DOI 10.31891/2307-5732-2024-345-6-4
УДК 004.94

КОЗЛОВСЬКИЙ ОЛЕКСАНДР
Херсонський національний технічний університет
https://orcid.org/0009-0006-1864-1107
e-mail: oleksandr.v.kozlovskyi@gmail.com
ЖАРІКОВА МАРИНА
Херсонський національний технічний університет
https://orcid.org/0000-0001-6144-480X
e-mail: marina.jarikova@gmail.com

РОЗРОБКА КОНЦЕПЦІЇ ФРЕЙМВОРКУ ЦИФРОВОГО ДВІЙНИКА ДЛЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ

У даній роботі представлено концепцію фреймворку цифрового двійника для багатокомпонентних кіберфізичних систем, що дозволить створити модель безпеки на основі стохастичної мережі Петрі і забезпечити стабільність роботи систем у випадку кібератак та інших інцидентів безпеки.

Ключові слова: Кіберфізична система, Стохастична мережа Петрі, Цифровий двійник, Фізичний об'єкт, Модель безпеки, Інцидент безпеки.

KOZLOVSKYI OLEKSANDR, ZHARIKOVA MARYNA
Kherson National Technical University

DEVELOPMENT OF A CONCEPT OF A DIGITAL TWIN FRAMEWORK FOR CYBER-PHYSICAL SYSTEM

In this article, the concept of a digital twin framework for multi-component cyber-physical systems, which will allow creating a security model based on a stochastic Petri net, was described. This framework consists of five connected logical layers. The physical layer includes physical system along with all sensors and actuators that collect security-related data from the system and generate a digital twin to control it through the feedback generation module. The PT-DT layer is added for storing and managing both security-related and general data that comes from the physical environment and is used by the digital twin to create the simulation model. The Digital Twin layer encompasses four key components: System Modeling, Simulation, Feedback Generation, and Visualization. In security modeling, attack graphs, attack trees, and Petri Nets are commonly used for modeling adversarial behavior, considering real assets and vulnerabilities. The DT-SERV layer gathers and organizes the specific knowledge and data required to develop, customize, and optimize higher-level services. This includes system and security rules that can be used for instance for attack/intrusion/anomaly detection. The service layer includes main services that can be classified by exploited operational mode. DTs can be executed in different operational modes, i.e., simulation, analysis, and replication based on what kind of data they use. Thus, the implementation of the framework will enable the identification of vulnerabilities in system components and the development of countermeasures to address attacks in the physical environment. This approach will help in proactively securing the system by detecting security incidents, analyzing their impact, mitigating potential risks, and preparing appropriate responses to address emerging threats effectively.

Key words: Cyber-physical system, Stochastic Petri net, Digital twin, Physical system, Security model, Security incident.

Постановка проблеми

Кіберфізична система (CPS) - це підключена до Інтернету система, яка об'єднує цифрові (віртуальні) та фізичні ресурси. Вони забезпечують взаємодію між фізичним об'єктом і комп'ютерними системами, дозволяючи автоматизувати, керувати та моніторити складні процеси в реальному часі. Останніми роками в різних сферах нехтували безпекою в кіберсистемах. Порівняно з традиційною IT-системою, CPS завжди мають велику кількість фізичних компонентів, що не підтримують сучасні стандарти безпеки.

На основі звіту, опублікованого організацією Dragos Inc. [1], було відмічено, що 64% вразливостей не виправляється через вразливу архітектуру системи, а система не здатна протидіяти загрозам навіть після випуску патчів. Як наслідок, це може призвести до руйнівних наслідків для всієї системи. Таким чином різні організації розглядають кібербезпеку як ключовий фактор стабільності, приділяючи питанням захищеності особливу увагу. Більше того, для підтримки системи безпеки CPS, було розроблено спеціальні стандарти, зокрема IEC 62443, VDI/VD2E 2182 та NIST SP 800-8.E 2182 [2].

Виявлення кібератак, спрямованих на дестабілізацію кіберфізичних систем, не є тривіальною задачею. Річ у тім, що в подібних системах регулярно відбуваються збої та аномалії, що спричинені фізичною деградацією компонентів системи. Ці аномалії може бути важко відрізнити від ретельно спланованої кібератаки, оскільки такі атаки часто імітують очікувану аномальну поведінку, щоб обманути механізм протидії вторгненням. Крім того, аномалії можуть виникати через ненавмисні дії, такі як помилки в налаштуванні або технічні збої, що ускладнює їх розрізнення від кібератак.

Система цифрових двійників може вирішити цю проблему. Цифровий двійник (DT) можна вважати віртуальною копією свого фізичного аналога, що може працювати незалежно у віртуальному середовищі. В такому випадку оператори зможуть проводити тестування так званих умовних сценаріїв (what-if), не ризикуючи втручанням у фізичне середовище. Більше того, використовуючи дані з віртуального середовища, оператори могли б використовувати їх для посилення безпеки фізичного середовища.

Аналіз досліджень та публікацій

Як зазначається в літературних джерелах, цифровий двійник - це нова концепція, яка використовується в CPS для підвищення ефективності та оптимізації виробничих процесів. Лише в останні

роки цифровий двійник починає розглядатися як можливе рішення для вирішення проблем безпеки у CPS, тому існує обмежена кількість робіт, присвячених цій галузі. Розглянемо декілька з них.

