DOI: https://doi.org/10.32836/2521-6643-2019-2-58-1
УДК 62-526

О. В. Іванченко, кандидат технічних наук,
доцент кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів

ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ СИСТЕМИ SCADA КРИТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ДОСТУПНОСТІ КІБЕРНЕТИЧНИХ І ХМАРНИХ АКТИВІВ

Зростання складності, масштабів і динаміки завдань, які виконує критична інфраструктура (КІ), потребує розширення функціональності та покращання інформаційного забезпечення системи управління нею. Значною мірою розв'язання цієї проблеми залежить від функціональної, інформаційної безпеки системи диспетчеризації та збирання даних типу SCADA, яка входить до контуру управління КІ. Особливу занепокоєність у цьому сенсі викликають не тільки відмови комп'ютерного обладнання, але й загрози, які пов'язані з реалізацією зловмисних впливів на відповідні кібернетичні активи. В запропонованій статті розглянуто можливість застосування додаткових хмарних активів з метою покращання рівня безпеки системи SCADA КІ.

Ключові слова: *система SCADA; кібернетичні та хмарні активи; структурні схеми надійності; марковське моделювання.*

Рост сложности, масштабов и динамики задач, решаемых критической инфраструктурой (КИ), требует расширения функциональности и улучшения информационного обеспечения ее системы управления. В значительной степени решение этой проблемы зависит от функциональной, информационной безопасности системы диспетчеризации и сбора данных типа SCADA, которая входит в контур управления КИ. Особую озабоченность в этом смысле вызывают не только отказы компьютерного оборудования, но и угрозы, связанные с реализацией вредоносных воздействий на соответствующие кибернетические активы. В предлагаемой статье рассмотрена возможность применения дополнительных облачных активов с целью улучшения уровня безопасности системы SCADA КИ.

Ключевые слова: *система SCADA; кибернетические и облачные активы; структурные схемы надежности; марковское моделирование.*

Growing complexness, scalable and dynamic of tasks for Critical Infrastructure (CI) create necessary preconditions to extend functionality and to improve information support of CI management system. According to distinct significance of this issue, the solution depends on safety and security of Supervisory Control and Data Acquisition System (SCADA), which includes into overall circuit of the CI Management System. Note that the malicious deliberate intrusions together with different Hard Ware failures of the SCADA as well reflect growing concern about low overall availability level of the SCADA system for CI. Proposed paper is devoted to possibility to use additional cloud assets in order to improve safety and cybersecurity of SCADA system for CI.

Nowadays researchers should understand that different negative events, such as data breaches, hacker attacks and malicious deliberate impacts are key causes of SCADA CI failures. Moreover, due to different sudden and hidden failures, the SCADA system of CI has low availability and safety that can lead to great damages for providers and users. Therefore, before begin to create management system for CI based on SCADA system vendors will perform justification of safety and security requirements for the SCADA system. In order to solve the task vendors can be used a proposed approach. The proposed approach is based on consistent application of new and unknown techniques and models. In fact researchers can use safety and dependability diagrams, including reliability block diagrams in order to build analytical and stochastic models for different assets of SCADA CI. These models can be used by researchers to get more modeling results, further these modeling results will be used by them in order to estimate overall safety assessment for SCADA CI. Using Markov Modelling Processes results for availability assessment of the SCADA components, firewalls and password models, researchers can estimate overall safety assessment based on the use of familiar stochastic equations. In according with proposed approach users can use additional Amazon Web Services (AWS) in order to build effective functioning safety and security protection system, which can be utilized by them to improve safety level of SCADA CI. Numerical modelling results for cyber assets with deployment of AWSs how additional cloud assets into overall management circuit allow to improve overall safety level of SCADA CI about ten percent. It means that in the near future time's vendors can use cloud assets in order to create effective functioning management systems for different Critical Infrastructures with reciprocal connection among their components, service-oriented resources and diverse users' clusters.

Key words: *SCADA system; cyber and cloud assets; reliability block diagrams; Markov Modeling Process.*

Постановка проблеми. Відомі аварії та інциденти критичної інфраструктури (КІ) засвідчують необхідність моніторингу і контролю великої кількості інформаційно-технічних станів, параметрів КІ, що значною мірою дає змогу усунути небезпечні інфраструктурні відмови. Аналогічне завдання актуальне для системи диспетчерського управління та збирання даних (SCADA) КІ.

Фактично SCADA являє собою сукупність комп'ютерного обладнання, програмного забезпечення, засобів комунікації та обміну інформацією і є одним з головних компонентів загальної системи управління КІ. Тому загрози, які існують для функціональної та інформаційної безпеки активів КІ, стосуються також системи SCADA, а для їхнього подальшого усунення пропонується застосовувати додатковий сервіс-орієнтований хмарний ресурс.

Аналіз останніх досліджень і публікацій. Відповідно до основного напряму дослідження виконаємо аналіз відомих публікацій з урахуванням впливу хмарних систем (ХМС) на функціональну та інформаційну безпеку КІ.

Нині використання ХМС як потужного інформаційного ресурсу дає змогу покращити ефективність застосування за призначенням КІ, це засвідчують результати аналізу відомих проектів [1–3]. Водночас ХМС дозволяють отримувати, обробляти й аналізувати інформаційні потоки даних у режимі реального часу, що суттєво розширює динамічний діапазон і покращує ефективність роботи системи управління КІ. Ці обставини сприяють усебічному висвітленню інформації щодо функціонування різноманітних компонентних складових інфраструктури, дозволяють запобігти їхнім відмовам і решті збоїв на основі реалізації певних сервіс-орієнтованих функцій ХМС.

Найбільш складні функції відтворення та аналізу аварійних ситуацій також можуть бути реалізовані у вигляді додаткових хмарних сервісів, які мають під собою відповідне наукове підґрунтя і розробляються з використанням сучасних наукових методів. Крім того, ХМС можуть бути задіяні для інформаційного забезпечення симуляторів, що відтворюють відповідні негативні події та застосовуються для підготовки обслуговуючого персоналу КІ до дій в екстремальних ситуаціях [4–6]. Таким чином, ХМС можуть суттєво впливати на важливі аспекти функціональної безпеки КІ та підтримувати необхідний рівень її готовності, безвідмовності та живучості.

Не менш суттєво ХМС можуть впливати на інформаційну безпеку КІ, доповнюючи її кібернетичні активи. На рис. 1 зображена спрощена структура активів критичних інфраструктур, яка існує на сьогоднішній день.

Незважаючи на відповідність певним нормативним вимогам, відомі факти й наслідки хакерських атак на кібернетичні активи національної КІ [7] підтверджують її вразливість. Своєю чергою, сам факт наявності вразливостей створює умови щодо виникнення загроз для кібернетичних активів

системи SCADA КІ, які реалізуються зловмисниками у вигляді тих чи інших несанкціонованих дій та впливів. Запобігти цьому можна, застосувавши додаткові хмарні ресурси та сервіси, які дають змогу реалізувати надлишковий принцип захисту кіберактивів КІ шляхом створення багатофункціональних адаптивних брандмауерів (БФАБ), що використовуються для двосторонньої фільтрації інформаційного трафіка.

Рис. 1. Структура фізичних та кібернетичних активів КІ

Критичні інфраструктури структуровано можна подати у вигляді сукупності фізичних (ФА), кібернетичних (КА) та хмарних активів. Спрощену структуру хмарних активів окремо взятої КІ зображено на рис. 2.

Серед переваг використання хмарних активів для забезпечення інформаційної безпеки КІ слід також зазначити можливість підтримки функцій резервного копіювання, аварійного відновлення інформації, контролю за точками доступу до сховищ даних інфраструктури та надання захищених (тунельних) каналів зв'язку.

Зазначені сервіси у вигляді основних моделей побудови і типів ХМС (рис. 2) можуть надаватися відповідними провайдерами, серед яких найбільш потужним є компанія Amazon (AWS). Однією з переваг AWS є застосування інфраструктурної організації фізичних машин (ФМ) з високим рів-

нем віртуалізації, що покращує гнучкість управління ХМС, але не завжди забезпечує доступність їхніх відповідних сервісів. Цьому сприяють різноманітні фактори негативного впливу, що збільшують час простоїв ФМ та призводять до суттєвих ресурсних, фінансових втрат для КІ. Розглянемо яким чином виконується моделювання поведінки ХМС КІ з урахуванням аспектів доступності сервіс-орієнтованих ресурсів.

Рис. 2. Структура хмарних активів КІ

Відомо, що для оцінювання рівня доступності хмарних активів використовуються різноманітні моделі, які адекватно відображають поведінку ХМС у ситуаціях, пов’язаних з їхнім застосуванням за призначенням. У більшості випадків моделювання здійснюється згідно зі сценарієм, який відображає реалізацію окремої або групи негативних подій, наприклад раптові, приховані відмови та збої, втрата інформації в результаті зловмисних впливів або втручань, цільовий фішинг тощо. На рис. 3 зображено класифікаційну схему (таксономію) десяти найпоширеніших аналітико-стохастичних методів моделювання поведінки ХМС, які утворюють відповідні хмарні активи і разом з кібернетичними та фізичними активами входять до складу КІ.

