_{FW_4}, A_{FW_5} – СКГ четвертого та п'ятого брандмауерів, відповідно.

В співвідношенні (22) перші три складові визначаються за результатами напівмарковського моделювання (НПМ) ЗВШВ на кібернетичні та хмарні активи SCADA КІ. Решта вхідних даних для компонентів SCADA задається у відповідності з процедурою параметризації, яка описана в роботах [23,24]. Розглянемо основні аналітичні співвідношення, що відображають специфіку реалізації конкретного сценарію ЗВШВ і використовуються для оцінки відповдіних складових.

Згідно ССБ системи SCADA КІ для першого сценарію ЗВШВ (рис. 14.) стаціонарний коефіцієнт готовності визначається за допомогою наступних виразів:

$$K_{SCADA_1}^{DMI} = 1 - \overline{K}_{SCADA_1}^{DMI}, \quad (23)$$

$$\overline{K}_{SCADA_1}^{DMI} = \overline{K}_{SCADA_{11}}^{DMI} \overline{K}_{SCADA_{12}}^{DMI} \overline{K}_{SCADA_{13}}^{DMI}, \quad (24)$$

$$\overline{K}_{SCADA_{11}}^{DMI} = 1 - K_{SCADA_{11}}^{DMI}, \ \overline{K}_{SCADA_{12}}^{DMI} = 1 - K_{SCADA_{12}}^{DMI}, \ \overline{K}_{SCADA_{13}}^{DMI} = 1 - K_{SCADA_{13}}^{DMI}, \quad (25)$$

$$K_{SCADA_{11}}^{DMI} = A_{Cluster1} A_{FW1} P_{ID}, \quad (26)$$

$$K_{SCADA_{12}}^{DMI} = A_{Cluster2} A_{FW2} P_{ID}, \quad (27)$$

$$K_{SCADA_{13}}^{DMI} = A_{Cluster3} A_{FW3} P_{ID}, \quad (28)$$

$$K_{SCADA_2}^{DMI} = 1 - \overline{K}_{SCADA_2}^{DMI}, \quad (29)$$

$$\overline{K}_{SCADA_2}^{DMI} = \overline{K}_{SCADA_{21}}^{DMI} \overline{K}_{SCADA_{22}}^{DMI} \overline{K}_{SCADA_{23}}^{DMI}, \quad (30)$$

$$\overline{K}_{SCADA_{21}}^{DMI} = 1 - K_{SCADA_{21}}^{DMI}, \ \overline{K}_{SCADA_{22}}^{DMI} = 1 - K_{SCADA_{22}}^{DMI}, \ \overline{K}_{SCADA_{23}}^{DMI} = 1 - K_{SCADA_{23}}^{DMI}, \quad (31)$$

$$K^{DMI}_{SCADA_{21}} = A_{AppSRV} K^{DMI}_{SCADA_{211}},\ K^{DMI}_{SCADA_{211}} = 1 - \overline{P}_{TI}\,\overline{P}_{SI},\ \overline{P}_{TI} = 1 - P_{TI},\ \overline{P}_{TI} = 1 - P_{SI}, \quad (32)$$

$$K^{DMI}_{SCADA_{22}} = A_{DBSRV} K^{DMI}_{SCADA_{221}},\ K^{DMI}_{SCADA_{221}} = K^{DMI}_{SCADA_{211}}, \quad (33)$$

$$K^{DMI}_{SCADA_{23}} = A_{DmnCTL} K^{DMI}_{SCADA_{231}},\ K^{DMI}_{SCADA_{231}} = K^{DMI}_{SCADA_{211}}, \quad (34)$$

$$K^{DMI}_{SCADA_{3}} = 1 - \overline{K}^{DMI}_{SCADA_{3}}, \quad (35)$$

$$\overline{K}^{DMI}_{SCADA_{3}} = \overline{K}^{DMI}_{SCADA_{31}} \overline{K}^{DMI}_{SCADA_{32}} \overline{K}^{DMI}_{SCADA_{33}} \overline{K}^{DMI}_{SCADA_{34}} \overline{K}^{DMI}_{SCADA_{35}} \overline{K}^{DMI}_{SCADA_{36}}, \quad (36)$$

$$\overline{K}^{DMI}_{SCADA_{31}} = 1 - K^{DMI}_{SCADA_{31}},\ \overline{K}^{DMI}_{SCADA_{32}} = 1 - K^{DMI}_{SCADA_{32}},\ \overline{K}^{DMI}_{SCADA_{33}} = 1 - K^{DMI}_{SCADA_{33}}, \quad (37)$$

$$\overline{K}^{DMI}_{SCADA_{34}} = 1 - K^{DMI}_{SCADA_{34}},\ \overline{K}^{DMI}_{SCADA_{35}} = 1 - K^{DMI}_{SCADA_{35}},\ \overline{K}^{DMI}_{SCADA_{36}} = 1 - K^{DMI}_{SCADA_{36}}, \quad (38)$$

$$K^{DMI}_{SCADA_{31}} = A_{AuthSRV} K^{DMI}_{SCADA_{311}},\ K^{DMI}_{SCADA_{311}} = K^{DMI}_{SCADA_{211}}, \quad (39)$$

$$K^{DMI}_{SCADA_{32}} = A_{CTU} K^{DMI}_{SCADA_{321}},\ K^{DMI}_{SCADA_{321}} = K^{DMI}_{SCADA_{211}}, \quad (40)$$

$$K^{DMI}_{SCADA_{33}} = A_{EntprSRV} K^{DMI}_{SCADA_{331}},\ K^{DMI}_{SCADA_{331}} = K^{DMI}_{SCADA_{211}}, \quad (41)$$

$$K^{DMI}_{SCADA_{34}} = A_{WebSRV} K^{DMI}_{SCADA_{341}},\ K^{DMI}_{SCADA_{341}} = K^{DMI}_{SCADA_{211}}, \quad (42)$$

$$K^{DMI}_{SCADA_{35}} = A_{EmailSRV} K^{DMI}_{SCADA_{351}},\ K^{DMI}_{SCADA_{351}} = K^{DMI}_{SCADA_{211}}, \quad (43)$$

$$K^{DMI}_{SCADA_{36}} = A_{\mathrm{Pr}oxySRV} K^{DMI}_{SCADA_{361}},\ K^{DMI}_{SCADA_{361}} = K^{DMI}_{SCADA_{211}}, \quad (44)$$

