УДК 519.004.056.53

П.М. Павленко, д.т.н., проф., Є.І. Самборський
(Національний авіаційний університет, Україна)

Управління подіями безпеки в інформаційному середовищі комп'ютерних мереж критичних об'єктів на основі цифрових двійників

Розглянуто підхід щодо управління інформаційними подіями безпеки у комп'ютерних мережах критичних об'єктів на основі розроблених цифрових двійників. Запропоновано використовувати при створенні цифрових двійників теорію гіперкомплексних логіко-динамічних систем.

Створення і ефективне використання сучасних систем управління подіями інформаційної безпеки (СУПІБ) для надійного захисту конфіденційної керуючої інформації у комп'ютерних мережах (КМ) інфраструктури критичних об'єктів (ІКО) є нагальним і перспективним напрямом фундаментальних, пошукових і прикладних наукових досліджень. Для їх реалізації особливий акцент необхідно зробити на проблемних задачах управління СУПІБ інформаційними подіями безпеки за рахунок надійних механізмів моніторингу, моделювання, прогнозування та оптимізації спеціальної (відомчої) інформації в ІКО СУПІБ. Поряд з цим, на думку авторів, доцільно також розглянути можливі підходи щодо вирішення низки ключових та актуальних задач створення оптимальних структур, алгоритмічного і програмного забезпечення для реалізації стійкої синхронізації інформаційних потоків СУПІБ КМ ІКО.

Як свідчать проведені теоретичні дослідження специфіки і особливостей вказаних систем, найбільш значущими з цих задач є [1-3]:

-оцінка та аналіз подій інформаційної безпеки (на основі розгляду процесів у КМ ІКО, описаних адекватними моделями гіперкомплексних логіко-динамічних систем (ГКЛДС);

- створення структури алгоритму формування еталонного (базового) масиву подій безпеки КМ ІКО;

- формування та реалізація оптимальних законів управління процесом компенсації (реалізація функцій протидії негативним наслідкам у КМ ІКО деструктивних факторів впливу подій комп'ютерної безпеки.

Аналіз існуючих парадигм (теоретико-методологічних моделей) щодо призначення та специфічних функціональних особливостей СУПІБ КМ, які розроблені світовими компаніями і зараз починають інтенсивно і широко використовуватися, показує наступне. Жодна з наявних в експлуатації СУПІБ не можна і не доцільно розглядати придатною у повному обсязі для управління подіями безпеки і інформацією в КМ ІКО.

Особливо необхідно акцентувати увагу на тому, що у зв'язку з постійно зростаючою нагальною потребою і необхідністю і значущістю СУПІБ КМ ІКО, а також прогнозованим (передбачуваним) ефектом від використання систем управління такого типу в різних інфраструктурах, виникає нагальна необхідність формування чітких рішень щодо синхронізації інформаційних даних СУПІБ, для

модернізації існуючих і створення нових засобів захисту такого класу. При цьому передбачається врахувати головну вимогу до таких систем, а саме: можливість оптимально, надійно, стійко і ефективно функціонувати в багатофазних гетерогенних інфраструктурах, до яких відноситься і широкий клас сучасних, і особливо перспективних, інфраструктур критичного призначення.

Відомо, що існуючим СУІПБ КМ притаманна низка суттєвих (щодо організації управління) недоліків, які значно впливають на якість організації процесу забезпечення безпеки функціонування ІКО, а саме:

-функціональні обмеження, які накладаються самими конкретними ІКО;

-обмежену здатність щодо узгодженої інтерпретації інцидентів і подій безпеки на різних структурних ієрархічних рівнях СУІПБ КМ;

-обмежені можливості щодо забезпечення необхідної (заданої) функціональної стійкості (відказостійкості) і надійності при зборі даних про інциденти безпеки;

-низький обсяг «масштабування» подій безпеки КМ ІКО.

Враховуючи, що існуючі наразі традиційні методи та сучасні технології захисту безпеки КМ не в повному (бажаному) обсязі можуть відповідати жорстким вимогам щодо надійності та стабільності та прогнозованості, було всебічно розглянуто та проаналізовано методи виявлення та реагування на аномалії безпеки в «цифровому» інформаційному просторі. Отримані результати аналізу дали змогу зробити висновок, що найбільш оптимальним із існуючих наразі методів є такий, в основу якого закладена ідеї цифрових двійників.

Згідно із проведеними дослідженням Markets and Markets, ринок цифрових двійників, який оцінюють у 6,9 млрд. доларів США у 2022 році, за прогнозами, підійметься до значної суми – 73,5 млрд. доларів США до 2027 року. Стрімке зростання 60,6% за 5-річний період обумовлене значними економічними вигодами, підвищенням ефективності та новими функціональними можливостями для різноманітних застосувань [4].

Так, з точки зору управління, цифровий двійник допомагає зрозуміти не тільки те, як працює певна СУПІБ КМ ІКО, а й те, як вона працюватиме і в майбутньому. Це дозволяє своєчасно відреагувати на зміни та приймати оптимальне управлінське рішення в реальному масштабі часу. Цифровий двійник може бути цифровою копією стабільного процесу функціонування КМ ІКО, а може використовуватися для відтворення критичних подій безпеки, з метою організації ефективного управління цим складним, динамічним і гіперкомплексним процесом. У цьому випадку, цифрові двійники процесів, які обумовлюють критичні події безпеки, дозволять передбачати необхідність блокуючих дій і механізмів захисту з використанням СУПІБ КМ ІКО в реальному часі. Для покращення результатів пропонується застосувати методи машинного навчання, методи імітаційного моделювання, прогнозні моделі, модальне управління гіперкомплексними логіко-динамічними структурами, тощо.