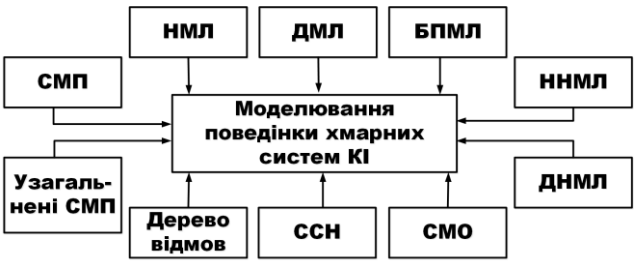

Рис. 3. Таксономія моделювання поведінки ХМС КІ [8]

Узагальнені дані оцінки можливостей використання зазначених методів (рис. 3) для моделювання поведінки та визначення характеристик гарантоздатності ХМС подано в табл. 1. Зокрема, стохастичні мережі Петрі (СМП) можуть бути використані для моделювання та оцінки можливостей забезпечення гнучкості управління хмарними системами. У разі наявності марковського альтернувального процесу відмов та відновлень для оцінки показників готовності ХМС доцільно використовувати узагальнені СМП [9–11]. Цей же апарат можна використовувати для оцінки показників гнучкості управління хмарною інфраструктурою (ХМІ), яка будується на основі ХМС (рис. 2). Не менш ефективно можна використовувати класичні методи побудови дерева відмов і структурних схем надійності (ССН) [1; 12] для виконання завдань забезпечення готовності ХМС. Для оцінки метрик якості послуг (QoS), що надають ХМС, може бути використано апарат побудови і моделювання як неперервних (НМЛ) [13], дискретних (ДМЛ) [14] та безпрограшних марковських ланцюгів (БПМЛ), так і систем масового обслуговування (СМО) [15; 16].

У разі порушення марковської властивості [17] пропонується застосовувати методи моделювання напівмарковських процесів, а саме напівмарковських ланцюгів (НМЛ). Наприклад, якщо виконуються різні види сервісного обслуговування, відновлення працездатності, контролю інформаційно-технічних станів (ІТС) компонентів ХМС КІ, то з'являються додаткові інтервали часу, тривалість яких є детермінованою або випадковою величиною з відомим стохастичним розподіленням, що відрізняється від експоненціального. Напівмарковські моделі також досить добре узгоджуються та адекватно описують ситуації, коли необхідно враховувати передісторію розвитку подій, які стосуються об'єкта дослідження. Наприклад, до та після проведення середнього або капітального ремонту; коли виникають приховані відмови, які виявляються за допомогою проведення додаткового багатофункціонального контролю ІТС і технічних параметрів ХМС КІ.

У випадку детермінованої величини для моделювання застосовується метод побудови дискретних напівмарковських ланцюгів (ДНМЛ); у разі стохастично розподілених інтервалів часу застосовується метод побудови неперервних напівмарковських ланцюгів (ННМЛ). Для виконання подібних завдань використовують апарат вкладених марковських ланцюгів, який враховує дискретний характер переходів моделі та час перебування об'єкта дослідження в конкретному стані перед переходом в інший. Крім того, застосування вкладених марковських ланцюгів дозволяє суттєво спростити рутинний процес отримання результуючих виразів для моделювання поведінки складних систем, до яких належать ХМС КІ.

Розширити можливості аналізу поведінки ХМС та ХМІ, що входять до складу інформаційно-управляючих систем КІ, дозволяє також використання прихованих напівмарковських моделей. Цей тип моделей використовується в умовах, коли інформації про ІТС системи, яка досліджується, немає, але доступна інформація щодо динаміки зміни її вхідних та вихідних параметрів. Приховані напівмарковські моделі будуються у вигляді ДНМЛ або ННМЛ. Особливістю прихованих напівмарковських ланцюгів є дискретний або стохастичний характер зміни тривалості наявних інтервалів, які у більшості випадків характеризують вхідний інформаційний потік даних [18].

Таблиця 1

Стохастичні методи моделювання поведінки ХМС КІ [17]

№	Моделі, які застосовуються для реалізації відповідного методу	Можливість використання для оцінки характеристик гарантоздатності ХМС КІ				
		готовність	продуктивність	енерговитрати	гнучкість	масштабованість
1	СМП	–	–	–	+	–
2	Узагальнені СМП	+	–	–	+	–
3	НМЛ	+	+	+	+	+
4	ДМЛ	+	+	+	+	+
5	БПМЛ	+	+	+	+	+
6	ННМЛ	+	+	+	+	+
7	ДНМЛ	+	+	+	+	+
8	СМО	+	+	–	+	–
9	ССН	+	–	–	–	+
10	Дерево відмов	+	–	–	+	–

Розглянуті методи та модельний ряд певною мірою претендують на універсальність і можуть бути використані для отримання оптимальних архітектурних рішень відповідно до встановлених критеріїв гарантоздатності, функціональної та інформаційної безпеки для ХМС КІ.

Мета статті. Виконаний аналіз дає змогу зосередитися на створенні перспективних науково-прикладних, організаційних методів забезпечення функціональної та інформаційної безпеки ХМС КІ, які базуються на попередніх оцінках доступності їхніх сервісів. Виходячи із зазначеного, мета статті – оціню-

вання загального рівня безпеки системи SCADA КІ з урахуванням спільного застосування наявних кібернетичних активів і додаткових сервіс-орієнтованих хмарних ресурсів компанії Amazon та отримання результатів марковського моделювання відповідно до сценарію розвитку певних негативних подій.

Виклад основного матеріалу. Забезпечення необхідного рівня безпеки базується на комплексному та системному застосуванні організаційних заходів і науково-методичного апарату оцінювання доступності КА та ФА системи SCADA КІ. Наприклад, методи побудови периметра фізичної безпеки (ФПБ) та електронного периметра кібербезпеки (ЕПКБ) розглядаються як найбільш популярні щодо реалізації відповідних організаційних заходів. Структурну схему організації ФПБ та ЕПКБ для системи SCADA та інших компонентів КІ зображено на рис. 4.

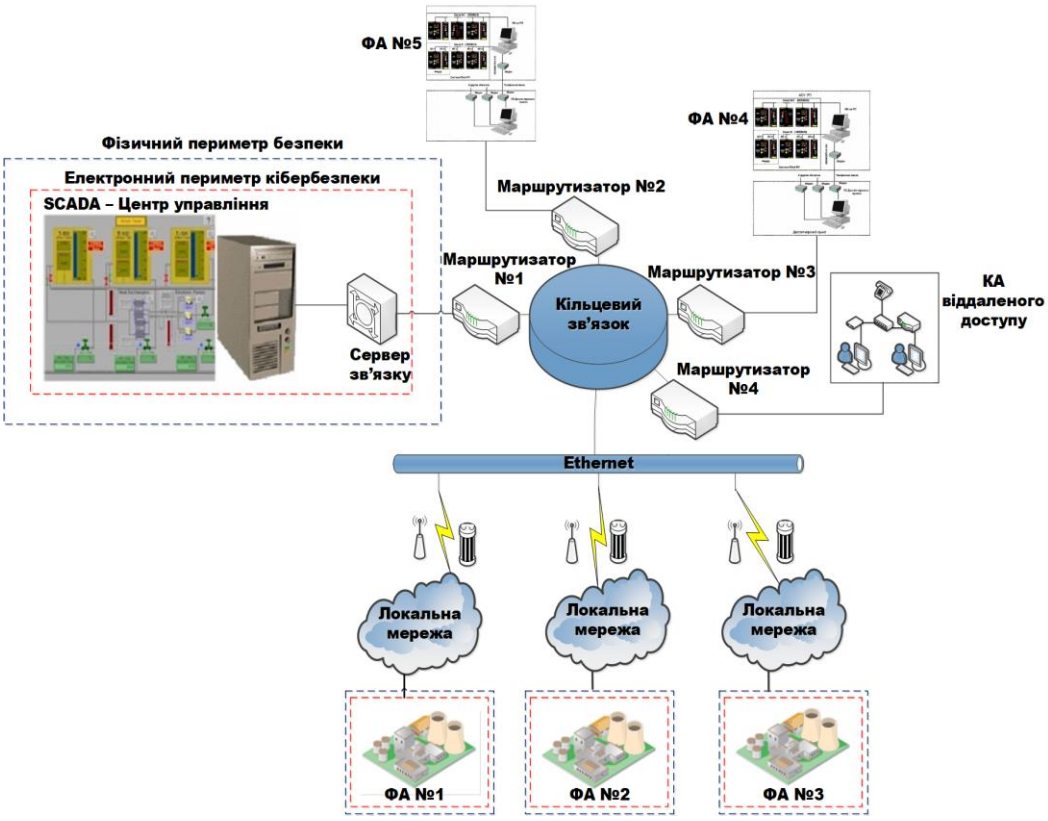

Рис. 4. Структурна схема організації фізичного периметра безпеки та електронного периметра кібернетичної безпеки компонентів КІ

Водночас перевірка ефективності застосування ФПБ та ЕПКБ для компонентів КІ, включаючи кібернетичні активи SCADA, може здійснюватися шляхом оцінювання їхнього рівня безпеки згідно з методом, запропонованим у праці [17]. Для цього послідовно виконуються такі дії: а) побудова спрощеної архітектурної реалізації кібернетичних, хмарних активів системи SCADA КІ з урахуванням мережних рівнів обробки даних, контролю та моніторингу ІТС, параметрів інфраструктури; б) застосування методів дерева відмов та побудови ССН [12] спільно з відповідним модельним рядом (табл. 1); в) визначення показника ризику кібернетичних, хмарних активів SCADA КІ у разі виникнення негативних подій, які впливають на функціональну та інформаційну безпеку інфраструктури.

