NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2025.13.1.328764
УДК 004.942

ПЕТРО ПАВЛЕНКО,
ЄВГЕН САМБОРСЬКИЙ

УПРАВЛІННЯ ІНФОРМАЦІЄЮ І ПОДІЯМИ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ ІЗ ВИКОРИСТАННЯМ ЛОГІКО - ДИНАМІЧНИХ МОДЕЛЕЙ

У статті розглядається один із можливих підходів до організації управління інформацією та подіями безпеки комп'ютерних систем. Проведений аналіз відомих результатів досліджень свідчить, що існуючим системам управління інформацією і подіями безпеки притаманна низка функціональних обмежень, які перешкоджають досягненню заданого рівня якості управління. Ці обмеження пов'язані з неможливістю оптимальної інтерпретації подій безпеки та забезпечення у повному обсязі адаптивного управління цими інцидентами з урахуванням реальних змін у поведінці загроз. Тому мета статті полягає в тому, щоб запропонувати ефективний підхід до синтезу алгоритмічного і програмного забезпечення систем управління інформацією і подіями безпеки, реалізація якого дозволить розширити їх можливості за рахунок формування в залежності від динаміки загроз автоматичних сценаріїв реагування на інциденти. Для досягнення цієї мети при моделюванні процесів організації управління інформацією і подіями безпеки комп'ютерних систем використані фундаментальні положення теорії логіко-динамічних систем. Ґрунтуючись на цій теорії, запропонована логіко-динамічна модель управління інформацією та подіями безпеки, яка має відмінності від існуючих моделей (наприклад, Petri Nets, Markov Chains, Bayesian Networks). Використання цієї моделі дозволяє формалізувати збір, обробку та аналіз інформації про інциденти, а також розробляти алгоритми їх компенсації. Відмічено, що застосування логіко-динамічних моделей дозволяє врахувати складність та динамічність процесів у комп'ютерних системах, а також неповноту інформації про події безпеки. Представлено алгоритм, який синергетизує відомості про різноманітні інциденти комп'ютерних систем та їх обробку в масивах подій безпеки з метою подальшого реагування на ці деструктивні події. Запропонованому алгоритму притаманна низка переваг, зокрема щодо адаптованості та гнучкості. Практична значущість роботи полягає у можливості впровадження отриманих результатів досліджень для вдосконалення існуючих та розробки перспективних систем захисту комп'ютерних систем, які входять в структуру об'єктів критичної інформаційної інфраструктури. Новизна запропонованого підходу полягає в поєднання традиційних сигнатурних та поведінкових методів ідентифікації загроз із їх логіко-динамічним аналізом. Це дозволяє підвищити точність і оперативність виявлення небезпекових аномалій в комп'ютерних системах.

Ключові слова: управління, інформація, подія, безпека, логіко-динамічна модель, захист, комп'ютерна система, інформаційна інфраструктура.

Постановка проблеми у загальному вигляді. На сучасні комп'ютерні системи (КС), які є основою процесів управління об'єктами критичної інформаційної інфраструктури (КІІ), постійно впливають різноманітні деструктивні загрози і несанкціоновані втручання. Це, як правило, може призвести до серйозних наслідків, включаючи витік конфіденційної інформації, значні фінансові втрати та порушення або повне припинення роботи критично важливих інформаційно-комунікаційних систем та об'єктів держави. Тому забезпечення їх надійного захисту і безпеки функціонування стає надзвичайно актуальним та важливим

завданням. Одним із домінуючих елементів забезпечення безпеки вказаних структур є ефективне і оптимальне управління інформацією та подіями безпеки. Організація цього управління передбачає збір, аналіз та накопичення даних із різних інформаційних джерел, таких, наприклад, як електронний журнал подій безпеки, мережевий трафік та системи виявлення несанкціонованих вторгнень у КС. Ці накопичені в масивах подій безпеки КС дані обробляються в масивах відповідними алгоритмами з метою виявлення можливих загроз та подальшого оперативного реагування на них за рахунок організації функціонування традиційних систем управління інформацією і подіями безпеки. Однак, вказані системи мають ряд функціональних обмежень, а саме:

– значну складність реалізації оптимального процесу аналізу великих обсягів даних, накопчених у масивах подій безпеки. Обмеження пов’язане з тим, що сучасні КС генерують надвеликі обсяги даних. Тому ця ситуація наразі суттєво ускладнює їх аналіз та виявлення можливих прихованих загроз;

– недостатню адаптивність до швидкоплинної та інтенсивної варіації інцидентів. Відомим традиційним система управління інформацією і подіями безпеки притаманні жорстко задані правила кореляції інцидентів, що значно ускладнює їх адаптацію до нових та невідомих загроз, і, особливо, загроз нульового дня;

– відсутність контекстного аналізу. Наявні наразі в експлуатації традиційні система управління інформацією і подіями безпеки не завжди та не в повному обсязі враховують специфічні особливості конкретних подій безпеки. Наслідком цього є помилкові спрацювання та пропуск цими системами реальних загроз безпеці КС;

– недостатній рівень автоматизація процесів управління інформацією і подіями безпеки. Наразі значний обсяг завдань, пов'язаних з аналізом подій безпеки та реагуванням на ці інциденти, виконуються обслуговуючим персоналом КС, як правило, в ручному режимі. Це суттєво збільшує час реагування на інциденти та великий ризик помилок щодо компенсації деструктивних наслідків безпекових атак.

