DOI: https://doi.org/10.32836/2521-6643-2019-1-57-6
УДК 62-526

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

АНАЛІТИКО-СТОХАСТИЧНИЙ МЕТОД ПОБУДОВИ СТРУКТУРНИХ СХЕМ БЕЗПЕКИ КІБЕРНЕТИЧНИХ АКТИВІВ СИСТЕМИ SCADA КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення інформаційної безпеки систем диспетчеризації та збирання даних типу SCADA, які застосовуються у відповідному контурі управління критичної інфраструктури (КІ) – одне з найважливіших завдань, які виконуються за напрямом критичний комп'ютинг та інженерія безпеки. Наочним прикладом цього є атаки на компоненти критичної енергетичної інфраструктури (КЕІ), коли фактично зловмисні впливи на кібернетичні активи системи SCADA призводили до відключення обласних енергетичних кластерів КЕІ. Тому актуальність статті, яка присвячена розробці методу побудови структурних схем безпеки SCADA КІ на основі оцінювання рівня надійності, готовності компонентів та можливості протидії зловмисним впливам на загальні кібернетичні активи, не викликає сумніву.

Ключові слова: *система SCADA; критична інфраструктура; кібернетичні активи; структурна схема безпеки; аналітико-стохастичне оцінювання.*

Обеспечение информационной безопасности систем диспетчеризации сбора данных типа SCADA, используемых в соответствующем контуре управления критической инфраструктуры (КИ), является одной из важнейших задач, которые решаются в рамках исследований, проводимых в сфере критического компьютинга и инженерии безопасности. Атаки на компоненты критической энергетической инфраструктуры (КЭИ), когда фактически злонамеренные воздействия на кибернетические активы системы SCADA приводили к отключению областных энергетических кластеров, – яркое тому свидетельство. Поэтому актуальность статьи, которая посвящена разработке метода построения структурных схем безо-

пасности SCADA КИ на основе оценивания уровня надёжности, готовности компонентов и возможности противодействия злонамеренным воздействиям на общие кибернетические активы, не вызывает сомнения.

Ключевые слова: *критическая инфраструктура; кибернетические активы; структурная схема безопасности; аналитико-стохастическое оценивание.*

Safety and security of supervisory control and data acquisition systems (SCADA), which utilize in corresponding management circuit of a critical infrastructure (CI) is one of the most important task that to be explored. This task is also serious issue for critical computing and security engineering realm. Familiar examples of the negative events for critical energy infrastructure's (CEI) components, when malicious deliberate impacts on cyber assets of SCADA system led to outages of the regional energy clusters are bright evidences of this issue. Therefore, the presented paper is devoted to a technique development of security block diagrams for CI SCADA systems based on assess of dependability and availability of their components considering malicious deliberate impacts on overall cyber assets. In fact, it is also undoubtedly distinct significant issue into critical computing realm. Proposed technique is developed based on taxonomy for risk assess considering some negative factors. These negative factors can influence on overall availability and cybersecurity of the CI. Therefore, how to get safety and security assessments and further how to ensure effective functioning of SCADA CI is a distinct significant issue, which to be explored. The technique involves concrete steps in order to build fault tree for cyber assets of the SCADA CI. Next step allows to write overall equation for system failure based on the use of received fault tree. In addition, the researcher continues to build a reliability block of diagram (RBD) in order to estimate overall availability level for cyber assets of the SCADA CI. Using RBD and information about deliberate malicious impacts (DMIs), researcher can be built a DMI block diagram in order to estimate probability assessment for different DMIs. As general results, the researcher can determine probability of compromise operation, when intruders want to implement the DMI. Thus, if you wanted to perform a deep analysis of safety and security of the SCADA system of the CI considering different negative events, such as sudden and hidden failures, accidents and disaster of the CI, including DMIs, you would be able to use the proposed technique.

Key words: *critical infrastructure; cyber assets; security block diagrams; analytical and stochastic assessments.*

Постановка проблеми. У сучасному суспільстві критична інфраструктура (КІ) є важливою складовою, яка безпосередньо впливає на якість життя людей та визначає певний рівень національної безпеки будь-якої країни. Тому інтенсифікація розвитку КІ супроводжується сталим зростанням ресурсів, сервісів та відповідної продукції, які постачаються саме нею, чому значною мірою сприяє широкомасштабне впровадження інформаційних технологій та розширення відповідних кібернетичних активів інфраструктури. Безумовно, це призводить до підвищення ефективності управління КІ на основі застосування програмно-апаратних засобів, які об'єднуються в системи диспетчеризації та збирання даних типу SCADA. Водночас замкнений контур управління КІ створюється за рахунок повсюдного використання технологій цифрової трансформації, звичайного та промислового Інтернету речей (IoT, IIoT) тощо.

Однак процес упровадження цих новітніх технологій супроводжується зниженням рівня функціональної та інформаційної безпеки КІ, що особливо чітко спостерігається на прикладі критичної енергетичної інфраструктури (КЕІ). Зокрема, відбуваються аварії, інциденти і катастрофи КЕІ, наприклад аварії на Саяно-Шушенській ГЕС (Росія, 2009 р.), на АЕС Фукусіма (Японія, 2011 р.), відомі випадки каскадних відключень енергопостачання в США та Європі, включаючи відключення вітчизняних обленерго за останні чотири роки. Відомо [1], що під час відключень українських обласних енергетичних кластерів здійснювалися зловмисні впливи на контур управління КЕІ з реалізацією хакерських атак на систему SCADA. Ці та інші фактори негативного впливу створили відповідні передумови для виникнення науково-прикладної проблеми, яка полягає в необхідності розробки методу оцінювання і контролю рівня функціональної, інформаційної безпеки системи SCADA КІ з урахуванням її мережних кібернетичних активів.

Аналіз останніх досліджень і публікацій. Розгляд публікацій за напрямом досліджень розпочнемо з праць [2; 3], присвячених цифровим пристроям функціонального контролю інформаційно-управляючих систем (ІУС) на основі застосування FPGA-логіки, тобто логіки, яка побудована на програмованих логічних інтегральних схемах. Нині застосування FPGA-логіки дає можливість покращити функціональність і відмовостійкість компонентних складових ІУС. Тому цілком виправдане прагнення як виробників, так і персоналу КІ використовувати FPGA-логіку для створення пристроїв оцінки та контролю функціональної безпеки систем SCADA інфраструктурного рівня.

У дослідженні [4] розглянуто моделі готовності, які застосовуються для оцінки рівня відмовостійкості систем SCADA з урахуванням можливості управління з використанням віддалених терміналів (ВТ). Значна частина

роботи висвітлює особливості застосування методу розбудови діаграм відмовостійкості саме для ВТ. Слід також зазначити, що для досягнення необхідного рівня кібербезпеки систем SCADA деякі автори пропонують застосовувати випробувальний стенд, до складу якого входять різноманітні компоненти, включаючи ВТ, інфокомунікаційні системи, фізичну інфраструктуру, сенсори та виконавчі механізми. Архітектурна реалізація стенда подана в праці [5].

Водночас у праці [6] відображено процес ітераційного моделювання для забезпечення надійного функціонування інфокомунікаційних мереж системи SCADA, яка входить до складу ІУС критичної енергетичної інфраструктури. Фактично автори реалізували процес моделювання відповідно до конкретних сценаріїв розвитку подій на основі застосування програмного інструментарію Möbius [7].

З погляду викладення фундаментальних основ застосування відомих аналітико-стохастичних методів та моделей, цікава праця [8], присвячена аналізу можливостей застосування відомих методів структурних схем надійності (ССН) [9], дерева відмов (ДВ) [10; 11], марковських моделей і стохастичних мереж Петрі [12–14] для оцінювання готовності різноманітних комп'ютерних систем критичного призначення. Моделювання процесів зміни рівня готовності, надійності та живучості комп'ютерних віртуальних систем, хмарної приватної та мобільної інфраструктур на основі застосування відомих методів ССН, ДВ [9–11] і неперервних марковських ланцюгів відображено в [15–18]. Марковський процес моделювання лежить також в основі аналітико-стохастичного підходу, який застосовується для аналізу та оцінки ефективності заходів щодо забезпечення необхідного рівня кібербезпеки системи домашнього Інтернету з урахуванням вразливостей компонентних складових [19].

