DOI 10.20535/2411-1031.2025.13.2.344719
УДК 004.77:004.056.5:004.94

ЄВГЕН САМБОРСЬКИЙ

УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА ПОДІЯМИ БЕЗПЕКИ МОБІЛЬНОЇ СТІЛЬНИКОВОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ЦИФРОВОГО ДВІЙНИКА

У статті акцентовано увагу на розгляді існуючих наразі підходів для ефективного забезпечення інформаційної безпеки сучасних і перспективних мобільних засобів цифрового зв'язку. Відмічено, що сучасна мобільна інформаційно-комунікаційна стільникова мережа є одним із найбільш важливих і водночас уразливих об'єктів критичної інформаційної інфраструктури держави. Ця мережа обслуговує значну кількість користувачів, які, як правило, приймають рішення для організації ефективного державного управління, а також забезпечує цифровим зв'язком низку інших абонентів, від широких верст населення до усіх відомчих корпоративних структур. Саме тому ця критична мережа і виступає як пріоритетний об'єкт у контексті організації ефективного управління подіями її інформаційної безпеки. Для організації надійного функціонування цього важливого критичного інформаційного об'єкта запропоновано новий підхід до синтезу алгоритмічного забезпечення цифрового двійника системи управління інформацією і подіями безпеки комп'ютерних систем стільникової мобільної інформаційно-комунікаційної мережі.

В основу запропонованого синтезу покладено логіко-динамічне моделювання існуючого наразі широкого спектра подій безпеки в сучасних управляючих системах інформаційно-комунікаційних мереж, сценаріїв атак та механізмів реагування на вказані інциденти інформаційної безпеки за рахунок формування відповідних ефективних управляючих впливів на процеси компенсації їх деструктивних наслідків. Розглянуто архітектуру цифрового двійника, алгоритм її синтезу, а також запропоновані можливі підходи для реалізації інтеграції цього віртуального об'єкта з такими платформами як Wazuh, Streamlit, Neo4j, AWS IoT. Проведено верифікацію та тестування на прикладі сценарію типової атаки DDoS, наведено результати реалізації алгоритму синтезу цифрового двійника. Показано ефективність моделі щодо адаптації до інтенсивних варіацій безпекового середовища комп'ютерної системи стільникової мобільної цифрової мережі. Відмічено, що запропонована архітектура цифрового двійника за рахунок реалізації відповідного алгоритмічно-програмного продукту забезпечуватиме синергетизацію вузлів інформаційно-комунікаційної мережі, подій безпеки, станів комп'ютерної системи при реалізації безпекового управління і сценаріїв реагування на переважну більшість усіх можливих інцидентів інформаційної безпеки.

Зроблено висновок, що запропонований алгоритм синтезу дозволяє послідовно реалізувати ключові етапи побудови цифрового двійника для віртуального представлення системи цифрового зв'язку, включаючи формалізацію подій безпеки, побудову логічних переходів у комп'ютерних системах і інтеграцію в реальні структури інформаційно-комунікаційної мережі.

Ключові слова: цифровий двійник, система управління, інформаційна безпека, логіко-динамічна модель, мобільна інформаційно-комунікаційна мережа, Wazuh.

Постановка проблеми у загальному вигляді. У сучасних умовах постійного і інтенсивного зростання темпів інформаційного протистояння та гібридної агресії цифровий

стільниковий зв'язок наразі відіграє ключову роль у функціонуванні об'єктів критичної інформаційної інфраструктури (КІІ) нашої держави, включаючи усі енергетичні структури, фінансову систему, логістичні мережі, державні реєстри, і особливо, корпоративний захищений зв'язок. Забезпечення безпеки комп'ютерних систем (КС), які є ядром організації та забезпечення управління системними процесами у мобільних інформаційно-комунікаційних мережах (МІКМ) стало надзвичайно актуальним у зв'язку із зростанням кількості та складності загроз інформаційній безпеці цих управляючих обчислювальних засобів.

Оцінка ймовірності виникнення атак у MANET в умовах невизначеності є не лише складним технічним завданням, а й важливою складовою національної та корпоративної кібербезпеки. Її вирішення вимагає впровадження інтелектуальних підходів – таких як нечітка логіка, моделі нечіткої агрегації, оцінка довіри до вузлів тощо.

Таким чином, розробка ефективних моделей і методів оцінювання загроз у MANET в умовах неповної, нечіткої або суперечливої інформації є одним із ключових наукових завдань сучасності. Вона має велике практичне значення для підвищення стійкості критичних інфраструктур, військових систем, аварійного зв'язку та автономних мереж в умовах надзвичайних ситуацій.