У зв'язку з цим виникає необхідність у розробці та реалізації нових дієвих підходів до організації процесів управління інформацією та подіями безпеки, які б дозволили подолати вказані обмеження та недоліки і суттєво підвищити ефективність виявлення та реагування на інциденти.

Одним із перспективних наукових напрямків, який доцільно використати для моделювання та аналізу подій безпеки КС є теорія логіко-динамічних систем (ЛДС). Проведені авторами теоретичні дослідження дозволяють стверджувати, що ця теорія дозволить формалізувати знання про поведінку КС у разі виникнення інцидентів, і особливо, складних та прихованих безпекових загроз. Використання теорії ЛДС для синтезу систем управління інформацією та подіями безпеки дозволить суттєво підвищити точність та оперативність виявлення можливих загроз. При цьому реалізація контекстного аналізу інцидентів суттєво збільшить гнучкість управління за рахунок використання логіко-динамічних моделей, які можуть бути оптимально адаптовані до нових та невідомих загроз. Вказане, в свою чергу, призведе до автоматизації процесів аналізу подій безпеки та реагування на інциденти. Тому створення та застосування методів управління інформацією та подіями безпеки на основі логіко-динамічних моделей є наразі актуальним та перспективним напрямком фундаментальних та прикладних досліджень у галузі комп’ютерних наук щодо забезпечення захисту КС об’єктів КІІ.

Аналіз останніх досліджень і публікацій. Для розуміння ролі і місця теорії логіко-динамічного моделювання при синтезі адаптивних систем управління інформацією і подіями безпеки розглянемо наукові праці, в яких викладені теоретичні аспекти щодо системних підходів організації управління процесами забезпечення безпеки КС. Засади теорії систем та методологія системних досліджень, які є підґрунтями системного підходу до управління інформаційною безпекою як складним логіко-динамічним процесом, викладені в [1]. Наукова

праця розглядає методи аналізу та прогнозування умов забезпечення стійкості систем, статистичну обробку даних у масивах подій, математичні моделі систем, методи нелінійної динаміки, методи управління процесами функціонування складних систем за умов неможливості прогнозувати їх стани та поведінку.

У роботі [2] особливий акцент зроблено на синтезі автоматизованих та автоматичних інформаційних систем управління кібернетичною безпекою складних об’єктів. Також сформулювані можливі підходи та принципи побудови вказаних систем для організації безпекової стійкості інформаційної інфраструктури.

Основні загрози інформаційній безпеці, що виникають у сучасних КС, розглянуто в науковій праці [3]. Значна увага приділена висвітленню питання оптимізації процесів захисту інформації у комп’ютерних мережах за рахунок функціонування системи управління інформаційною безпекою. Вказано, що основа системи управління інформаційною безпекою ґрунтується на оцінці ризиків і управлінню ними.

У роботі [4] досліджується можливість застосування мультиагентних технологій для суттєвого підвищення ефективності управління інформаційною безпекою КС. Автори акцентують особливу увагу на тому, що інформаційна безпека є комплексною проблемою організації управління, яка вимагає оперативного реагування та інтеграції різних систем для забезпечення захисту інформації від можливих загроз.

Праці [5], [6] та [7] описують методологію створення систем управління інформаційною безпекою. Автори аналізують різні підходи до управління ризиками інформаційної безпеки та пропонують реалізацію цієї методології в комп’ютерній моделі Ця модель допомагає ефективно розробляти та впроваджувати безпекові системи управління. Запропоновано розглядати структури систем управління інформаційною безпекою як сукупність підсистем, комплексів, компонентів, так і специфіку відношень між ними. Такий підхід дозволив представити запропоновану систему управління структурним деревом модульних одиниць.

Діалектичний розвиток започаткованих у наукових публікаціях [5], [6] та [7] підходах щодо створення методології побудови системи управління інформаційною безпекою продовжено в роботах [8] та [9]. Для цього використовувався функціональний аналізу систем управління інформаційною безпекою. Автори досліджують основні підходи до проектування та впровадження цих систем управління, акцентуючи увагу на важливості системного підходу до управління ризиками, а також на важливій ролі технічних, організаційних і кібернетичних заходів у забезпеченні безпеки інформаційних систем.

Методу аналізу логіко-динамічних процесів перетворення аргументів в обчислювальних вузлах цифрових систем управління присвячена наукова публікація [10]. Визначені обмеження і недоліки формальних методів, які використовуються для опису складних процесів обробки даних у цифрових системах управління та запропоновано метод опису процесів перетворення аргументів із використанням графоаналітичних моделей.

