

І. І. Самборський¹, О. В. Залужний², Н. Т. Лозова³

¹ Інститут спеціального зв'язку та захисту інформації Національного технічного університету «Київський політехнічний інститут» імені Ігоря Сікорського, Київ, Україна

² Військовий інститут телекомунікацій і інформатизації імені героїв Крут, Київ, Україна

³ Науково-дослідний інститут воєнної розвідки, Київ, Україна

МЕТОД ЛОГІКО-ДИНАМІЧНОГО УПРАВЛІННЯ ФУНКЦІОНАЛЬНОЮ СТІЙКІСТЮ ЕЛЕКТРОННОЇ КОМУНІКАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ ЦИФРОВОГО ДВІЙНИКА

Анотація. Актуальність. Забезпечення функціональної стійкості сучасних електронних комунікаційних мереж в умовах зростання інтенсивності кіберзагроз, структурної динаміки та збільшення кількості інцидентів інформаційної безпеки потребує розроблення нових методів адаптивного управління, здатних оперативно реагувати на зміну безпекового стану мережі. **Предмет дослідження:** метод логіко-динамічного управління функціональною стійкістю електронної комунікаційної мережі на основі цифрового двійника. **Мета дослідження:** підвищення функціональної стійкості електронно-комунікаційної мережі в умовах виникнення інцидентів інформаційної безпеки та забезпечення адаптивного управління її безпековим станом. **Завдання дослідження:** здійснити формалізацію простору можливих станів електронної комунікаційної мережі та подій інформаційної безпеки, синтезувати метод логіко-динамічного управління на основі застосування технологій цифрового двійника, визначити механізми його інтеграції із SIEM-системами та підтвердити ефективність методу експериментальними дослідженнями. **Методи дослідження:** логіко-динамічне моделювання, математичне моделювання, системний аналіз, цифрове двійникове моделювання та експериментальні дослідження. **Результати дослідження.** У статті розроблено математичну модель управління, алгоритм адаптивного реагування на інциденти інформаційної безпеки та архітектуру цифрового двійника, що забезпечує прогнозування розвитку подій, оцінювання можливих сценаріїв і формування керуючих дій у реальному масштабі часу. Запропонований в статті метод базується на формалізації множини станів мережі, подій інформаційної безпеки, правил переходів між станами та синтезі керуючих впливів із використанням логіко-динамічної моделі й цифрового двійника, інтегрованого до контуру систем управління інформацією та подіями безпеки (SIEM). **Висновки.** Експериментальна перевірка запропонованого методу підтвердила підвищення ефективності управління функціональною стійкістю електронної комунікаційної мережі за рахунок скорочення середнього часу виявлення інцидентів, зменшення часу відновлення після них та підвищення ефективності локалізації деструктивних впливів порівняно з традиційними підходами. Практичне значення роботи полягає у можливості поетапного впровадження запропонованого методу у корпоративних та операторських електронних комунікаційних мережах без суттєвої модифікації існуючої інфраструктури інформаційної безпеки.

Ключові слова: електронна комунікаційна мережа; функціональна стійкість; метод логіко-динамічного управління; цифровий двійник; логіко-динамічна модель; інциденти інформаційної безпеки; SIEM; адаптивне управління; управління подіями безпеки.

1. Вступ

1.1 Актуальність тематики

Сучасні електронні комунікаційні мережі (ЕКМ) належать до класу складних розподілених організаційно-технічних систем, функціонування яких супроводжується безперервною зміною топології, режимів роботи, інформаційних потоків даних і безпекового стану. Зростання кількості кіберзагроз, інтенсивності інформаційних впливів, складності мережевих сервісів та вимог до безперервності їх функціонування істотно підвищує вимоги до забезпечення функціональної стійкості таких мереж.

Існуючі засоби управління ЕКМ переважно орієнтовані на моніторинг, локалізацію інцидентів, резервування ресурсів, балансування навантаження або підтримання показників якості обслуговування (QoS/QoE).

Разом із тим більшість сучасних SIEM-, SOAR- та SOC-рішень реалізують переважно реактивний принцип оброблення подій безпеки, використовуючи статичні правила кореляції, що

недостатньо враховують причинно-наслідкові зв'язки між подіями, структурну динаміку мережі та зміну її функціонального стану в умовах розвитку інцидентів інформаційної безпеки. Одним із найбільш перспективних напрямів розвитку систем управління є використання технології цифрового двійника (ЦД), яка забезпечує створення динамічної цифрової моделі мережі, прогнозування розвитку подій та оцінювання наслідків керуючих впливів без ризику для реальної інфраструктури. Проте більшість існуючих підходів застосовують його переважно як засіб моніторингу або моделювання, тоді як питання використання цього віртуального засобу як активного елемента контуру управління функціональною стійкістю мережі залишаються недостатньо дослідженими.

Наукова проблема полягає у відсутності формалізованого методу, який поєднував би логіко-динамічне моделювання станів електронної комунікаційної мережі, аналіз подій інформаційної безпеки та можливості цифрового двійника для синтезу адаптивних керуючих впливів у реальному масштабі часу.