В окремих випадках дослідження та аналіз заходів безпеки систем SCADA може здійснюватись із застосуванням немарковського апарата моделювання. Це стосується ситуацій, коли не спостерігається марковська властивість, скажімо, перевищено період виконання сезонного технічного обслуговування та діагностики технологічного комп'ютерного обладнання SCADA; коли протягом декількох років не проводиться оновлення програмного забезпечення системи SCADA; внаслідок помилок обслуговуючого персоналу виникають непередбачені тривалі простої обладнання SCADA тощо. Серед немарковських моделей, як правило, перевагу віддають напівмарковським моделям. Це пов'язано з тим, що цей тип моделей дозволяє враховувати як різні режими застосування за призначенням, так і різноманітну природу виникнення негативних явищ для ІУС КІ. Отже, на відміну від ма-

рковського, напівмарковський процес моделювання (НПММ) може бути реалізовано для багатофункціональних компонентів КІ, які застосовуються за призначенням протягом випадкового і детермінованого інтервалів часу з урахуванням усієї попередньої історії розвитку та для різноманітних стохастичних залежностей параметрів об'єкта дослідження [20]. Тому на основі НПММ було виконано аналіз ефективності системи контролю та моніторингу технічного стану критичної інфраструктури [20; 21], обґрунтовано перехід до управління КІ за технічним мегастаном з урахуванням надійності її компонентних складових [22; 23]. У праці [24] розглянуто, яким чином НПММ може бути застосовано для аналізу аварій та інцидентів критичної енергетичної інфраструктури. Порівняльний аналіз кількісних результатів марковського та НПММ моделювання підтверджує [20], що напівмарковський процес моделювання краще відображає реальну ситуацію щодо інформаційно-технічного стану КІ і повною мірою відповідає вимогам критичного комп'ютингу [25].

Не зважаючи на відповідність певним нормативним вимогам, нині відомі факти та наслідки хакерських атак на кіберактиви національної КІ [1], що підтверджують її вразливість. Цей негативний фактор впливу, який створено ненавмисно штучно, відображає кіберфізичну природу КІ [26] та відкриває різноманітні можливості щодо втручання в контур управління інфраструктури завдяки використанню активів системи SCADA. Відповідно до [27], серйозною загрозою для систем SCADA можуть бути вразливості їхнього програмного забезпечення, які створюють передумови для успішної реалізації кібератак різноманітного походження. Ці обставини викликають серйозну стурбованість як у виробників, так і в користувачів систем SCADA, які закликають створювати законодавчу базу для розробки різних механізмів забезпечення кібербезпеки [28].

Справжнім відкриттям щодо реалізації зловмисних впливів (ЗЛВ) на кібернетичні ресурси SCADA стали віруси Stuxnet і Flame, які у 2010 та 2012 рр. були реалізовані у вигляді розподіленої бот-мережі, завдяки чому в усьому світі було інфіковано від 50 до 100 тисяч комп'ютерних систем одночасно [29; 30]. Отже, в минулі роки й досі актуальне завдання – створення ефективного кіберзахисту всіх видів активів КІ, включаючи системи SCADA.

Заходи кіберзахисту SCADA системи КІ можуть бути реалізовані на рівні архітектурних рішень. Так, у [31–34] розглянуто й виконано аналіз архітектурних рішень щодо забезпечення кіберзахисту типової системи SCADA як на рівні додатків, каналів передачі даних, так і на мережному рівні.

Подальші перспективи розвитку систем SCADA значною мірою залежать від можливостей застосовувати додаткові хмарні ресурси та сервіси, що дуже посилює інформаційно-обчислювальний потенціал і розширює динамічний діапазон управління КІ. Виходячи з цього, виправданим є застосування мобільної хмарної інфраструктури (МХІ) в системі управління КІ. Для оптимізації енергоспоживання та частотного діапазону кінцевих пристроїв МХІ в [35] автори використали напівмарковські моделі прийняття рішень. Останні дослідження у сфері кібербезпеки ІУС КІ [36] підтверджують високу ефективність застосування адаптивних багатофункціональних хмарних систем як брандмауерів, які використовуються для двосторонньої фільтрації інформаційного трафіку. В працях [37; 38] викладено результати досліджень щодо застосування додаткового хмарного ресурсу з метою створення системи управління інтелектуальною розподіленою енергетичною інфраструктурою майбутнього.

Мета статті. За результатами виконаного аналізу можна зробити висновок, що для посилення наявної системи функціональної та інформаційної безпеки КІ необхідно вдосконалювати відомі аналітико-стохастичні методи оцінювання рівня готовності та кібербезпеки SCADA. Виходячи із цього, мета статті – розробка аналітико-стохастичного методу побудови структурних схем безпеки (ССБ) системи SCADA критичної інфраструктури з урахуванням аспектів, пов’язаних із забезпеченням доступності та захисту її кібернетичних активів від зловмисних впливів і проникнень.

Виклад основного матеріалу. Особливо гостро проблема забезпечення доступності та захисту кібернетичних активів стоїть перед національною КЕІ. Про це свідчить зростання кількості кібератак та суттєве зниження готовності фізичних активів національної КЕІ за останні п’ять років. Значною мірою цьому сприяє той факт, що рівень зношеності енергетичного обладнання національної мережі КЕІ перевищує 70 %. Саме ці два потужних негативних фактори впливу враховуватимемо в розбудові структурних схем безпеки SCADA КІ.

Як базову розглянемо спрощену архітектурну реалізацію кібернетичних активів SCADA КІ (рис. 1). Основною функцією системи на мережному рівні є обробка даних, які надходять безпосередньо від КІ, а також контроль та моніторинг інформаційно-технічних станів, параметрів інфраструктури. Згідно з рис. 1 перший рівень створено мережею кінцевих пристроїв, до складу яких входять програмні логічні контролери (ПЛК) та пристрої зв’язку з об’єктом (ПЗО). Фактично ПЛК та ПЗО забезпечують обробку інформації від сенсорних систем і модулів КІ.

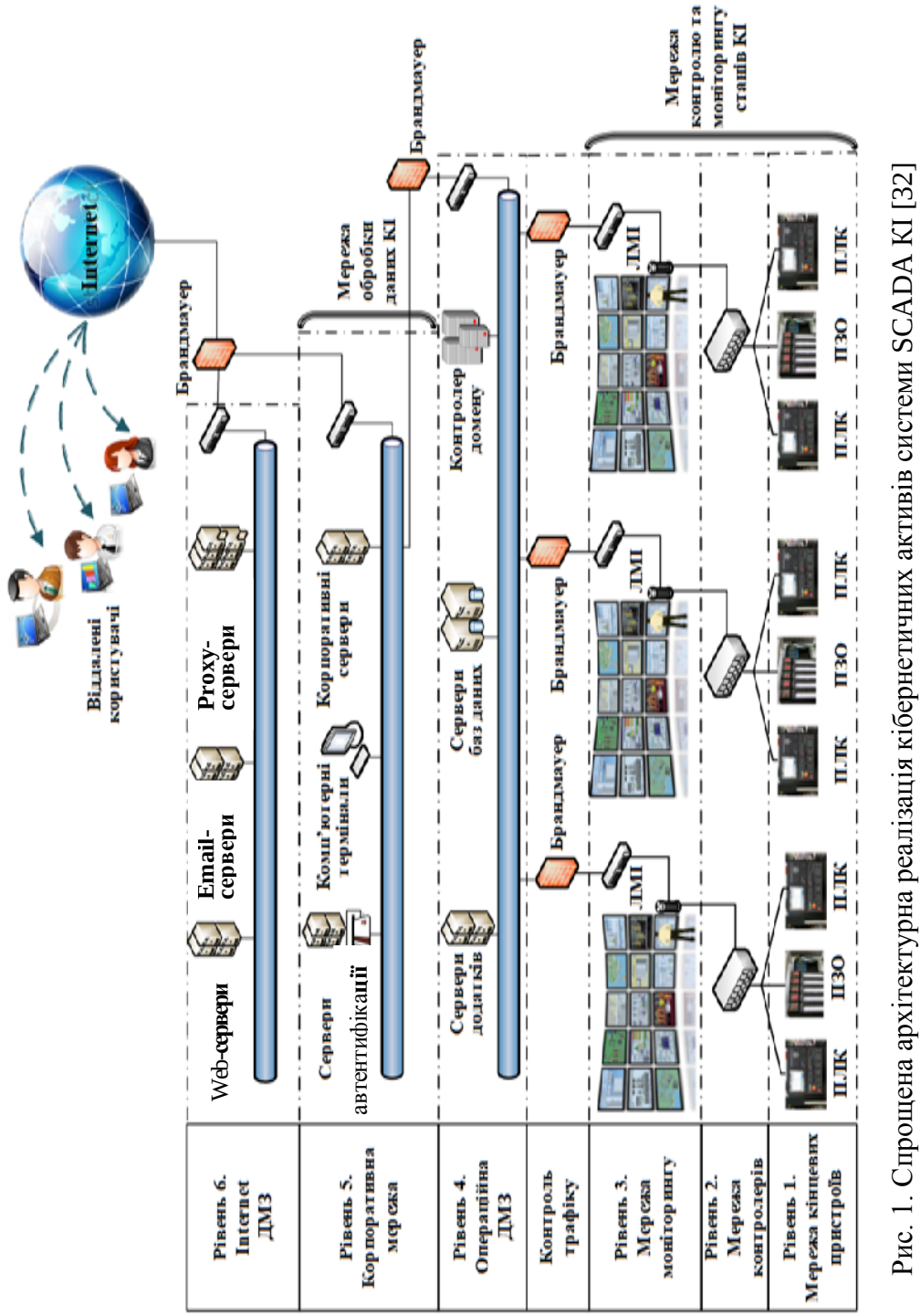

Рис. 1. Спрощена архітектурна реалізація кібернетичних активів системи SCADA КІ [32]

Детальний аналіз функціональних особливостей побудови мережних рівнів кібернетичних активів SCADA КІ (рис. 1) виконано в [32]. Зауважимо, що в розробці пропонованого методу було враховано негативні фактори, які впливають на рівень функціональної (ФБ) та інформаційної безпеки (ІБ) SCADA відповідно до вимог стандартів IEC 61508, ISA/IEC 62443 та рекомендацій, наведених у [39; 40]. Логічним завершенням виконаного аналізу є пропонований аналітико-стохастичний метод побудови ССБ кібернетичних активів системи SCADA КІ, який містить такі кроки.