На рис. 5 зображено спрощену архітектурну реалізацію кібернетичних та хмарних активів системи SCADA КІ. Головна особливість наведеної архітектури полягає в утворенні паралельно підключеного контура хмарних активів AWS, який працює за принципом функціональної та ресурсної надмірності. Отже, необхідно виконати моделювання і дослідити, яким чином застосування додаткових сервісів AWS впливає на гарантоздатність, загальний рівень безпеки кібернетичних та хмарних активів системи SCADA КІ. В табл. 2 згідно з рис. 5 відображено результати аналізу можливостей використання сервісів AWS щодо забезпечення гарантоздатності SCADA КІ.

У табл. 2 враховано такі аспекти оцінки та забезпечення гарантоздатності [19] SCADA КІ, розвитку яких сприяє застосування сервісів AWS: А1 – узагальнення викликів, які обумовлені несправностями та змінами вимог і умов використання системи SCADA КІ; А2 – покращання аналізу забезпечення відмовостійкості кібернетичних активів SCADA КІ; А3 – багатоверсійні обчислення у контексті факторів еволюційного розвитку кібернетичних активів SCADA КІ.

Побудуємо теоретико-множинну модель ІТС системи SCADA КІ, виходячи з таксономії загрози її функціональній та інформаційній безпеці [17; 19], відповідно до вимог стандартів ISA/IEC 62443, IEC 61508. На першому етапі розбудови моделі розглянемо схему її реалізації з урахуванням зловмисних впливів (ЗЛВ) на функціональну та інформаційну безпеку SCADA КІ (рис. 6), яка враховує дефекти компонентних складових ФА, вразливості й загрози для кібернетичних та хмарних активів системи. Вважатимемо, що різноманітні зовнішні та внутрішні фактори ЗЛВ спричиняють погіршення ІТС SCADA КІ за рахунок виникнення відмов, збоїв, проникнення шкідливого трафіка, компрометації системи тощо.

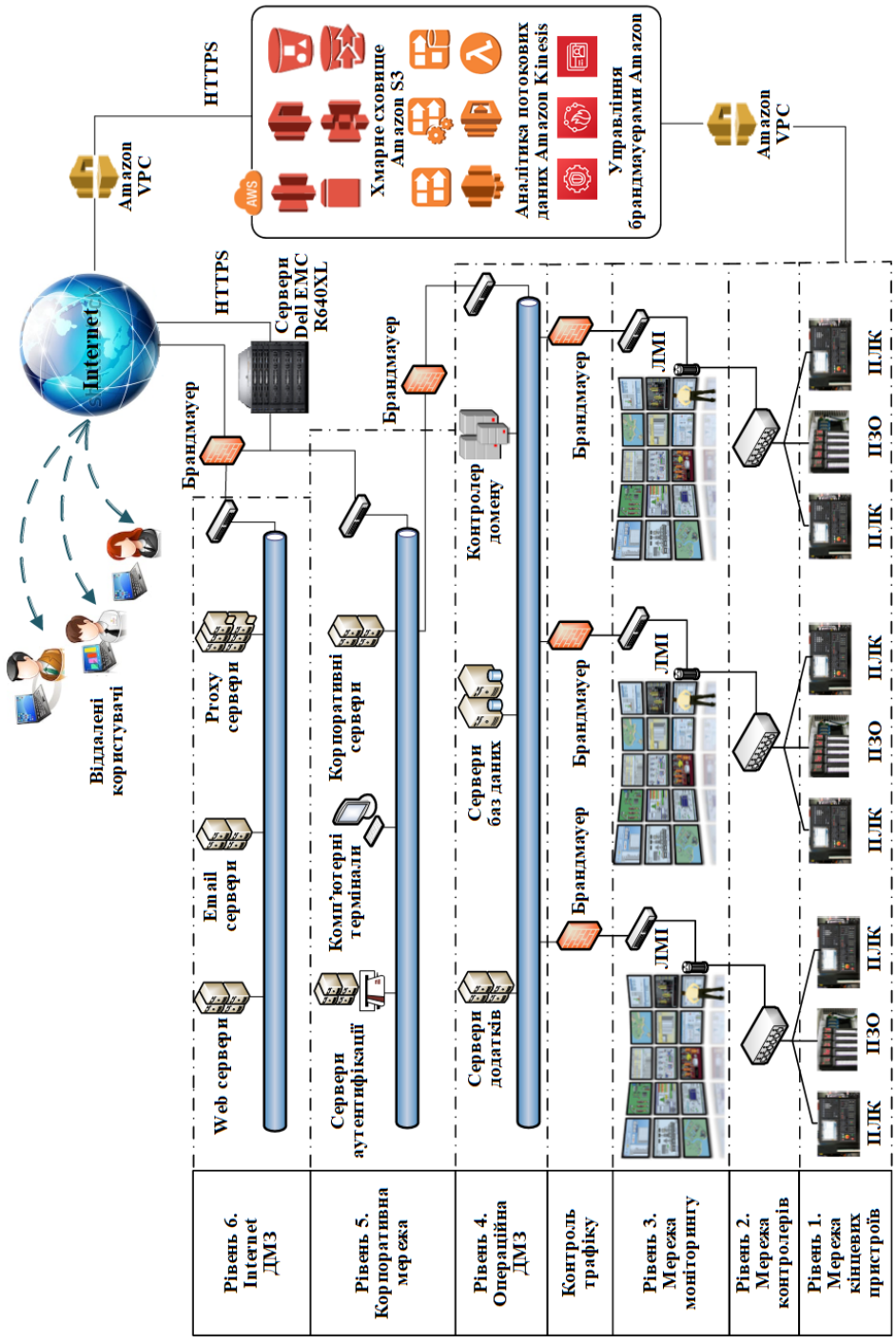

Рис. 5. Спрощена архітектурна реалізація кібернетичних [20] та хмарних активів системи SCADA KI

Таблиця 2

Застосування AWS для забезпечення гарантоздатності SCADA

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

Рис. 6. Схема реалізації теоретико-множинної моделі ІТС SCADA КІ з урахуванням ЗЛВ на її фізичні, кібернетичні та хмарні активи

Згідно з поданою схемою (рис. 6), можливі моделі ІТС опишемо за допомогою таких нотацій: M_{FF}^{PhA} – множина станів, що описують безпечні відмови та збої ФА; M_{DMI}^{CbrA} – множина станів, що описують ЗЛВ на КА; M_{DMI}^{CldA} – множина станів, що описують ЗЛВ на хмарні активи; M_{SS}^{SCADA} – множина станів, що характеризують функціональну та інформаційну безпеку SCADA. Тоді, виходячи із загальної теорії, відображення $\Omega(x_1): M_{FF}^{PhA} \Rightarrow M_{SS}^{SCADA}$ задає відношення між множинами M_{FF}^{PhA} та M_{SS}^{SCADA}, яке ототожнюється з деякою підмножиною H_{PhA}^{SCADA} декартового добутку [21] $M_{FF}^{PhA} \times M_{SS}^{SCADA}$, що має назву графіка відображення $\Omega(x_1)$ і визначається як:

$$H_{PhA}^{SCADA} = \left\{ (x_1, y_1) \middle| x_1 \in M_{FF}^{PhA} \wedge y_1 \in M_{SS}^{SCADA} \wedge \Omega(x_1) = y_1 \right\}. \quad (1)$$

Аналогічно до відображення $\Omega(x_1)$ та відповідно до (1) задаються відображення $\Omega(x_2): M_{DMI}^{CbA} \Rightarrow M_{SS}^{SCADA}$, $\Omega(x_3): M_{DMI}^{CldA} \Rightarrow M_{SS}^{SCADA}$, $\Omega(w_1): M_{DMI}^{CbrA} \Rightarrow$
M_{FF}^{PhA}, $\Omega(w_2): M_{DMI}^{CldA} \Rightarrow M_{FF}^{PhA}$, тобто

$$H_{CbrA}^{SCADA} = \left\{ (x_2, y_2) \middle| x_2 \in M_{DMI}^{CbrA} \wedge y_2 \in M_{SS}^{SCADA} \wedge \Omega(x_2) = y_2 \right\}, \quad (2)$$

$$H_{CldA}^{SCADA} = \left\{ (x_3, y_3) \middle| x_3 \in M_{DMI}^{CldA} \wedge y_3 \in M_{SS}^{SCADA} \wedge \Omega(x_3) = y_3 \right\}, \quad (3)$$

$$N_{CbrA}^{PhA} = \left\{ (w_1, z_1) \middle| w_1 \in M_{DMI}^{CbrA} \wedge z_1 \in M_{FF}^{PhA} \wedge \Omega(w_1) = z_1 \right\}, \quad (4)$$

$$N_{CldA}^{PhA} = \left\{ (w_2, z_2) \middle| w_2 \in M_{DMI}^{CldA} \wedge z_2 \in M_{FF}^{PhA} \wedge \Omega(w_2) = z_2 \right\}. \quad (5)$$