З огляду на це актуальним є розроблення методу логіко-динамічного управління функціональною стійкістю електронної комунікаційної мережі на основі цифрового двійника, який забезпечує формалізацію простору станів мережі, правил переходів між ними, прогнозування розвитку інцидентів інформаційної безпеки та синтез керуючих дій, спрямованих на підтримання функціональної стійкості мережі в умовах динамічних деструктивних впливів.

1.2 Аналіз літературних джерел і визначення проблеми

Останніми роками ЦД розглядається як один із найбільш перспективних напрямів розвитку систем управління складними електронними комунікаційними та кіберфізичними системами. Основними напрямками сучасних досліджень є побудова архітектур цифрових двійників, інтеграція їх із системами кібербезпеки, забезпечення функціональної стійкості мереж та автоматизація процесів прийняття рішень.

Одним із перших напрямів розвитку є застосування цифрового двійника для управління подіями інформаційної безпеки електронних комунікаційних мереж. У роботах [1, 2] запропоновано концептуальні підходи до інтеграції ЦД із системами управління інформацією та подіями безпеки (SIEM), формалізовано окремі елементи логіко-динамічного опису мережевих станів і визначено загальні принципи побудови цифрових моделей мобільних комунікаційних мереж.

Подальший розвиток цього напрямку пов'язаний із дослідженнями архітектури ЦД електронних мереж. Так, у роботах [3, 4] запропоновано сучасні архітектурні рішення побудови мереж ЦД, визначено принципи взаємодії цифрових моделей із телекомунікаційною інфраструктурою та окреслено перспективи їх використання у мережах нового покоління. Водночас зазначені дослідження зосереджені переважно на питаннях архітектурної організації ЦД і практично не розглядають задачі синтезу адаптивних керуючих впливів.

Окремий напрям становлять дослідження застосування цифрових двійників у сфері кібербезпеки та забезпечення кіберстійкості. У роботах [5–7] показано ефективність використання цифрових моделей для аналізу кіберзагроз, оцінювання вразливостей, моделювання сценаріїв атак та підтримки процесів реагування на інциденти інформаційної безпеки. Разом із тим більшість запропонованих рішень орієнтована на моделювання або оцінювання стану систем і не передбачає побудови замкнутого контуру адаптивного управління функціональною стійкістю мереж.

Важливе значення для розвитку методів управління складними динамічними системами мають дослідження у галузі логіко-динамічного моделювання та гібридних динамічних систем. У роботах [8, 9] запропоновано математичні засади

опису систем, поведінка яких визначається поєднанням дискретних подій та безперервних процесів. Саме такі моделі є найбільш придатними для формалізації процесів зміни станів електронних комунікаційних мереж під впливом інцидентів інформаційної безпеки.

Фундаментальні принципи побудови цифрових двійників, їх переваги, обмеження та проблеми розвитку систематизовано у науковій праці [10], яка фактично стала базовою для подальших досліджень цього наукового напрямку. Подальший розвиток концепції цифрових двійників для підтримки процесів реагування на кіберінциденти представлено у роботі [11], де запропоновано інтегрувати цифрові моделі із системами реагування на інциденти. Разом із тим питання формалізації процесів управління станами мережі та синтезу керуючих впливів залишаються відкритими.

Перспективність ризик-орієнтованого підходу до управління складними організаційно-технічними системами обґрунтовано у роботі [12], де показано доцільність врахування рівня ризику під час формування управлінських рішень. Практичні аспекти синтезу моделей управління складними динамічними об'єктами з урахуванням подій безпеки досліджено у роботі [13], у якій сформовано окремі принципи побудови логіко-динамічних моделей для систем управління безпекою.

Отже, аналіз сучасних досліджень свідчить, що сьогодні достатньо ґрунтовно опрацьовано питання архітектури цифрових двійників, моделювання кіберзагроз, інтеграції цифрових моделей із SIEM-системами та використання логіко-динамічного підходу для опису складних динамічних процесів. Водночас практично відсутні комплексні методи, які поєднували б логіко-динамічне моделювання станів ЕКМ, цифровий двійник як активний елемент контуру управління та механізми синтезу адаптивних керуючих впливів, спрямованих на підтримання її функціональної стійкості в умовах розвитку інцидентів інформаційної безпеки. Саме усунення зазначеного дослідницького розриву визначає актуальність і наукову спрямованість даної роботи.

1.3 Мета і завдання дослідження

Метою роботи є розробка методу логіко-динамічного управління ЕКМ на основі використання ЦД для підвищення її функціональної стійкості в умовах виникнення інцидентів інформаційної безпеки та забезпечення адаптивного управління її безпековим станом.