Один з можливих підходів щодо практичного застосування системи управління інформаційною безпекою запропоновано в [11]. Автори відмічають, що використання системних підходів до забезпечення безпеки інформації в КС дозволяє виявляти слабкі місця та недоліки в системі та вчасно їх усувати. Це сприятиме забезпеченню ефективності, оптимальності та економічності організаційних заходів інформаційної безпеки.

Фундаментальні аспекти синтезу моделей **управління складними динамічними об'єктами (з урахуванням специфіки подій їх безпеки) наведені в роботі** [12]. Автори всебічно аналізують вплив інтенсивності варіацій динамічних процесів складних об'єктів на їх функціонування. Описані методи гнучкої інтеграції подій безпеки в моделі управління для підвищення надійності та функціональної стійкості системи. Акцентована особлива увага щодо важливості своєчасного реагування на загрози безпеці цих об’єктів. У статті пропонуються практичні рекомендації для розробки ефективних стратегій управління з використанням теорії ЛДС.

Метою статті є розробка теоретичних та практичних засад для створення моделей алгоритмічного забезпечення оптимальних і ефективних систем управління інформацією та подіями безпеки КС, реалізація якого дозволить досягти бажаного рівня оперативності, точності і оптимальності обробки даних у масивах подій безпеки цих обчислювальних систем. Це передбачає системний синтез логічних і динамічних моделей процесів автоматизації виявлення та запобігання загрозам інформаційній безпеці КС.

Виклад основного матеріалу дослідження. Організація процесу управління інформацією і подіями безпеки КС має значну складність і не завжди повну визначеність. Для врахування вказаних особливостей доцільне використання дієвих теоретичних обґрунтувань, які стануть підґрунтям створення оптимального алгоритмічного забезпеченні цих програмованих обчислювальних систем. Отримані результати проведених авторами досліджень, які репрезентовані в наукових працях [12], [13] щодо особливостей і специфіки процесів, пов’язаних із подіями безпеки КС свідчать, що для їх моделювання і формалізації доцільно використовувати теорію ЛДС. Відмітимо, що синтезованим на цій теорії логіко-динамічним моделям притаманні можливості та властивості опису гіперкомплексних процесів в управлінні інформацією і подіями безпеки КС (і особливо тих, які забезпечують надійне функціонування різноманітних об’єктів КІІ.

Розглянемо фундаментальні положення теорії ЛДС, їх аксіоматику, специфіку та можливості щодо реалізації в логіко-динамічних моделях. Аксіоматичне визначення, опис та формалізація цих систем полягає в наступному. ЛДС – це складна, велика, організаційна, гіперкомплексна структура. У формалізованих моделях ЛДС складові компоненти, що описують логіку процесів (варіації станів системи) та складові компоненти, що характеризують динаміку зміни параметрів цих систем (швидкоплинну варіацію її стану в реальному часі) синергетично пов’язані. При цьому в ЛДС можуть бути взаємопов’язані як правила логіки так і варіації цих правил або динамічних станів системи, які функціонально залежать від низки зовнішніх та внутрішніх факторів [14].

Акцентуємо увагу, що головна особливість ЛДС полягає в тому, що зміни відбуваються за чітко встановленими логічними правилами. Але в багатьох ситуаціях ці правила динамічно можуть бути змінені низкою впливів, наприклад, таких як зворотній зв'язок у системі або адаптація до зовнішніх збурень. З цього витікає, що ця динамічна система відноситься до класу управляємих систем (процеси в яких змінюються в часі у відповідності до чітко встановлених правил або логіки), яким притаманна адаптивна зміна її внутрішньої структури. Модель можливих станів таких систем пропонується описувати з використанням класичної теорії управління, врахувавши, що переходи між змінами цих станів відбуваються за чіткими логічними [1]. Тому моделі станів ЛДС – це математичні моделі, які використовуються для опису та аналізу поведінки складних систем, що змінюють свій стан у часових координатах. При цьому ЛДС поєднують логічні вирази з динамічними рівняннями. Такий підхід дозволяє моделювати як дискретні, так і неперервні зміни в системі. Крім того, він дозволяє врахувати специфіку процесів при організації управління інформацією та подіями безпеки КС. Тому теорію ЛДС пропонується застосувати для аналізу складових етапів забезпечення безпеки КС та моделювання процесів такого забезпечення.

До вказаних етапів відносяться:

– виявлення вторгнень. ЛДС доцільно використовувати для синтезу субсистем виявлення можливих вторгнень. Ці субсистеми виявлятимуть аномальні стани в усій КС КІІ або на її окремих компонентах;

– аналіз ризиків. На цьому підетапі ЛДС пропонується використовувати для оцінки ризиків безпеки КС на основі аналізу різних факторів (кількість вразливостей, частота атак та потенційні збитки тощо) для формування в подальшому стратегій їх мінімізації або компенсації деструктивних наслідків небезпечних інцидентів в КС КІІ;

– управління інцидентами. Реалізація процесів управління, які ґрунтуються на алгоритмах, синтезованих із застосуванням логіко-динамічних моделей, дозволить повністю автоматизувати процес надійного, оперативного і оптимального реагування на події безпеки КС, наприклад, блокування шкідливого трафіку або повну «ізоляцію» заражених комп'ютерів у КС КІІ;

– прогнозування можливих загроз. Використання технологій із застосуванням логіко-динамічних моделей забезпечать прогнозування можливих загроз безпеці на основі аналізу накопичених апостеріорі даних про їх специфічні особливості.