Отримана таким чином опорна теоретико-множинна модель (1)–(5), доповнена формалізованим описом початкових умов, режимів експлуатації та напрямків переходів відповідного графа ІТС, може бути використана для побудови оцінної аналітико-стохастичної моделі безпеки (ОМБ) системи SCADA КІ, яка враховує зовнішні та внутрішні фактори негативного впливу на ФА, зловмисні впливи на кібернетичні та хмарні активи. Для моделювання застосуємо таку систему обмежень:

$$\mathfrak{I}=\begin{cases}\theta\subset\Theta,\vartheta_k=\varnothing,k\notin i,i=\overline{1,n};\\ \varphi\subset\Theta,\vartheta_f\neq\varnothing,f\in j,j=\overline{1,m};\\ \varepsilon\subset\Theta,\vartheta_p=\varnothing,p\notin s,s=\overline{1,\ell};\\ \rho\subset\Theta,\vartheta_g\neq\varnothing,g\in z,z=\overline{1,h};\\ A_{SCADA_{i,s}}(t)\geq A_{SCADA_0};\\ A_{SCADA_{j,z}}(t)<A_{SCADA_0};\\ C_{min_0}\leq C_0\leq C_{max_0};\\ C_0>C_{max_0};\end{cases} \tag{6}$$

де $\Theta=\theta\cup\varphi\cup\varepsilon\cup\rho$ – показник цикломатичної складності (ЦКС), значення якого відповідає сукупності графів інформаційно-технічних станів марковського процесу моделювання (МПМ) поведінки системи SCADA КІ (далі скорочено – графів МПМ); $\theta=\{\vartheta_i\}_{i=1}^{n}$ – множина ІТС, яка відповідає значенню показника ЦКС для графів МПМ без поглинаючих станів; $\varphi=\{\vartheta_j\}_{j=1}^{m}$ – множина ІТС, яка відповідає значенню показника ЦКС для графів МПМ з поглинаючими станами; $\varepsilon=\{\vartheta_s\}_{s=1}^{\ell}$ – множина ІТС, що відповідає значенню показника ЦКС для графів МПМ, які не містять станів вразливості та дефектів (рис. 6); $\rho=\{\vartheta_s\}_{s=1}^{\ell}$ – множина ІТС, що відповідає значенню показника ЦКС для графів МПМ, які містять стани вразливості та дефектів (рис. 6); ϑ_k,ϑ_f – значення показника ЦКС для графів МПМ, які містять поглинаючи стани; ϑ_p,ϑ_g – значення показника ЦКС для графів

МПМ, які містять стани вразливості та дефектів; A_{SCADA_0} – граничні допустимі значення стаціонарного коефіцієнта готовності (КГ); C_0 – граничні витрати на підтримання необхідного рівня готовності системи SCADA КІ.

У системі обмежень (6) показник ЦКС визначається згідно зі співвідношенням [22]:

$$\vartheta = E - N + 2, \tag{7}$$

де E – кількість переходів графа; N – кількість вершин графа.

Подальший процес моделювання відбувається за відповідним сценарієм розвитку ЗЛВ, функціональну схему реалізації якого зображено на рис. 7. Вважатимемо, що зловмисники створюють і застосовують шкідливий трафік (ШКТ), який впливає на ФА, КА та хмарні активи SCADA КІ. Формально ШКТ можна подати у вигляді пуасонівської течії подій, основні характеристики якої можна отримати, застосувавши експоненціальний закон розподілу та співвідношення, за допомогою яких описується МПМ [23].

Діючи відповідно до зображеної функціональної схеми (рис. 7), зловмисники прагнуть досягти таких цілей [24]:

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

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

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

4) створити умови (наприклад, DoS атака, розгортання шкідливої ботмережі), коли за рахунок відключення КА та хмарних активів виникають відмови компонентів, які утворюють ФА.

Отримаємо результати оцінювання рівня безпеки без урахування вартості наслідків ЗЛВ для поданого сценарію (рис. 7), коли всі зазначені процеси відбуваються як марковські, враховуючи випадкові події, які трапляються на інтервалах застосування за призначенням брандмауерів, системи паролізації та SCADA КІ. Сукупність цих інтервалів утворює загальний робочий цикл або цикл оцінювання, протягом якого відбувається складна подія *A* (рис. 8).

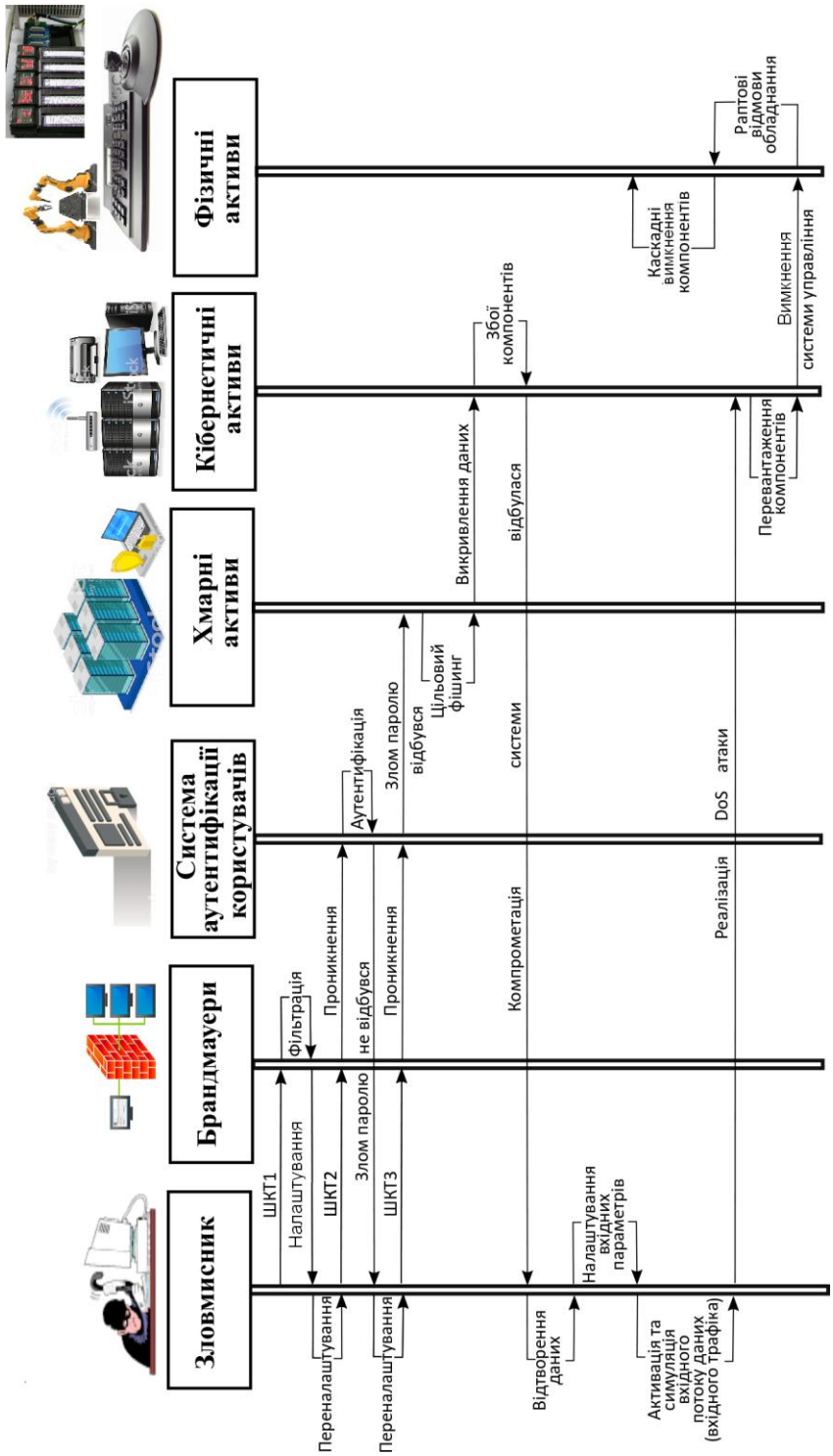

Рис. 7. Функціональна схема реалізації сценарію ЗЛВ на активи SCADA КІ

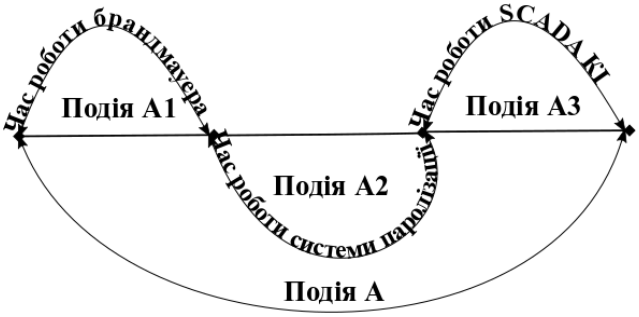

Рис. 8. Загальний цикл оцінювання рівня безпеки SCADA КІ

Відповідно до рис. 8 випливає, що комплексний показник безпеки W_{SCADA} можна визначити як імовірність події A, застосувавши відомі теореми складання та множення імовірностей [23], а саме:

$$W_{SCADA} = P_{FW} P_{PS} A_{SCADA} + \left[1 - P_{FW}\right] P_{PS} A_{SCADA} + P_{FW} \left[1 - P_{PS}\right] A_{SCADA} + \left[1 - P_{FW}\right] \left[1 - P_{PS}\right] A_{SCADA}, \quad (8)$$

де P_{FW} – ймовірність успішного виконання брандмауером функцій фільтрації вхідних інформаційних потоків (вхідного трафіка); P_{PS} – ймовірність успішного виконання системою паролізації автентифікаційної процедури перевірки пароля; A_{SCADA} – стаціонарний коефіцієнт готовності SCADA КІ.