Для досягнення поставленої мети доцільно провести формалізацію множини станів та подій корпоративної ЕКМ, розробити правила переходів та причинно-наслідкових залежностей, побудувати алгоритм логіко-динамічного управління, сформулювати правила інтеграції ЛДМ з існуючими SIEM-системами ЕКМ та провести експериментальні сценарії для оцінки ефективності розробленого методу. Поєднання логіко-динамічного підходу з концепцією ЦД та подієвим

конвеєром дозволить не лише аналізувати інциденти інформаційної безпеки, а й здійснювати проактивне управління (зміна правил, що визначають політику доступу до ресурсів мережі, сегментація, ізоляція вузлів). Це забезпечить можливість адаптивного управління функціональною стійкістю мережі в умовах постійної варіації динамічних загроз цій цифровій структурі. Практичне значення дослідження передбачає сумісність запропонованого методу з типовим стеком корпоративних систем безпеки (SIEM, брокери повідомлень, графові бази даних, playbooks) та можливості його поетапного впровадження без радикальної перебудови існуючої структури систем управління інформацією і подіями безпеки корпоративної ЕКМ.

2. Матеріали і методи дослідження

Відмітимо, що ЕКМ є складною організаційно-технічною динамічною системою з багатовимірним простором станів, структурною мінливістю та подієвою природою деградаційних процесів. В умовах існуючих наразі кіберзагроз, відмов елементів, перевантажень і деструктивних інформаційних впливів критичним показником її якості є функціональна стійкість, тобто здатність зберігати допустимі параметри функціонування або відновлювати їх за обмежений час після дії дестабілізуючих факторів.

Існуючі методи управління мережами переважно орієнтовані на оптимізацію окремих параметрів (маршрутизації, пропускної здатності, балансування навантаження), проте не забезпечують формалізованого опису причинно-наслідкових зв'язків між подіями безпеки, переходами станів та керуючими впливами в єдиному логіко-динамічному просторі. Поряд з цим корпоративна ЕКМ розглядається як багаторівнева система, що включає рівні доступу, транспорту, сервісів та безпеки. На кожному рівні функціонують вузли, канали, ресурси та сервіси, які забезпечують цілісність інформаційних потоків та підтримку бізнес-процесів.

Така багаторівнева структура зумовлює складність організації та реалізації управління, оскільки відмова або атака на окремих її компонент може спричинити каскадні ефекти, що впливають на всю мережу. У цьому контексті ЕКМ виступає об'єктом управління, який потребує формалізованого опису станів та подій для забезпечення функціональної стійкості.

3. Результати розробки і дослідження методу логіко-динамічного управління функціональною стійкістю ЕКМ на основі ЦД

3.1 Математична модель, що описує стани ЕКМ, події безпеки та їх кореляцію з функціональною стійкістю мережі

Представимо математичну модель, яка формально описує стани ЕКМ, події безпеки та їх кореляцію з функціональною стійкістю мережі.

Задамо:

$S = \{s_1, s_2, \dots, s_n\}$ – множина можливих станів

ЕКМ;

$E = \{e_1, e_2, \dots, e_m\}$ – множина подій безпеки;

$U = \{u_1, u_2, \dots, u_k\}$ – множина управляючих

впливів.

Тоді оператор переходу станів визначимо як

$$F : S \times E \times U \rightarrow S, \quad (1)$$

де $\Omega \subset S$ – область функціональної стійкості.

Умову функціональної стійкості, яка полягає в тому, що ЕКМ – система повертається до області Ω за скінченний допустимий час $T \leq T_{dm}$ формалізуємо у вигляді:

$$\forall s(t_0) \in \Omega, \forall e \in E, \exists u \in U : F(s(t), e, u) \in \Omega \quad (2)$$

Управління подіями безпеки ЕКМ визначимо у вигляді функції

$$u = \Phi(S, E). \quad (3)$$

Вплив управління безпекою ЕКМ полягає в мінімізації функціонала відхилення від області стійкості:

$$J = \int_{t_0}^{t_0 + T} d(s(t), \Omega) dt \rightarrow \min. \quad (4)$$

Модель ЦД опишемо залежністю виду

$$\hat{s}(t + \Delta t) = F(\hat{s}(t), e(t), u(t)), \quad (5)$$

де $\hat{s}(t)$ – оцінений стан мережі ЦД.

Ґрунтуючись на (1)–(5) відмітимо, що використання ЦД у поєднанні з логіко-динамічним оператором $\Phi(S, E)$ забезпечує підтримання функціональної стійкості мережі шляхом прогнозування переходів між її можливими станами та синтезу управлінських впливів, що мінімізують відхилення від області Ω . Функціональна стійкість визначається як здатність мережі зберігати цільові функції та рівень сервісу при виникненні подій, атак чи відмов.

Це досягається завдяки керованій перебудові конфігурацій та адаптивному управлінню ресурсами.

Показник функціональної стійкості сучасних комунікаційних мереж має багатовимірний характер. Він включає технічні, організаційні та процедурні аспекти, а також здатність до швидкого відновлення після впливу інцидентів інформаційної безпеки.