Можливий підхід щодо застосування логіко-динамічних моделей пропонується реалізувати в алгоритмі, наведеному в таблиці 1.

Таблиця 1 – Структура алгоритму управління інформацією і подіями безпеки КС КІІ

Складові алгоритму		Функції, які ґрунтуються на логіко-динамічних моделях
Адаптивне управління подією безпеки	Виявлення загроз безпеці	- моделювання динамічного характеру інцидентів - виявлення в режимі реального часу аномалії в КС КІІ
	Реагування на події безпеки	- оперативне формування управляючих впливів - -автоматичне блокування шкідливого трафіку передачі інформації в КС КІІ
Оцінка ризиків та мінімізація їх деструктивних впливів	Аналіз ступеня вразливостей	- моделювання сценаріїв атак та процесів виявлення вразливостей - формування пріоритетів в управлінні КС
	Динамічне управління ризиками безпеки	- оперативне коригування процесів управління заходами безпеки - автоматичне підвищення рівня моніторингу безпеки КС КІІ
Забезпечення дотримання вимог політик безпеки	Формалізація моделей політик безпеки	- моделювання політик безпеки КС - формування логічних правил, які інтерпретують політики безпеки - коригування у відповідності до заданих вимоги безпеки правил захисту інформаційних масивів
	Підтримка політик безпеки	- перевірка конфігурації системи на відповідність визначеним політикам безпеки - виявлення нештатних відхилень у конфігурації системи від еталонних політик безпеки
Виявлення подій безпеки для оперативного запобігання вторгненню	Виявлення аномалій	- оперативне виявлення несанкціонованих вторгнень - синергетизація логічних правил заданої поведінки системи - виявлення та інтерпретація невідомих аномалій
	Реагування на вторгнення	- автоматичне реагування на несанкціоноване вторгнення - автоматичне блокування шкідливих трафіків передачі інформації - блокування підозрілих процесів в обробки інформації

Аналіз цих етапів свідчить, що реалізація формалізованих логіко-динамічних моделей забезпечить управління інформацією і подіями безпеки КС КІІ. При цьому використання таких моделей дозволить реалізувати низку суттєвих переваг перед відомими традиційними методами управління інформацією та подіями безпеки КС, а саме:

– гнучкість;

– точність;

– автоматизацію процесів управління та прогнозування станів обчислювальної системи.

Результати проведених теоретичних досліджень свідчать, що ускладнення законів управління функціонуванням КС КІІ може призвести до того, що отриманими моделями буде проблематично описувати об'єкт синтезу як єдине (неподільне) ціле. Як наслідок, складно виконати операцію кількісного порівняння альтернатив або інтерпретувати чисельними показниками процесу моделювання об’єкту – КС КІІ. Сам процес синтезу з використанням моделей системного, структурно-логічного та програмно-технічного підходів проблематично поєднуватися функціонально. Виникає необхідність комплексної реалізації єдиної структурної процедури, оскільки результати синтезу законів управління потребують гнучкої адаптації [15], [16]. Критерії якості управління, основними з яких є час та швидкість відпрацювання управляючих впливів, мінімум затрат часу на реалізацію управління представимо елементами моделей у множинах векторних просторів. Відмітимо, що особливість цих просторів полягає у тому, що вони майже повністю «розмикаються» як єдина система оцінок у категоріях моделей структурно-логічного і програмно-технічного підходів. Це свідчить, що критерії якості управління конструктивні в межах моделей і є інваріантними по відношенню до критеріїв ефективності функціонування синтезуємої системи управління інформацією і подіями безпеки [16], [17].

Для створення методики організації управління інформацією і подіями безпеки в КС (структура якого наведена в табл. 1) за рахунок конкретизації та необхідних довизначень адаптуємо класичну теорію ЛДС та представимо відповідну математичну модель КС КІІ для подальшої реалізації управління безпековими процесами з метою суттєвого пом’якшення або компенсації наслідків комп'ютерних інцидентів [15]–[17].

При описі процесів управління інформацією і подіями безпеки в математичній моделі використаємо формалізаційний описів її складових компонентів:

$$S = \left(X, Y, Z, f, g', L, h \right). \quad (1)$$

Враховуючи аксіоматику ЛДС [25], розглянемо компоненти моделі (1) більш детально.

1) $X = \left\{ x_1, x_2, \ldots, x_n \right\}$ – множина, яка описує поточні стани КС. Ці стани формалізуємо за такими показниками:

– обсяги ресурсів КС (процесора, оперативної пам'яті, обсягів накопичення даних в масивах події безпеки);

– кількість шаблонів мережевого трафіку, які використовуються для забезпечення інформаційної безпеки в каналах передачі інформації (на фізичному рівні);

– кількість задіяних алгоритмів для безпечної обробки інформації;

– показники стану захисного програмного забезпечення (брандмауери, антивіруси тощо);

– показник статусу вразливості КС КІІ.