Перший крок. Визначення кількості мережних рівнів згідно з архітектурною реалізацією кібернетичних активів SCADA КІ (рис. 1).

Другий крок. Побудова таксономічної схеми ризику негативного впливу на ФБ та ІБ системи SCADA КІ. На рис. 2 зображено таксономію виникнення ризику ФБ та ІБ системи SCADA КІ з урахуванням двох найбільш суттєвих негативних факторів впливу, а саме: зловмисних впливів на кібернетичні активи; відмов та збоїв комп'ютерного обладнання і відповідних програмних модулів. Фактично наведена таксономічна схема (рис. 2) пояснює природу виникнення загрози безпеці системи SCADA.

Відповідно до рис. 2 концепція безпеки полягає в зниженні ризику системи SCADA КІ за рахунок зменшення відмов та збоїв її комп'ютерного обладнання і програмного забезпечення, а також завдяки усуненню ЗЛВ на кібернетичні активи, які застосовуються в контурі управління інфраструктурою. Слід ще раз звернути увагу на те, що суттєвим обмеженням дії запропонованої концепції є врахування лише двох найбільш актуальних негативних факторів впливу.

Третій крок. Розробка логіко-ймовірнісної моделі ризику для ФБ та ІБ (далі – безпеки) системи SCADA КІ.

Згідно з таксономічною схемою (рис. 2) логіко-ймовірнісна модель ризику для безпеки (РБ) системи SCADA КІ з урахуванням факторів негативного впливу може бути записана у такому вигляді:

$$Risk = P\left\{\left[\left(SAF \cup INS\right) \cap FF\right] \cap \left[FF \cap DMI\right] \cap \left[\left(SAF \cup INS\right) \cap DMI\right]\right\}, \qquad (1)$$

де SAF – ФБ системи SCADA КІ;

INS – ІБ системи SCADA КІ;

FF – відмови та збої комп'ютерного обладнання і програмного забезпечення SCADA КІ; DMI – ЗЛВ на кібернетичні активи SCADA КІ.

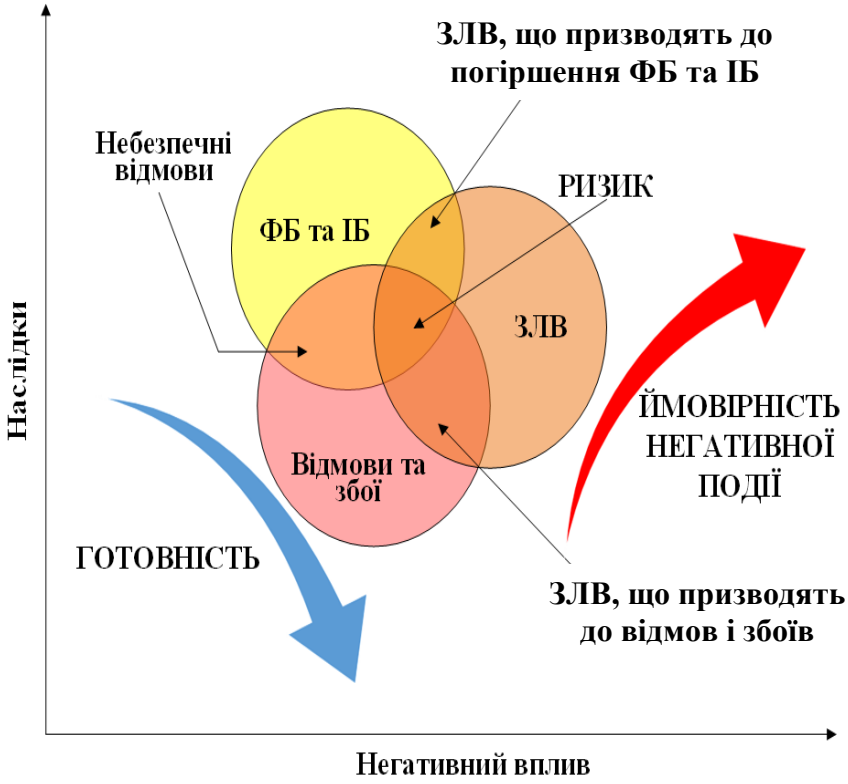

Рис. 2. Таксономія ризику для функціональної та інформаційної безпеки системи SCADA КІ

Четвертий крок. Побудова діаграми системної відмови (ДСВ) з урахуванням факторів негативного впливу на кібернетичні активи системи SCADA КІ.

На рис. 3 зображено ДСВ відповідно до отриманої логіко-ймовірнісної моделі РБ (1) системи SCADA КІ, яка враховує відмови комп'ютерного обладнання, збої програмного забезпечення та зловмисні впливи на кібернетичні активи. Пропозиції, наведені в [10; 11], були використані як теоретичне підґрунтя в побудові ДСВ.

Головна особливість отриманої ДСВ (рис. 3), на відміну від відомих, полягає у відображенні ЗЛВ (позначається як DMI) на сервери відповідного мережного рівня. Це дає можливість отримати комплексну ймовірнісну оцінку готовності (доступності) кіберактивів SCADA з урахуванням природи виникнення та механізмів дії ЗЛВ. Моделі ЗЛВ на кіберактиви системи SCADA КІ на основі НПММ перспективні з погляду подальших досліджень.