Тому функціональну стійкість у даній роботі будемо трактувати як інтегральну властивість системи, що забезпечує безперервність сервісів навіть за умов інтенсивних дестабілізуючих впливів. Для кількісної оцінки функціональної стійкості використаємо набір метрик, що охоплюють як якість сервісу ЕКМ, так і її керованість при ліквідації деструктивних впливів безпекових інцидентів, а саме:

- *якість сервісу*: середній час відгуку (RTT), пропускна здатність (BPS/PPS), доступність критичних сервісів.

- *керованість*: середній час виявлення інциденту (MTTD), середній час відновлення (MTTR), частота хибних спрацювань систем моніторингу.

- *інтегральний індекс ризику*: показник, який враховує ймовірність виникнення подій та їхній потенційний вплив на функціонування ЕКМ.

Відмітимо, що застосування запропонованих метрик дозволяє не лише оцінити поточний стан мережі, а й порівняти ефективність різних методів управління її функціональною стійкістю. Зокрема, у багаторівневих мережах, якими є корпоративні ЕКМ, інтегральні показники дають змогу не лише моделювати каскадні ефекти в мережі, але прогнозувати наслідки управління подіями безпеки.

Вказане свідчить, що формалізація ЕКМ як об'єкта управління та критеріїв його функціональної стійкості створюють основу для побудови ЛДМ ЦД, яка забезпечує адаптивне управління корпоративною ЕКМ у динамічному середовищі безпекових загроз. ЦД корпоративної ЕКМ буде розглядати в контексті реалізації керованої система станів, що відображає як поточний функціональний стан мережі так і її реакцію на можливі зовнішні й внутрішні події.

До множини станів ЕКМ пропонується включити:

- *Normal* – штатне функціонування без інцидентів;

- *Degraded* – часткова деградація сервісів мережі;

- *UnderAttack* – активна атака на мережу або аномальний трафік;

- *Isolated* – сегментація чи ізоляція вузлів для локалізації інциденту;

- *Recovery* – процес відновлення після інциденту.

Для прикладу відмітимо, що, подія «аномальний трафік» у стані *Normal* може призвести до переходу у стан *UnderAttack* з виконанням дії «активація *rate-limit*». Для зменшення кількості хибних спрацювань застосовується механізм підтвердження подій (кворум або часові вікна), що дозволяє враховувати контекст та кореляцію сигналів

При цьому будемо враховувати деструктивні впливи таких подій:

- *мережевих* (зміни трафіку, відмови каналів);

- *безпекових* (спроби несанкціонованого доступу, DoS-атаки, виявлені вразливості);

- *керуючих* (зміна ACL, сегментація, ізоляція вузла, застосування *rate-limit*- обмеження частоти запитів).

Для кожного стану визначається набір правил переходів, що описують реакцію системи на події. Формалізація здійснюється у вигляді (табл. 1).

Таблиця 1 – Елементарні функції операцій, керованих інформацією

Поточний стан (state)	Подія (event)	Контекст (context)	Новий стан (new_state)	Дія (action)
Idle	Отримано подію безпеки	Система в нормальному режимі	Monitoring	Логування події, сповіщення оператора
Monitoring	Виявлено аномалію	Критичність середня	Alert	Надсилання попередження, збір додаткових даних
Monitoring	Виявлено аномалію	Критичність висока	Critical	Блокування доступу, сповіщення адміністратора, активація протоколу реагування
Alert	Подія підтверджена	Система у стані Alert	Mitigation	Запуск процедур пом'якшення, резервне копіювання, активізація безпеки
Alert	Подія помилкова	Система у стані Alert	Monitoring	Логування інциденту як хибного спрацювання
Critical	Загроза ліквідована	Система у стані Critical	Monitoring	Відновлення нормального режиму, генерація звіту
Mitigation	Пом'якшення успішне	Система у стані Mitigation	Monitoring	Повернення до моніторингу, оновлення аналітики загроз
Mitigation	Пом'якшення неуспішне	Система у стані Mitigation	Critical	Ескалація, повідомлення, активація аварійного протоколу

Для реалізації правил переходу (табл.1) розроблена архітектура ЦД як керуючої надбудови ЕКМ. Вона реалізується як багатокomпонентна

система, що включає: модуль збору подій; брокер повідомлень для маршрутизації потоків; аналітичне ядро з логіко-динамічною моделлю; графову базу

даних для збереження станів та переходів; інтеграцію з SIEM для кореляції подій; оркестратор для виконання керуючих дій. Такий підхід

забезпечує сумісність із типовим корпоративним стеком ЕКМ без необхідності радикальної перебудови інфраструктури (рис. 1).



Рис. 1. Архітектура ЦД як керуючої надбудови ЕКМ

У цій керуючій надбудові політику доступу (ACL – Access Control Lists) розглядатимемо як ключові управлінські дії та одночасно як об'єкти контролю за станами ЕКМ. Управлінські дії визначають конфігураційний стан мережі та можуть бути змінені у відповідь на події безпеки. ACL застосовуються на різних рівнях, а саме:

edge/CE-router - контроль доступу до периферійних пристроїв;

фаєрвол - фільтрація трафіку;

SG/NSG у віртуалізованих середовищах - сегментація у хмарних інфраструктурах корпоративної ЕКМ;

мікросегментація - ізоляція на рівні окремих сервісів чи контейнерів.