Яскравим прикладом прояви деструктивних наслідків вказаних загроз була масштабна кібератака у грудні 2023 року на одного з найбільших мобільних операторів нашої держави – "Київстар". Ця атака призвела до тривалого і серйозного порушення цифрового зв'язку, в тому числі і захищеного корпоративного, затяжних збоїв у роботі банківських, логістичних, енергетичних та адміністративних сервісів. Цей інцидент крім організаційних проблем в управлінні вказаною цифровою стільниковою структурою виявив наразі як технічну, так і концептуальну неспроможність традиційних систем управління інформацією і подіями безпеки (СУІПБ), які сьогодні експлуатуються в МІКМ, оперативно, ефективно і надійно протистояти у реальному часі сучасним складним багаторівневим інцидентам інформаційної безпеки (ІІБ).

Організація ефективного управління інформацією та подіями безпеки в умовах експлуатації динамічних, гетерогенних та розподілених мобільних стільникових цифрових мереж потребує нагальної реалізації суттєво нових підходів. Особливої уваги заслуговують методи, що дозволяють синтезувати функціонально ефективні, адаптивні та стійкі до атак засоби управління інформацією і подіями безпеки. У цьому контексті важливу роль відіграє застосування та реалізація концепції цифрових двійників (ЦД), яка дозволяє відтворювати віртуальні моделі об'єктів МІКМ та однозначно відображати їх у режимі реального часу. Як правило, концепція синтезу ЦД ґрунтується на сучасних технологіях, а саме: технології Industry 4.0. При цьому обов'язково враховуємо, що МІКМ є одним із найбільш уразливих та водночас особливо важливих об'єктів КІІ щодо забезпечення їх безпекової та функціональної стійкості. Вона обслуговує надширокe коло користувачів – від населення до відомчих структур держави. Саме тому МІКМ виступає як пріоритетний об'єкт щодо організації управління подіями її інформаційної безпеки. Тому науково-прикладна задача синтезу алгоритмічно-програмного забезпечення ЦД СУІПБ КС МІКМ потребує розробки нових моделей, методів та алгоритмів для суттєвого підвищення рівня захищеності та функціональної стійкості цих сучасних і перспективних засобів мобільного цифрового зв'язку.

Аналіз останніх досліджень і публікацій. Останніми роками спостерігається суттєве зростання наукового інтересу до створення та постійного удосконалення концепції і технологій ЦД як ефективного інструменту підвищення безпеки МІКМ. У сфері управління інформацією і подіями безпеки КС МІКМ ЦД дозволяють створювати та практично реалізовувати віртуальні копії об'єктів КІІ, яким притаманна здатність до моніторингу, аналізу станів і моделювання розвитку ПБ у реальному часі цих критичних систем. Проаналізуємо

результати останніх фундаментальних та прикладних досліджень, які викладені у низці відомих наукових праць.

Відмітимо, що наукова праця [1] є визначальною для організації та проведення синтезу логіко-динамічних моделей (ЛДМ) ЦД СУІПБ КС МІКС та обґрунтовує актуальність даного підходу для складних інформаційних управляючих систем. У працях [2] та [3] автори всебічно обґрунтовують доцільність використання ЛДМ в задачах забезпечення безпеки КС у разі наявності подій безпеки із високим ступенем критичності, демонструючи її адаптивність, масштабованість та відповідність динамічній природі ІІБ.

Особливу увагу приділяють проблематиці виявлення атак типу APT, MITM, DDoS у сучасних цифрових мобільних мережах, що мають високу динамічність топології та обмеженість у реакціях із боку класичних SIEM / SOAR платформ. У цьому контексті ЦД із вбудованою ЛДМ здатен не лише відтворювати архітектуру МІКМ, а також і моделювати можливі деструктивні наслідки подій безпеки, прогнозувати критичні стани й запускати управління цими ІІБ. Систематизований підхід до синтезу вказаних моделей всебічно описано в роботах [4]-[7]. У наведених працях запропоновано алгоритмічні рішення щодо реагування на події безпеки з використанням моделей несанкціонованого впливу і логіко-подієвих схем організації процесів управління.

Проведений аналіз наукових джерел свідчить про актуальність і потужний потенціал ЛДМ для вирішення складних задач алгоритмізації ЦД КС у розподілених критичних середовищах – МІКМ.

СУІПБ КС МІКМ з ЦД, в яких реалізовано розглянутий підхід, мають суттєві переваги над класичними SIEM/SOAR – системами за рахунок можливості адаптивного реагування на низку ПБ, прогнозування розвитку ІІБ, моделювання взаємної кореляції ПБ в МІКМ, а також оперативного і ефективного формування управління подіями безпеки у таких мережах. Це визначає наукову новизну і практичну цінність подальших досліджень щодо синтезу ЦД із логіко-динамічним ядром у КС стільникових МІКМ.