де P_{ID} – ймовірність працездатного стану (ПРС) відповідної ресурсної компоненти, яка входить до складу кібернетичних або хмарних активів системи SCADA КІ, за умови, що здійснюється ЗВШВ у вигляді РЗІ (табл. 3, 4); P_{TI} – ймовірність ПРС відповідної ресурсної компоненти, яка входить до складу кібернетичних або хмарних активів системи SCADA КІ, за умови, що здійснюється ЗВШВ у вигляді ФСФ (табл. 3, 4); P_{SI} – ймовірність ПРС відповідної ресурсної компоненти, яка входить до складу кібернетичних або хмарних активів системи SCADA КІ, за умови, що здійснюється ЗВШВ у вигляді ПДМ (табл. 3, 4).

Для отримання оцінки комплексного показника гарантоздатності кібернетичних та хмарних активів системи SCADA КІ згідно співвідношень (1)–(44) на основі реалізації НПМ розроблено відповідний алгоритм. На рис. 19, 20 зображено розмічені графи переходів напівмарковських моделей (НПММ) з виродженими станами, які застосовуються для визначення ймовірностей трьох видів ЗВШВ. Процес побудови та обчислення вказаних НПММ з урахуванням необхідних формальних ознак описано в роботах [22,26,27].

Алгоритм 1: ОЦІНКА КОМПЛЕКСНОГО ПОКАЗНИКА ГАРАНТОЗДАТНОСТІ КІБЕРНЕТИЧНИХ ТА ХМАРНИХ АКТИВІВ SCADA КІ

1 Визначення часу моделювання $K_{SCADA}^{DMI}(T)$ як $T = \sum_{i=1}^{n} t_i$

2 Ввод вхідних параметрів $\lambda_{DMI_{\max}}$, $\lambda_{DMI_{step}}$, λ_{TP}, λ_{RK}

3 Ввод вхідних параметрів $t_{\min}$, t_{step}, A_{SCADA_i}, A_{AWS}

5 **for** *i = 1 to n* **do**

6 $\lambda_{DMI_i} = \lambda_{DMI_{\max}} - i \cdot \lambda_{DMI_{step}}$; $c_i = \lambda_{DMI_i} + \lambda_{TP} + \lambda_{RK}$;

7 **for** *j = 1 to m* **do**

8 $T_j = t_{min} + j \cdot t_{step}$;

9 Обчислення перехідних ймовірностей $p_{SI_{ij}}$ для НПМ ПДМ;

10 Обчислення середнього часу $t_{SI_{ij}}$ для НПМ ПДМ;

11 Визначення стаціонарних ймовірностей $\pi_{SI_{ij}}$ та P_{SI};

12 Обчислення перехідних ймовірностей $p_{ID_{ij}}$ для НПМ РЗІ;

13 Обчислення середнього часу $t_{ID_{ij}}$ для НПМ РЗІ;

14 Визначення стаціонарних ймовірностей $\pi_{ID_{ij}}$ та P_{ID};

15 Обчислення перехідних ймовірностей $p_{TI_{ij}}$ для НПМ ФСФ;

16 Обчислення середнього часу $t_{TI_{ij}}$ для НПМ ФСФ;

17 Визначення стаціонарних ймовірностей $\pi_{TI_{ij}}$ та P_{TI};

18 Обчислення $K_{SCADA_{11}}^{DMI}, K_{SCADA_{12}}^{DMI}, K_{SCADA_{13}}^{DMI}, K_{SCADA_{21}}^{DMI}, K_{SCADA_{22}}^{DMI}, K_{SCADA_{23}}^{DMI}$;

19 Обчислення $K_{SCADA_{31}}^{DMI}, K_{SCADA_{32}}^{DMI}, K_{SCADA_{33}}^{DMI}, K_{SCADA_{34}}^{DMI}, K_{SCADA_{35}}^{DMI}, K_{SCADA_{36}}^{DMI}$;

20 Визначення $K_{SCADA_{ij}}^{DMI}$ для першого сценарію;

21 Визначення $K_{SCADA_{ij}}^{DMI}$ для другого сценарію;

22 Визначення $K_{SCADA_{ij}}^{DMI}$ для третього сценарію;

23 Визначення $K_{SCADA_{ij}}^{DMI}$ для четвертого сценарію;

24 Визначення $K_{SCADA_{ij}}^{DMI}$ для п'ятого сценарію;

25 **end**

26 **end**

27 **meshgrid(**T_j, λ_{DMI_i}**);surf (**$T_j, \lambda_{DMI_i}, K_{SCADA_{ij}}^{DMI}$**)**; **hold on; colorbar;**

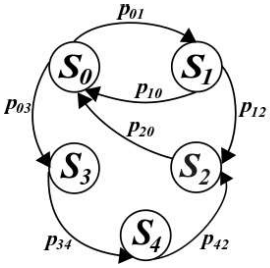

Рис. 19. Граф станів НПММ ЗВШВ у вигляді РЗІ та ФСФ для активів системи SCADA КІ [22,26]

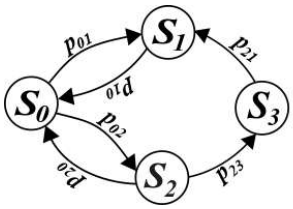

Рис. 20. Граф станів НПММ ЗВШВ у вигляді ПДМ для активів системи SCADA КІ [27]

За результатами НПМ отримано графічні залежності щодо реалізації ЗВШВ по відношенню до активів SCADA КІ, коли здійснюється розкриття, фальсифікація та підміна інформації. На рис. 21 відображено відповідні залежності.