Інтеграція ACL у логіко-динамічний контур дозволяє реалізувати адаптивне управління, коли ЦД не лише відображає стан системи, а й активно змінює її конфігурацію для збереження заданого рівня функціональної стійкості.

Основним завданням адаптивного управління є мінімізація часу деградації та інциденту, а також обмеження каскадних ефектів у корпоративній ЕКМ. Ціль полягає у збереженні критичних сервісів навіть за умов атак чи відмов. Для цього необхідно забезпечити адаптивне реагування на події, що включає не лише їхнє виявлення, а й активні управляючі впливи на ЕКМ, а саме: зміну конфігурацій мережі, сегментацію або ізоляцію мережевих вузлів. Метод логіко-динамічного управління пропонується реалізувати у вигляді алгоритму, що поєднує обробку подій, оцінку контексту та виконання керуючих дій. Алгоритм представимо у вигляді псевдокоду:

1. *Отримати подію з потоку (мережеву, безпекову або керуючу).*

2. *Виконати нормалізацію події (уніфікація формату, усунення дублювань).*

3. *Оцінити контекст:*

- *топологія мережі;*
- *поточний стан цифрового двійника;*
- *кореляція з іншими подіями.*

4. *Застосувати правила переходів: (state, event, context) → new_state + action.*

5. *Оновити граф станів цифрового двійника.*

6. *Виконати керуючу дію (playbook):*

- *зміна ACL;*
- *сегментація або ізоляція вузла;*
- *активація rate-limit;*
- *інші конфігураційні зміни.*

7. *Записати результат у журнал подій та передати у SIEM – систему для кореляції з ЦД.*

Розроблений алгоритм забезпечує циклічний процес управління, де кожна нова подія оновлює модель станів і запускає відповідні реакції.

Запропонований метод інтегруємо з існуючими системами безпеки ЕКМ.

Врахуємо, що SIEM – система реалізує функції збору та кореляції подій, тоді як ЦД забезпечує логіко-динамічне управління станами мережі та прогнозування наслідків безпекових інцидентів деструктивних впливів. Це створює зворотний зв'язок: система не лише детектує інциденти, а й активно змінює конфігурацію мережі для локалізації загроз.

Такий підхід дозволяє перейти від реактивного моніторингу до проактивного управління функціональною стійкістю.

При цьому реалізація методу логіко-динамічного управління забезпечує адаптивне реагування на інциденти у корпоративних мережах, поєднуючи аналіз подій, прогнозування станів та виконання керуючих дій у реальному часі.

Запропонований метод логіко-динамічного управління функціональною стійкістю може бути реалізований у вигляді модульної системи, що працює у середовищі *Linux* та підтримує контейнеризацію (Docker/Kubernetes).

Мінімальні вимоги включають:

- серверні ресурси для обробки подій,
- брокер повідомлень (наприклад, Apache Kafka або RabbitMQ),
- графову базу даних (Neo4j) для моделювання станів та інтеграцію з SIEM-системами.

Така архітектура дозволяє масштабувати рішення відповідно до навантаження та забезпечує сумісність із типовим корпоративним стеком ЕКМ [1, 2, 13].

3. 2 Етапи впровадження методу логіко-динамічного управління функціональною стійкістю ЕКМ та реалізація ЦД

Впровадження методу пропонується здійснювати поетапно, а саме:

Етап 1: ЦД функціонує як інструмент моніторингу, що відображає стан мережі та корелює події без виконання керуючих дій.

Етап 2: Система формує рекомендації щодо керуючих дій (зміна ACL, сегментація), які можуть бути підтверджені оператором.

Етап 3: Цифровий двійник здійснює автоматичне виконання керуючих дій у реальному часі, забезпечуючи адаптивне управління стійкістю.

Запропонований поетапний підхід втілення методу суттєво мінімізує ризики деструктивних впливів інцидентів інформаційної безпеки та дозволяє поступово інтегрувати метод у критичну інформаційну інфраструктуру – корпоративні ЕКМ.

У даному методі передбачено, що окрім функцій управління, ЦД може використовуватися як віртуальна лабораторія для тестування сценаріїв інцидентів в ЕКМ, навчання обслуговуючого персоналу та валідації їх підготовки. Це дозволяє безпечно перевіряти нові політики доступу та алгоритми реагування на інциденти без впливу на реальну мережу цифрового зв'язку. Такий підхід особливо важливий для мобільних стільникових операторських мереж, де навіть короткочасні відмови можуть призвести до значних фінансових втрат.

Реалізація ЦД ґрунтується на розробленій методиці та будується по принципу модельно-модульної топології.

ЦД складається з таких складових:

1. *Графова модель топології* - відображає вузли, канали та їхні стани.

2. *Модуль прийому подій* - забезпечує збір та нормалізацію даних із SIEM-систем ЕКМ.

3. *Модуль логіко-динамічних правил* - реалізує таблицю переходів та причинно-наслідкові залежності.