2) $Y = \left\{ y_1, y_2, \ldots, y_m \right\}$ – множина, яка ідентифікує події безпеки в КС, а саме:

– спроби несанкціонованого вторгнення;

– наявність шкідливого програмного забезпечення;

– атаки типу «відмова в обслуговуванні»;

– витік конфіденційних даних;

– системні помилки обробки інформації тощо.

3) $Z = \left\{ z_1, z_2, \ldots, \mathrm{z}_k \right\}$ – множина, яка описує дії щодо реалізації управління подіями безпекою:

– блокування IP-адрес;
– реалізація карантинних досьє;
– екстрене завершення процесів небезпечної обробки інформації;
– компенсація наслідків вразливостей;
– оперативне оповіщення персоналу служби безпеки КС.

4) $f: X \times Y \to X$ – функція, яка формально описує зміни станів системи. Ця функція характеризує зміни в реальному часі стану системи в залежності від наслідків деструктивних впливів подій безпеки. Із врахуванням метрики поточного стану системи $x \in X$ і подій безпеки $y \in Y$ опис формалізуємо функцією $f(x, y) = x' \in X$, де x' – новий стан системи, який характеризує варіації її динаміки в залежності від деструктивних наслідків інцидентів.

5) $g: X \times Y \to Z$ – функція вибору дій з управління безпекою на основі поточного стану системи та події безпеки КС. Визначає, які дії необхідно оперативно вжити у відповідь на подію безпеки для забезпечення функціональної стійкості КС. Задано поточний стан $x \in X$ і безпекову подію $y \in Y$. Функція $g(x, y) = z \in Z$ ідентифікує політику безпеки та описує процес прийняття рішень щодо пом'якшення деструктивних наслідків інцидентів або їх повної компенсації.

6) $L = \{l_1, l_2, \ldots, l_p\}$ – множина логічних умов забезпечення безпекового стану системи. Ці умови можна використовувати для уточнення підходів вибору дії, наприклад:

– завантаження процесора понад 80%;
– брандмауер вимкнено;
– кількість невдалих спроб входу в систему перевищує три спроби.

7) $h: X \to \{True, False_p\}$ – функція, яка описує стани КС набором логічних умов (істинних або хибних), $h(x) = (h_1(x), h_2(x), \ldots, h_p(x))$, де $h_i(x)$ – значення істинності логічної умови l_i при всіх можливих станах x.

8) $g': X \times Y \times \{True, False\}_p \to Z$ – розширена функція вибору дії, яка враховує не тільки стан системи і подію, але і значення істинності $h(x)$ логічних умов $g'(x, y, h(x)) = z \in Z$, що дозволяє реалізувати більш складні та контекстно-залежні реакції на забезпечення безпеки в КС КІІ.

Розроблену динаміку компенсації інцидентів представимо у вигляді формалізованої моделі, яка реалізує поетапні кроки цієї компенсації та відобразимо у її вигляді алгоритму:

Крок 1: [Початковий стан] – система знаходиться (запускається) у початковому стані $x_0 \in X$.

Крок 2: [Виникнення події – поява інциденту безпеки] – відбувається подія безпеки $y_i \in Y$.

Крок 3: [Зміна (перехід) станів] – система під впливом події безпеки y_i переходить у новий стан $x_i' = f(x_i, y_i)$.

Крок 4: [Оцінка умови] – логічні умови L описуються кортежом $h(x') = \langle b_1, b_2, \ldots, b_p \rangle$, де $b_i \in \{True, False\}$.

Крок 5: [Формування управлінських впливів] – на основі нового стану x_i' та події безпеки y_i формується управління інформацією та подіями безпеки $z_i = g\left(x_i', y_i, h\left(x'\right)\right)$.

Крок 6: [Реалізація управлінських дій] – дія z_i відпрацьовується системою та впливає на швидкоплинну зміну її стану.

Крок 7: [Повторення] – при появі нових подій безпеки) процес із кроку 2 по крок 6 циклічно повторюється.

Розглянемо приклад щодо реалізації моделі (1) із врахуванням структури запропонованого покрокового алгоритму. У цьому прикладі, якщо система знаходиться в безпечному стані та відбувається спроба входу в систему, то вона залишається в безпечному стані, а дія з управління інформацією і подіями безпеки полягає в блокуванні доступу. У разі, якщо виявлено подію безпеки, система переходить у вразливий стан, а дія з управління процесами забезпечення безпеки КС КІІ передбачає компенсацію деструктивних наслідків інцидентів.

Формалізація вказаного підходу представлена у вигляді зміни станів КС:

$X = \{safe,\ vulnerable\}$ – стани системи.

$Y = \{login\ attempt,\ incident\ detected\}$ – події безпеки.

$Z = \{block\ access,\ compensate\ for\ the\ consequences\ of\ theincident\}$ – формування управління процесами забезпечення інформаційної безпеки.