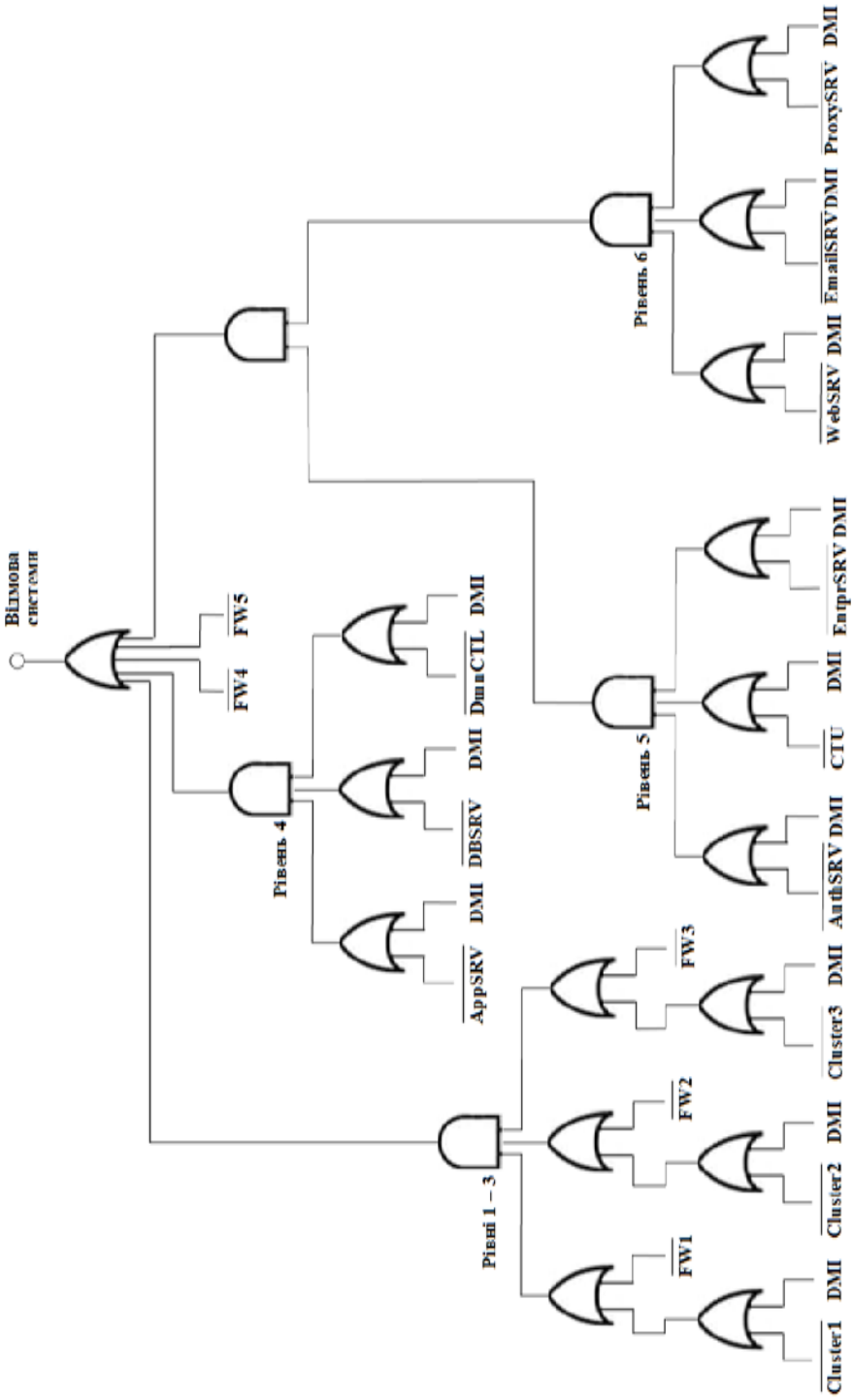

Рис. 3. Діаграма системної відмови кібернетичних активів системи SCADA КІ

Відображені на діаграмі (рис. 3) кластери $Cluster1,2,3$ утворені шляхом укрупнення та об'єднання елементів мережних рівнів 1, 2, 3, а саме: ПЛК, ПЗО, контролерів та людино-машинних інтерфейсів (ЛМІ).

П'ятий крок. Визначення комплексної ймовірнісної оцінки неготовності кіберактивів SCADA КІ.

Відповідно до зображеної рис. 3 ДСВ комплексна ймовірнісна оцінка готовності кіберактивів SCADA КІ може бути визначена так:

$$UnAvailability = P\left(\Phi\left(X\right)=0\right) = P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \right.$$
$$\left. \cup \overline{FW4} \cup \overline{FW5} \right\}, \quad (2)$$

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

$$UA_4 = \left[\overline{AppSRV} \cup DMI\right] \cap \left[\overline{DBSRV} \cup DMI\right] \cap \left[\overline{DmnCTL} \cup DMI\right], \quad (4)$$

$$UA_5 = \left[\overline{AuthSRV} \cup DMI\right] \cap \left[\overline{CTU} \cup DMI\right] \cap \left[\overline{EntprSRV} \cup DMI\right], \quad (5)$$

$$UA_6 = \left[\overline{WebSRV} \cup DMI\right] \cap \left[\overline{EmailSRV} \cup DMI\right] \cap \left[\overline{Pr\,oxySRV} \cup DMI\right], \quad (6)$$

де $\overline{Cluster1}, \overline{Cluster2}, \overline{Cluster3}$ – події, які полягають у неготовності кластерів $Cluster1,2,3$;

$\overline{FW1}, \overline{FW2}, \overline{FW3}, \overline{FW4}, \overline{FW5}$ – події, які полягають у неготовності брандмауерів 1–5;

$\overline{AppSRV}$ – подія, яка полягає в неготовності серверів додатків;

$\overline{DBSRV}$ – подія, яка полягає в неготовності серверів баз даних;

$\overline{DmnCTL}$ – подія, яка полягає в неготовності контролера домену;

$\overline{AuthSRV}$ – подія, яка полягає в неготовності серверів автентифікації;

$\overline{CTU}$ – подія, яка полягає в неготовності комп'ютерних терміналів;

$\overline{EntprSRV}$ – подія, яка полягає в неготовності корпоративних серверів;

$\overline{WebSRV}$ – подія, яка полягає в неготовності web-серверів;

$\overline{EmailSRV}$ – подія, яка полягає в неготовності поштових серверів;

$\overline{Pr\,oxySRV}$ – подія, яка полягає в неготовності проксі-серверів.

Тоді ймовірність події, яка полягає в надійному функціонуванні кібернетичних активів SCADA КІ з урахуванням факторів їхньої готовності та захисту від ЗЛВ, записується у такому вигляді:

$$Availability = 1 - UnAvailability = 1 - P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \right.$$
$$\left. \cup \overline{FW4} \cup \overline{FW5} \right\}. \quad (7)$$

Шостий крок. Побудова структурної схеми надійності кібернетичних активів SCADA КІ.

На рис. 4 зображена ССН, побудована відповідно до рекомендацій і вимог, розглянутих у [8; 9]. Процес розбудови ССН базується на реалізації попередніх кроків і враховує фактор забезпечення надійної роботи кіберактивів SCADA КІ.

Сьомий крок. Оцінка готовності (доступності) кібернетичних активів SCADA КІ із застосуванням їхньої ССН.

Використовуючи отриману ССН та відомі моделі [16], співвідношення для визначення показника готовності у вигляді стаціонарного коефіцієнта готовності (КГ) A_{SCADA} можна записати так:

$$A_{SCADA} = \left\{1 - \left[1 - A_{Cluster1}A_{FW1}\right] \times \left[1 - A_{Cluster2}A_{FW2}\right] \times \left[1 - A_{Cluster3}A_{FW3}\right]\right\} \times$$
$$\times \left\{1 - \left[1 - A_{AppSRV}\right] \times \left[1 - A_{DBSRV}\right] \times \left[1 - A_{DmnCTL}\right]\right\} \times \left\{1 - \left[1 - A_{AuthSRV}\right] \times \right.$$
$$\times \left[1 - A_{CTU}\right] \times \left[1 - A_{EntprSRV}\right] \times \left[1 - A_{WebSRV}\right] \times \left[1 - A_{EmailSRV}\right] \times \quad (8)$$
$$\left. \times \left[1 - A_{ProxySRV}\right]\right\} \times A_{FW4} \times A_{FW5}.$$

Складові A_{SCADA} у формулі (8) визначаються як значення стаціонарних КГ відповідних кластерів, серверів, комп'ютерних терміналів та брандмауерів.

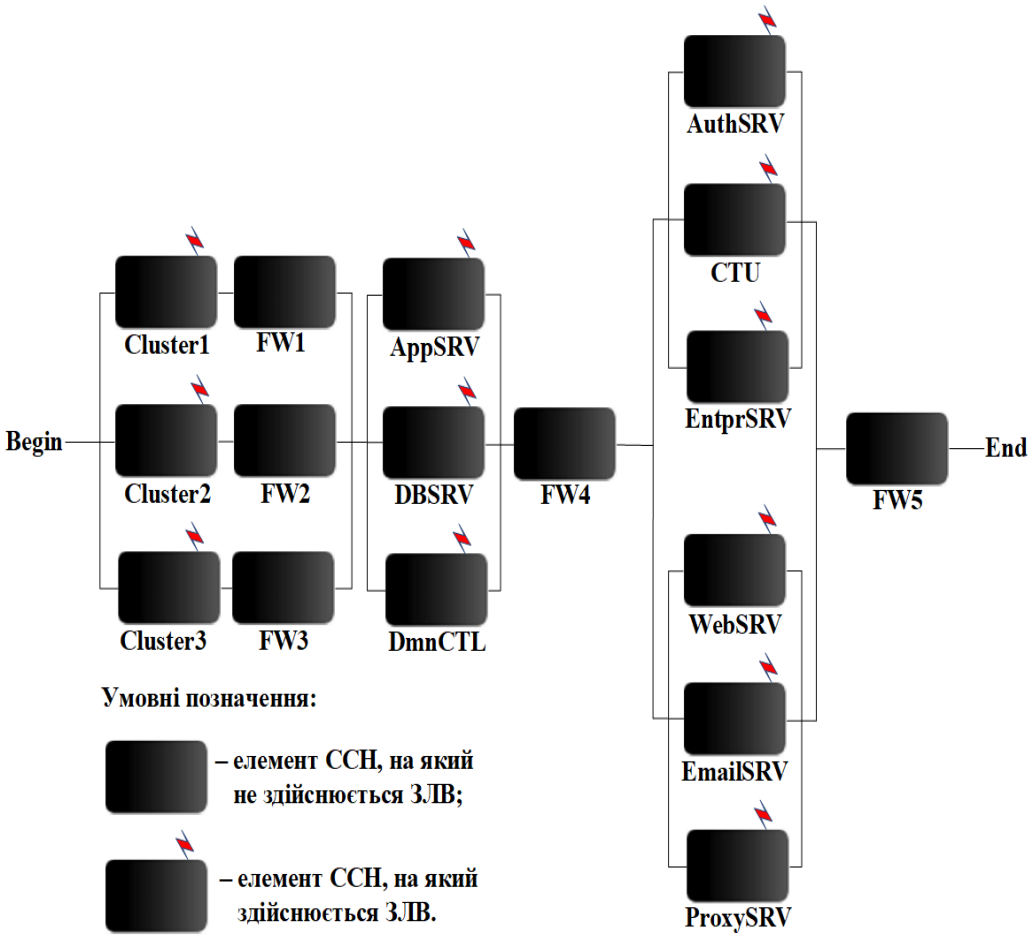

Рис. 4. Структурна схема надійності системи SCADA КІ
з урахуванням ЗЛВ на її кібернетичні активи

Восьмий крок. Параметризація вхідних даних компонентних складових ССН кібернетичних активів SCADA КІ для виконання аналітико-стохастичного моделювання.