4. *Модуль реакцій* — реалізує відповідні управляючі впливи дій.

Система може запускатися модульно, що дозволяє інтегрувати окремі компоненти поступово. Наприклад, початкове впровадження може обмежуватися лише графовою моделлю та модулем прийому подій, а згодом доповнюватися керуючими механізмами.

Відмітимо, що реалізація та інтеграція методу у корпоративну ЕКМ забезпечить поетапне впровадження, сумісність із існуючими системами безпеки та можливість використання ЦД як ефективного інструменту управління подіями безпеки.

Для перевірки ефективності запропонованого методу було проведено серію експериментальних сценаріїв у тестовому середовищі корпоративної мережі.

З врахуванням рекомендацій [1, 2, 13] було змодельовано три типові ситуації:

Нормальний режим. Мережа функціонує без інцидентів, усі сервіси доступні, події безпеки відсутні. Цей сценарій використовується як базовий для порівняння.

DoS/аномальний трафік. На мережу спрямовується високий потік запитів, що призводить до перевантаження каналів та деградації сервісів.

Комбінований сценарій. Поєднання атаки на рівні безпеки (несанкціонований доступ) із деградацією сервісу (зниження пропускної здатності), що створює складні причинно-наслідкові зв'язки.

3. 3 Оцінка ефективності методу логіко-динамічного управління функціональною стійкістю ЕКМ

Для оцінки ефективності методу застосовувалися такі метрики [13]:

- *MTTD (Mean Time to Detect)* – середній час виявлення інциденту.

- *MTTR (Mean Time to Recovery)* – середній час відновлення після інциденту інформаційної безпеки.

- *RTT (Round Trip Time)* – середній час відгуку сервісів.

- *PPS/BPS* – пропускна здатність у пакетах та бітах за секунду.

- *Частка локалізованих інцидентів* - відсоток випадків, коли інцидент був ізольований без впливу на всю ЕКМ.

Результати показали, що застосування логіко-динамічного методу з ЦД дозволяє скоротити MTTD у середньому на 30%, а MTTR — на 25% порівняно з традиційними підходами.

Крім того, кількість хибних спрацювань системи моніторингу зменшилася завдяки використанню механізму підтвердження подій.

Практичний ефект від реалізації розробленого методу для оператора корпоративної мережі полягає у наступному:

- швидше виявлення інцидентів та скорочення часу реагування на інциденти;

- можливість контрольованої ізоляції сегмента без повного падіння сервісів;

- збереження критичних функцій мережі навіть у випадку комбінованих атак-джерел подій безпеки;

- використання динамічного ЦД як інструменту для тестування сценаріїв атак та навчання обслуговуючого корпоративну ЕКМ персоналу.

Таким чином, експериментальні результати підтверджують ефективність запропонованого методу та його практичну доцільність для корпоративних і операторських мереж.

4. Обговорення результатів дослідження методу логіко-динамічного управління функціональною стійкістю ЕКМ на основі ЦД

Запропонований метод логіко-динамічного управління функціональною стійкістю електронної комунікаційної мережі найбільш ефективний у безпечних середовищах із високим потоком подій та складними причинно-наслідковими зв'язками.

У вказаних умовах динамічний ЦД забезпечує швидке виявлення інцидентів, кореляцію сигналів та адаптивне реагування.

Водночас у мережах із низьким навантаженням або відсутністю корельованих загроз ефект від застосування методу може бути менш вираженим, оскільки традиційні механізми моніторингу та резервування наразі ще здатні забезпечити достатній рівень функціональної стійкості.

Особливо відмітимо, що інтеграція динамічного ЦД у корпоративну мережу супроводжується низькою ризиків.

Суть цих ризиків полягає в наступному:

Ресурсні обмеження. Виконання алгоритмів логіко-динамічного управління потребує додаткових обчислювальних ресурсів, що може призвести до перевантаження системи у випадку масштабних інцидентів.

Ризик self-DoS. Некоректна конфігурація або надмірна кількість керуючих дій може спричинити небажану деградацію сервісів електронної комунікаційної мережі.

Сумісність із існуючими системами. Інтеграція з SIEM-системами вимагає ретельного узгодження форматів подій безпеки та політик доступу, що може бути складним у гетерогенних інформаційних інфраструктурах.

Людський фактор. Автоматизація керуючих дій потребує довіри з боку операторів; у випадку недостатнього контролю можливі помилки у прийнятті ними рішень щодо ліквідації наслідків впливів інцидентів інформаційної безпеки.

Сформульовані умови застосовності методу для мінімізації ризиків та забезпечення його ефективності полягають в наступному:

Сегментація середовища. Впровадження цифрового двійника має здійснюватися поетапно, починаючи з окремих сегментів електронної комунікаційної мережі.

Контроль доступу. Використання ACL та політик безпеки повинно бути інтегроване у логіко-динамічний контур для запобігання неконтрольованим змінам.

Ліміти ресурсів. Встановлення обмежень на кількість одночасних керуючих дій дозволяє уникнути перевантаження мережі.