Функцію переходу станів f визначена наступним чином:

$f\{secure,\ login\ attempt\}$ = безпечний.

$f\{safe,\ safety\ event\ detected\}$ = вразливий.

$f\{vulnerable,\ login\ attempt\}$ = вразливий.

$f\{vulnerable,\ virus\ detected\}$ = вразливий.

При цьому функцію вибору дій g представимо таким чином:

$g\{safe,\ login\ attempt\}$ = заблокувати доступ.

$g\{safe,\ incident\ detected\}$ = компенсувати наслідки інциденту.

$g\{vulnerable,\ login\ attempt\}$ = заблокувати доступ.

$g\{vulnerable,\ safety\ event\ detected\}$ = компенсувати наслідки інциденту.

Із врахуванням результатів цієї формалізації процес виявлення інцидентів представимо у спрощеному вигляді:

$X = Normal,\ High,\ Attacked$.

$Y = LoginFailure,\ MalwareDetected$.

$Z = BlockIP,\ QuarantineFile,\ LogAlert$.

$L = FaildLoginAttempts > 3$.

Переходи і дії, які описують виявлення інцидентів у КС:

$f\left(Normal,\ LoginFailure\right) = HighCPU(in\ case\ of\ \ many\ failed\ \ logins)$.

$g'\left(HighCPU,\ LoginFailure,\ True\right) = BlockIP\left(if\ \ "FailedLoginAttempts > 3"\ \ True\ \right)$.

$f\left(Normal,\ Malware\ detected\right) = Attacked$.

$g'\left(Attacked,\ MalwareDetected\right) = QuarantineFile\ \left(regardless\ of\ \ other\ conditions\right)$.

Отриманий алгоритм доцільно використати при синтезі структури, алгоритмічного і програмного забезпечення цифрових двійників інформаційно-комунікаційних мереж та обчислювальних систем.

Висновки. Таким чином, у статті розглянуто один з можливих підходів щодо застосування логіко-динамічних моделей для управління інформацією та подіями безпеки КС КІІ. Було продемонстровано, що формалізація управління процесами безпеки за допомогою фундаментальних положень теорії ЛДС дозволяє підвищити ефективність виявлення загроз та оперативно реагування на них.

Показано, що використання теорії ЛДС дозволяє враховувати динаміку розвитку загроз і адаптувати системи безпеки КС до варіації умов інтенсивного впливу подій безпеки на процеси функціонування обчислювальних засобів.

Наукова цінність проведених досліджень полягає в тому, що запропонований підхід доцільно використати для розробки математичних моделей, алгоритмічного і програмного забезпечення інтелектуальних систем управління подіями безпеки, здатних до гнучкої адаптації при інтенсивних варіаціях інцидентів. Отримані результати теоретичних досліджень у разі їх реалізації в алгоритмічному і програмному забезпеченні КС сприятимуть підвищенню рівня захищеності КІІ.

Започатковані дослідження - перспективні. У подальшому вони можуть бути спрямовані на синтез складніших логіко-динамічних моделей систем управління інформацією і подіями безпеки при створенні їх цифрових двійників. Практичне значення роботи полягає в можливості адаптації запропонованих рішень до конкретних об’єктів критичної інфраструктури, що дозволить суттєво підвищити рівень захищеності КІІ, скоротити час реагування на інциденти та забезпечити задану функціональну стійкість цих об’єктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] П.М. Грицюк, О.І. Джоші, та О.М. Гладка, *Основи теорії системи і управління: підручник.* Рівне, Україна: НУВГП, 2021.

[2] В.І. Ящук, “Проектування автоматизованих інформаційних систем управління кібернетичною безпекою об’єктів критичної інфраструктури України”, на *Наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави,* Київ, 2021, с. 233-235.

[3] А.М. Гребенюк, та Л.В. Рибальченко, *Основи управління інформаційною безпекою: навчальний посібник.* Дніпро, Україна: ДДУВС, 2020.

[4] І.П. Хавіна, Ю.В. Гнусов, та О.О. Можаєв, “Розробка мультиагентної системи управління інформаційною безпекою”, *Право і безпека*, № 4 (87), с. 171-183, 2022, doi: https://doi. org/10.32631/pb.2022.4.14.

[5] В.В. Мохор, та В.В. Цуркан, “Комп’ютерна модель розробки систем управління інформаційною безпекою”, *Information Technology and Security,* вип. 9 (1), с.80-90, 2021, doi: https://doi.org/10.20535/2411-1031.2021.9.1.249814.

[6] В.В. Цуркан, “Метод синтезу структури системи управління інформаційною безпекою”, *Укр. наук. жур. інформаційної безпеки,* том 26, вип. 2, с. 116-122, 2020, doi: https://doi.org/10.18372/2225-5036.26.14926.

[7] В.В. Цуркан, та О.М. Шаповал, “Аналіз методів оцінки ризиків безпеки комп'ютерної мережі”, *Information Technology and Security*, вип. 10 (2), с.204–215, 2022, doi: https://doi.org/10.20535/2411-1031.2022.10.2.270437.