Бітон та ін. [3] зосередилися у своїй роботі на балансі між бюджетом та точністю системи. Вони запропонували схему побудови системи цифрових двійників, що орієнтована на безпеку конкретної мережі, що є економічно вигідною та високонадійною. Така система складається з двох модулів: конструктора задач та розв'язувача. Конструктор задач збирає дані з CPS і перетворює їх на набір правил, який може відображати структуру системи і та вказати на обмеження щодо реалізації цифрового двійника. Розв'язувач може знайти оптимальне рішення для проблем безпеки в CPS, використовуючи методи нелінійного програмування. Крім того, автори протестували свій підхід, використовуючи спрощену мережу промислової системи керування (ICS). Мережі ICS - це група технологій та пристроїв, що використовуються для автоматизації та управління процесами на промислових підприємствах. Головним недоліком є те, що вони не надали чіткого пояснення щодо процесу обміну даними між фізичним та віртуальним середовищем. Що ще важливіше, фізична система, яка використовується в цьому дослідженні, не є універсальною. Отже, спосіб побудови системи цифрового двійника не може застосовуватися для будь-яких CPS.

Екхарт і Екельхарт [4] запропонували фреймворк, який дозволяє користувачам створювати цифрові системи-двійники на основі своїх фізичних систем автоматизовано. У своєму фреймворку вони прагнуть автоматично генерувати віртуальне середовище на основі специфікацій, отриманих з фізичних систем. Таким чином, спеціалісти зможуть проводити тестування системи безпеки у віртуальному середовищі, не впливаючи на процеси в реальних системах. Описаний фреймворк включає в себе два основних компонента: модуль генерації системи цифрових двійників та модуль аналізу безпеки. Найбільшою проблемою цієї системи є обмеження щодо формату даних і мережевих протоколів (TCP/IP). Деякі типи даних, такі як числа з плаваючою комою (2.4567…) не обробляються в їх системі. Іншими словами, запропонований ними фреймворк не підтримує всі типи даних. Крім того, деякі дані потрібно вводити вручну, оскільки схема автоматизації ще не повністю допрацьована.

Пізніше Екхарт [5] та ін. продовжили свою роботу, запропонувавши фреймворк, що продемонстрував як можна інтегрувати механізми безпеки на основі правил безпосередньо в DT. Правила безпеки – це набір принципів, норм і практик, які спрямовані на забезпечення стабільної роботи кіберфізичних систем. Вони використали підхід, заснований на специфікаціях, для реплікації стану фізичних пристроїв шляхом моніторингу їх вхідних та вихідних сигналів, що продемонструвало успішне виявлення атак проти тестового середовища CPS. У їхньому фреймворку спочатку визначаються специфікації фізичної системи, після чого ці дані реплікуються у віртуальне середовище. Під час процесу реплікації використовується технологія автомату станів, яка описує систему, що може перебувати в одному з кількох можливих станів, і в залежності від вхідних сигналів або подій може переходити з одного стану в інший. Вона застосовується для забезпечення узгодженості між фізичним та віртуальним середовищем.

Германн і Гуннарссон [6] також розглянули модель цифрового двійника як засіб вирішення проблем безпеки в CPS. У своїй концепції вони спочатку визначили основні вимоги до безпеки цифрового двійника, засновані на обміні та управлінні даними. Крім того, вони також використали технологію автомату станів для забезпечення синхронізації між фізичним і віртуальним середовищем. Що ще важливіше, вони використовували часові інтервали як параметр для запуску цієї синхронізації. У своїй роботі вони продемонстрували ефективність запропонованого протоколу синхронізації і довели, що безпека системи залежить від безпеки використовуваного мережевого каналу. Тому необхідно проводити аналіз безпеки всієї мережі та всіх протоколів системи. Недоліки цієї концепції полягають у тому, що вони обмежувалися спрощеною версією цифрового двійника, що створена для моделювання фізичної системи без надмірної складності.

Метою роботи є розробка концепції фреймворку цифрового двійника для кіберфізичних систем, який забезпечуватиме виявлення, аналіз, та протидію кібератакам, а також управління безпекою системи на основі даних. На відміну від існуючих підходів, запропонований фреймворк інтегруватиме багатокомпонентну модель безпеки, засновану на стохастичних мережах Петрі, що дозволить враховувати ймовірнісні характеристики системи та моделювати складні сценарії атак і збоїв.

Виклад основного матеріалу

Модель цифрового двійника є імітаційною моделлю, яка є віртуальним представленням реальної системи, що використовується для вивчення її поведінки, прогнозування результатів та оптимізації процесів. Вона створюється за допомогою математичних, статистичних або логічних методів і дозволяє експериментувати з системою без ризику для реальних об'єктів. Такі моделі можуть бути створені за допомогою одного з чотирьох основних підходів: дискретно-подійне моделювання (DES), безперервне моделювання, також відоме як системна динаміка (SD), агентне моделювання (ABS) та гібридне моделювання (HS) [7].