Для визначення складових співвідношення (8) застосуємо МПМ та метод побудови структурних схем безпеки [17]. На рис. 9 зображено граф станів спрощеної марковської моделі функціонування брандмауера (БДМ), на яку поширюються дії системи обмежень (6).

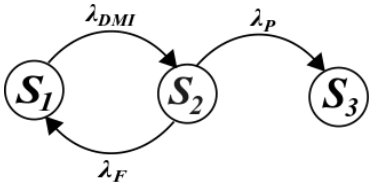

Рис. 9. Граф станів спрощеної марковської моделі функціонування БДМ

У процесі функціонування (рис. 9) БДМ може перебувати в трьох станах:

1) стан S_1 – БДМ працездатний та готовий до фільтрації вхідного трафіка;

2) стан S_2 – БДМ здійснює фільтрацію ШКТ (тобто загрозу усунуто) з інтенсивністю λ_F, який надходить на вхід з інтенсивністю λ_{DMI} і характеризує спробу зловмисника проникнути в систему;

3) стан S_3 – функція фільтрації БДМ вимкнена (тобто наявність загрози) та ШКТ з інтенсивністю λ_P успішно потрапляє в систему.

У початковий момент часу, коли $t=0$, модель перебуває в стані, в якому характеризується імовірностями $P_1(0)=1$, $P_2(0)=P_3(0)=0$. Для отримання результатів моделювання запишемо систему диференціальних рівнянь Колмогорова [23] за умови, що $\sum_{i=1}^{3} P_i(t)=1$

$$\begin{cases} \dfrac{dP_1(t)}{dt} = \lambda_F P_2(t) - \lambda_{DMI} P_1(t); \\ \dfrac{dP_2(t)}{dt} = \lambda_{DMI} P_1(t) - (\lambda_F + \lambda_P) P_2(t); \\ \dfrac{dP_3(t)}{dt} = \lambda_P P_2(t). \end{cases} \tag{9}$$

Виконавши пряме перетворення Лапласа для системи диференціальних рівнянь (9) з урахуванням початкового розподілення імовірностей, перейдемо до системи лінійних рівнянь виду

$$\begin{cases} (s+\lambda_{DMI})\pi_1(s) - \lambda_F \pi_2(s) = 1; \\ -\lambda_{DMI}\pi_1(s) + (s+\lambda_F+\lambda_P)\pi_2(s) = 0; \\ -\lambda_P \pi_2(s) + s\pi_3(s) = 0. \end{cases} \tag{10}$$

Розв’язавши систему лінійних рівнянь (10) методом Крамера та виконавши зворотне перетворення Лапласа, отримаємо співвідношення для визначення імовірностей $P_i(t)$, де i = 1, 2, 3. Зважаючи на те, що система паролізації працює синергічно з брандмауерами, як її характеристики використовуватимемо аналогічні ймовірнісні показники. Тому для кількісної оцінки зазначених показників системи паролізації доцільно використовувати системи рівнянь (9) та (10).

Оцінка стаціонарного коефіцієнта готовності A_{SCADA} може бути отримана шляхом використання аналітико-стохастичного методу побудови структурних схем безпеки та відповідних вхідних даних, які подано в [17]. Зокрема, на рис. 10 зображено діаграму системної відмови (ДСВ) кібернетичних та хмарних активів SCADA КІ.

Відповідно до ДСВ (рис. 10) комплексна ймовірнісна оцінка готовності КА та хмарних активів SCADA КІ може бути визначена так:

$$UnAvailability = P\left(\Phi\left(X\right)=0\right) = P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \overline{FW4} \cup \cup \left[\overline{FW5} \cap \left(\overline{Dell\ \ EMC} \cup DMI\right)\right]\right\}, \quad (11)$$

$$UA_{1-3} = \left\{\left[\overline{Cluster1} \cup DMI\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup DMI\right] \cup \overline{FW2}\right\} \cap \cap \left\{\left[\overline{Cluster3} \cup DMI\right] \cup \overline{FW3}\right\}, \quad (12)$$

$$UA_4 = \left[\overline{AppSRV} \cup DMI\right] \cap \left[\overline{DBSRV} \cup DMI\right] \cap \left[\overline{DmnCTL} \cup DMI\right], \quad (13)$$

$$UA_5 = \left[\overline{AuthSRV} \cup DMI\right] \cap \left[\overline{CTU} \cup DMI\right] \cap \left[\overline{EntprSRV} \cup \cup DMI\right] \cap \left[\overline{AWS} \cup DMI\right], \quad (14)$$

$$UA_6 = \left[\overline{WebSRV} \cup DMI\right] \cap \left[\overline{EmailSRV} \cup DMI\right] \cap \left[\overline{Pr\,oxySRV} \cup DMI\right], \quad (15)$$

де $\overline{Dell\ \ EMC}$ – подія, яка полягає в неготовності універсальної серверної платформи для IT-інфраструктур [25], яка розгорнута на основі масштабованої системної архітектури для збереження великих обсягів даних, проведення складних обчислювальних операцій та розподілення вхідних потоків даних (вхідного трафіка); $\overline{AWS}$ – подія, що полягає в неготовності сервіс-орієнтованих ресурсів хмарного провайдера Amazon, характеристику яких наведено в табл. 2.

У запропонованій моделі подія, позначена як $\overline{AWS}$, заслуговує особливої уваги, тому що характеризує відмову всієї XMI Amazon. Саме ця подія відбулася в лютому 2017 р., коли всі хмарні сервіси AWS були недоступні внаслідок неправильних дій обслуговуючого персоналу [26]. Характеристика решти складових, які входять у співвідношення (11–15), наведена в [17].

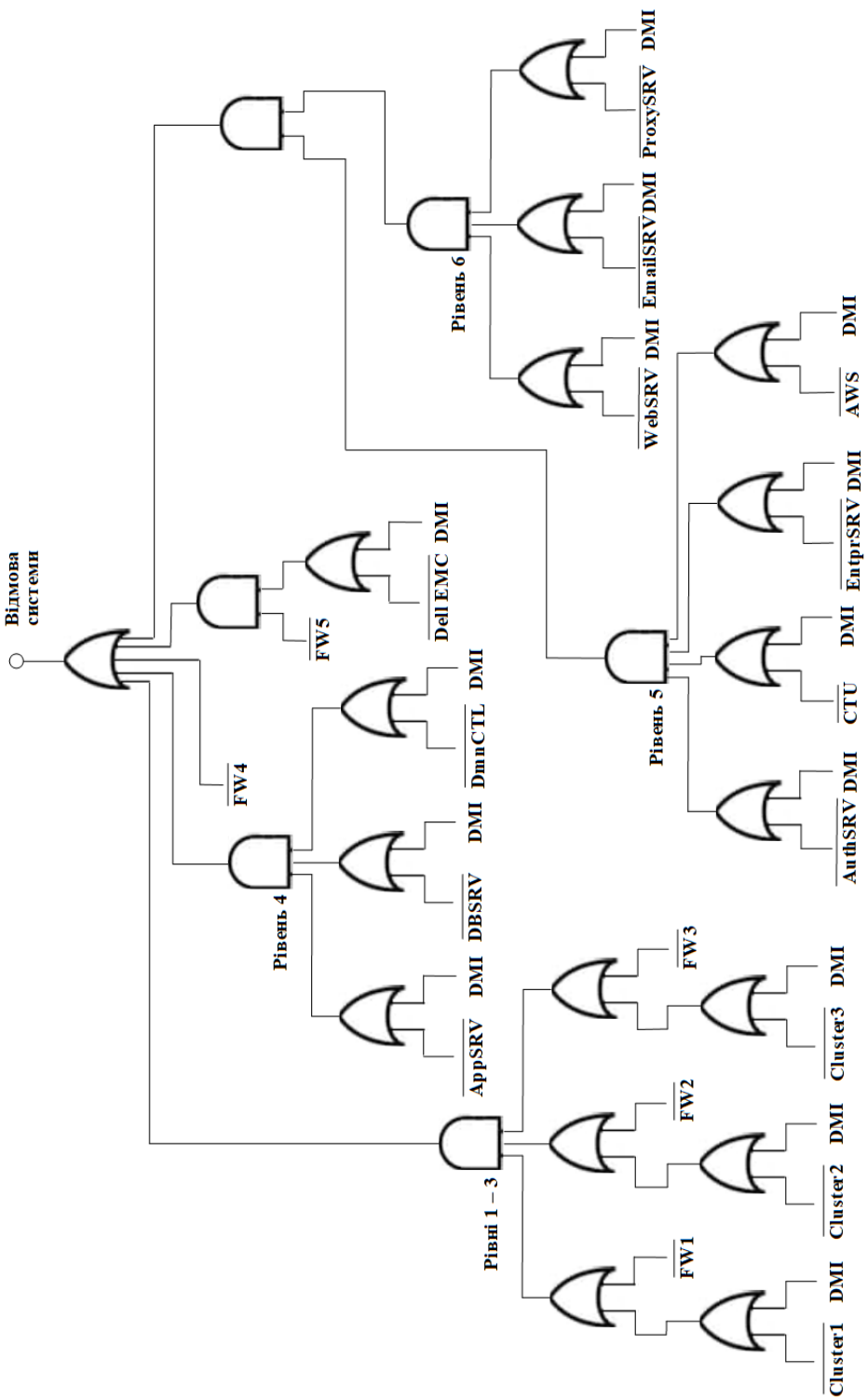

Рис. 10. Діаграма системної відмови кібернетичних та хмарних активів системи SCADA KI

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

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

$$\left. \cup \left[\overline{FW5} \cap \left(\overline{Dell\ \ EMC} \cup DMI\right)\right]\right\}. \qquad (16)$$

Застосуємо отриману ДСВ (рис. 10) для побудови ССН [1; 12; 17]. На рис. 11 зображено ССН кібернетичних та хмарних активів SCADA КІ, що побудована з урахуванням послідовності подій, логіка реалізації яких визначається співвідношеннями (11)–(16).