Для обчислення загальної оцінки A_{SCADA} необхідно визначити значення складових, які входять у співвідношення (8). Розв'язати цю задачу можна шляхом виконання аналітико-стохастичного моделювання на основі застосування апарата НПММ [20–25] з метою отримання кількісних значень стаціонарних КГ компонентів, які входять до складу ССН (рис. 4). У табл. 1 наведено результати скороченого аналізу найбільш відомих джерел щодо проблематики НПММ.

Таблиця 1

Аналіз відомих наукових праць щодо застосування НПММ

Атрибути	Проблематика	Розв’язування
НПММ з виродженими станами [41]	Застосування процесу НПММ для моделювання деградаційних процесів промислової системи за умови виконання періодичних профілактичних ремонтів та контролю технічного стану	Обчислення динаміки зміни стаціонарного КГ на основі використання вкладених дискретних марковських ланцюгів (ВДМЛ)
НПММ з використанням стохастичних не експоненціальних розподілень [42]	Застосування процесу НПММ для моделювання поведінки системи енергоживлення з двома типами відключень	Визначення точкової оцінки стаціонарного КГ на основі використання ВДМЛ
НПММ з визначенням перехідних імовірностей для стохастичних псевдоекспоненціальних розподілень [43; 44]	Застосування процесу НПММ для моделювання процесів зміни готовності серверних систем з реалізацією режиму очікування (режим холодного резервування)	Визначення точкових оцінок стаціонарного КГ, середнього часу напрацювання до системної відмови на основі використання ВДМЛ

З погляду відповідності розв’язуваної задачі та зважаючи на мережний рівень забезпечення серверними системами, доцільно виконати параметризацію, застосувавши вхідні дані, які використовувались у працях [43; 44]. Певну зацікавленість викликає праця [45], яка присвячена моделюванню поведінки серверних систем хмарної інфраструктури з урахуванням кількості фізичних машин. Хоча обчислення були виконані на основі стохастичних мереж Петрі та марковських ланцюгів [13; 45], ці результати можуть бути використані для завдання вхідних даних з метою реалізації аналітико-стохастичного моделювання. В табл. 2, 3 подано результати параметризації з урахуванням виконаного аналізу.

Таблиця 2

Значення стаціонарного КГ компонентних складових ССН кібернетичних активів SCADA КІ за результатами НПММ [43, 44]

Типи серверів та іншого обладнання	Інтенсивність відмов кластерів SCADA КІ $\lambda_{Cluster1,Cluster2,Cluster3} = 0,1$ 1/год	
	Інтенсивність відмов серверів та іншого обладнання γ, 1/год	
	$\gamma = 0,3$	$\gamma = 0,5$
AppSRV	0,91 352	0,871 814
DBSRV	0,914 446	0,873 394
DmnCTL	0,915 307	0,874 806
AuthSRV	0,916 103	0,876 112
CTU	0,916 837	0,877 318
EntprSRV	0,917 514	0,878 431
WebSRV	0,918 138	0,87 946
EmailSRV	0,918 715	0,880 412
ProxySRV	0,919 248	0,881 294
FW	0,919 742	0,882 113

Таблиця 3

Значення показників надійності компонентних складових ССН кібернетичних активів SCADA КІ [45]

Показники надійності серверів та іншого обладнання	Кількісне значення
$1/\gamma_{SRV}$, $1/\gamma_{DmnCTL,CTU}$, $1/\gamma_{FW}$	500 год, 1750 год, 2500 год
$1/\mu$	3 год

Дев'ятий крок. Побудова структурної схеми ЗЛВ на кібернетичні активи SCADA КІ.

Для побудови структурної схеми (СС) ЗЛВ використовується ССН (рис. 4). Результати попереднього аналізу свідчать, що СС ЗЛВ є результатом трансформації ССН за умови, що на схемі відображаються тільки ком-

поненти, на які здійснюється зловмисний вплив або втручання в їхній контур управління. Схема будується з використанням факторного аналізу ЗЛВ на кібернетичні активи SCADA КІ.

До уваги також слід узяти обмеження, яке стосується дії ЗЛВ на всі сервери та комп'ютерне обладнання, крім брандмауерів, які виконують функції захисту і фільтрації інформаційних потоків SCADA КІ. На рис. 5 зображена СС ЗЛВ, отримана відповідним чином.

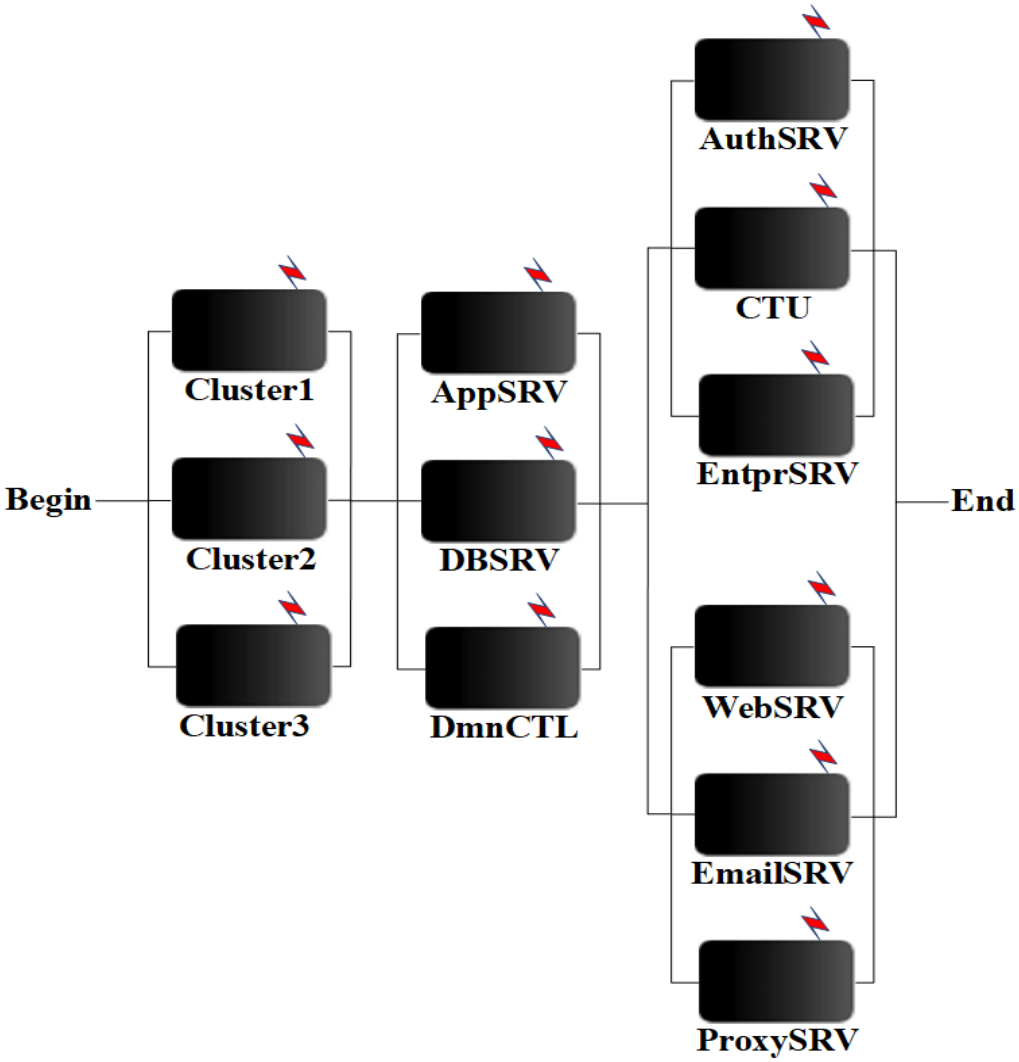

Рис. 5. Структурна схема ЗЛВ на кібернетичні активи SCADA КІ

Десятий крок. Оцінка ймовірності зловмисного впливу на кібернетичні активи SCADA КІ із застосуванням структурної схеми ЗЛВ.