Метою статті є обґрунтування та розроблення ефективного підходу до синтезу ЦД логіко-динамічної СУІПБ КС стільникової МІКМ як критичного об’єкта національної інформаційної інфраструктури. Особливу увагу при цьому буде акцентовано на побудові синергетизованої архітектури ЦД, створення алгоритму його функціонування на основі ЛДМ, а також інтеграції ЦД із сучасними платформами моніторингу й обробки безпекових подій, а саме:

- Wazuh;
- Streamlit;
- Neo4j;
- AWS IoT тощо.

Поряд з цим метою також є дослідження ефективності запропонованої моделі в умовах DDoS-сценаріїв і високодинамічних безпекових процесів у КС МІКМ. Це дозволить забезпечити високий рівень безпекової та функціональної стійкості КС, передбачити розвиток можливих загроз (і особливо “нульового дня”), автоматично формувати стратегії реагування та адаптивне управління подіями безпеки та низкою інших ризиків у критичних умовах функціонування сучасних стільникових мобільних засобів зв’язку.

Отже, головна мета статті полягає в тому, щоб запропонувати нові та ефективні підходи до синтезу ЦД СУІПБ КС МІКС, реалізація яких забезпечить надійний захист КС від сучасних і можливих майбутніх загроз.

Виклад основного матеріалу дослідження. Для розроблення принципово нових та ефективних способів синтезу ЦД СУІПБ із використанням ЛДМ, реалізація яких забезпечить надійний захист КС МІКМ від існуючих загроз їх безпеці, і, особливо, від загроз нульового дня, врахуємо, що МІКМ – найбільш уразлива поміж усіх об’єктів КІІ. Серед основних типів можливих інформаційних загроз, котрі є генераторами подій безпеки КС, найбільш критичними є такі:

- перехоплення трафіку;
- глушіння (подавлення) радіоканалів цифрового зв'язку;
- атаки, пов'язані із шкідливим програмним забезпеченням;
- внутрішні безпекові загрози КС МІКМ;
- APT-атаки з поетапним впливом на структуру МІКМ.

Вказаним загрозам безпеці КС притаманні ознаки високої динамічності, неоднозначності та взаємозалежності, що унеможливлює їх ефективне оброблення та компенсацію вказаних ІІБ традиційними засобами. У зв'язку з цим для вирішення цієї проблеми спочатку формалізуємо організацію управління ПБ КС МІКМ як логіко-динамічної системи з метою інтеграції її у структуру ЦД СУІПБ. При цьому врахуємо, що стільниковій МІКМ притаманна низка специфічних особливостей та характеристик, які суттєво впливають на вимоги до синтезу ЦД. Найбільш важливими з них є:

- динамічна топологія МІКМ, яка об'єднує вузли мережі (базові станції, маршрутизатори, комутатори тощо), які постійно та динамічно змінюють своє розташування та навантаження залежно від географічної структури та варіацій кількості користувачів;
- гетерогенність (неоднорідність) пристроїв (різні типи терміналів, протоколів, стандартів (4G, 5G, LTE тощо);
- висока щільність трафіку (особливо в сильно урбанізованих зонах, що суттєво ускладнює моніторинг, аналіз, ідентифікацію та оперативне реагування на ПБ КС МІКС);
- критичність сервісів, яка полягає в забезпеченні вимог щодо обслуговуванні екстрених та спеціальних служб, медичних закладів, енергетичних і логістичних об'єктів.

Ці особливості вимагають від ЦД спроможності адаптивно та оперативно формувати управляючі реакції на зміну параметрів та гнучку інтеграцію з наявними в структурі СУІПБ КС МІКС.

Для цієї формалізації вимог до ЦД запропонуємо модель виду:

$$DT = (F, T, A, O). \tag{1}$$

де F – функціональні вимоги;
T – технічні вимоги;
A – аналітичні вимоги;
O – організаційні вимоги.

Кожен із цих елементів запропонованої моделі (1) деталізуємо у вигляді підмножин, а саме:

$$F = (f_1, f_2, \ldots, f_n);$$
$$T = (t_1, t_2, \ldots, t_n);$$
$$A = (a_1, a_2, \ldots, a_n);$$
$$O = (o_1, o_2, \ldots, o_n).$$

Реалізація процесів ефективного управління ПБ КС стільникової МІКМ передбачає відповідність ЦД СУІПБ низці вимог, які охоплюють функціональні, технічні, аналітичні та організаційні аспекти. Його архітектура повинна бути гнучкою, масштабованою, безпечною та відповідати у повному обсязі міжнародним безпековим стандартам. Визначимо ці вимоги, які стануть підгрунтям для побудови ефективної логіко-динамічної СУІПБ із використанням ЦД. При цьому цей віртуальний об'єкт має забезпечувати реалізацію важливих функцій, які передбачають моніторинг поточних та попередніх подій безпеки, реконструкцію ланцюгів цих подій та їх деструктивних впливів на процеси функціонування КС МІКМ, прогнозування стану ІКМ у відповідь на усі можливі інциденти інформаційної безпеки КС, генерацію управлінський дій для оперативної та ефективної протидії загрозам цим управлячим засобам. Врахуємо, що вимоги до ЦД СУІПБ КС МІКМ передбачають:

- можливість інтеграції з телеметричними засобами, логами, NetFlow, syslog МІКС;
- відображення актуального (поточного) стану топології МІКМ;

– формалізацію поведінки системи з використанням ЛДМ;

– прогнозування наслідків від ПБ та оперативне формування управлінських реакцій на інциденти; сумісність із реальними безпековими платформами сучасних МІКМ типу SIEM / SOAR.