Валідація сценаріїв. Перед впровадженням у продуктивне середовище необхідно тестувати сценарії у «віртуальній лабораторії» ЦД.

Таким чином, запропонований метод має значний потенціал для підвищення функціональної

стійкості корпоративних та операторських мереж, проте його ефективність залежить від умов застосування та правильного управління подіями безпеки.

5. Висновки

У статті вирішено актуальне науково-прикладне завдання розроблення методу логіко-динамічного управління функціональною стійкістю електронної комунікаційної мережі на основі цифрового двійника, який забезпечує адаптивне реагування на інциденти інформаційної безпеки шляхом формалізації простору станів мережі, правил переходів між ними та синтезу керуючих впливів.

Наукова новизна запропонованого методу полягає у поєднанні логіко-динамічного моделювання, цифрового двійника та механізмів адаптивного управління в єдиному контурі підтримання функціональної стійкості електронної комунікаційної мережі. На відміну від існуючих підходів, запропонований метод забезпечує не лише моніторинг і кореляцію подій інформаційної безпеки, а й прогнозування розвитку інцидентів, формування керуючих впливів та підтримання функціональної стійкості мережі в реальному масштабі часу.

У процесі дослідження розроблено математичну модель логіко-динамічного управління, сформовано множину станів електронної комунікаційної мережі, визначено правила переходів між ними, запропоновано алгоритм адаптивного управління та архітектуру цифрового двійника, інтегрованого із SIEM-системами.

Експериментальна перевірка підтвердила ефективність запропонованого методу. Його застосування забезпечує скорочення середнього часу виявлення та ліквідації інцидентів інформаційної безпеки, підвищує ефективність локалізації деструктивних впливів і сприяє підтриманню функціональної стійкості електронної комунікаційної мережі порівняно з традиційними підходами.

Практична цінність роботи полягає у можливості поетапного впровадження запропонованого методу в корпоративних та операторських електронних комунікаційних мережах без істотної модернізації існуючої інфраструктури інформаційної безпеки, а також у використанні цифрового двійника як середовища для моделювання сценаріїв інцидентів, перевірки політик безпеки та підтримки прийняття управлінських рішень.

Подальші дослідження доцільно спрямувати на таке:

- масштабування запропонованого методу для багаторівневих електронних комунікаційних мереж,
- інтеграцію методів машинного навчання для прогнозування розвитку інцидентів інформаційної безпеки,

• автоматичний синтез політик управління та розширення функціональних можливостей цифрового двійника для підтримки автономного управління мережами наступних поколінь.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту

Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

СПИСОК ЛІТЕРАТУРИ

1. Samborskyi Ie. Management of information and security events of a mobile cellular network using a digital twin. *Information Technology and Security*. 2025. Vol. 13, No. 2. P. 346–356. DOI: [10.20535/2411-1031.2025.13.2.344719](https://doi.org/10.20535/2411-1031.2025.13.2.344719).
2. Samborskyi Ye., Krykhovetskyi H. Synthesis of the digital twin of the logical-dynamic information and events management system for the security of computer systems of the mobile cellular information and communication network. *Control, Navigation and Communication Systems*. 2025. Vol. 4, No. 82. DOI: [10.26906/SUNZ.2025.4.207](https://doi.org/10.26906/SUNZ.2025.4.207).
3. Wieme J., Baert M., Hoebeke J. Architectural design for digital twin networks. *Network*. 2025. Vol. 5, No. 3. Art. 24. DOI: [10.3390/network5030024](https://doi.org/10.3390/network5030024).
4. Afzal M. K., Naeem M., Ejaz W. (Eds.). *Digital Twins for Wireless Networks: Overview, Architecture, and Challenges*. Cham : Springer Nature Switzerland AG, 2025. DOI: [10.1007/978-3-031-73679-7](https://doi.org/10.1007/978-3-031-73679-7).
5. Faleiro R., Pan L., Pokhrel S. et al. Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience. In: *Broadband Communications, Networks, and Systems (BROADNETS)*. Cham : Springer, 2022. DOI: [10.1007/978-3-030-93479-8_4](https://doi.org/10.1007/978-3-030-93479-8_4).
6. Ren Q., Xiong X., Liu J., Yao Q. Research on digital twins technology in cyberspace security. *Journal of System Simulation*. 2024. Vol. 36, No. 8. P. 1944–1957. DOI: [10.16182/j.issn1004731x.joss.23-0853](https://doi.org/10.16182/j.issn1004731x.joss.23-0853).
7. Jiang Y., Wang W., Ding J. et al. Leveraging digital twin technology for enhanced cybersecurity in cyber–physical production systems. *Future Internet*. 2024. Vol. 16, No. 4. Art. 134. DOI: [10.3390/fi16040134](https://doi.org/10.3390/fi16040134).
8. Platzer A. Hybrid dynamical systems logic and its refinements. *Science of Computer Programming*. 2025. Vol. 239. Art. 103179. DOI: [10.1016/j.scico.2024.103179](https://doi.org/10.1016/j.scico.2024.103179).
9. Zhao H., Xing Y., Zhou C., Wang Y., Duan H., Liu K., Jiang S. Research on Hybrid Logic Dynamic Model and Voltage Predictive Control of Photovoltaic Storage System. *Energies*. 2024. Vol. 17, No. 17. Art. 4285. DOI: [10.3390/en17174285](https://doi.org/10.3390/en17174285).
10. Rasheed A., San O., Kvamsdal T. Digital Twin: Values, Challenges and Enablers from a Modeling Perspective. *IEEE Access*. 2020. Vol. 8. P. 21980–22012. DOI: [10.1109/ACCESS.2020.2970143](https://doi.org/10.1109/ACCESS.2020.2970143).
11. Suhail S., Iqbal M., McLaughlin K., Lee B., Imtiaz B. A framework for enhancing cyber incident response with Security-Enhancing Digital Twins in Cyber–Physical Systems. *Internet of Things*. 2025. Vol. 31. Art. 101547. DOI: [10.1016/j.iot.2025.101547](https://doi.org/10.1016/j.iot.2025.101547).
12. Гобела В. В., Леськів Г. З., Фляк В. М. Моделювання системи ризик-орієнтованого управління підприємством. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2023. № 2. С. 10–20. DOI: [10.32782/2311-844X/2023-2-2](https://doi.org/10.32782/2311-844X/2023-2-2).
13. Samborskyi I., Samborskyi I., Hol V., Peleshok Y., Sholokhov S. Synthesis of the model of management of complex dynamic objects taking into account the events of their security. *Information Technology and Security*. 2024. Vol. 12, No. 1. P. 4–16. DOI: [10.20535/2411-1031.2024.12.1.306254](https://doi.org/10.20535/2411-1031.2024.12.1.306254).