Кожен з вищеперерахованих підходів має свої переваги та сфери застосування, а також пропонує унікальні можливості, особливо у контексті забезпечення стабільності кіберфізичних систем. У моделях DES вважається, що стан системи змінюється лише в певні дискретні моменти часу, викликані певними подіями (тригерами). На відміну від DES, в SD зазначається, що стан системи змінюється та фіксується перманентно впродовж тривалого часу. ABS в свою чергу концентрується на активних частинах системи, описуючи їх як агентів, кожен з яких має свій поведінковий патерн. HS моделює системи, що поєднують в собі вищеописані принципи.

У цьому розділі ми розробимо та детально опишемо фреймворк цифрового двійника, призначеного для моделювання і аналізу безпеки кіберфізичних систем на основі стохастичної мережі Петрі. Ми опишемо ключові елементи фреймворку, включаючи основні модулі, алгоритми їхньої взаємодії, а також механізми інтеграції з фізичними системами. Модель цифрового двійника буде реалізована з використанням дискретно-подійного підходу, який передбачає, що стан системи безпеки реєструється та аналізується лише в дискретні, чітко визначені моменти часу, що дозволить ефективно відстежувати динаміку її роботи та реагувати на інциденти безпеки.

Як зазначають останні дослідження, технологія DT все частіше розглядається як засіб підвищення безпеки кіберфізичних систем, таких як автоматизовані системи керування і "розумні" енергосистеми. У літературі запропоновано кілька підходів, які дозволяють визначити набір різних (хоча і споріднених) цілей кібербезпеки, які можуть бути досягнуті за допомогою DT. Визначені цілі кібербезпеки в основному належать до наступних категорій:

Тестування стану безпеки: DT можуть використовуватися під час роботи системи для проведення неінвазивного вторгнення, не спричиняючи при цьому збоїв або пошкоджень в роботі системи та її обладнання.

Навчання основам кібербезпеки: DT можуть бути використані для створення віртуальних майданчиків для допомоги персоналу в навчанні основам кібербезпеки.

Виявлення атак/вторгнень/аномалій: вхідні дані в режимі реального часу можуть оброблятися віртуальною системою для виявлення поточних або майбутніх спроб вторгнень шляхом симуляції. Крім того, поведінку або стан віртуальної репліки можна порівняти з поведінкою або станом реальної системи, щоб виявити аномалії, спричинені кібератаками [8]. Це включає також виявлення неправильних конфігурацій програмного і апаратного забезпечення, які можуть свідчити про зловмисні маніпуляції, а також виявлення проблем конфіденційності шляхом об'єднання і кореляції даних про конфіденційність та оцінки відповідності загальним регламентам захисту даних (GDPR).

Вибір засобів контролю безпеки: DT можна використовувати для попередньої оцінки впливу на систему конкретних засобів контролю безпеки (і пов'язаних з ними рішень по реалізації) до їх фактичної імплементації. Ця діяльність може здійснюватися на основі аналізу та оцінки ризиків, що може допомогти операторам визначити пріоритетність впровадження засобів контролю безпеки для оптимізації витрат та максимізації переваг. Оцінку впливу засобу контролю безпеки до його фактичного застосування в системі, іноді називають керуванням оновленнями безпеки, особливо при розгляді систем операційних технологій (наприклад SCADA) [9], де оновлення, ймовірно, вплине на всю інфраструктуру системи і повинно бути ретельно оцінене заздалегідь. Можливість оцінити впровадження засобів безпеки заздалегідь є особливо корисною у випадках, коли мова йде про дороговартісні засоби, наприклад, реплікація компонентів системи або застосування методу диверсифікації (програмної, архітектурної тощо).

Генерація даних про кіберзагрози: DT можуть бути використані також для розробки та розповсюдження даних, що вилучаються в ході симуляції спланованих інцидентів (порушень) безпеки, що можуть загрожувати інформаційній або операційній безпеці системи.

Діагностика: на основі історичних даних, зібраних і проаналізованих DT, можна проводити діагностичні заходи, спрямовані на дослідження причин порушень безпеки.

Після огляду останніх публікацій стосовно DT, очевидно, що впровадження технології DT для цілей кібербезпеки є дуже перспективним і, ймовірно, привертатиме все більше уваги в наступні роки з боку наукової спільноти, яка працює над різними аспектами циклу управління ризиками кібербезпеки. Однак слід зазначити, що, незважаючи на наявність декількох імплементацій в різних сферах (наприклад, Інтернет речей, ICS, мікромережі), запропоновані рішення, як правило, не показують наочно, як методи, що використовуються для досягнення розглянутих цілей кібербезпеки (наприклад, імітація вторгнень або виявлення атак), інтегровані в базовий DT.

У світлі наведених вище міркувань ми пропонуємо фреймворк DT, який чітко ідентифікує та інтегрує основні функції DT з функціями, пов'язаними з безпекою, та організовує їх у вигляді набору логічних рівнів. Фреймворк, схематично зображений на рисунку 1, розширює базову архітектуру DT рівнями та функціями, орієнтованими на забезпечення безпеки кіберфізичної системи. Зокрема було розроблено п'ять основних рівнів, включаючи: **Фізичний об'єкт**, де розміщена CPS; **Цифровий двійник**, що містить віртуальну копію системи; **Службовий рівень**, що пропонує різні засоби контролю безпеки; **PT-DT (Physical Twin – Digital Twin)**, що зберігає та керує даними з фізичного середовища у вигляді журналів; **DT-SERV (Digital Twin services)**, що керує даними згенерованими цифровим двійником.