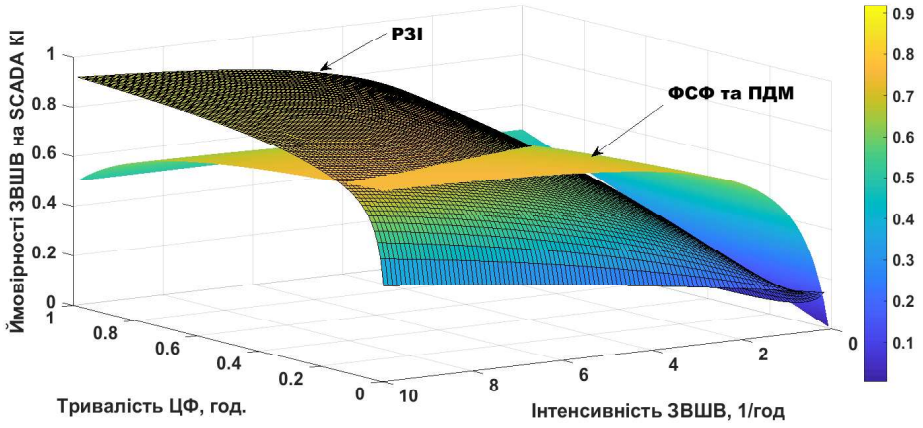

Рис. 21. Залежності ймовірності реалізації ЗВШВ у вигляді РЗІ, ФСФ та ПДМ для активів системи SCADA КІ

Результати моделювання на основі використання розробленого алгоритму 1 для отриманих п'ятьох сценаріїв ЗВШВ представлено на рис. 22–24. При відображенні результатів моделювання (рис. 22–24) значна увага приділялася визначенню залежностей між комплексним показником гарантоздатності кібернетичних, хмарних активів SCADA КІ та інтенсивністю ЗВШВ, тривалостями інтервалів часу, який витрачається на зміну ключів і цільовий фішинг.

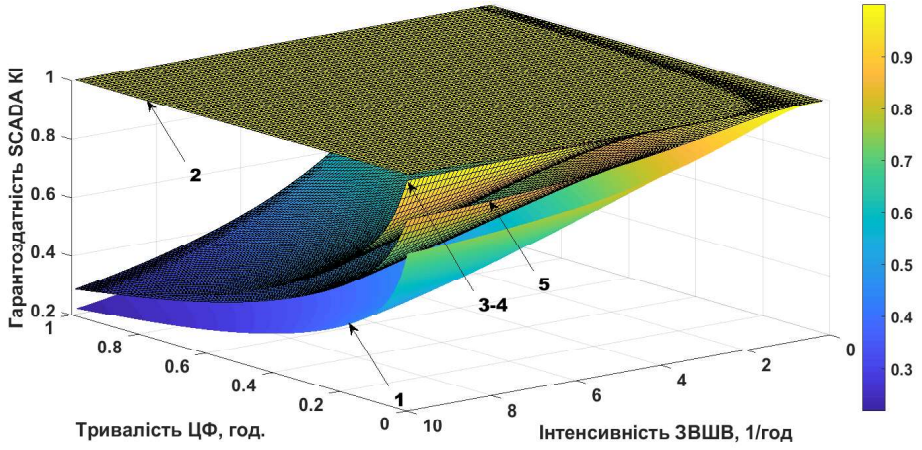

Рис. 22. Комплексний показник ГРТЗ активів SCADA КІ для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається три хвилини

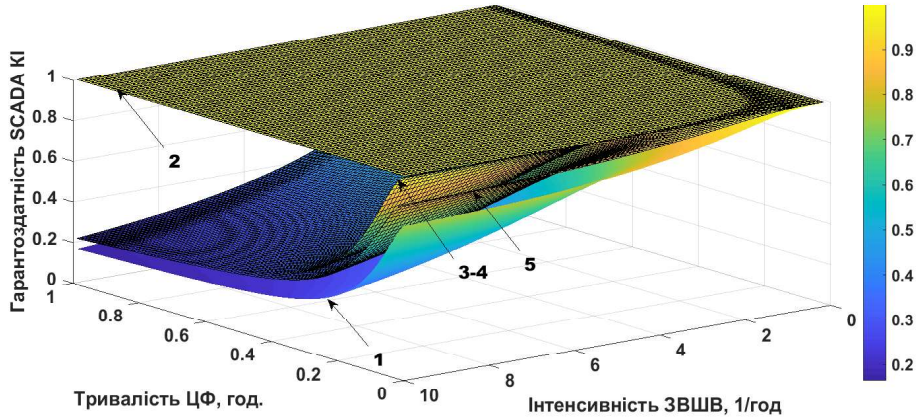

Рис. 23. Комплексний показник ГРТЗ активів SCADA КІ для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається тридцять хвилин

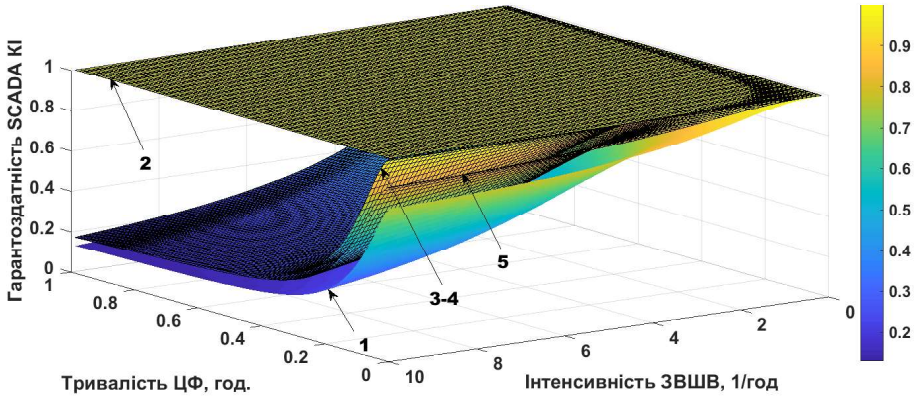

Рис. 24. Комплексний показник ГРТЗ активів SCADA KI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається одна година

Динаміку зміни величини комплексного показника ГРТЗ для другого сценарію ЗВШВ (рис. 22–24) в залежності від інтенсивності зловмисного шкідливого впливу, тривалостей інтервалів часу, який витрачається на проведення цільового фішингу та зміну ключів відображено на рис. 25.