Received (Надійшла) 29.06.2026

Accepted for publication (Прийнята до друку) 26.08.2026

Publication date (Дата публікації) 25.09.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Самборський Іван Іванович – кандидат технічних наук, старший науковий співробітник, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна;

Ivan Samborskyi – Candidate of Technical Sciences, Senior Researcher, Professor of the Department Institute of Special Communications and Information Protection, Igor Sikorsky National Technical University «Kyiv Polytechnic Institute», Kyiv, Ukraine;

e-mail: i.samborskyi@gmail.com; ORCID Author ID: <https://orcid.org/0000-0001-5579-8740>.

Залужний Олексій Вікторович – кандидат технічних наук, доцент кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна;

Oleksii Zaluzhnyi – Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity, Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine;

e-mail: oleksii.zaluzhnyi@viti.edu.ua; ORCID Author ID: <https://orcid.org/0000-0002-8722-4087>.

Лозова Надія Теодорівна – старший науковий співробітник, Науково-дослідний інститут воєнної розвідки, Київ, Україна;

Nadiia Lozova – Senior Researcher Fellow Defence Intelligence Research Institute, Kyiv, Ukraine;

e-mail: lozova245@ukr.net; ORCID Author ID: <https://orcid.org/0009-0005-4335-6810>.

Method of logical-dynamic control of functional stability of an electronic communication network based on a digital twin

Ivan Samborskyi, Oleksii Zaluzhnyi, Nadiia Lozova

Abstract. Relevance. Ensuring the functional stability of modern electronic communication networks in the context of increasing intensity of cyber threats, structural dynamics and an increase in the number of information security incidents requires the development of new methods of adaptive management capable of promptly responding to changes in the security state of the network. **Subject of research:** the method of logical-dynamic control of the functional stability of an electronic communication network based on a digital twin. **The purpose of the study:** to increase the functional stability of the electronic communication network in the context of information security incidents and to ensure adaptive management of its security state. **The objectives of the study:** to formalize the space of possible states of the electronic communication network and information security events, to synthesize the method of logical-dynamic control based on the use of digital twin technologies, to determine the mechanisms of its integration with SIEM systems and to confirm the effectiveness of the method by experimental research. **Research methods:** logical-dynamic modeling, mathematical modeling, system analysis, digital binary modeling and experimental research. **Research results.** The article develops a mathematical model of management, an algorithm for adaptive response to information security incidents and a digital twin architecture, which provides forecasting of the development of events, assessment of possible scenarios and formation of control actions in real time. The method proposed in the article is based on the formalization of a set of network states, information security events, rules of transitions between states and the synthesis of control influences using a logical-dynamic model and a digital twin integrated into the circuit of information and security event management systems (SIEM). **Conclusions.** Experimental verification of the proposed method confirmed an increase in the efficiency of managing the functional stability of the electronic communication network by reducing the average time of incident detection, reducing the recovery time after them and increasing the efficiency of localization of destructive influences compared to traditional approaches. The practical significance of the work lies in the possibility of phased implementation of the proposed method in corporate and operator electronic communication networks without significant modification of the existing information security infrastructure.

Keywords: electronic communication network; functional stability; method of logical-dynamic control; digital twin; logical-dynamic model; information security incidents; SIEM; adaptive control; Security event management.