Рівень фізичного об'єкта включає вихідну CPS разом зі всіма сенсорами (датчиками) та актуаторами (активними елементами), необхідними для збору даних з системи і створення цифрового двійника для управління системою на основі модуля зворотного зв'язку. На цьому рівні ми інтегруємо функціонал збору даних про безпеку системи, шляхом розгортання зондів та агентів безпеки, що призначені для моніторингу та захисту системи (SIEM, EDR) [10], а також вилучення даних та метрик про стан безпеки. Крім того, ми додаємо механізм безпеки CPS, який полягає у фактичному розгортанні та активації засобів контролю безпеки в результаті процесу аналізу, доступному на службовому рівні. Забезпечення безпеки в CPS може вимагати додаткового етапу розробки та тестування або, якщо це можливо, може використовувати автоматизовані механізми.

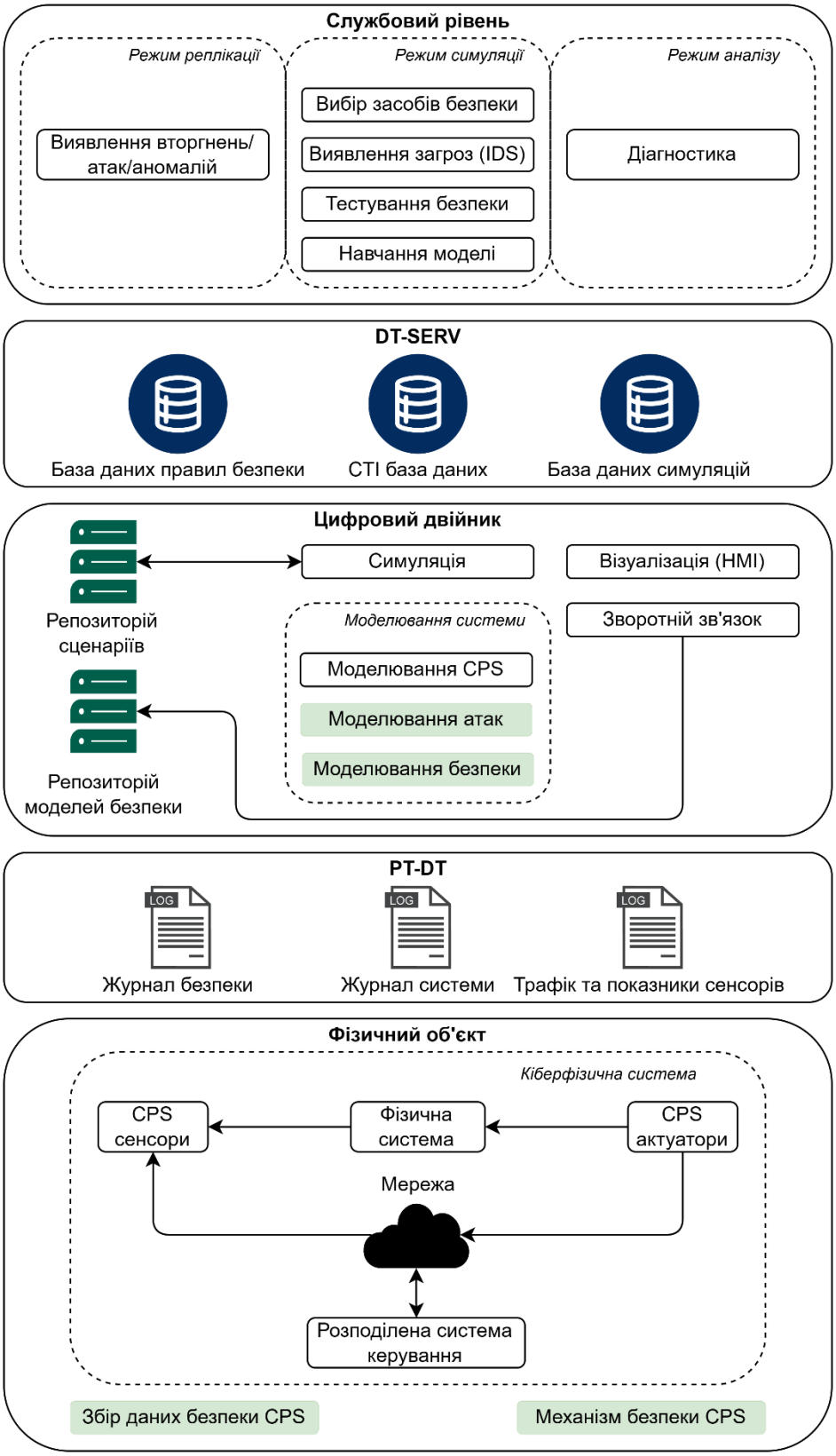

Рис. 1. Фреймворк цифрового двійника для кіберфізичних систем

Рівень PT-DT відповідальний за зберігання та управління даними (як пов'язаними, так і не пов'язаними з безпекою), що генеруються фізичним середовищем і використовуються цифровим двійником для фактичної побудови імітаційної моделі. Дані PT-DT включають журнали безпеки, а також (агреговані та відфільтровані) дані датчиків та інші системні журнали, що стосуються, наприклад, операцій, виконаних підсистемами CPS. Ці дані можуть бути використані в діагностичних цілях для виявлення джерела або причини інциденту безпеки.