Згідно з отриманою СС ЗЛВ співвідношення для визначення ймовірності ЗЛВ $P_{SCADA_{DMI}}$ може бути записано у такому вигляді:

$$P_{SCADA_{DMI}} = \left\{1-\left[1-P_{Cluster1_{DMI}}\right]\times\left[1-P_{Cluster2_{DMI}}\right]\times\left[1-P_{Cluster3_{DMI}}\right]\right\}\times$$
$$\times\left\{1-\left[1-P_{AppSRV_{DMI}}\right]\times\left[1-P_{DBSRV_{DMI}}\right]\times\left[1-P_{DmnCTL_{DMI}}\right]\right\}\times$$
$$\left\{1-\left[1-P_{AuthSRV_{DMI}}\right]\times\left[1-P_{CTU_{DMI}}\right]\times\left[1-P_{EntprSRV_{DMI}}\right]\times\left[1-P_{WebSRV_{DMI}}\right]\times\right. \quad (9)$$
$$\left.\times\left[1-P_{EmailSRV_{DMI}}\right]\times\left[1-P_{Pr\,oxySRV_{DMI}}\right]\right\},$$

де $P_{Cluster1_{DMI}}$, $P_{Cluster2_{DMI}}$, $P_{Cluster3_{DMI}}$ – ймовірність ЗЛВ на кластери $Cluster1,2,3$;

$P_{AppSRV_{DMI}}$ – ймовірність ЗЛВ на сервери додатків;

$P_{DBSRV_{DMI}}$ – ймовірність ЗЛВ на сервери баз даних;

$P_{DmnCTL_{DMI}}$ – ймовірність ЗЛВ на контролер домену;

$P_{AuthSRV_{DMI}}$ – подія, яка полягає в неготовності серверів автентифікації;

$P_{CTU_{DMI}}$ – ймовірність ЗЛВ на комп'ютерні термінали;

$P_{EntprSRV_{DMI}}$ – ймовірність ЗЛВ на корпоративні сервери;

$P_{WebSRV_{DMI}}$ – ймовірність ЗЛВ на web-сервери;

$P_{EmailSRV_{DMI}}$ – ймовірність ЗЛВ на поштові сервери;

$P_{Pr\,oxySRV_{DMI}}$ – ймовірність ЗЛВ на проксі-сервери.

Одинадцятий крок. Параметризація вхідних даних компонентних складових СС ЗЛВ на кібернетичні активи SCADA КІ для виконання аналітико-стохастичного моделювання.

Параметризація виконується для визначення ймовірності ЗЛВ $P_{SCADA_{DMI}}$ (9) шляхом виконання аналітико-стохастичного моделювання на основі застосування апарата НПММ [46]. Процедура аналогічна тій, що була

реалізована на восьмому кроці пропонованого методу. В табл. 4 наведено вхідні дані для виконання чергового етапу аналітико-стохастичного моделювання.

Таблиця 4

Значення параметрів для виконання НПММ ЗЛВ на кібернетичні активи SCADA КІ [46]

Параметр	Кількісне значення
Інтенсивність успішного злому контуру кіберзахисту γ_{break}, 1/год	0,5
Інтенсивність повернення системи в працездатний стан роботи зі стану ЦФ γ_{return}, 1/год	2
Середній час цільового фішингу (ЦФ) $1/\gamma_{fishing}$, год	0,5–1
Середній час зміни ключів кодування $1/\gamma_{rekeying}$, год	0,017–1

Числові результати НПММ ЗЛВ на кібернетичні активи SCADA КІ для вхідних даних згідно з табл. 4 зображено на рис. 6.

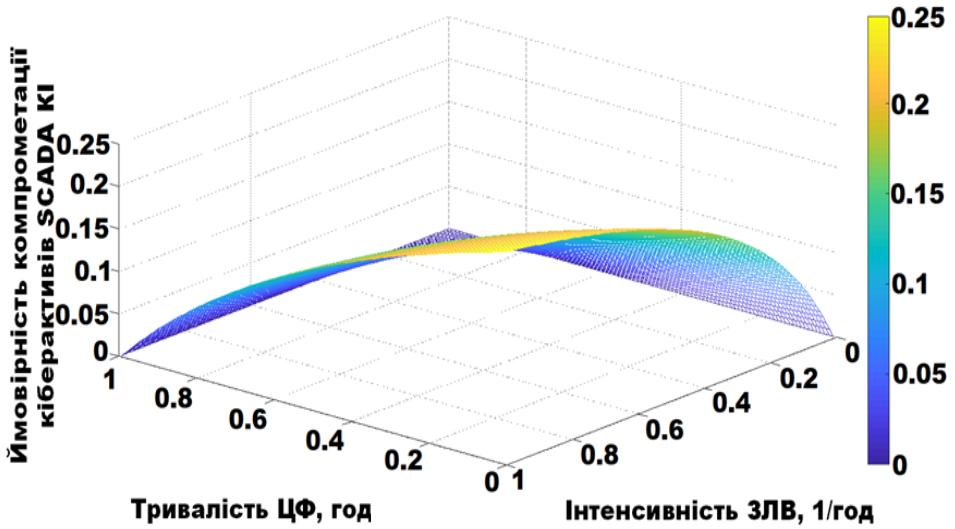

Рис. 6. Числові результати НПММ ЗЛВ на кіберактиви SCADA КІ

Отримані результати моделювання (рис. 6) у вигляді залежності ймовірності компрометації кібернетичних активів SCADA КІ від тривалості цільового фішингу та інтенсивності зловмисних впливів свідчать про досить високий рівень кіберзагроз і можуть бути використані для обґрунтування вимог щодо створення ефективної системи кіберзахисту.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. В досліджені розглянуто етапи побудови ССБ кібернетичних активів системи SCADA КІ з урахуванням аспектів, пов'язаних із забезпеченням необхідного рівня їхньої готовності (доступності) та захисту від кіберзагроз у вигляді зловмисних впливів і проникнень. Результати проведених досліджень у концентрованому вигляді сформульовані як відповідний метод.

Запропонований метод базується на таксономії виникнення ризику для функціональної та інформаційної безпеки системи SCADA КІ для мережного рівня її архітектурної реалізації. Проведений аналіз підтвердив доцільність застосування НПММ для отримання числових результатів моделювання поведінки компонентних складових як ССН, так і СС ЗЛВ, що дає можливість отримати кількісні оцінки загального рівня безпеки кіберактивів SCADA КІ. Результати моделювання можуть бути використані для розробки оптимізаційних процедур щодо побудови ефективної системи забезпечення функціональної та інформаційної безпеки КІ і системи SCADA як важливої компонентної складової ІУС інфраструктури. Зокрема, за результатами НПММ ймовірність компрометації кібернетичних активів SCADA КІ залежно від тривалості цільового фішингу та інтенсивності зловмисних впливів становить 25 %.

Перспективи подальшого застосування цього методу пов'язані з розробкою концепції управління КІ за мегастаном на основі ризик-аналізу різноманітних факторів негативного впливу як на фізичні, так і на кібернетичні активи інфраструктури.

Список використаних джерел:

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

2. *Дрозд А. В., Харченко В. С.* Рабочее диагностирование безопасных информационно-управляющих систем. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2012. 614 с.

3. *Никул В. В., Дрозд А. В., Дрозд Ю. В., Озеранский В. С.* Эффективность поразрядной конвейеризации вычислений в FPGA-компонентах систем критического применения // Технология и конструирование в электронной аппаратуре. 2018. № 4. С. 3–13.

4. *Misbahuddin S.* Faulttolerant remote terminal units (RTUs) in SCADA systems : materials of the International Symposium on Collaborative Technologies and Systems. Chicago, 2010. P. 440–446.

5. A testbed for secure and robust SCADA systems / Giani A., Karsai G., Roosta T. and oth. : materials of the 14th Real-Time and Embedded Technology and Applications Symposium, SIGBED Review. 2008. St. Louis, USA. P. 93–96.

6. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network / Bobbio A., Bonanni G., Ciancamerla E. and oth. // Reliability Engineering & System Safety. 2010. Vol. 95 (12). P. 1345–1357.

7. *Lipman Y., Funkhouser T.* Möbius voting for surface correspondence // ACM Transactions on Graphics (TOG). 2009. Vol. 28 (3). P. 1–12.

8. *Hassan B. Diab, Albert Y. Zomaya.* Dependable Computing Systems: Paradigms, Performance Issues, and Applications. New York: John Wiley & Sons, 2005. 688 p.

9. *Острейковский В. А.* Теория надёжности. Москва: Высшая школа, 2003. 463 с.

10. *Zang X., Wang D., Sun H., Trivedi K. A* BDD-based algorithm for analysis of multistate components // IEEE Transactions on Computers. 2003. Vol. 52 (12). P. 1608–1618.

11. *Kuo W., Zuo M.* Optimal reliability modeling: principles and applications. New York: John Wiley & Sons, 2003. 544 p.