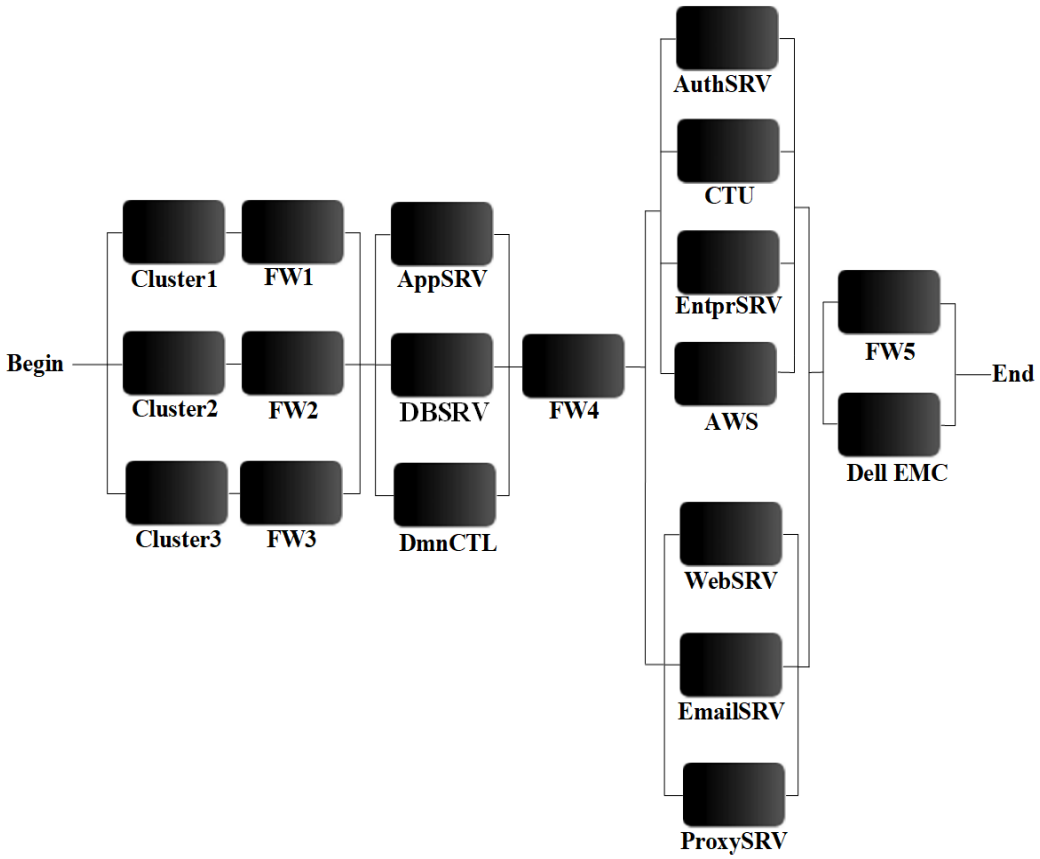

Рис. 11. Структурна схема надійності КА та хмарних активів SCADA КІ

Використовуючи зображену ССН (рис. 11), співвідношення для визначення стаціонарного коефіцієнта готовності КА та хмарних активів SCADA КІ можна записати так:

$$A_{SCADA} = \left\{1-\left[1-A_{Cluster1}A_{FW1}\right]\times\left[1-A_{Cluster2}A_{FW2}\right]\times\left[1-A_{Cluster3}A_{FW3}\right]\right\}\times$$
$$\times\left\{1-\left[1-A_{AppSRV}\right]\times\left[1-A_{DBSRV}\right]\times\left[1-A_{DmnCTL}\right]\right\}\times\left\{1-\left[1-A_{AuthSRV}\right]\times\right.$$
$$\left.\times\left[1-A_{CTU}\right]\times\left[1-A_{EntprSRV}\right]\times\left[1-A_{WebSRV}\right]\times\left[1-A_{EmailSRV}\right]\times\left[1-A_{AWS}\right]\times\right.$$
$$\left.\times\left[1-A_{ProxySRV}\right]\right\}\times\left\{1-\left[1-A_{FW5}\right]\times\left[1-A_{Dell\ EMC}\right]\right\}\times A_{FW4}. \qquad (17)$$

Співвідношення (6)–(17) пов'язані між собою аналітико-стохастичною залежністю і можуть бути використані для розробки відповідного алгоритму оцінки комплексного показника безпеки W_{SCADA} (8) з урахуванням доступності КА та хмарних активів SCADA КІ.

Алгоритм 1: ОЦІНКА КОМПЛЕКСНОГО ПОКАЗНИКА БЕЗПЕКИ W_{SCADA} SCADA КІ

1 Визначення часу моделювання $W_{SCADA}(T)$ як $T = \sum_{i=1}^{n} t_i$
2 Ввод вхідних параметрів $\lambda_{DMI_{max}}$, $\lambda_{DMI_{step}}$, λ_F, λ_P, t_{min}, t_{step}, A_{SCADA_i}
3 Визначення $A_{SCADA} = \prod_k A_{SCADA_k}$
3 **for** $i = 1\ to\ n$ **do**
4 $\lambda_{DMI_i} = \lambda_{DMI_{max}} - i \cdot \lambda_{DMI_{step}}$
5 **for** $j = 1\ to\ m$ **do**
6 $T_j = t_{min} + j \cdot t_{step}$;
7 $k1_{ij} = \lambda_P \cdot \lambda_{DMI_i}$; $k2_{ij} = 1/\left[\lambda_{DMI_i} \cdot \left(\lambda_P - \lambda_F\right)\right]$;
8 $c1_{ij} = -\lambda_P/2 - \lambda_{DMI_I}/2$; $c2_{ij} = sqrt\left(\lambda_P^2 - 2\lambda_P \cdot \lambda_{DMI_I} + \lambda_{DMI}^2 + 4\lambda_{DMI_I} \cdot \lambda_F\right)$;
9 $c3_{ij} = -exp\left\{c1_{ij} - 0{,}5 \cdot c2_{ij}\right\}$; $c4_{ij} = exp\left\{c1_{ij} + 0{,}5 \cdot c2_{ij}\right\}$; $k3_{ij} = -c3_{ij} \cdot \lambda_P$;
10 $k4_{ij} = c4_{ij} \cdot \lambda_P$; $k4_{ij} = c4_{ij} \cdot \lambda_P$; $k5_{ij} = c3_{ij} \cdot \lambda_{DMI}$; $k6_{ij} = c4_{ij} \cdot \lambda_{DMI}$;
11 $k7_{ij} = c2_{ij} \cdot c3_{ij}$; $k8_{ij} = c2_{ij} \cdot c4_{ij}$; $L_{ij} = k3_{ij} + k4_{ij} - k5_{ij} + k6_{ij} + k7_{ij} + k8_{ij}$;
12 $Z_{ij} = 2\lambda_{DMI_i} \cdot c2_{ij}\left(\lambda_P - \lambda_F\right)$; $P_{FW_{ij}} = P_{PS_{ij}} = k1_{ij} \cdot \left[k2_{ij} - L_{ij}/Z_{ij}\right]$;
13 $W_{SCADA_{IJ}} = P_{FW_{ij}}^2 + (1 - P_{FW_{ij}}) \cdot A_{SCADA}\big|_{AWS}^{Networks} \cdot [2P_{FW_{ij}} + (1 - P_{FW_{ij}})]$;
14 **end**
15 **end**
16 **figure**;
17 **meshgrid(**T_j, λ_{DMI_i}**);surf (**$T_j, \lambda_{DMI_i}, W_{SCADA_{IJ}}$**);**
18 **shading interp; colormap parula; colorbar;**

На рис. 12–14 зображено результати моделювання із застосуванням розробленого алгоритму 1 у вигляді тривимірної залежності для випадку, коли протягом доби зловмисники здійснюють атаку на активи SCADA КІ. Результати отримано за умови, що атака здійснюється за сценарієм, функціональна схема реалізації якого зображена на рис. 7.