Рівень цифрового двійника включає в себе чотири основних компоненти, зокрема моделювання системи, симуляція, зворотній зв'язок та візуалізація. Системне моделювання включає функціонал, спрямований на статичну або динамічну побудову комплексної моделі CPS, здатної охопити функціональні та безпекові аспекти. Ця функціональність спирається на репозиторій моделей безпеки, який керує всіма доступними моделями. Існує декілька підходів до моделювання, як для презентації елементів та функцій CPS, так і для представлення властивостей безпеки (конфіденційність, цілісність, доступність тощо). Наприклад, AMP (Automation Markup Language) – популярний інструмент, який можна використовувати для опису повного інженерного ланцюжка виробничих систем, пропонуючи стандартизований формат обміну даними XML. Він використовується для автоматичного створення цифрових двійників CPS на основі їх специфікацій (компонентів, функцій тощо). Що стосується моделювання безпеки, то найпопулярнішими інструментами є графи атак, дерева атак та мережі Петрі. Такі мережі можна використовувати для моделювання поведінки зловмисника з урахуванням реальних активів (компонентів) системи і пов'язаних з ними вразливостей, вони широко застосовуються для імітації вторгнень і тестування моделі безпеки.

Насправді, функціонал моделювання безпосередньо використовується модулем симуляції, який дозволяє запускати моделі на основі попередньо визначених сценаріїв (доступних у репозиторії сценаріїв) або на основі даних у реальному часі, що надходять з фізичного об'єкта. Нарешті, модуль зворотного зв'язку дозволяє запускати оновлення як на фізичному рівні (наприклад, шляхом запуску виконання певних контрзаходів), так і в імітаційних моделях відповідно. На завершення, візуалізація представляє традиційну функцію DT, яка полягає в тому, аби повідомляти систему або користувача про поточний і майбутній стан безпеки, щоб допомогти їм приймати рішення і реагувати на інциденти безпеки. Візуалізувати поточний стан системи можна через інтерфейс HMI (Human-Machine Interface), що дозволяє людині взаємодіяти з механізмами, системами або пристроями.

Рівень DT-SERV інтегрований з метою видобування спеціалізованих даних для побудови високорівневих сервісів. Сюди входять правила безпеки, які можна використовувати, наприклад, для виявлення атак/вторгнень/аномалій, а також дані CTI (Cyber Threat Intelligence), які можна використовувати для тестування моделі безпеки. CTI в даному контексті це процес дослідження інформації про потенційні загрози та вторгнення. Крім того, на цьому рівні зберігаються результати симуляцій різних сценаріїв, необхідні для систем безпеки.

Службовий рівень зберігає сервіси, класифіковані на основі використовуваного режиму роботи DT. Вони можуть працювати в різних режимах, зокрема симуляції, аналізу та реплікації, залежно від того, які дані вони використовують [11]. У режимі аналізу дані ретроспективно аналізуються за допомогою статистичних засобів для вилучення даних, а запуск діагностики виявляє першопричини небезпеки. У режимі симуляції дані, взяті з моделей, використовуються для імітації або симуляції поведінки системи: це корисно для проведення тестування, навчання, дослідження та оцінки наявних засобів безпеки. Нарешті, в режимі реплікації DT функціонує в реальному часі, синхронізуючись із фізичною системою, для виявлення аномалій, попередження про можливі несправності та ідентифікації загроз.

Для аналізу та оцінки ризиків у складних системах, зокрема в контексті кіберфізичних систем, а також для створення моделей безпеки для компонентів CPS використовуються стохастичні мережі Петрі (SPN). Такі мережі використовуються для моделювання поведінки систем із ймовірнісними характеристиками для відображення невизначеності, пов'язаної з ризиками та загрозами.

Мережа Петрі - це кортеж з 5-ти елементів $PN = (P, T, F, W, M_0)$ [12].P - це скінченна множина позицій (станів), що позначається колами. T - множина маркерів, що позначається прямокутниками. F - множина дуг, що з'єднують позиції з переходами або переходи з позиціями. $W: F \to \{1,2,\dots\}$- це множина вагових функцій. $M_0: P \to \{1,2,\dots\}$- це множина початкових маркерів (токенів). $P \cap T = \emptyset$ та $P \cup T \neq \emptyset$. Перехід активований, якщо і тільки якщо кожна з його вхідних позицій містить принаймні один маркер. Активація переходу вилучає один маркер з кожної вхідної позиції та додає один маркер до кожної вихідної позиції.

Стохастична мережа Петрі – це кортеж з 6-ти елементів $SPN = (P, T, F, W, M_0\lambda)$ [12]. $\lambda = \{\lambda_1, \lambda_2, \dots, \lambda_{|T|}\}$- це набір середніх швидкостей активації переходів. Кожен перехід t_i асоціюється випадковою затримкою активації, щільність ймовірності якої описується експоненційним розподілом з параметром λ_i. $\tau_i = \frac{1}{\lambda_i}$ це середня затримка активації переходу t_i.