Вказане свідчить, що синтез ЦД СУІПБ КС ІКМ з логіко-динамічним ядром є складною задачею, яка охоплює проєктування архітектури, формалізацію станів, моделювання переходів і інтеграцію з реальними інформаційно-управлінськими платформами сучасних цифрових мереж.

Синтезуємо функціональну архітектуру ЦД СУІПБ КС ІКМ. У процесі синтезу врахуємо, що цей алгоритмічно-програмний засіб є віртуальним аналогом фізичної системи, який в реальному часі забезпечує моніторинг, аналіз, прогнозування та управління ПБ. Архітектура такого двійника буде ґрунтуватися на застосуванні ЛДМ, що забезпечить моделювання дискретних станів КС та їх переходів під впливом зовнішніх та внутрішніх безпекових подій та можливих ІІБ. Розроблена структура цього віртуального аналога фізичної системи – ЦД СУІПБ КС МІКМ складається з синергетизованих модульних підсистем (рис. 1).

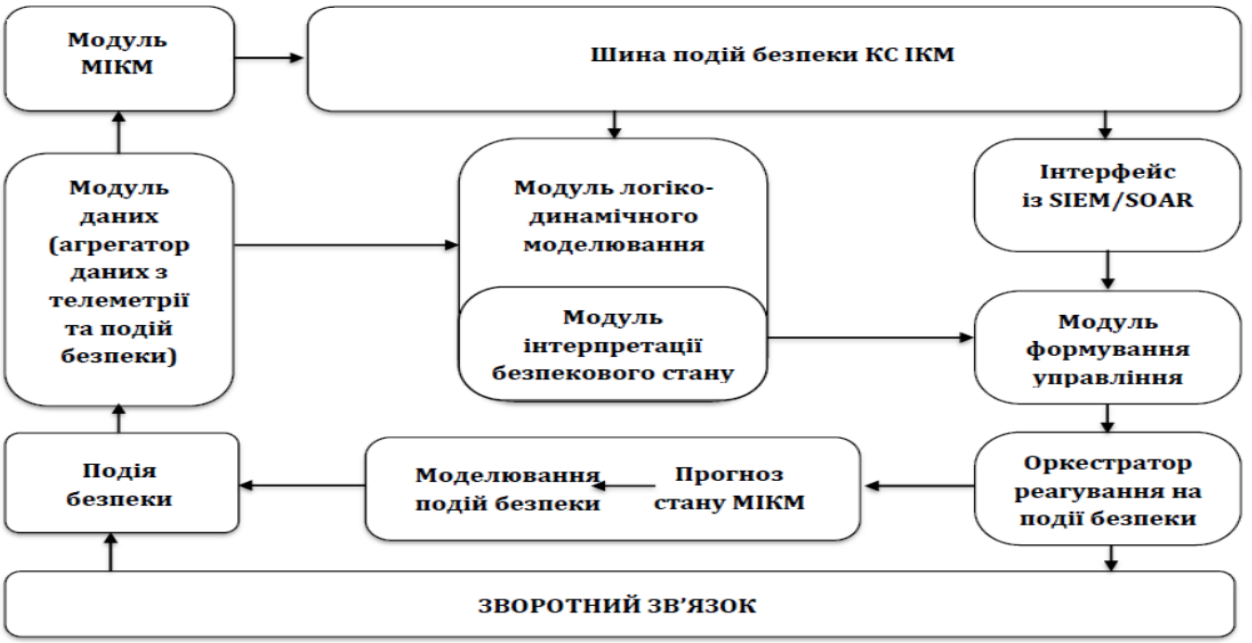

Рисунок 1 – Архітектура ЦД СУІПБ управляючої КС ІКМ, побудованої на логіко-динамічному підході

Розглянемо функціональне призначення модулів, які входять в запропоновану архітектуру.

Модуль структури ІКМ – віртуальна модель топології мобільної стільникової ІКМ. Вона включає вузли, канали, базові станції, комутатори, маршрутизатори. Реалізується через Neo4j – графові бази даних і постійно оновлюється в реальному часі за інформацією від інтерфейсу програмування застосунків API (Application Programming Interface) та телеметричних засобів про стан мережі.