Використання цифрових двійників в управлінні інформаційними подіями безпеки СУПІБ дозволить суттєво підсилити стратегічні рішення,

запобігти вартісним і ресурсним збоям, використовуючи сучасні аналітичні, прогностичні та моніторингові можливості.

На нашу думку, цифрові двійники – це комп'ютерні моделі фізичного і віртуального продукту чи процесу, або їхнього повного життєвого циклу, які синхронізовані в реальному часі за допомогою їх двостороннього зіставлення з реальними об’єктами, з метою прогнозування їх характеристик, усунення проблем та з забезпеченням необхідної якості управління [5].

Принцип їх функціонування полягає у постійній синхронізації і порівнянні, в реальному масштабі часу, інформаційних потоків КМ ІКО, з метою моніторингу, оцінки та локалізації інформаційних подій безпеки та забезпеченні надійного функціонування СУІПБ КМ.

КМ ІКО – складні, розосереджені, великі організаційні системи, які відносяться до класу гіперкомплексних логіко-динамічних систем (ГКЛДС) [6]. Для адекватного опису систем цього класу доцільно застосувати метод інваріантного моделювання (МІМ). Цей метод передбачає використанням основних законів системного рівня загальності, які розповсюджуються на об'єкти, процеси і явища у цих складних системах. Існуючий інструментарій моделювання дозволить будувати, аналізувати системні моделі складних об'єктів, прогнозувати їх поведінку і давати адекватне представлення цих моделей, яке прийнятне для реалізація управління такими структурами. Рівнями реалізації формального апарату ГКЛДС є: вербальні, символьні, алгоритмічні та комп'ютерно-реалізовані «мови», сукупність яких становить аксіоматичну основу «мови системи» в рамках МІМ.

Базуючись на фундаментальній теорії ГКЛДС, математичну модель *(S)* представимо у вигляді інтегральної сукупності системних інваріантів, які описують структуру і процеси в таких системах:

$$S = S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6. \quad (1)$$

S-позначення інтегральної сукупності інваріантів ГКЛДС;

S_1-опис гіперскладності системи, яка пов’язана з наявністю сукупності різнорідних елементів у ній із урахуванням властивостей;

S_2-опис динамічності, яка характеризує здатність елементів ГКЛДС до взаємодії, а також реалізація у повному обсязі міжсистемної взаємодії між ними;

S_3-опис структурності, яка характеризує послідовність, механізм і особливості реалізації взаємозв'язків між елементами системи;

S_4–опис цілісності, яка характеризує загальну властивість сукупності структурованих елементів системи в цілому, а не кожного з її окремих складових;

S_5-опис ієрархії, пов’язаної із наявністю різноманіття внутрішньосистемних рівнів, а також їх специфічних властивостей і закономірностей, які проявляються при функціонуванні ГКЛДС;

S_6- опис реалізуємості управління інформаційними процесами ГКЛДС за рахунок «гнучкої» інтеграції СУІПБ в її функціональну структуру.

Особливо відмітимо, що враховуючи специфіку термінології, яка використовується при описі ГКЛДС і особливостей прогнозування станів цієї системи, знак *U*-об'єднання множин розглядаємо в цій моделі як «інтегральну сукупність інваріантів».

Результати проведених досліджень свідчать про те, що існування ГКЛДС і управління інформаційними процесами в ній, можливе лише у разі забезпечення її структурної цілісності усіх наведених інваріантних рівнів - складових її функціональних субсистем.

Використовуючи математичну модель (1) ГКЛДС, реалізовано прогнозне моделювання цифрового двійника. Суть його полягає в тому, що модель синтезує її прогнозовані можливі стани, або, на багатовимірних прогнозах, сценарії подій. Завдяки використанню теорії ГКЛДС, втілена концепція цифрового двійника, керованого еталонною моделью СУІПБ. Організація управління, з використанням даних і симуляторів та розробленого програмного засобу, забезпечує виконання моніторингу, симуляції, прогнозування та оптимізацію процесу управління інформацією і подіями безпеки в цих структурах.

Таким чином, можливо зробити висновок, що застосування цифрового двійника суттєво підвищить ефективність і безпеку функціонування КМ ІКО.

Список літератури

1. Jiaxing G. , Dongliang Z. , Chunxiang G., Xi C. , Xieli Z. Mengcheng J., An enhanced state-aware model learning approach for security analysis in lightweight protocol implementations, Journal of Cloud Computing: Advances, Systems and Applications, 2024, 13:28, P.2 – 17.
2. Tao F., Xiao B., Qi Q., Cheng J., Ji P., Digital twin modeling. J Manuf Syst 2022, 64:372–389.
3. VanDerHorn E., Mahadevan S., Digital twin: Generalization, characterization and implementation. Decis Support Syst, 2021, 145:113524.
4. Markets and Markets. Digital Twin Market. Available online: https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html
5. Павленко П.М., Цифрові двійники та адитивні технології у металообробних галузях. XIV міжнародна науково-практична конференція «Комплексне забезпечення якості технологічних процесів і систем», 23 - 24 травня 2024 р. м. Чернігів, С.139-142.
6. Sholokhov S.M., Pavlenko P.M., Nikolaienko B.A., Samborsky I.I., Samborsky E.I., (2023/2024), The method of optimizing the distribution of radio suppression means and destructive software influence on computer networks. Radio Electronics, Computer Science, Control. 2023/2024. № 4 (67). P. 16-29.