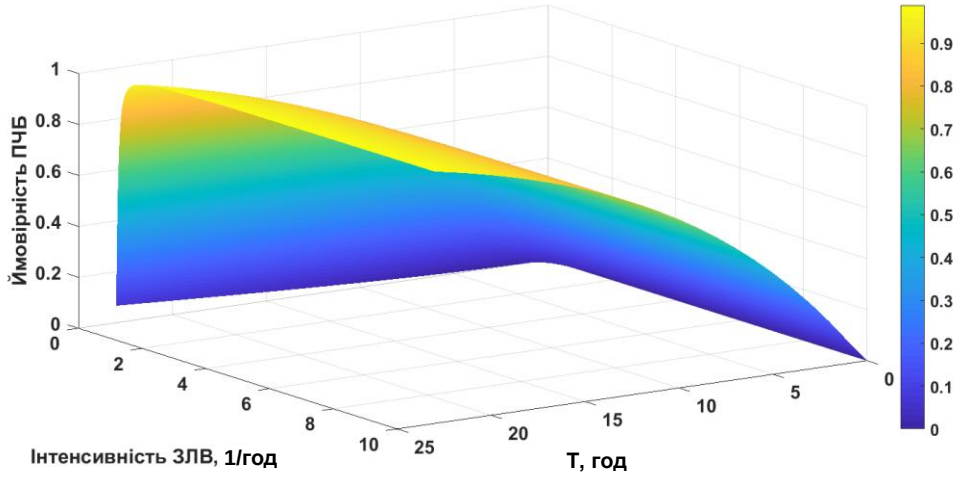

Рис. 12. Залежність імовірності проникнення ЗЛВ через брандмауери (ПЧБ) та злому системи паролізації SCADA КІ від інтенсивності та тривалості дії ШКТ

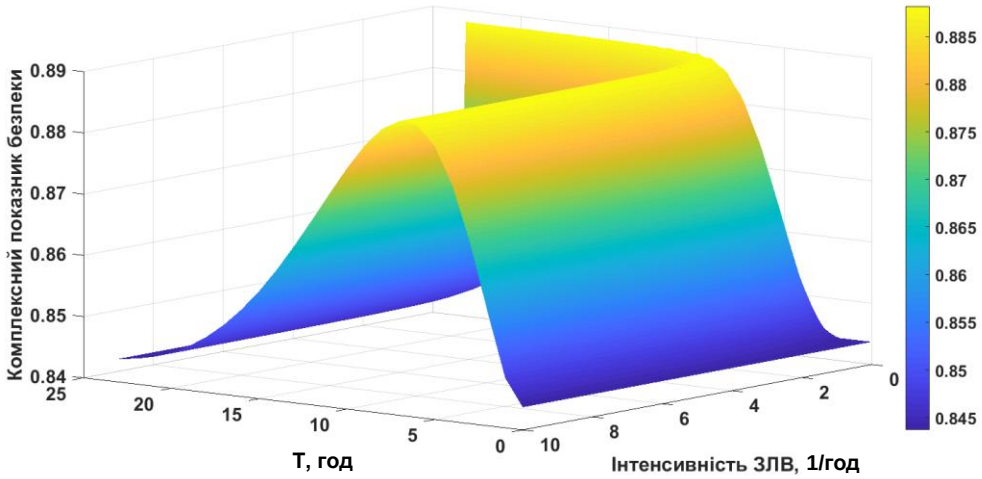

Рис. 13. Залежність комплексного показника безпеки кібернетичних активів SCADA КІ від інтенсивності ЗЛВ та тривалості дії ШКТ

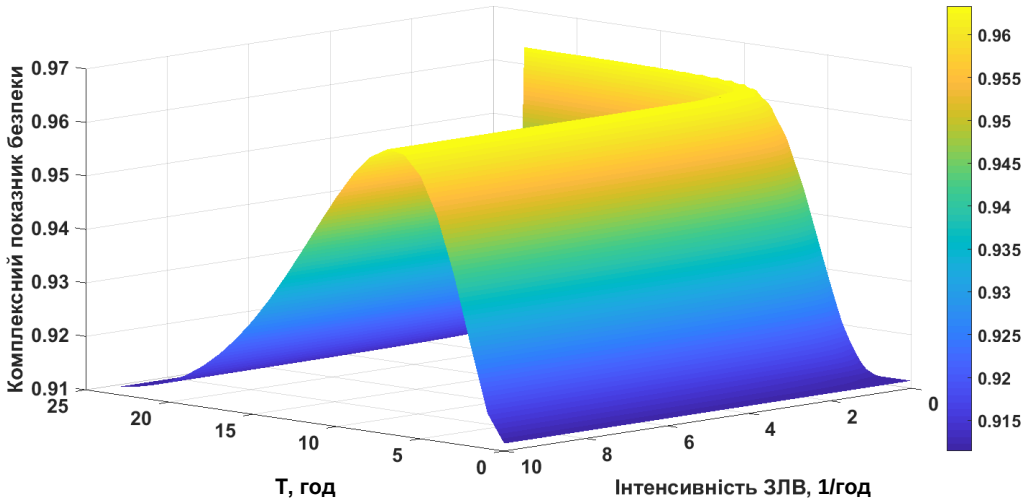

Рис. 14. Залежність комплексного показника безпеки кібернетичних і хмарних активів SCADA КІ від інтенсивності ЗЛВ та тривалості дії ШКТ

Узагальнені результати моделювання залежності комплексного показника безпеки W_{SCADA} від інтенсивності фільтрації шкідливого трафіка λ_F за умови, що ймовірність ПЧБ змінюється відповідно до рис. 12 та інтенсивність зловмисного впливу $\lambda_{DMI_{max}} = 10$ 1/год, зображено на рис. 15.

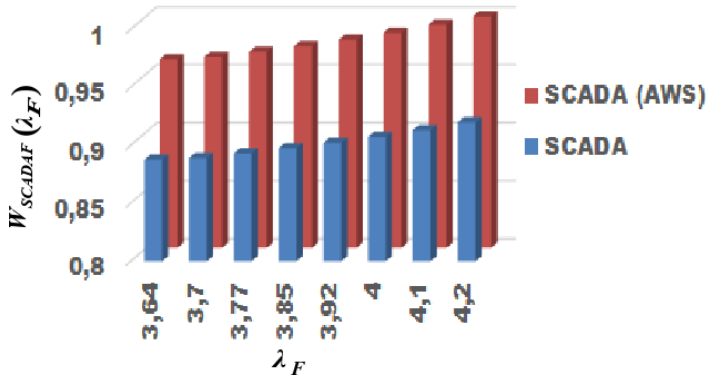

Рис. 15. Узагальнені результати моделювання залежності $W_{SCADA}(\lambda_F)$ для кібернетичних та хмарних активів SCADA КІ

Отримані результати моделювання (рис. 12–15) підтверджують доцільність застосування додаткових хмарних ресурсів для підтримання необхідного рівня функціональної та інформаційної безпеки SCADA КІ.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Отримані результати аналітико-стохастичного моделювання в умовах зловмисних впливів та дії шкідливого трафіка свідчать про переваги застосування додаткових хмарних активів, що дає змогу підтримувати необхідний рівень безпеки системи SCADA КІ. Кількісні результати моделювання підтверджують, що використання хмарних активів спільно з відповідними системами кіберзахисту дозволяє підвищити значення комплексного показника безпеки на 10 % порівняно з рівнем безпеки на основі застосування лише кібернетичних активів.

Подальші перспективи розвитку розглянутого науково-методичного апарату, сервіс-орієнтованих систем, інформаційної технології пов'язані з можливістю їхньої реалізації в контурі управління критичними інфраструктурами для підвищення ефективності використання КІ за призначенням з дотриманням високих стандартів гарантоздатності й доступності всіх видів ресурсів.

Дослідження виконано в рамках науково-дослідних та дослідно-конструкторських робіт (державний реєстраційний номер: 0119U100979), які проводяться Національним аерокосмічним університетом ім. М. Є. Жуковського у галузі забезпечення інформаційної безпеки критичних інфраструктур.

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.

Список використаних джерел:

1. *Dantas J., Matos R., Araujo J., Maciel P.* Eucalyptus-based private clouds: availability modeling and comparison to the cost of a public cloud // Computing. 2015. Vol. 97 (11). P. 1121–1140.

2. *Byun J., Kim Y., Hwang Z., Park S.* An intelligent cloud-based energy management system using machine to machine communications in future energy environments: materials in *2012 IEEE International Conference on Consumer Electronics (ICCE)*. USA, 2012. P. 664–665.

3. *Yigit M., Gungor V. C., Baktir S.* Cloud computing for smart grid applications // Computer Networks. 2014. Vol. 70. P. 312–329.

4. *Anderson D., Gkountouvas T., Meng M.* GridCloud: infrastructure for cloud-based wide area monitoring of bulk electric power grids // *IEEE* Transactions on Smart Grid. 2018. Vol. 10 (2). P. 2170–2179.

5. *Bakken D.* Smart grids: clouds, communications, open source and automation. London: CRC Press, 2014. 60 p.