Модуль даних – агрегує дані від телеметричних засобів МІКМ, лог-файли, мережеві події безпеки, SNMP-запити, NetFlow, syslog. Забезпечує нормалізацію, синхронізацію у часі та обробляє дані. Працює з використанням Kafka, Fluentd або OpenTelemetry.

Модуль логіко-динамічного моделювання представляє собою логіко-динамічне ядро ЦД та реалізує ЛДМ у вигляді кортежу:

$$LDM = (S, E, M, T),$$

де S – множина станів МІКМ;

E – множина ПБ;

M – функції моніторингу стану КС,

T – правила переходів між станами КС.

Цей модуль аналізує поведінку цієї обчислювально-управляючої системи та виявляє її критичні стани з врахуванням моделі (1).

Модуль інтерпретації безпекового стану – інтерактивний інтерфейс для відображення поточного стану системи, результатів прогнозування та рекомендацій щодо оперативного реагування за рахунок формування та реалізації управляючих впливів. Реалізується за допомогою Streamlit, Grafana, Kibana.

Інтерфейс інтеграції із SIEM / SOAR реалізує оперативний обмін інформацією про події безпеки в МІКМ, сповіщеннями та керуючими командами з системами типу Wazuh, Splunk, TheHive, OpenCTI. Забезпечує двосторонній обмін з SOC-аналітикою.

Оркестратор реагування на події безпеки– підсистема автоматизації реагування на події, що підтримує сценарії плану реагування на ІІБ, реалізовані у вигляді логічних дерев. Ці логічні дерева активуються ЦД у залежності від моделі векторів загроз КС МІКМ.

Взаємодія між компонентами реалізується через шину даних із підтримкою publish–subscribe моделі- шаблону обміну повідомленнями у програмній архітектурі КС. Такий підхід дозволяє динамічно оновлювати модель, адаптувати її до зміни станів МІКМ та забезпечувати циклічний механізм в алгоритмі обробки безпекових подій, який представлений у вигляді:

“Подія безпеки → Аналіз → Прогноз → Управлінське рішення → Реагування → Зворотній зв’язок”.

Запропонований алгоритм складається з низки синергетизованих послідовних етапів. Кожен з них передбачає поступову формалізацію з подальшою інтеграцією ЛДМ в архітектурі ЦД (рис.1). Підґрунтям побудова ЦД є забезпечення вимог до реалізації його здатності до самостійного аналізу ПБ, прогнозування їх наслідків, і, особливо, оптимізації підтримки прийняття рішень у безпековому середовищі мобільної стільникової МІКМ. Алгоритм синтезу включає наступні етапи:

Етап 1. Ідентифікація об'єкта моделювання: на цьому етапі проводиться визначення складових ІКМ як об’єкта КІІ та виділення ключових контрольних точок подій безпеки, інформаційних потоків і типових ІІБ.

Етап 2. Формалізація подій та станів: передбачає побудову множини дискретних станів S (наприклад: “нормальний”, “загроза виявлена”, “реакція активована”), визначаються множини подій E (інциденти, аномалії, несанкціоновані вторгнення), визначаються функції моніторингу M для фіксації умов певних подій безпеки з подальшою формалізацією у вигляді логічних правил чи графів переходів T між станами КС.

Етап 3. Побудова ЛДМ: передбачає об’єднання множин станів КС у кортеж $LD = (S, E, M, T)$, перевірку моделі на конфліктність, повноту та відсутність циклів без розв’язання, а також моделювання типових сценаріїв ІІБ і перевірку реакції моделі на ці події безпеки.

Етап 4. Інтеграція з цифровою інфраструктурою ІКМ: реалізує кореляцію з джерелами телеметрії (лог-файли, мережеві події, SNMP) та формуються адаптери для візуалізації, оркестрації реагування і взаємодії з SOC.

Етап 5. Навчання ЦД: передбачає адаптацію ЛДМ до нових можливих подій безпеки за рахунок застосування методів машинного навчання для виявлення нових сценаріїв подій

безпеки, а також навчання правилам переходів T на основі статистичних даних про ці ІІБ. Це навчання має на меті формування рефлексивної моделі поведінки ЦД.

Аналіз синтезованого алгоритму ЦД свідчить, що його реалізації в реальних СУІПБ КС МІКМ дозволить поступово перейти від опису об'єкта до функціональної моделі з прогнозними, реактивними та адаптивними можливостями управління подіями безпеки, яка може гнучко інтегруватися в сучасні комплексні системи захисту цих критично важливих цифрових мереж.

Відмітимо, що після побудови цього віртуального цифрового засобу СУІПБ КС МІКМ важливим етапом є його верифікація та валідація.

Врахуємо, що верифікація передбачає внутрішню комплексну перевірку логіки роботи моделі та її складових компонентів, а саме:

– перевірку правильності визначення множин станів S, подій безпеки E та правил переходів T;

– відсутністості логічних конфліктів, неоднозначних переходів або зациклення моделей;

– відповідності моделі заданій архітектурі та структурі ЦД.