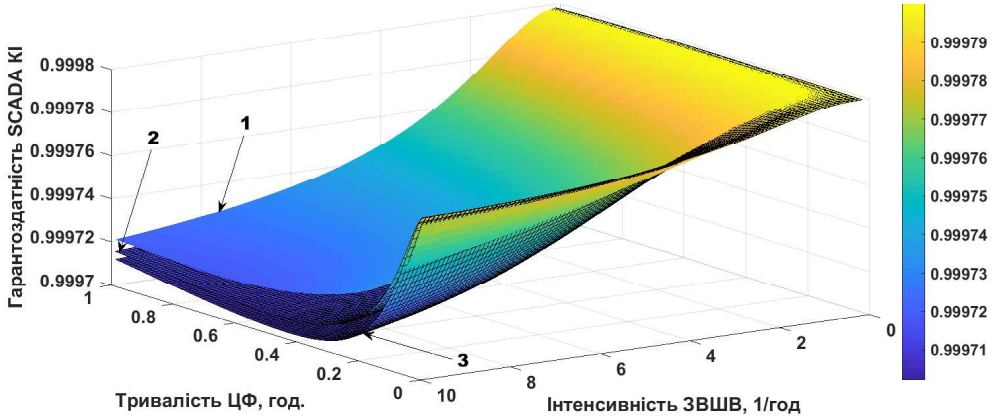

Рис. 25. Динаміка зміни величини комплексного показника ГРТЗ активів SCADA KI для другого сценарію ЗВШВ за умови, що на зміну ключів витрачається: 1 – три хвилини; 2 – тридцять хвилин; 3 – одна година

Оцінимо виграш від використання ХМС при створенні хмарних активів SCADA КІ з урахуванням ЗВШВ шляхом обчислення стаціонарного коефіцієнта неготовності (простою) (СКНГ) по формулі

$$\overline{K}_{SCADA}^{DMI} = 1 - K_{SCADA}^{DMI}. \quad (45)$$

Результати обчислення СКНГ кібернетичних та хмарних активів SCADA КІ представлено на рис. 26–28.

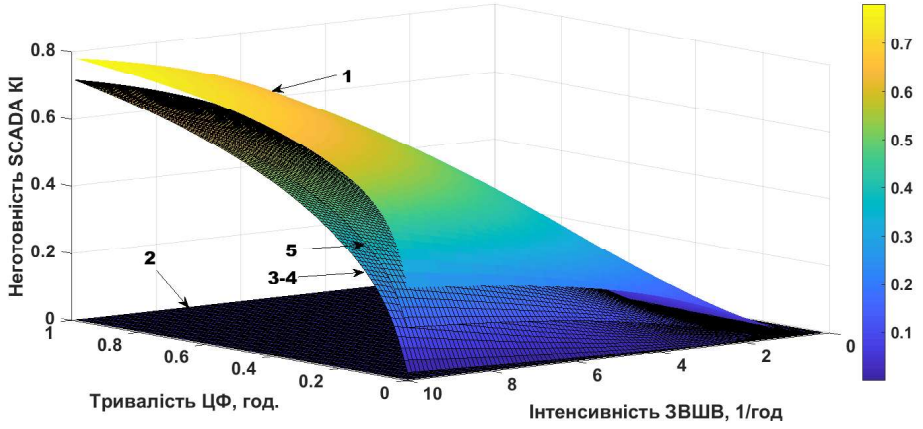

Рис. 26. Стаціонарний коефіцієнт неготовності активів SCADA КІ для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається три хвилини

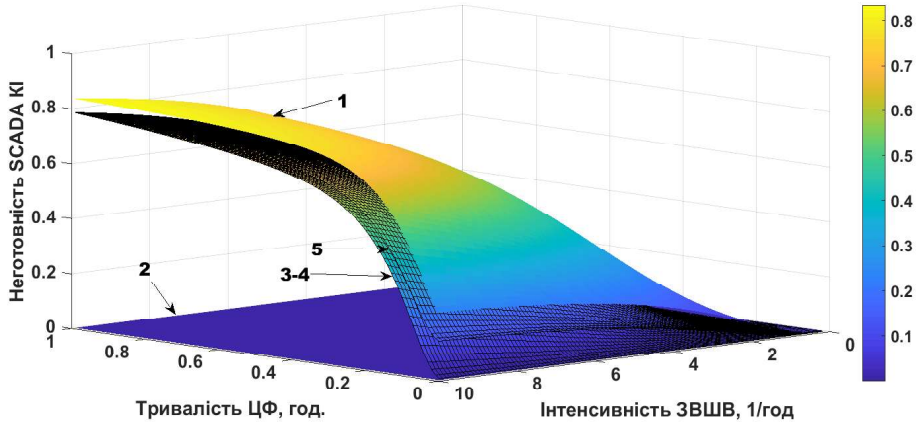

Рис. 27. Стаціонарний коефіцієнт неготовності активів SCADA КІ для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається тридцять хвилин

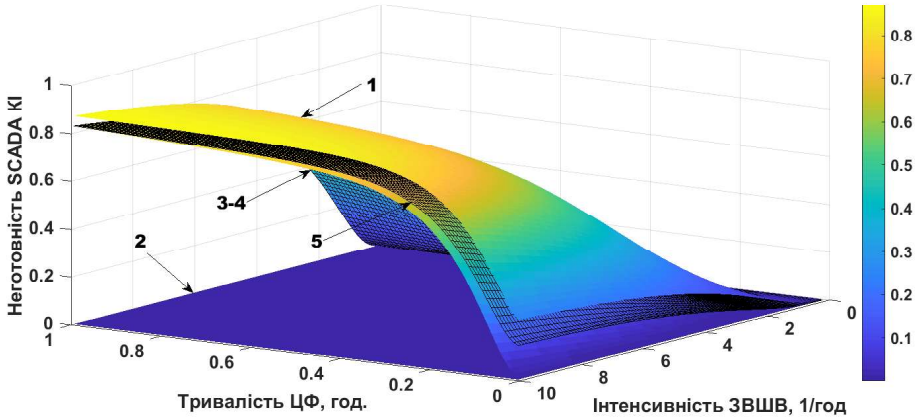

Рис. 28. Стаціонарний коефіцієнт неготовності активів SCADA KI для 1–5-го сценаріїв ЗВШВ за умови, що на зміну ключів витрачається одна година