[8] В.В. Мохор, та В.В. Цуркан, “Методологія побудови систем управління інформаційною безпекою”, *Захист інформації*, том 23, №4, с. 200-212, 2021, doi: https://doi.org/10.18372/2410-7840.23.16766.

[9] В.В. Цуркан, “Метод функціонального аналізування систем управління інформаційною безпекою”, *Ел. фах. наук. вид.* “*Кібербезпека: освіта, наука, техніка*”, № 4 (8), с. 192-201, 2020, doi: https://doi.org/10.28925/2663-4023.2020.8.192201.

[10] О.О. Ушкаренко, “Метод аналізу процесів перетворення даних в обчислювальних вузлах цифрових систем управління”, *Вчені записки Таврійського національного університету імені В.І. Вернадського, серія: Технічні науки,* том 32 (71), № 4, с. 162-168, 2021, doi: https://doi.org/10.32838/2663-5941/2021.4/25.

[11] О.І. Скіцько, Р.О. Ширшов, “Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об’єктів критичної інфраструктури”, *Inter. Scien. Journ. of Engin. & Agricul.,* том 2, №6, 2023, с. 12-22, doi: https://doi.org/10.46299/j.isjea.20230206.02.

[12] I.I. Samborskyi, Ie.I. Samborskyi, V.D. Hol, Y.V. Peleshok, and S.M. Sholokhov, “Synthesis of the model of management of complex dynamic objects taking into account the events of their security”, *Information Technology and Security,* vol. 1 iss. 22, pp. 4-16, 2024, doi: https://doi.org/10.20535/2411-1031.2024.12.1.

[13] 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, 2024, doi: https://doi.org/10.15588/1607-3274-2023-4-2.

[14] О.М. Кричевець, “Застосування елементів теорії кінцевих автоматів для досліджень динамічних властивостей обчислювальних компонентів вимірювальних систем”, *Вимірювальна техніка та метрологія*, № 77, 2016, с.121-126.

[15] Д.І. Рабчун, “Логіко-динамічна модель процесу управління ресурсами захисту в умовах інформаційного протистояння”, *Сучасний захист інформації*, № 3, 2016, с.62-67. [Електронний ресурс]. Доступно: https://journals.dut.edu.ua/index.php/dataprotect/article/view/707/654. Дата звернення: Січ. 19, 2025.

[16] К.Д. Жук, “Питання аксіоматичного підходу до побудови теорії логіко-динамічних систем керування”, *Автоматика*, № 3-6, 1971, с. 62-74.

[17] М.В. Грайворонський, та О.М. Новіков, *Безпека інформаційно-комунікаційних систем: підручник*. Київ, Україна: Видавнича група BHV, 2009.

Стаття надійшла до редакції 31.03.2025.

REFERENCES

[1] P.M. Hrytsyuk, O.I. Joshi, and O.M. Gladka, *Fundamentals of System and Management Theory: Textbook.* Rivne, Ukraine: NUWMNR Publ., 2021.

[2] V.I. Yashchuk, “Design of Automated Information Systems for Managing Cybernetic Security of Critical Infrastructure Facilities of Ukraine”, in *Proc. Scien. and Prac. Conf. Actual Problems of Information Security Management of the State*, Kyiv, 2021, pp. 233-235.

[3] A.M. Grebenyuk, and L.V. Rybalchenko, *Fundamentals of Information Security Management: Textbook.* Dnipro, Ukraine: DSUIA Publ., 2020.

[4] I.P. Khavina, Y.V. Gnusov, and O.O. Mozhaev, “Development of a Multi-Agent Information Security Management System”, *Law and Security*, no. 4 (87), pp. 171-183, 2022, doi: https://doi. org/10.32631/pb.2022.4.14.

[5] V.V. Mohor, and V.V. Tsurkan, “Computer Model for the Development of Information Security Management Systems”, *Information Technologies and Security*, vol. 9 (1), pp. 80-90, 2021, doi: https://doi.org/10.20535/2411-1031.2021.9.1.249814.

[6] V.V. Tsurkan, “Method of Synthesis of the Structure of the Information Security Management System”, *Ukrainian Scientific Journal of Information Security*, vol. 26, iss. 2, pp. 116-122, 2020, doi: https://doi.org/10.18372/2225-5036.26.14926.

[7] V.V. Tsurkan, and O.M. Shapoval, “Analysis of Methods for Assessing Computer Network Security Risks”, *Information Technologies and Security*, vol. 10 (2), pp. 204-215, 2022, doi: https://doi.org/10.20535/2411-1031.2022.10.2.270437.

[8] V.V. Mokhor, and V.V. Tsurkan, “Methodology for Building Information Security Management Systems”, *Information Protection*, vol. 23, no. 4, pp. 200-212, 2021, doi: https://doi.org/10.18372/2410-7840.23.16766.

[9] V. V. Tsurkan, “Method of Functional Analysis of Information Security Management Systems”, *El. Prof. Scien. Ed. Cybersecurity: Education, Science, Technology*, no. 4 (8), pp. 192-201, 2020, doi: https://doi.org/10.28925/2663-4023.2020.8.192201.