Валідація спрямована на перевірку моделі в реальних або близьких до реальності умовах функціонування МІКМ.

Вона передбачає:

– тестування поведінки ЦД на основі сценаріїв атак (наприклад, DoS, APT, MITM);

– порівняння реакції моделі з еталонними сценаріями реагування в реальній SIEM – системі МІКМ;

– визначення точності, повноти та своєчасності виявлення ІІБ.

Алгоритм сценарію валідації полягає в наступному:

1. Генерується подія "аномальне перевантаження каналу зв'язку".
2. Модель фіксує зміну метрики через агрегатор телеметрії.
3. ЛДМ переходить у стан "загроза виявлена".
4. Активується сценарій реагування оркестратором для блокування трафіку.
5. Результат зберігається та виводиться на інтерфейс візуалізації.

Проведена верифікація забезпечує структурну узгодженість ЦД, а результати валідації свідчать про його ефективність у контексті компенсації деструктивних наслідків для КС МІКМ у разі появи реальних загроз її безпеці. Синергетизація верифікації та валідації дозволяє підвищити довіру до моделі та забезпечити її придатність для реалізації процесів інтеграції в реальне середовище – сучасні МІКМ (табл.1).

Для підтвердження працездатності синтезованого ЦД СУІПБ КС ІКМ було реалізовано експериментальну модель у віртуальному середовищі.

Як тестовий сценарій обрано умовну DDoS-атаку на КС, який є вузлом управління МІКМ.

Вибрано такі інструментальні середовища реалізації [8]-[10]:

– Streamlit – середовище моделювання використано для побудови інтерфейсу взаємодії та візуалізації процесів ЦД;

– Python – середовище моделювання використано для реалізація логіко-динамічного ядра та алгоритмів аналізу подій безпеки в КС МІКМ;

– Neo4j – графова база застосована для моделювання варіацій структури МІКМ та її можливих станів;

– MQTT – середовище моделювання використано для генерування потоків інформаційних даних із телеметричних засобів;

– Wazuh – середовище моделювання використано як джерело для генерування реальних логів та можливих подій безпеки.

Таблиця 1 – Інтеграція цифрового двійника з реальним середовищем МІКМ

Компонент / платформа	Завдання / функції	Особливості інтеграції	Приклад реалізації в МІКМ
Wazuh (SIEM)	Моніторинг подій безпеки та логів вузлів ІКМ	Використання агентів, REST API, підключення до менеджера Wazuh	Виявлення DDoS, MITM, інцидентів у базових станціях
Streamlit	Інтерактивна візуалізація станів моделі	Веб-інтерфейс, відображення станів, what-if моделювання	Граф переходів станів моделі у реальному часі
AWS IoT Core	Збір телеметрії, підключення пристроїв у ІКМ	MQTT, Lambda-функції, Amazon Timestream для аналізу та зберігання ПБ	Аналіз перевантаження каналів, зберігання часових рядів
Брокери повідомлень (Kafka, MQTT)	Передача подій у реальному часі до ЦД	Забезпечення publish–subscribe логіки, буферизація подій безпеки	Доставка телеметричної інформації з вузлів ІКМ до модуля LDM
Механізми реагування (SOAR/Playbook)	Ініціювання дій у відповідь на реальну загрозу	Підтримка обміну та реалізація сценаріїв реагування на події безпеки	Автоматичне блокування трафіку при DDoS

У ході експерименту ЦД фіксував підозріле навантаження, що надходило з певного сегмента мережі. Було сформовано подію “аномалія перевищення навантаження на трафік”, яка ініціювала перехід до стану “загроза виявлена”. Модель активувала сценарій реагування, який полягав у тимчасовому ізолювюнні трафіку, перенаправлення логів до SIEM. Під час тестування отримано наступні результати функціонування ЦД (табл. 2).

Таблиця 2 – Результати тестування ЦД під час сценарію реальної подій безпеки

Параметри	Значення параметрів	Оцінка ефективності	Коментарі експерименту
Середній час виявлення загрози	до 3 сек.	Висока швидкість	В межах цільового порогу (<5 сек.)
Кількість хибних спрацювань	1 із 20 подій	хибнопозитивних спрацювань – до 5%	Допустимий рівень для SIEM-класу
Навантаження на процесор	45–60%	Середнє навантаження	Пікове – під час обробки складних сценаріїв
Оновлення правил під час атаки	3 нових правила (при автоматичному оновленні)	Адаптивність підтверджено	Збережено до графової бази даних – масиву ПБ

Висновки. У результаті проведеного дослідження було реалізовано один з можливих підходів до побудови ЦД МІКМ, підґрунтям якого є логіко-динамічне моделюванні процесів управління ПБ.