На рисунку 2 зображено модель безпеки для компонента CPS у вигляді стохастичної мережі Петрі. Для зручності компонент буде позначатися символом c_i. Функції щільності ймовірності для трьох переходів (нормальний процес, атака, відновлення) описуються експоненційним розподілом з відповідними параметрами швидкості $\lambda_{i1}, \lambda_{i2}, \lambda_{i3}$. Перехід t_i^e позначає нормальну поведінку компонента з швидкістю активації λ_{i1}. Атака на компонент з боку зловмисника представляється переходом t_i^a з швидкістю активації λ_{i2}. Маркер, що з'являється в позиції відмови p_i^f (failure place), сигналізує що компонент c_i зазнав несанкціонованого доступу або злому. Після злому слід вжити заходів для відновлення, наприклад, перезавантажити систему. Перехід t_i^r позначає процес відновлення після виведення компонента з ладу, де швидкість активації λ_{i3}. Маркер, що з'являється в позиції успіху p_i^s (success place), вказує на те, що програма чи процес виконали всі операції без помилок і досягли бажаного результату по протидії загрозам. Позиції p_i^b та p_i^s є відповідно вхідною та вихідною в структурі компонента.

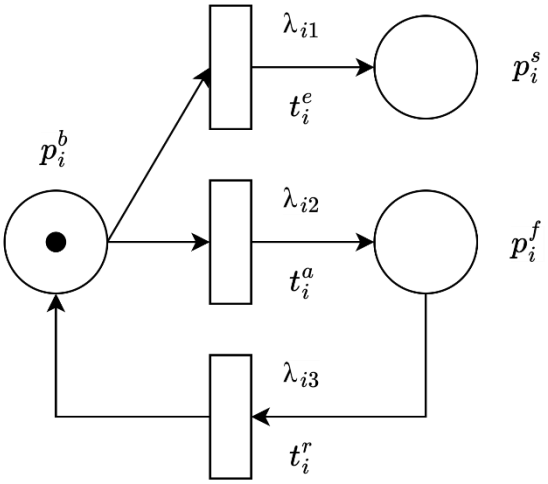

Рис. 2. Модель безпеки для компонента CPS

Кожен програмний компонент має вразливості, які можуть бути використані для компрометації (атаки, зламу, порушення). Система, що складається більш ніж з одного компонента може бути організована одним з чотирьох підходів. *Послідовний підхід* застосовується до систем, де кожен наступний компонент залежить від результатів виконання функцій попереднього компонента, наприклад в системах автентифікації. *Паралельний підхід* використовується для систем, в яких можна виконувати задачі незалежно, наприклад, аналіз великих обсягів даних або обробка багатьох запитів одночасно. *Циклічний підхід* застосовується у системах, де завдання потрібно виконувати повторно для оновлення або збору нових даних, наприклад в моніторингових системах. *Вибірковий підхід* використовується в системах, де потрібна гнучкість і адаптивність, оскільки виконуються тільки ті функції, які необхідні для певного контексту або умов.

Розглянемо модель безпеки на рисунку 3, що зазвичай використовується в багатокомпонентних системах на основі паралельного підходу, в яких функції виконуються паралельно для підвищення швидкості та ефективності роботи системи.