12. CASE-оценка критических программных систем / *Одарущенко О. Н., Харченко В. С., Маевский Д. А. и др.* Том 2. Надёжность. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского “ХАИ”, 2012. 292 с.

13. *Bolch G., Greiner S., Hermann de Meer, Trivedi K.* Queueing Networks and Markov Chains: modeling and performance evaluation with computer science applications. New Jersey: John Wiley & Sons, 2006. 878 p.

14. *Patel A., Joshi A.* Modeling and Analysis of Stand by Redundancy System to Generate the Reachability Tree using Petri Net System // Asian Journal of current Engineering and Maths. 2013. Vol. 2 (3). P. 145–150.

15. *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.

16. Sensitivity analysis of a hierarchical model of mobile cloud computing / *Matos R., Araujo J., Oliveira D. and oth.* // Simulation Modelling Practice and Theory. 2015. Vol. 50. P. 151–164.

17. *Kim D., Machida F., Trivedi K.* Availability modeling and analysis of a virtualized system: materials of the 2009 15th IEEE Pacific Rim International Symposium on Dependable Computing. Shanghai, China. 2009. P. 365–371.

18. *Changa X., Zhang Z., Li X., Trivedi K.* Model-Based Survivability Analysis of a Virtualized System: materials of the 2016 IEEE 41st Conference on Local Computer Networks. Dubai, 2016. P. 611–614.

19. Dynamically-Enabled Defense Effectiveness Evaluation in Home Internet Based on Vulnerability Analysis / *Wang T., Lei M., Chen J. and oth.* : materials of the International Conference on Cloud Computing and Security. Springer, 2017. P. 805–815.

20. Распределённые критические системы и инфраструктуры: практикум / *О. В. Иванченко, Ловягин В. С., Мащенко Е. Н. и др.* Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", Севастопольский национальный технический университет, 2013. 179 с.

21. *Иванченко О. В.* Полумарковские модели мониторинга информационно-технического состояния критических інфраструктур // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 219–224.

22. *Ivanchenko O., Kharchenko V., Skatkov A.* Management of Critical Infrastructures Based on Technical Megastate // Information and Security. Critical Infrastructures Safety and Security. 2012. Vol. 28 (1). P. 37–51.

23. *Яцек Я. Ф., Иванченко О. В., Войтюк А. В., Степанов В. А.* Комплексный подход к управлению критическими инфраструктурами по техническому мегасостоянию // Збірник наукових праць Академії Військово-морських сил ім. П. С. Нахімова. 2010. № 4 (4). С. 91–99.

24. *Иванченко О. В., Харченко В. С., Бирюков Д. Ю.* Полумарковская модель протекания аварии критической инфраструктуры // Радіоелектронні і комп'ютерні системи. 2013. № 5 (64). С. 45–51.

25. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения: учеб. пособие / под ред. В. С. Харченко. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2011. 641 с.

26. *Sundararajan A., Khan T., Moghadasi A., Sarwat A.* Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. URL: https://doi.org/10.1007/s40565-018-0473-6

27. *Hentea M.* Improving security for SCADA control systems // Interdisciplinary Journal of Information, Knowledge, and Management. 2008. Vol. 3 (1). P. 73–86.

28. *Brandle M., Naedele M.* Security for Process Control systems: An Overview // IEEE Security & Privacy. 2008. Vol. 6 (6). P. 24–29.

29. *Chen T., Abu-Nimeh S.* Lessons from Stuxnet // IEEE Computer Magazine. 2011. Vol. 44 (4). P. 91–93.

30. *Keizer G.* Development timeline key to linking Stuxnet, Flame malware. 2012. URL: http://www.computerworld.com/s/article/9227580/ Development_ timeline_key_to_linking_Stuxnet_Flame_ma lware

31. Centre for the Protection of National Infrastructure, Viewpoint // Securing the Move to IP-Based SCADAlPLC networks. URL: http://www.cpni.gov.ukldocuments/publications/2011/2011035-securing-move-to-ip-based-networks.pdf?epslanguageen-gb

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

33. *Pidikiti B., Kalluri R., Kumar R., Bindhumadhava B.* SCADA communication protocols: vulnerabilities, attacks and possible mitigations // CSITransactions on ICT. 2013. Vol. 1 (2). P. 135–141.

34. *Nazir S., Patel S., Patel D.* Assessing and augmenting SCADA cyber security: A survey of techniques // Computers & Security. 2017. Vol. 70. P. 436–454.

35. *Chen S., Wang Y., Pedram M.* A semi-markovian decision process based control method for offloading tasks from mobile devices to the cloud: materials of the 2013 IEEE Global Communications Conference (GLOBECOM). Atlanta, GA, USA, 2013. P. 2885–2890.

36. Juniper Networks // Juniper connected security: dynamic, adaptive multicloud security. 2019. URL: https://media.bitpipe.com/io_14x/io_146335/ item_1879854/3510634-en.pdf

37. *Hauser C., Bose A., Meng M.* Cloud Data Sharing Platform (S-67G), Final Project Rep. Cornell University and Washington State University, 2016. 29 p.

38. Smart Grids. Clouds, Communications, OpenSource, and Automation / Edited byBakken D. CRC. Taylor and Francis Group, New York, 2014. 468 p.

39. *Скляр В. В.* Функциональная безопасность. Часть 2 из 7. МЭК 61508: кем быть Шерлоком Холмсом или Дата Туташхиа? URL: https://habr.com/ru/post/309636

40. *Скляр В. В.* Информационная безопасность АСУ ТП: Дон Кихот в эру кибероружия. URL: https://habr.com/ru/post/316184

41. *Vinayk R., Dharmaraja S.* Semi-Markov Modeling Approach for Deteriorating Systems with Preventive Maintenance // International Journal of Performability Engineering. 2012. Vol. 8 (5). P. 515–526.

42. *Distefano S., Trivedi K.* Non-Markovian State-Space Models in Dependability Evaluation // Quality and Reliability Engineering International. 2013. Vol. 29 (2). P. 225–239.

43. *Bhardwaj R., Singh R.* Semi-Markov approach for asymptotic performance analysis of a standby system with server failure // International Journal of Computer Applications. 2014. Vol. 98 (3). P. 9–14.

44. *Bhardwaj R., Singh R.* A Cold-Standby System with Server Failure and Delayed Treatment // International Journal of Computer Applications. 2015. Vol. 124 (17). P. 31–36.

45. *Ghosh R.* Scalable stochastic models for cloud services: Doctoral dissertation. Duke University, 2012. 494 p.

46. *Meng T.* Security and Performance Tradeoff Analysis of Offloading Policies in Mobile Cloud Computing: Doctoral dissertation. Institute for Computer and Systems Engineering, 2017. 150 p.

References:

1. *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), pp. 11–13.

2. Drozd A. V. and Kharchenko V. S. (2012), *Rabocheye diagnostirovaniye bezopasnykh informatsionno-upravlyayushchikh sistem* [Working diagnostics of secure management information systems], National Aerospace University named after N. Ye. Zhukovskogo "KhAI", Khar'kov, 614 p. [Ukraine].

3. Nikul V. V., Drozd A. V., Drozd Yu. V. and Ozeranskiy V. S. (2018), *"Effektivnost' porazryadnoy konveyyerizatsii vychisleniy v FPGA-komponentakh sistem kriticheskogo primene-niya"* ["Efficiency of bitwise pipelining of computations in FPGA components of critical application systems"], journal *Tekhnologiya i konstruirovaniye v elektronnoy apparature* [Technology and Electronic Design], vol. 4, pp. 3–13 [Ukraine].

4. Misbahuddin S. (2010), "Faulttolerant remote terminal units (RTUs) in SCADA systems", materials of the International Symposium on Collaborative Technologies and Systems, Press Chicago, pp. 440–446 [USA]

5. Giani A., Karsai G., Roosta T., Shah A. and oth. (2008),"A testbed for secure and robust SCADA systems", materials of the 14th Real-Time and Embedded Technology and Applications Symposium, SIGBED Review, St. Louis, pp. 93–96 [USA].

6. Bobbio A., Bonanni G., Ciancamerla E., Clemente R. and oth. (2010), "Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network", journal Reliability Engineering & System Safety, vol. 95 (12), pp. 1345–1357.

7. Lipman Y. and Funkhouser T. (2009), "Möbius voting for surface correspondence", journal ACM Transactions on Graphics (TOG), vol. 28(3), pp. 1–12.

8. Hassan B. Diab and Albert Y. Zomaya (2005), Dependable Computing Systems: Paradigms, Performance Issues, and Applications. New York: John Wiley& Sons, 688 p. [USA].

9. Ostreykovskiy V. A. (2003), *Teoriya nadozhnosti* [Theory of Reliability], Press Vysshaya shkola [Higher School], Moscow, 463 p. [Russia].