Синтезована архітектура ЦД забезпечує структуровану синергетизацію вузлів МІКМ, ПБ, станів КС і сценаріїв реагування а можливі інциденти інформаційної безпеки.

Запропонований алгоритм синтезу моделі дозволяє послідовно реалізувати ключові етапи побудови цифрового представлення системи, включаючи формалізацію можливих подій безпеки, а також їх сукупність – ІІБ, побудову логічних переходів і інтеграцію в реальні середовища МІКМ.

Особливу увагу приділено практичним аспектам інтеграції ЦД з відомими засобами забезпечення безпеки:

- Wazuh;
- WS IoT;
- Streamlit;
- Neo4j.

Проведене тестування у віртуальному середовищі ІКМ показало здатність синтезованого ЦД до:

- швидкої ідентифікації загроз (часові параметри реакції при цьому складають порядка 3 с.);
- мінімізації хибних спрацювань (кількість спрацювань складає $\approx 5\%$);
- динамічного оновлення реакційної логіки;
- гнучкої візуалізації поточного стану і сценаріїв “what-if”, які формували гіпотетичні ситуації з метою оцінки потенційних наслідків конкретних подій безпеки, змін в прийнятті та реалізації управлінських рішень.

Отримані результати свідчать про ефективність логіко-динамічного моделювання до управління подіями безпеки у КС МІКС та доцільність застосування ЦД для підвищення рівня ситуаційної обізнаності, адаптивності та реактивності в глобальному управління такими інформаційно-комунікаційнми критичними інфраструктурами як МІКМ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] E.I. Samborskyi, and E.V. Peleshok,“Synthesis of Logical-Dynamic Information Management Systems and Security Events of Computer Structures”, *Control, Navigation and Communication Systems,* no. 2 (72), pp. 185-194, 2025, doi: https://doi.org/ 10.26906/SUNZ.2025.2.185-194.

[2] П. Павленко, та Є. Самборський, “Управління інформацією і подіями безпеки комп’ютерних систем із використанням логіко-динамічних моделей”, *Information Technology and Security,* т. 13, вип. 1 (24), с. 43-54, 2025, doi: https://doi.org/10.20535/2411-1031.2025.13.1.328764.

[3] S.M. Sholokhov, P.M. Pavlenko, B.A. Nikolaienko, I.I. Samborsky, and E.I. Samborsky “The method of optimizing the distribution of radio suppression means and destructive software influence on computer networks”, *Radio Electronics, Computer Science, Control,* no. 4 (67), pp. 16-29, 2023, doi: https://doi.org/10.15588/1607-3274-2023-4-2.

[4] Y. Cherdantseva et al., “A review of cyber security risk assessment methods for SCADA systems”, *Computers & Security*, vol. 56, pp. 1-27, 2016, doi: https://doi.org/10.1016/j.cose.2015.09.009.

[5] M. Repetto, “Cybersecurity Digital Twins: Concept, blueprint, and challenges for multi-ownership digital service chains”, *Journal of Information Security and Applications,* vol. 96, art. 104299, 2025, doi: https://doi.org/10.1016/j.jisa.2025.104299.

[6] K. Praveenkumar et al., “Digital Twins Driven by Artificial Intelligence to Mitigate, Detect, and Simulate Virtual Space Cyber Threats”, in *Proc 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES)*, Coimbatore, Tamilnadu, India, 2025. DOI: 10.1109/ICCIES63851.2025.11032312.
[7] Т. Куклінова, “Інтелектуалізація кіберзахисту енергетичних підприємств: управлінський підхід”, у *Безпека інформації та інфраструктури інформаційно-комунікаційних систем: міждисциплінарний підхід: монографія*, С. Горбаченко та А. Соколов, Ред. Львів, Україна: Liha-Pres, 2025 с. 71-102. Doi: https://doi.org/10.36059/978-966-397-537-5-3.
[8] “The Open-Source Security Platform. Documentation”, *Wazuh*. [Online]. Available: https://documentation.wazuh.com. Accessed: Aug. 1, 2025.
[9] “AWS IoT Developer Guide”, *Amazon Web Services*. [Online]. Available: https://docs.aws.amazon.com/iot. Accessed: Aug. 1, 2025.
[10] “Graph Data Platform”, *Neo4j*. [Online]. Available: https://neo4j.com. Accessed: Oct. 1, 2025.

Стаття надійшла до редакції 21.10.2025.