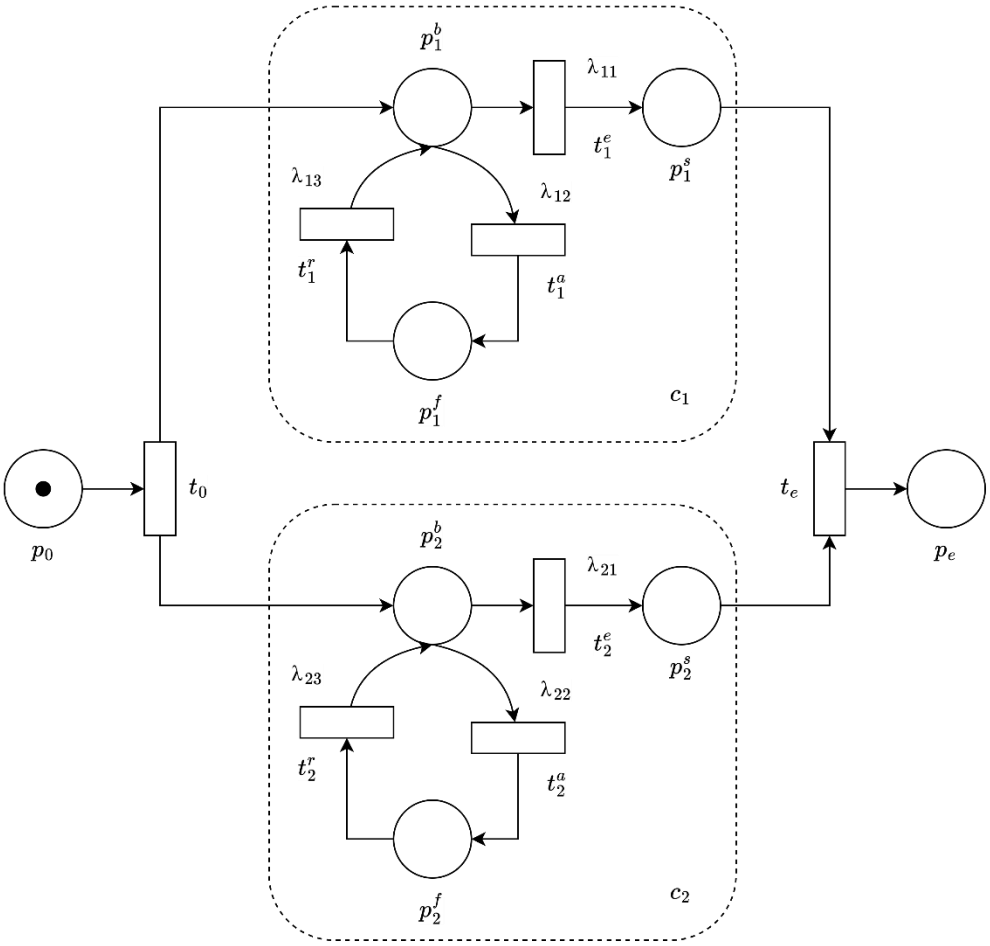

Рис. 3. Модель безпеки для багатокомпонентної паралельної CPS

Ймовірність успішного вторгнення зловмисника в системі, що складається з n компонентів визначається через формулу $\beta_i = max_{i=1}^{n}$. А ймовірність успішного виконання функції в системі, що складається з n компонентів визначається через формулу $\beta_i = 1 - max_{i=1}^{n}$.

Ймовірність успішного вторгнення (SAP) – це метрика, що оцінює систему безпеки, вимірюючи ймовірність того, що система буде зламана чи скомпрометована. У сталому стані, коли система досягає рівноваги, SAP обчислюється як сума ймовірностей тих станів системи, де є маркери у позиціях відмов. Позиції відмов в моделі системи позначають ситуації, коли компоненти або частини системи зазнали зламу або порушень безпеки. Чим вищий SAP, тим більша ймовірність того, що система може бути дестабілізована, оскільки більше позицій (станів) системи вказують на наявність уразливих місць, які можуть бути атаковані. SAP можна розрахувати за формулою:

$$SAP = \sum_{j=1}^{n} \sum_{r=1}^{k} P\left[M_j(p_{fr}) \geq 1\right],$$

де P означає ймовірність того, що позиція p_{fr} містить більше ніж один маркер сталого стану M.

Ймовірність компрометації системи визначається компонентом, який має найбільшу ймовірність компрометації і визначається за формулою:

$$1 - \overset{i=1}{\underset{n}{max}}(SAP_i).$$

Аналіз чутливості можна використовувати для виявлення вузьких місць у ефективності, надійності та безпеці, а також для відстеження вразливостей. Це необхідно для оптимізації системи на ранніх етапах проектування. Деякі параметри моделі важко визначити на стадії проектування. Аналіз чутливості полягає в оцінці впливу зміни вихідних параметрів системи на її кінцеві характеристики. Цей вплив можна розрахувати за формулою:

$$\left| \frac{d\left(1 - \overset{i=1}{\underset{n}{max}}(SAP_i)\right)}{d\lambda} \right|,$$

де d - це похідна, λ - швидкість активації переходу, n - кількість компонентів.

Таким чином можна побудувати модель безпеки для кожного окремого компонента або системи в цілому, зважаючи на принцип побудови системи. Процес побудови моделі безпеки відбувається безпосередньо на рівні цифрового двійника, що дозволяє оцінити стабільність віртуальної копії у випадках несанкціонованого доступу та інших інцидентів безпеки. Завдяки цифровому двійнику можна імітувати різні сценарії атак, аналізувати їх наслідки та виявляти слабкі місця в системі. Тестування за допомогою умовних сценаріїв (what-if) дозволить передбачати поведінку фізичного компонента та його вплив на систему під час протидії загрозам. Це також дає можливість протестувати ефективність різних стратегій захисту ще на етапі проектування системи. У результаті забезпечується більш високий рівень стійкості до кібератак і знижується ризик збоїв у фізичній системі.

Висновки

У даній роботі було розроблено фреймворк цифрового двійника для кіберфізичної системи у вигляді п’яти взаємопов’язаних логічних рівнів, що спрямований на вирішення основних потенційних проблем безпеки, які можуть виникнути в фізичній системі. Описано ключові елементи фреймворку, включаючи основні модулі, алгоритми їхньої взаємодії, а також механізми інтеграції з фізичними системами. Побудовано модель безпеки для багатокомпонентної паралельної CPS на базі стохастичної мережі Петрі з використанням дискретно-подійного підходу. Такий підхід передбачає, що стан системи безпеки реєструється та аналізується лише в дискретні моменти часу. Проаналізовано основні метрики, що дозволяють визначити рівень стабільності системи та її компонентів під час інцидентів безпеки. Запропонований фреймворк може бути застосований у системах протидії та виявлення вторгнень (IPS/IDS) в галузі інформаційних технологій для аналізу вразливостей, тестування поведінки системи під впливом потенційних загроз та розробки моделі безпеки, що забезпечить стабільність системи. Інтеграція фреймворку для систем розумного виробництва (SMS) в галузі промисловості дозволить змоделювати виробничі процеси та ідентифікувати вузькі місця, аномалії в компонентах системи, що призведе до оптимізації енергоспоживання та витрат.