6. *Marzal S., González-Medina R., Salas-Puente R.* An embedded Internet of energy communication platform for the future smart microgrids management // IEEE Internet of Things Journal. 2019. Vol. 6 (4). P. 7241–7252.

7. *Fairley P.* Cybersecurity at U.S. utilities due for an upgrade: tech to detect intrusions into industrial control systems will be mandatory IEEE Spectrum. 2016. Vol. 53 (5). P. 11–13.

8. *Иванченко О., Харченко В.* Анализ стохастических методов метамоделирования и оценивания готовности облачных инфраструктур // Радіоелектронні і комп'ютерні системи. 2016. № 6 (80). С. 6–11.

9. *Ghosh R., Longo F., Xia R.* Stochastic Model Driven Capacity Planning for an Infrastructure-as-a-Service Cloud // IEEE Transaction on Services Computing. 2013. Vol. 7(4). P. 667–680.

10. *Tuffin B., Trivedi K.* Implementation of Importance Splitting Techniques in Stochastic Petri Net PAckage: materials in 11th International Conference, TOOLS 2000 Schaumburg, USA. 2000. P. 216–229.

11. *Trivedi K., Sahner R.* SHARPE at the Age of Twenty Two // ACM Sigmetrics Performance Evaluation Review. 2009. Vol. 36 (4). P. 52–57.

12. *Melo M., Maciel P., Araujo J.* Availability study on cloud computing environments: live migration as a rejuvenation mechanism: materials in 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Hungary, 2013. P. 1–6.

13. *Khazaei H., Barna C., Litoiu M.* Performance modeling of microservice platforms considering the dynamics of the underlying cloud infrastructure. 2019. URL: https://arxiv.org/pdf/1902.03387v1.pdf

14. *Trivedi K., Sharma V.* Quantifying software performance, reliability and security: an architecture-based approach // Journal of Systems and Software, 2007. Vol. 80 (4) P. 493–509.

15. *Mateo-Fornés J., Solsona-Tehàs F., Vilaplana-Mayoral J.* CART, a decision SLA model for SaaS providers to keep QoS regarding availability and performance // IEEE Access. 2019. Vol. 7. P. 38195–38204.

16. *Ardagna D., Ciavotta M., Passacantando M.* Generalized nash equilibria for the service provisioning problem in multi-cloud systems // IEEE Transactions on Services Computing. 2019. Vol. 10 (3). P. 381–395.

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

18. *Yu S.-Z., Kobayashi H.* A hidden semiMarkov model with missing data and multiple observation sequences for mobility tracking // Signal Processing. 2003. Vol. 83 (2). P. 235–250.

19. *Харченко В. С.* Гарантоздатні системи та багатоверсійні обчислення, аспекти еволюції // Радіоелектронні і комп'ютерні системи. 2009. № 7 (41). С. 46–59.

20. *Ahmed I., Obermeier S., Naedele M., Richard III G. G.* Scada systems: Challenges for forensic investigators // Computer. 2012. Vol. 45 (12), P. 44–51.

21. *Касьянов В.* Применение графов в программировании // Программирование. 2001. № 27 (3). С. 51–76.

22. *Ammann P., Offutt J.* Introduction to software testing. Cambridge University Press, 2016. 50 p.

23. *Bolch G., Greiner S., De Meer H., Trivedi K.* Queueing networks and Markov chains: modeling and performance evaluation with computer science applications. John Wiley & Sons, 2006. 878 p.

24. *Ten C. W., Liu C., Manimaran G.* Vulnerability assessment of cybersecurity for SCADA systems // IEEE Transactions on Power Systems. 2008. Vol. 23 (4). P. 1836–1846.

25. Dell Incorporation (2018) // EMC PowerEdge R640, Technical Guide. URL: https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/us/PowerEdge-R640-Technical-Guide.pdf

26. AWS (2018) // Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region. URL: https://aws.amazon.com/ru/message/41926

References:

1. Dantas J., Matos R., Araujo J., & Maciel P. (2015), *Eucalyptus-based private clouds: availability modeling and comparison to the cost of a public cloud*, journal *Computing*, vol. 97(11), pp. 1121–1140.

2. Byun J., Kim Y., Hwang Z., Park S. (2012), "An intelligent cloud-based energy management system using machine to machine communications in future energy environments", materials in *2012 IEEE International Conference on Consumer Electronics (ICCE)*, USA. P. 664–665.

3. Yigit M., Gungor V. C. and Baktir S. (2014), "*Cloud computing for smart grid applications*", journal *Computer Networks*, vol. 70, pp. 312–329.

4. Anderson D., Gkountouvas T., Meng M., Birman K., Bose A., Hauser C., Zhang Q. (2018), *"GridCloud: infrastructure for cloud-based wide area monitoring of bulk electric power grids"*, journal *IEEE Transactions on Smart Grid*, vol. 10(2), p. 2170-2179.

5. Bakken D. (2014) Smart Grids: clouds, communications, open source and Automation. London: CRC Press, 2014, 60 p.

6. Marzal S., González-Medina R., Salas-Puente R., Garcerá G., Figueres E. (2019), *"An Embedded Internet of Energy Communication Platform for the Future Smart Microgrids Management"*, journal *IEEE Internet of Things Journal*, vol. 6(4), p. 7241–7252.

7. Fairley P. (2016). *"Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory*", journal *IEEE Spectrum*, vol. 53(5), p. 11–13.

8. Ivanchenko O., Kharchenko V. (2016), *"Analysis of stochastic methods for metamodeling and availability estimation for cloud infrastructure",* journal Radioelectronic and computer systems, vol. (80), p. 6–11.

9. Ghosh R., Longo F., Xia R., Naik K. and Trivedi K. (2013). *"Stochastic Model Driven Capacity Planning for an Infrastructure-as-a-Service Cloud",* journal *IEEE Transaction on Services Computing*, vol. 7(4), p. 667–680.

10. Tuffin B. and Trivedi K. (2000), *"Implementation of Importance Splitting Techniques in Stochastic Petri Net PAckage",* materials in *11th International Conference, TOOLS 2000 Schaumburg*, USA, p. 216–229.

11. Trivedi, K. and Sahner, R. (2009). *"SHARPE at the Age of Twenty Two",* journal *ACM Sigmetrics Performance Evaluation Review*, vol. 36(4), p. 52–57.

12. Melo M., Maciel P., Araujo J., Matos R. and Araujo C. (2013), "Availability study on cloud computing environments: Live migration as a rejuvenation mechanism", materials in *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Hungary, P. 1–6.

13. H. Khazaei, C. Barna and M. Litoiu (2019), *Performance Modeling of Microservice Platforms Considering the Dynamics of the Underlying Cloud Infrastructure*, [Online], available at: https://arxiv.org/pdf/1902.03387v1.pdf

14. Trivedi K. and Sharma V. (2007), *"Quantifying software performance, reliability and security: An architecture-based approach"*. *Journal of Systems and Software*, vol. 80 (4), p. 493–509.

15. Mateo-Fornés J., Solsona-Tehàs F., Vilaplana-Mayoral J., Teixidó-Torrelles I., Rius-Torrentó J. (2019). *"CART, a Decision SLA Model for SaaS Providers to Keep QoS Regarding Availability and Performance",* journal *IEEE Access*, vol. 7, p. 38195–38204.

16. Ardagna D., Ciavotta M. and Passacantando M. (2015). *"Generalized nash equilibria for the service provisioning problem in multi-cloud systems",* journal *IEEE Transactions on Services Computing*, vol. 10(3), p. 381–395.

17. Ivanchenko O. (2019). *"Analytical and stochastic method in order to build safety and security block diagrams of cyber assets of SCADA system for critical infrastructure"*, journal *Systems and Technologies*, vol. 1(57), p. 81–106.

18. Yu S.-Z. and Kobayashi H. (2003). *"A hidden semiMarkov model with missing data and multiple observation sequences for mobility tracking",* journal *Signal Processing, vol. 83(2), pp. 235–250.*

19. Kharchenko and V. (2009). *"Dependable systems and multi-version computing: aspects of evolution",* journal *Radioelectronic and computer systems*, vol. 7(41), p. 46–59.

20. Ahmed I., Obermeier S., Naedele M. and Richard III, G. G. (2012), *"Scada systems: Challenges for forensic investigators",* journal *Computer*, vol. 45(12), pp. 44–51.

21. Kasyanov V. (2001), "*Primenenie grafov v programmirovanii*", nauchno-tehnicheskiy zhurnal *Programmirovanie*, vol. 27(3), pp. 51–76.

22. *Ammann P.* and *Offutt J.* Introduction to software testing. Cambridge University Press, 2016, 50 p.

23. Bolch G., Greiner S., De Meer H. and Trivedi K. *Queueing networks and Markov chains: modeling and performance evaluation with computer science applications.* John Wiley & Sons, 878 p.

24. Ten C. W., Liu C. and Manimaran, G. (2008). *"Vulnerability assessment of cybersecurity for SCADA systems",* journal *IEEE Transactions on Power Systems*, vol. 23(4), p. 1836–1846.

25. Dell Incorporation (2018), *EMC PowerEdge R640, Technical Guide*, [Online], available at: https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/us/PowerEdge-R640-Technical-Guide.pdf

26. AWS (2018), *Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region*, [Online]. available at: https://aws.amazon.com/ru/message/41926