REFERENCES

[1] E.I. Samborskyi, and E.V. Peleshok,“Synthesis of Logical-Dynamic Information Management Systems and Security Events of Computer Structures”, *Control, Navigation and Communication Systems,* no. 2 (72), pp. 185-194, 2025, doi: https://doi.org/10.26906/SUNZ.2025.2.185-194.
[2] P. Pavlenko, and E. Samborsky, “Management of information and security events of computer systems using logical-dynamic models”, *Information Technology and Security,* vol. 13, iss. 1 (24), pp. 43-54, 2025, doi: https://doi.org/10.20535/2411-1031.2025.13.1.328764.
[3] S.M. Sholokhov, P.M. Pavlenko, B.A. Nikolaienko, I.I. Samborsky, and E.I. Samborsky “The method of optimizing the distribution of radio suppression means and destructive software influence on computer networks”, *Radio Electronics, Computer Science, Control,* no. 4 (67), pp. 16-29, 2023, doi: https://doi.org/10.15588/1607-3274-2023-4-2.
[4] Y. Cherdantseva et al., “A review of cyber security risk assessment methods for SCADA systems”, *Computers & Security*, vol. 56, pp. 1-27, 2016, doi: https://doi.org/10.1016/j.cose.2015.09.009.
[5] M. Repetto, “Cybersecurity Digital Twins: Concept, blueprint, and challenges for multi-ownership digital service chains”, *Journal of Information Security and Applications,* vol. 96, art. 104299, 2025, doi: https://doi.org/10.1016/j.jisa.2025.104299.
[6] K. Praveenkumar et al., “Digital Twins Driven by Artificial Intelligence to Mitigate, Detect, and Simulate Virtual Space Cyber Threats”, in *Proc 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES)*, Coimbatore, Tamilnadu, India, 2025. DOI: 10.1109/ICCIES63851.2025.11032312.
[7] T. Kuklinova, “Intellectualization of Cybersecurity of Energy Enterprises: A Management Approach”, in *Information Security and Infrastructure of Information and Communication Systems: An Interdisciplinary Approach: Monograph*, S. Horbachenko, and A. Sokolov, Eds. Lviv, Ukraine: Liha-Pres, 2025 pp. 71-102. doi: https://doi.org/10.36059/978-966-397-537-5-3.
[8] “The Open-Source Security Platform. Documentation”, *Wazuh*. [Online]. Available: https://documentation.wazuh.com. Accessed: Aug. 1, 2025.
[9] “AWS IoT Developer Guide”, *Amazon Web Services*. [Online]. Available: https://docs.aws.amazon.com/iot. Accessed: Aug. 1, 2025.
[10] “Graph Data Platform”, *Neo4j*. [Online]. Available: https://neo4j.com. Accessed: Oct. 1, 2025.

IYEVGEN SAMBORSKYI

MANAGEMENT OF INFORMATION AND SECURITY EVENTS OF A MOBILE CELLULAR NETWORK USING A DIGITAL TWIN

The article focuses on the consideration of currently existing approaches to effectively ensure the information security of modern and promising mobile means of digital communication. It is noted that the modern mobile information and communication cellular network is one of the most important and at the same time vulnerable objects of the critical information infrastructure of the state. This network serves a significant number of users, who, as a rule, make decisions for the organization of effective state management, and also provides digital communication to a number of other subscribers, from the general population to all departmental corporate structures. That is why this critical network acts as a priority object in the context of the organization of effective management of its information security events.

To organize the reliable functioning of this important critical information object, a new approach to the synthesis of algorithmic support of the digital twin of the information and event management system of computer systems of the cellular mobile information and communication network has been proposed.The proposed synthesis is based on the logical and dynamic modeling of the currently existing wide range of security events in modern control systems of information and communication networks, attack scenarios and response mechanisms to these information security incidents due to the formation of appropriate effective control influences on the processes of compensation for their destructive consequences. The architecture of the digital twin, the algorithm for its synthesis are considered, as well as possible approaches for the implementation of the integration of this virtual object with such platforms as Wazuh, Streamlit, Neo4j, AWS IoT are proposed. Verification and testing are carried out on the example of a scenario of a typical DDoS attack, the results of the implementation of the algorithm for the synthesis of a digital twin are presented. The effectiveness of the model in adapting to intensive variations in the security environment of the computer system of the cellular mobile digital network is shown.

It is noted that the proposed architecture of the digital twin due to the implementation of the appropriate algorithmic and software product will provide cyberization of information and communication network nodes, security events, computer system states in the implementation of security management and response scenarios to the vast majority of all possible information security incidents. It is concluded that the proposed synthesis algorithm allows sequentially implementing the key stages of building a digital twin for the virtual representation of a digital communication system, including the formalization of security events, the construction of logical transitions in computer systems and integration into real structures of the information and communication network.

Keywords: digital twin, control system, information security, synthesis, logical-dynamic model, mobile network, Wazuh.

Самборський Євген Іванович, старший викладач кафедри комп'ютерних наук та кібербезпеки, Волинський національний університет імені Лесі Українки, Луцьк, Україна, ORCID 0000-0003-4441-1947, seinauedu@gmail.com.

Samborskyi Ievgen, senior lecturer of the department of computer science and cybersecurity, Lesya Ukrainka Volyn National University, Lutsk, Ukraine.