Література

1. Review on cyber vulnerabilities of communication protocols in industrial control systems / Yikai Xu [та ін.] // 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, 2017. DOI: 10.1109/EI2.2017.8245509

2. Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements / Holger Flatt [та ін.] // 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, 2016. DOI: 10.1109/ETFA.2016.7733634

3. Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation / Ron Bitton [та ін.] // Computer Security. – Cham, 2018. – С. 533–554. DOI: 10.1007/978-3-319-99073-6_26

4. Eckhart M. Towards Security-Aware Virtual Environments for Digital Twins / Matthias Eckhart, Andreas Ekelhart // ASIA CCS '18: ACM Asia Conference on Computer and Communications Security, Incheon Republic of Korea. – New York, NY, USA, 2018. DOI: 10.1145/3198458.3198464

5. Eckhart M. A Specification-based State Replication Approach for Digital Twins / Matthias Eckhart, Andreas Ekelhart // CCS '18: 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto Canada. – New York, NY, USA, 2018. DOI: 10.1145/3264888.3264892

6. Gehrmann C. A Digital Twin Based Industrial Automation and Control System Security Architecture / Christian Gehrmann, Martin Gunnarsson // IEEE Transactions on Industrial Informatics. – 2020. – Т. 16, № 1. – С. 669–680. DOI: 10.1109/TII.2019.2938885

7. Banks J. Introduction to discrete-event simulation / Jerry Banks, John S. Carson // the 18th conference, Washington, D.C., USA, 1986. DOI: 10.1145/318242.318253

8. On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks / Ahmed Saad [та ін.] // IEEE Transactions on Smart Grid. – 2020. – Т. 11, № 6. – С. 5138–5150. DOI: 10.1109/TSG.2020.3000958

9. Digital Twins and Cyber Security – solution or challenge? / David Holmes [та ін.] // 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Preveza, Greece, 2021. DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277

10. A Security Metric Catalogue for Cloud Applications / Valentina Casola [та ін.] // Advances in Intelligent Systems and Computing. – Cham, 2017. – С. 854–863. DOI: 10.1007/978-3-319-61566-0_81

11. Empl P. Digital-Twin-Based Security Analytics for the Internet of Things / Philip Empl, Günther Pernul // Information. – 2023. – Т. 14, № 2. – С. 95. DOI: 10.3390/INFO14020095

12. Murata T. Petri nets: Properties, analysis and applications / T. Murata // Proceedings of the IEEE. – 1989. – Т. 77, № 4. – С. 541–580. DOI: 10.1109/5.24143

References

1. Review on cyber vulnerabilities of communication protocols in industrial control systems / Yikai Xu [et al.] // 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, 2017. DOI: 10.1109/EI2.2017.8245509

2. Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements / Holger Flatt [et al.] // 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, 2016. DOI: 10.1109/ETFA.2016.7733634

3. Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation / Ron Bitton [et al.] // Computer Security. – Cham, 2018. – P. 533–554. DOI: 10.1007/978-3-319-99073-6_26

4. Eckhart M. Towards Security-Aware Virtual Environments for Digital Twins / Matthias Eckhart, Andreas Ekelhart // ASIA CCS '18: ACM Asia Conference on Computer and Communications Security, Incheon Republic of Korea. – New York, NY, USA, 2018. DOI: 10.1145/3198458.3198464

5. Eckhart M. A Specification-based State Replication Approach for Digital Twins / Matthias Eckhart, Andreas Ekelhart // CCS '18: 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto Canada. – New York, NY, USA, 2018. DOI: 10.1145/3264888.3264892

6. Gehrmann C. A Digital Twin Based Industrial Automation and Control System Security Architecture / Christian Gehrmann, Martin Gunnarsson // IEEE Transactions on Industrial Informatics. – 2020. – Vol. 16, no. 1. – P. 669–680. DOI: 10.1109/TII.2019.2938885

7. Banks J. Introduction to discrete-event simulation / Jerry Banks, John S. Carson // the 18th conference, Washington, D.C., USA, 1986. DOI: 10.1145/318242.318253

8. On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks / Ahmed Saad [et al.] // IEEE Transactions on Smart Grid. – 2020. – Vol. 11, no. 6. – P. 5138–5150. DOI: 10.1109/TSG.2020.3000958

9. Digital Twins and Cyber Security – solution or challenge? / David Holmes [et al.] // 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Preveza, Greece, 2021. DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277

10. A Security Metric Catalogue for Cloud Applications / Valentina Casola [et al.] // Advances in Intelligent Systems and Computing. – Cham, 2017. – P. 854–863. DOI: 10.1007/978-3-319-61566-0_81

11. Empl P. Digital-Twin-Based Security Analytics for the Internet of Things / Philip Empl, Günther Pernul // Information. – 2023. – Vol. 14, no. 2. – P. 95. DOI: 10.3390/INFO14020095

12. Murata T. Petri nets: Properties, analysis and applications / T. Murata // Proceedings of the IEEE. – 1989. – Vol. 77, no. 4. – P. 541–580. DOI: 10.1109/5.24143