Для покращення наочного уявлення про отриманий виграш обчислимо абсолютну різницю між значеннями СКНГ для відповідних пар сценаріїв ЗВШВ, застосовуючи наступне співвідношення:

$$\Delta_{SCADA} = \left| \overline{K}^{DMI}_{SCADA_{k,h}} - \overline{K}^{DMI}_{SCADA_{2,h}} \right|, \qquad (46)$$

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

Слід зазначити, що у співвідношенні (46) друга складова, яка визначає можливість отримання h-го зрізу СКНГ для другого сценарію ЗВШВ може бути замінена на іншу складову, що дозволяє отримати аналогічну оцінку для іншого сценарію. Результати обчислень з застосуванням співвідношень (45), (46) для конкретних сценаріїв ЗВШВ на активи SCADA KI представлені на рис. 29–31. Ці результати отримано за умови, що тривалість цільового фішингу і час, який відводиться на зміну ключів (ЗМНК) становить три хвилини. Зазначені вхідні параметри обрано не даремно, а саме, виходячи з міркувань щодо необхідності створення найбільш жорстких умов реалізації ЗВШВ. А саме, вважається, що за досить невеликий час проведення ЦФ зловмисник здійснює атаку на КА та ХМА

системи SCADA КІ з інтенсивністю ЗВШВ, яка дозволяє нанести максимальної шкоди.

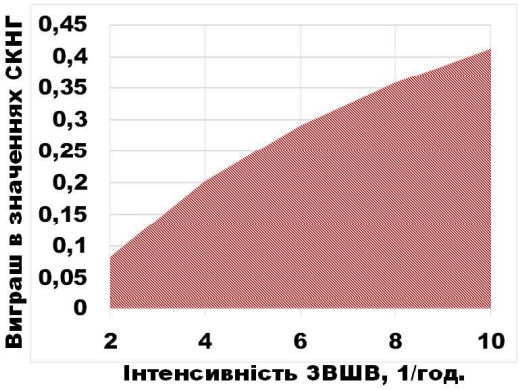

Рис. 29. Виграш в СКНГ для 2-го сценарію ЗВШВ у порівнянні з 1-м

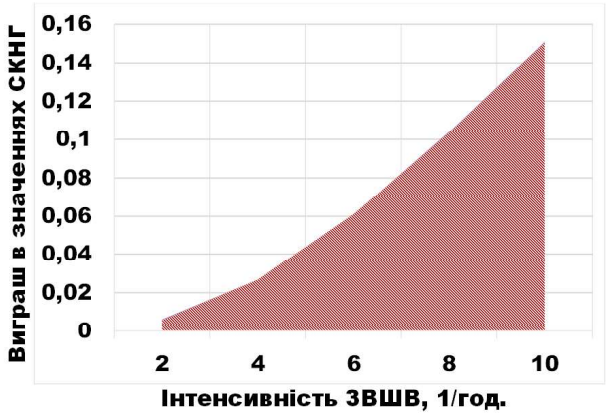

Рис. 30. Виграш в СКНГ для 2-го сценарію ЗВШВ у порівнянні з 3-м та 4-м

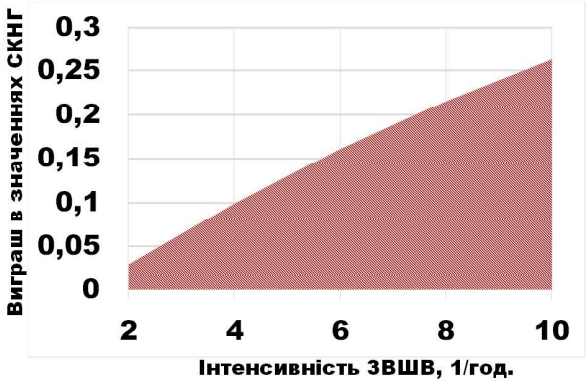

Рис. 31. Виграш в СКНГ для 2-го сценарію ЗВШВ у порівнянні з 5-м

Згідно рис. 29–31 найбільш критичною за результатами обчислення СКНГ є ситуація для ЗВШВ, що реалізується за першим сценарієм. Другими за критичністю є третій та четвертий сценарії з однаковим максимальним виграшем лише 15%. Тому будемо розглядати їх як один сценарій і отримаєм розрахунки виграшу в значеннях СКНГ, використовуючи аналогічний підхід, тобто за формулою

$$\Delta_{SCADA} = \left| \overline{K}^{DMI}_{SCADA_{r,h}} - \overline{K}^{DMI}_{SCADA_{3,h}} \right|, \tag{47}$$

де $r=1,5$ – номери відповідних сценаріїв ЗВШВ; h – номер зрізу СКНГ, для якого виконується обчислення; $\overline{K}^{DMI}_{SCADA_{3,h}}$ – значення h-го зрізу СКНГ для третього сценарію ЗВШВ.

На рис. 32, 33 представлено результати розрахунків з використанням співвідношень (45), (47).