10. Zang X., Wang D., Sun H. and Trivedi K. (2003), “A BDD-based algorithm for analysis of multistate components”, journal IEEE Transactions on Computers, vol. 52(12), pp. 1608–1618.

11. Kuo W. and Zuo M. (2003), Optimal reliability modeling: principles and applications, John Wiley & Sons, New York, 544 p. [USA].

12. Odarushchenko O. N., Kharchenko V. S., Mayevskiy D. A., Ponochovnyy Yu. L. and oth. (2012), *CASE-otsenka kriticheskikh programmnykh sistem* [CASE-evaluation of critical software systems], Volume 2, *Nadozhnost'* [Reliability], Press National Aerospace University named after N. Ye. Zhukovskogo “KhAI”, Khar'kov, 292 p. [Ukraine].

13. Bolch G., Greiner S., Hermann de Meer and Trivedi K. (2006), Queueing Networks and Markov Chains: modeling and performance evaluation with computer science applications. New Jersey: John Wiley & Sons, 878 p. [USA].

14. Patel A. and Joshi A. (2013), “Modeling and Analysis of Stand by Redundancy System to Generate the Reachability Tree using Petri Net System”, Asian Journal of current Engineering and Maths, vol. 2 (3), pp. 145–150 [USA].

15. Dantas J., Matos R., Araujo J. and 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.

16. Matos R., Araujo J., Oliveira D. and oth. (2015), “Sensitivity analysis of a hierarchical model of mobile cloud computing”, journal Simulation Modelling Practice and Theory, vol. 50, pp. 151–164.

17. Kim D., Machida F. and Trivedi K. (2009), “Availability modeling and analysis of a virtualized system”, materials of the 15th IEEE Pacific Rim International Symposium on Dependable Computing, Shanghai, pp. 365–371 [China].

18. Changa X., Zhang Z., Li X. and Trivedi K. (2016), “Model-Based Survivability Analysis of a Virtualized System”, materials of the 41th IEEE Conference on Local Computer Networks, Dubai, pp. 611–614 [United Arab Emirates].

19. Wang T., Lei M., Chen J. and oth. (2017), “Dynamically-Enabled Defense Effectiveness Evaluation in Home Internet Based on Vulnerability Analysis”, materials of the International Conference on Cloud Computing and Security, Springer, pp. 805–815 [Cham, Switzerland].

20. Ivanchenko O. V., Lovyagin V. S., Mashchenko Ye. N. and oth. (2013), *Raspredelonnyye kriticheskiye sistemy i infrastruktury* [Distributed critical systems and infrastructures], workshop, National Aerospace University named after N. Ye. Zhukovskogo “KhAI”, Khar'kov, Sevastopol National Technical University, 2013, 179 p. [Ukraine].

21. *Ivanchenko O. V.* (2010), “*Polumarkovskiye modeli monitoringa informatsionno-tekhnicheskogo sostoyaniya kriticheskikh infrastruktur. Radíoyelektronní í komp’yuterní sistemi”* [Polumarkov’s models for monitoring the information and technical state of critical infrastructures. Radio and Computer Systems], vol. 7 (48), pp. 219–224 [Ukraine].

22. IvanchenkoO., Kharchenko V. and Skatkov A. (2012), "Management of Critical Infrastructures Based on Technical Megastate", International Journal Information and Security, Critical Infrastructures Safety and Security, vol. 28 (1), pp. 37–51.

23. Yatsek Ya. F., Ivanchenko O. V., Voytyuk A. V. and Stepanov V. A. (2010), *"Kompleksnyy podkhod k upravleniyu kriticheskimi infrastrukturami po tekhnicheskomu megasostoyaniyu"* ["An integrated approach to managing critical infrastructures for technical mega-state"], Collection of scientific works of the Academy of Naval Forces. P. S. Nakhimova, vol. 4 (4), pp. 91–99 [Ukraine].

24. Yvanchenko O. V., Kharchenko V. S. and Biryukov D. Yu. (2013), *"Polumarkovskaya model' protekanyya avaryy krytycheskoy infrastruktury"* ["Semi-Markov model of critical infrastructure emergency failure"], Journal *Radioelektronni i komp'yuterni systemy* [Radio electronic and computer systems], vol. 5 (64), pp. 45–51 [Ukraine].

25. Edited by V. S. Kharchenko (2011), *Bezopasnost' kriticheskikh infrastruktur: matematicheskiye i inzhenernyye metody analiza i obespecheniya* [Safety of critical infrastructures: mathematical and engineering methods of analysis and software], Tutorial, Press National Aerospace University named after N. Ye. Zhukovskogo "KhAI", Khar'kov, 641 p. [Ukraine].

26. Sundararajan A., Khan T., Moghadasi A. and Sarwat A. (2018), Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies, available at: https://doi.org/10.1007/s40565-018-0473-6

27. Hentea M. (2008), "Improving security for SCADA control systems", Interdisciplinary Journal of Information, Knowledge, and Management, vol. 3 (1), pp. 73–86.

28. Brandle M. and Naedele M. (2008), "Security for Process Control systems: An Overview", in journal IEEE Security & Privacy, vol. 6(6), pp. 24–29.

29. Chen T. and Abu-Nimeh S. (2011), "Lessons from Stuxnet", in journal IEEE Computer Magazine, vol. 44(4), pp. 91–93.

30. Keizer G. (2012), "Development timeline key to linking Stuxnet, Flame malware", Computerworld, official site, available at: http://www.computerworld. com/s/article/9227580/Development_timeline_key_to_linking_Stuxnet_Flame_ma lware

31. Centre for the Protection of National Infrastructure, Viewpoint (2011), Securing the Move to IP-Based SCADAlPLC networks, available at: http://www.cpni.gov.ukldocuments/publications/2011/2011035-securing-move-to-ip-based-networks.pdf?epslanguageen-gb

32. 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.

33. Pidikiti B., Kalluri R., Kumar R. and Bindhumadhava B. (2013), "SCADA communication protocols: vulnerabilities, attacks and possible mitigations", journal CSITransactions on ICT, vol. 1 (2), pp. 135–141.

34. Nazir S., Patel S. and Patel D. (2017), “Assessing and augmenting SCADA cyber security: A survey of techniques”, journal Computers & Security, vol. 70, pp. 436–454.

35. Chen S., Wang Y. and Pedram M. (2013), “A semi-markovian decision process based control method for offloading tasks from mobile devices to the cloud”, materials of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA. P. 2885–2890.

36. Juniper Networks (2019), Juniper connected security: dynamic, adaptive multicloud security, available at: https://media.bitpipe.com/io_14x/io_146335/item_1879854/3510634-en.pdf

37. Hauser C., Bose A., Meng M., Anderson D. and oth., (2016), Cloud Data Sharing Platform (S-67G), Final Project Rep., Press Cornell University and Washington State University, 29 p. [the USA].

38. Edited by Bakken D. (2014), Smart Grids. Clouds, Communications, OpenSource, and Automation, CRC Press Taylor and Francis Group, New York, 468 p. [USA].

39. Sklyar V.V. (2016), *Funktsional'naya bezopasnost'* [Functional safety], Part 2 of 7. IEC 61508: *kem byt' Sherlokom Kholmsom ili Data Tutashkhia?* [Who should be Sherlock Holmes or Date Tutashkhia?], available at: https://habr.com/ru/post/309636/

40. Sklyar V. V. (2016), Informatsionnaya bezopasnost' ASU TP: Don Kikhot v eru kiberoruzhiya / habr: ofitsial'nyy sayt [Information security of the automated control systems for industrial control: Don Quixote in the cyber weapon era], available at: https://habr.com/ru/post/316184/

41. Vinayk R. and Dharmaraja S. (2012), “Semi-Markov Modeling Approach for Deteriorating Systems with Preventive Maintenance”, International Journal of Performability Engineering, vol. 8 (5), pp. 515–526.

42. Distefano S. and Trivedi K. (2013), “Non-Markovian State-Space Models in Dependability Evaluation”, journalQuality and Reliability Engineering International, vol. 29 (2), pp. 225–239.

43. Bhardwaj R. and Singh R. (2014), “Semi-Markov approach for asymptotic performance analysis of a standby system with server failure”, International Journal of Computer Applications, vol. 98 (3), pp. 9–14.

44. Bhardwaj R. and Singh R. (2015), “A Cold-Standby System with Server Failure and Delayed Treatment”, International Journal of Computer Applications, vol. 124 (17), pp. 31–36.

45. Ghosh R. (2012), Scalable stochastic models for cloud services, Doctoral dissertation, Duke University, 494 p. [USA].

46. Meng T. (2017), Security and Performance Tradeoff Analysis of Offloading Policies in Mobile Cloud Computing, Doctoral dissertation, Institute for Computer and Systems Engineering, 150 p. [Germany].