[10] O.O. Ushkarenko, “Method of Analysis of Data Conversion Processes in Computing Nodes of Digital Control Systems”, *Scien. Notes of V.I. Vernadsky Taurida National University, series: Technical Sciences*, vol. 32 (71), no. 4, pp. 162-168, 2021, doi: https://doi.org/10.32838/2663-5941/2021.4/25.

[11] O.I. Skitsko, and R.O. Shirshov, “Information security management system as a tool for enhancing the protection and efficiency of critical infrastructure objects”, *Inter. Scien. Journ. of Engin. & Agricul.*, vol. 2, no. 6, 2023, pp. 12-22, doi: https://doi.org/10.46299/ j.isjea.20230206.02.

[12] I.I. Samborskyi, Ie.I. Samborskyi, V.D. Hol, Y.V. Peleshok, and S.M. Sholokhov, “Synthesis of the model of management of complex dynamic objects taking into account the events of their security”, *Information Technology and Security*, vol. 1 iss. 22, pp. 4-16, 2024, doi: https://doi.org/10.20535/2411-1031.2024.12.1.

[13] 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, 2024, doi: https://doi.org/10.15588/1607-3274-2023-4-2.

[14] O.M. Krychevets, “Application of elements of the theory of finite state machines for the study of dynamic properties of computational components of measuring systems”, *Measuring Engineering and Metrology*, no. 77, 2016, pp. 121-126.

[15] D.I. Rabchun, “Logical-dynamic model of the process of managing protection resources in the conditions of information confrontation”, *Modern Information Protection*, no. 3, 2016, pp. 62-67. [Online]. Available: https://journals.dut.edu.ua/index.php/dataprotect/article/ view/707/654. Accessed on: Jan. 19, 2025.

[16] K.D. Zhuk, “The Question of the Axiomatic Approach to the Construction of the Theory of Logical-Dynamic Control Systems”, *Automation*, no. 3-6, 1971, pp. 62-74.

[17] M.V. Grayvoronsky, and O.M. Novikov, *Security of Information and Communication Systems: Textbook*. Kyiv, Ukraine: BHV Publishing Group, 2009.

PETRO PAVLENKO,
IYEVGEN SAMBORSKYI

MANAGEMENT OF INFORMATION AND SECURITY EVENTS OF COMPUTER SYSTEMS USING LOGICAL-DYNAMIC MODELS

The article discusses one of the possible approaches to the organization of information management and security events of computer systems. The analysis of the known research results shows that the existing information and security event management systems are characterized by a number of functional limitations that prevent the achievement of a given level of management quality. These limitations are associated with the impossibility of optimal interpretation of security events and ensuring the full adaptive management of these incidents, taking into account real changes in the behavior of threats. Therefore, the purpose of the article is to offer an effective approach to the synthesis of algorithmic and software for information and security event management systems, the implementation of which will expand their capabilities by forming, depending on the dynamics of threats, automatic scenarios for responding to incidents. To achieve this goal, the fundamental provisions of the theory of logical-dynamic systems are used in modeling the processes of organization of information management and security events of computer systems. Based on this theory, a logical-dynamic model of information and security event management has been proposed, which has differences from existing models (for example, Petri Nets, Markov Chains, Bayesian Networks). The use of this model makes it possible to formalize the collection, processing and analysis of information about incidents, as well as to develop algorithms for their compensation. It is noted that the use of logical-dynamic models allows taking into account the complexity and dynamism of processes in computer systems, as well as the incompleteness of information about security events. An algorithm is presented that synergizes information about various incidents of computer systems and their processing in arrays of security events in order to further respond to these destructive events. The proposed algorithm has a number of advantages, including adaptability and flexibility. The practical significance of the work lies in the possibility of implementing the obtained research results to improve the existing and develop promising systems for protecting computer systems, which are part of the structure of critical information infrastructure facilities.

The novelty of the proposed approach lies in the combination of traditional signature and behavioral methods of threat identification with their logical-dynamic analysis. This allows you to increase the accuracy and efficiency of detecting dangerous anomalies in computer systems.

Keywords: management, information, event, security, logical-dynamic model, protection, computer system, information infrastructure.

Павленко Петро Миколайович, доктор технічних наук, професор, професор кафедри організації авіаційних перевезень Національного університету “Київський авіаційний інститут”, Київ, Україна. ORCID 0000-0002-2581-230X, petrpav@ukr.net.

Самборський Євген Іванович, аспірант кафедри організації авіаційних перевезень Національного університету “Київський авіаційний інститут”, Київ, Україна. ORCID 0000-0003-4441-1947, seinauedu@gmail.com.

Pavlenko Petro, Doctor of Technical Sciences, Professor, Professor of the Department of Air Transportation Organization, National University “Kyiv Aviation Institute”, Kyiv, Ukraine.

Samborskyi Ievgen, Postgraduate student, Department of Air Transportation Organization, National University “Kyiv Aviation Institute”, Kyiv, Ukraine.