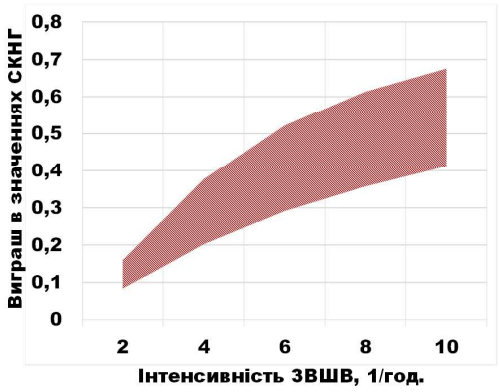

Рис. 32. Виграш в СКНГ для 3-го та 4-го сценаріїв ЗВШВ у порівнянні з 1-м

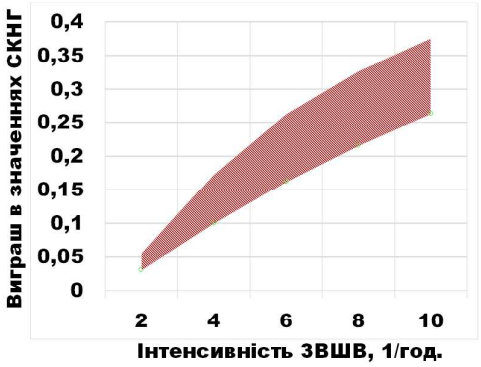

Рис. 33. Виграш в СКНГ для 3-го та 4-го сценаріїв ЗВШВ у порівнянні з 5-м

Порівняльний аналіз результатів моделювання (рис. 29–32) свідчить, що при використанні функцій післяаварійного відновлювання та копіювання, які виконуються завдяки застосуванню відповідних систем ХМА, значення стаціонарного коефіцієнта неготовності SCADA КІ в залежності від реалізуємого сценарію ЗВШВ зменшується від 41,2% до 11,25%. Узагальнені результати аналізу динаміки зміни величини СКНГ (тобто діапазон зменшення значень СКНГ), який визначає фактичний виграш в готовності кібернетичних та хмарних активів SCADA КІ для найбільш жорстких умов реалізації ЗВШВ відображено в табл. 5.

Таблиця 5.

Аналіз динаміки зміни величини стаціонарного коефіцієнта неготовності системи SCADA КІ з урахуванням ЗВШВ на кібернетичні та хмарні активи

Порівняльна комбінація сценаріїв ЗВШВ	Загальні параметри ЗВШВ		Тривалість процедури ЗМНК, хв.	Діапазон зменшення значень СКНГ (виграш)
	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	3	41,2% 15% 26,3% 26,2% 11,25%
(2;1) (2;3) (2;5) (3;1) (3;5)			10	36,4% 10,1% 22% 26,3% 11,9%
(2;1) (2;3) (2;5) (3;1) (3;5)			30	34,9% 8,7% 20,8% 26,2% 12,1%
(2;1) (2;3) (2;5) (3;1) (3;5)			60	36,6% 10,3% 22,2% 26,3% 11,9%

Продовження таблиці 5.

1	2	3	4	5
(2;1)	6	10	3	49,5%
(2;3)				25%
(2;5)				34,6%
(3;1)				24,5%
(3;5)				9,5%
(2;1)			10	48,4%
(2;3)				23,7%
(2;5)				33,4%
(3;1)				24,7%
(3;5)				9,7%
(2;1)			30	49,4%
(2;3)				25%
(2;5)				34,5%
(3;1)				24,5%
(3;5)				9,5%
(2;1)			60	53,2%
(2;3)				29,5%
(2;5)				38,5%
(3;1)				23,6%
(3;5)				9%

Отримані результати моделювання дозволяють сформулювати критерій забезпечення гарантоздатності КА та ХМА системи SCADA КІ, який записується у наступному вигляді:

$$\Im = \begin{cases} K_{SCADA}^{DMI}\left(t_{TP}, \tau_{RK}, \lambda_{DMI}\right) \geq K_{SCADA_0}^{DMI}; \\ t_{TP} \xrightarrow[t_{TP}\in[0;T]]{\lambda_{TP_{\max}}} \min; \\ \tau_{RK} \xrightarrow[\tau_{RK}\in[0;T]]{\lambda_{RK_{\max}}} \min; \\ \lambda_{DMI} \longrightarrow \max; \\ \Delta_{SCADA} \longrightarrow \max; \\ A_{SCADA_i}\left(T\right) \geq A_{SCADA_{0_i}}; \\ C_{\min_0} \leq C_0 \leq C_{\max_0}; \end{cases} \quad (48)$$

де T – загальний час застосування системи SCADA КІ за призначенням; t_{TP} – тривалість ЦФ; τ_{RK} – тривалість процедури ЗМНК; λ_{DMI} – інтенсивність ЗВШВ; $\lambda_{TP_{\max}}$ – максимальне значення інтенсивності ЦФ; $\lambda_{RK_{\max}}$ – максимальне значення інтенсивності процедури ЗМНК; $A_{SCADA_{0_i}}$ – граничні припустимі значення СКГ i-их компонентних складових системи SCADA КІ, які відповідають рівням готовності HAL [22]; $C_0 \in \left[C_{\min_0}; C_{\max_0}\right]$ – граничні витрати необхідні на підтримання необхідного рівня гарантоздатності КА та ХМА системи SCADA КІ; $K_{SCADA_0}^{DMI}$ – граничне припустиме значення комплексного показника гарантоздатності КА та ХМА системи SCADA КІ.

В системі умов та обмежень (48) поточне значення комплексного показника гарантоздатності $K_{SCADA}^{DMI}\left(t_{TP}, \tau_{RK}, \lambda_{DMI}\right)$ SCADA КІ визначається у відповідності зі співвідношеннями (1)–(44) за результатами напівмарковського моделювання.

Висновки та перспективи подальших досліджень у даному напрямі. Таким чином, в розглянутій статті запропоновано застосування додаткових ХМС з метою створення відповідних активів, що посилюють захисні властивості системи SCADA КІ від трьох видів зловмисних шкідливих впливів, за допомогою яких здійснюється розкриття, фальсифікація та підміна інформації. Процес моделювання самих шкідливих впливів на кібернетичні та хмарні активи SCADA було реалізовано як напівмарковський у відповідності з п'ятьма можливими сценаріями ЗВШВ. Розвиток негативних подій згідно розроблених сценаріїв відображено за допомогою діаграм ЗВШВ (рис. 4–12).

У якості комплексного показника гарантоздатності КА та ХМА системи SCADA КІ застосовувався стаціонарний коефіцієнт готовності. Виграш щодо реалізації захисних заходів від дії ЗВШВ на основі використання ХМС оцінювався за допомогою стаціонарного коефіцієнта неготовності (рис. 29–33). За результатами аналітико-стохастичного моделювання встановлено, що реалізація захисних заходів для кібернетичних активів SCADA КІ від зловмисних шкідливих впливів на основі застосування хмарних систем (перевага віддається, як правило, системам AWS) дозволяє знизити значення стаціонарного коефіцієнта неготовності в залежності від реалізуємого сценарію ЗВШВ на 8,7– 49,5% (табл. 5).

Перспективи подальших досліджень пов'язані з використанням запрпонованої аналітико-стохастичної моделі для розробки заходів, інформаційних технологій по забезпеченню готовності та гарантоздатності активів системи SCADA КІ. Крім того, описаний в статті науково-методичний апарат в перспективі планується застосовувати для вибору найкращої архітектурної реалізації SCADA КІ за критерієм забезпечення гарантоздатності її кібернетичних та хмарних активів.

Результати досліджень отримані в рамках науково-дослідних робіт «Методологічні засади та технології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур» (державний реєстраційний номер: 0119U100979) та «Методологія сталого розвитку та інформаційні технології зеленого комп'ютингу та комунікацій» (державний реєстраційний номер: 0118U003822), які виконуються Національним аерокосмічним університетом ім. М. Є. Жуковського «Харківський авіаційний інститут».

Список використаних джерел:

1. Ruijters, E., Stoelinga, M.: Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review 15, 29-62 (2015).

2. Kumar, R, Stoelinga, M.: Quantitative Security and Safety Analysis with Attack-Fault Trees. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 25-32. Singapore (2017). doi: 10.1109/HASE.2017.12.

3. Jürjens, J.: UMLsec: Extending UML for secure systems development. In: International Conference on The Unified Modeling Language, pp. 412-425. Springer, Berlin, Heidelberg (2002).

4. Roudier, Y., Apvrille, L.: SysML-Sec: A model driven approach for designing safe and secure systems. In: 2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD), pp. 655-664. Angers (2015).

5. Hermanns, H, Kramer, J, Krcal, J and Stoelinga, M.: The Value of Attack-Defence Diagrams. In: 5th International Conference on Principles of Security and Trust, POST, pp. 163-165. Springer, Berlin, Heidelberg (2016).

6. Kumar, R., Ruijters, E. and Stoelinga, M.: Quantitative attack tree analysis via priced timed automata. In: 13th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS, pp. 156-171. Springer, Cham (2015).

7. Kriaa, S., Cambacedes, L, Bouissou, M. and Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety 139, pp. 156-178 (2015).

8. Popov, P.: Stochastic modeling of safety and security of the e-motor, an ASIL-D device. In: 34th International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2015, pp. 385-399. Delft University of Technology, Netherlands (2014).

9. Ten, C., Liu, C., Manimaran, G.: Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems 23(4), 1836-1846 (2008).

10. Liu, X. and Li, Z.: Trilevel Modeling of Cyber Attacks on Transmission Lines. IEEE Transactions on Smart Grid 8(2), 720-729 (2017). doi: 10.1109/TSG.2015.2475701.

11. Kumar, P., Singh, L. K., and Kumar, C.: Suitability analysis of software reliability models for its applicability on NPP systems. Quality and Reliability Engineering International 34(8), pp. 1491-1509 (2018).

12. Xiang, J., Weng, C., Zhao, D. et al.: Software aging and rejuvenation in android: new models and metrics. Software Quality Journal 28, 85-106 (2020). doi: 10.1007/s11219-019-09475-0.

13. Huo, S., Zhao, D., Liu, X., Xiang, J., Zhong, Y. and Yu, H.: Using machine learning for software aging detection in Android system. In: 2018 Tenth International Conference on Advanced Computational Intelligence (ICACI), pp. 741-746. Xiamen (2018). doi: 10.1109/ICACI.2018.8377553.

14. Gribaudo, M., Pinciroli, R., and Trivedi, K.: Epistemic uncertainty propagation in power models. Electronic Notes in Theoretical Computer Science 337, 67-86 (2018).

15. Xia, Y., Zhou, M., Luo, X., Pang, S. and Zhu, Q.: A Stochastic Approach to Analysis of Energy-Aware DVS-Enabled Cloud Datacenters. IEEE Transactions on Systems, Man, and Cybernetics: Systems 45(1), pp. 73-83 (2015).

16. da Silva Pinheiro, Silva, T, Fé, F., Kosta, I., and Maciel, P.: Performance prediction for supporting mobile applications' offloading. The Journal of Supercomputing 74(8), pp. 4060-4103 (2018).

17. Ivanchenko, O., Kharchenko, V., Moroz, B., Kabak, L., and Konovalenko, S.: Risk Assessment of Critical Energy Infrastructure Considering Physical and Cyber Assets: Methodology and Models. In: 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), pp. 225-228. Lviv (2018). doi: 10.1109/IDAACS-SWS.2018.8525594.

18. Liang, S., He, C., Fang, W., Zhou, Z., Li, Y., and Wang, Y.: A SCADA platform architecture for cloud-based micro-service system with real time data process. In: IOP Conference Series: Materials Science and Engineering, p. 042056. IOP Publishing (2019).

19. Scott, P.: Distributed Coordination and Optimisation of Network-Aware Electricity Prosumers. Ph.D. The Australian National University (2016).

20. Ahmed, I., Obermeier, S., Naedele, M., Richard III, G. G.: SCADA Systems: Challenges for Forensic Investigators. Computer 45(12), pp. 44-51 (2012).

21. Fairley, P.: Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [News]. IEEE Spectrum 53(5), 11-13 (2016). doi: 10.1109/MSPEC.2016.7459104.

22. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : навчальний посібник / за заг. ред. В. С. Харченка. – Харків : Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», 2011. – 641 с.

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

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

25. Matos R., Araujo J., Oliveira D., Maciel P., Trivedi K.: Sensitivity analysis of a hierarchical model of mobile cloud computing. Simulation Modelling Practice and Theory 50, 151-164 (2015).

26. Распределённые критические системы и инфраструктуры : практикум / [О. В. Иванченко, В. С. Ловягин, Е. Н. Мащенко та ін.] ; за заг. ред. А. В. Скаткова, В. С. Харченка. – Харків : Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Севастопольський національний технічний університет, 2013. – 179 с.

27. Ivanchenko, O., Kharchenko, V., Brezhnev, E., Ponochovnyi, Y., Moroz, B. and Kabak, L.: Dependability Assessment for SCADA System Considering Usage of Cloud Resources. In: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 13-17. IEEE Press, Kyiv, Ukraine (2020). doi: 10.1109/DESSERT50317.2020.9125052.

References:

1. Ruijters, E., Stoelinga, M.: Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review 15, 29-62

(2015).

2. Kumar, R, Stoelinga, M.: Quantitative Security and Safety Analysis with Attack-Fault Trees. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 25-32. Singapore (2017). doi: 10.1109/HASE.2017.12.

3. Jürjens, J.: UMLsec: Extending UML for secure systems development. In: International Conference on The Unified Modeling Language, pp. 412-425. Springer, Berlin, Heidelberg (2002).

4. Roudier, Y., Apvrille, L.: SysML-Sec: A model driven approach for designing safe and secure systems. In: 2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD), pp. 655-664. Angers (2015).

5. Hermanns, H, Kramer, J, Krcal, J and Stoelinga, M.: The Value of Attack-Defence Diagrams. In: 5th International Conference on Principles of Security and Trust, POST, pp. 163-165. Springer, Berlin, Heidelberg (2016).

6. Kumar, R., Ruijters, E. and Stoelinga, M.: Quantitative attack tree analysis via priced timed automata. In: 13th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS, pp. 156-171. Springer, Cham (2015).

7. Kriaa, S., Cambacedes, L, Bouissou, M. and Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety 139, pp. 156-178 (2015).

8. Popov, P.: Stochastic modeling of safety and security of the e-motor, an ASIL-D device. In: 34th International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2015, pp. 385-399. Delft University of Technology, Netherlands (2014).

9. Ten, C., Liu, C., Manimaran, G.: Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems 23(4), 1836-1846 (2008).

10. Liu, X. and Li, Z.: Trilevel Modeling of Cyber Attacks on Transmission Lines. IEEE Transactions on Smart Grid 8(2), 720-729 (2017). doi: 10.1109/TSG.2015.2475701.

11. Kumar, P., Singh, L. K., and Kumar, C.: Suitability analysis of software reliability models for its applicability on NPP systems. Quality and Reliability Engineering International 34(8), pp. 1491-1509 (2018).

12. Xiang, J., Weng, C., Zhao, D. et al.: Software aging and rejuvenation in android: new models and metrics. Software Quality Journal 28, 85-106 (2020). doi: 10.1007/s11219-019-09475-0.

13. Huo, S., Zhao, D., Liu, X., Xiang, J., Zhong, Y. and Yu, H.: Using machine learning for software aging detection in Android system. In: 2018 Tenth

International Conference on Advanced Computational Intelligence (ICACI), pp. 741-746. Xiamen (2018). doi: 10.1109/ICACI.2018.8377553.

14. Gribaudo, M., Pinciroli, R., and Trivedi, K.: Epistemic uncertainty propagation in power models. Electronic Notes in Theoretical Computer Science 337, 67-86 (2018).

15. Xia, Y., Zhou, M., Luo, X., Pang, S. and Zhu, Q.: A Stochastic Approach to Analysis of Energy-Aware DVS-Enabled Cloud Datacenters. IEEE Transactions on Systems, Man, and Cybernetics: Systems 45(1), pp. 73-83 (2015).

16. da Silva Pinheiro, Silva, T, Fé, F., Kosta, I., and Maciel, P.: Performance prediction for supporting mobile applications' offloading. The Journal of Supercomputing 74(8), pp. 4060-4103 (2018).

17. Ivanchenko, O., Kharchenko, V., Moroz, B., Kabak, L., and Konovalenko, S.: Risk Assessment of Critical Energy Infrastructure Considering Physical and Cyber Assets: Methodology and Models. In: 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), pp. 225-228. Lviv (2018). doi: 10.1109/IDAACS-SWS.2018.8525594.

18. Liang, S., He, C., Fang, W., Zhou, Z., Li, Y., and Wang, Y.: A SCADA platform architecture for cloud-based micro-service system with real time data process. In: IOP Conference Series: Materials Science and Engineering, p. 042056. IOP Publishing (2019).

19. Scott, P.: Distributed Coordination and Optimisation of Network-Aware Electricity Prosumers. Ph.D. The Australian National University (2016).

20. Ahmed, I., Obermeier, S., Naedele, M., Richard III, G. G.: SCADA Systems: Challenges for Forensic Investigators. Computer 45(12), pp. 44-51 (2012).

21. Fairley, P.: Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [News]. IEEE Spectrum 53(5), 11-13 (2016). doi: 10.1109/MSPEC.2016.7459104.

22. Kharchenko, V. (Edit): Critical Infrastructures Safety: Mathematical and Engineering Methods of Analysis and Assurance, Department of Education and Science of Ukraine, National Aerospace University named after N. Zhukovsky "KhAI" (2011).

23. Ivanchenko, O.V.: Analytical and stochastic method in order to build safety and security block diagrams of cyber assets of SCADA system for critical infrastructure. J. Systems and Technologies 1(57), 81-106. doi: 10.32836/2521-6643-2019-1-57-6.

24. Ivanchenko, O.V.: Safety assessment for SCADA system of a critical infrastructure considering availability of cyber and cloud assets. J. Systems and Technologies 2(58), 5-32. doi: 10.32836/2521-6643-2019-2-58-1.

25. Matos R., Araujo J., Oliveira D., Maciel P., Trivedi K.: Sensitivity analysis of a hierarchical model of mobile cloud computing. Simulation Modelling Practice and Theory 50, 151-164 (2015).

26. Ivanchenko, O., Lovyagin, V., Maschenko, E., Skatkov, A., Shevchenko, V.: Distributed critical systems and infrastructures. National Aerospace University named after N. Zhukovsky “KhAI”, Kharkiv (2013).

27. Ivanchenko, O., Kharchenko, V., Brezhnev, E., Ponochovnyi, Y., Moroz, B. and Kabak, L.: Dependability Assessment for SCADA System Considering Usage of Cloud Resources. In: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 13-17. IEEE Press, Kyiv, Ukraine (2020). doi: 10.1109/DESSERT50317.2020.9125052.