УДК: 004.01/.08+004.942 DOI: **10.33099/2311-7249/2025-52-1-77-84**

ГОРГУЛЕНКО Владислав Андрійович,
Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна,
https://orcid.org/0000-0001-6382-5075

МАТЕМАТИЧНА МОДЕЛЬ ВИЗНАЧЕННЯ ЙМОВІРНІСНИХ СТАНІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ В УМОВАХ ВЕДЕННЯ КІБЕРБОРОТЬБИ

У статті викладено основні положення математичної моделі визначення ймовірнісних станів інформаційно-комунікаційної системи в умовах ведення відносно до неї кіберборотьби.

***Метою статті** є розроблення математичної моделі визначення ймовірнісних станів інформаційно-комунікаційної системи в умовах ведення кіберборотьби як випадкового дифузійного марковського процесу. На відміну від існуючих, розроблена автором математична модель враховує ймовірнісний характер факторів, які впливають на перебіг та результати кіберборотьби, розглядає її як дифузійний випадковий марковський процес з дискретними станами та неперервним часом.*

***Методи дослідження.** Під час дослідження використано метод системного аналізу для визначення множини можливих станів інформаційно-комунікаційної системи, а також математичний апарат теорії стохастичних диференціальних рівнянь для аналітичного моделювання її функціонування. За допомогою методу системного аналізу було формалізовано процес кіберборотьби, проаналізовано трирівневу архітектуру кіберпростору (кібердомену) як середовища її ведення та сформовано множину можливих станів функціонування інформаційно-комунікаційної системи, що складається з шести станів. Математичний апарат теорії стохастичних диференціальних рівнянь дав змогу сформувати систему диференціальних рівнянь Колмогорова у стохастичній постановці для визначення ймовірностей станів інформаційно-комунікаційної системи.*

***Отримані результати дослідження.** У результаті дослідження було формалізовано процес ведення кіберборотьби у якості дифузійного марковського процесу з дискретними станами та неперервним часом, узагальнено за структурною ознакою основні об'єкти ведення кіберборотьби як інформаційно-комунікаційні системи, запропоновано граф станів функціонування такої системи та розроблено математичну модель визначення її ймовірнісних станів в умовах ведення кіберборотьби на основі математичного апарату теорії стохастичних диференціальних рівнянь.*

***Елементи наукової новизини.** Науковою новизною отриманих результатів дослідження є запропонований у статті концептуально інший підхід до оцінювання ефективності ведення кіберборотьби, який зводиться до її математичного моделювання як випадкового (стохастичного) процесу та отримання, завдяки цьому, саме ймовірнісних показників, за якими в подальшому буде можливо аналізувати величину прогнозованого ефекту від кібердій та використовувати в якості критеріїв прийняття рішення на їх проведення.*

***Теоретична й практична значущість.** Теоретичною значущістю отриманого наукового результату є прикладне використання потужного математичного апарату теорії стохастичних диференціальних рівнянь для аналітичного математичного моделювання дій у кіберпросторі, яким за означенням притаманна невизначеність та випадковість. Практичною значущістю результатів дослідження є можливість програмної реалізації запропонованої у статті математичної моделі визначення ймовірнісних станів інформаційно-комунікаційної системи для прогнозування перебігу та результатів ведення кіберборотьби в інтересах застосування угруповань військ (сил) оперативно-стратегічного рівня.*

***Ключові слова:** дифузійні випадкові процеси, кібербезпека, кіберборотьба, кіберпростір, кібероборона, математична модель, марковський ланцюг, стохастичні диференціальні рівняння.*

Вступ

Постановка проблеми. Сьогодні сутність поняття кіберборотьби розглядається як процес ведення визначеним комплектом сил і засобів взаємоузгоджених воєнних дій у середовищі кібердомену (сегменті кіберпростору) [1]. Наразі в науці відсутня обґрунтована система показників та критеріїв оцінювання ефективності ведення кіберборотьби, а дослідження у цьому напрямі висвітлюють лише часткові показники продуктивності (результативності) окремих її складових – кіберзахисту, кіберрозвідки та кібервпливу. Такі показники, як правило, базуються на обсязі перехоплених, модифікованих чи знищених даних (інформації) та їх важливості, яка, в свою чергу, може бути оціненою лише експертним шляхом, що апріорі породжує суб'єктивізм.

Математичне моделювання кіберборотьби, як досить новітнього та інноваційного напряму діяльності Збройних Сил України (далі – ЗС України), є

беззаперечно важливим та таким, що дасть змогу всебічно досліджувати питання стосовно оцінювання ефективності її ведення, якому наразі не надається достатньої уваги.

Практика аналізу та синтезу складних технічних систем військового призначення свідчить про, здебільшого, ймовірнісний характер процесів, які протікають в них. Ймовірнісними процесами є такі, перебіг та результати яких залежать від низки випадкових факторів (умов і чинників), що призводять до зміни стану (параметрів) системи в часі у випадковому, заздалегідь непередбачуваному порядку. Тобто, ймовірнісний процес може бути описаним сімейством випадкових величин за параметром часу t та є випадковою функцією часу, значення якої в кожній точці $t + \Delta t$ дорівнюють випадковій величині $X(t + \Delta t)$.

Не виключенням, а швидше й одним найвиразніших подібних процесів, є процес кіберборотьби. Відповідно, для оцінювання ефективності ведення кіберборотьби необхідною є побудова саме ймовірнісної математичної моделі, яка дасть змогу враховувати вплив згаданих випадкових факторів, що притаманні досліджуваному процесу.

Аналіз останніх досліджень і публікацій. В [2] розглянуто питання оцінювання поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі, запропоновано узагальнений індекс напруженості ситуації у кіберпросторі, індекс змін кількості виявлених кіберінцидентів, композитний показник кіберстійкості та низку інших показників здатності систем до протидії виникненню кіберінцидентів. Робота [3] висвітлює обґрунтування таких кількісних показників ефективності окремих заходів за кіберборотьби, як кількість перехоплених (знищених) даних у результаті кібератаки, відсоткове відношення кількості виявлених вразливостей ІКС, у добутку з їх важливістю, до усіх можливих, на виявлення яких сканувалася мережа. Однак, ймовірнісність процесу кіберборотьби ці праці не враховують.

Дослідження [4–7] підтверджують доцільність побудови детермінованих графо-аналітичних математичних моделей на основі систем диференціальних рівнянь для опису воєнних дій у кіберпросторі. Проте проблема врахування випадковості притаманної процесу кіберборотьби в актуальних роботах за даним напрямом не піднімалася.

Водночас, розкриттю особливостей чисельного вирішення диференційних рівнянь моделей ланчестерського типу у стохастичній постановці присвячено статтю [8]. У цій праці наглядно доведено адекватність та дієвість використання теорії стохастичних диференціальних рівнянь для пошуку аналітичних розв'язків ймовірнісних процесів.

Теорія стохастичних диференціальних рівнянь набула широкого прикладного застосування у таких сферах як біологія, фізика, теорія оптимального керування системами з розподіленими параметрами, фінансова математика та ін. Втім, у військовій сфері – царині, перебіг та результати процесів якої є ймовірнісними за означенням, теорія стохастичних диференціальних рівнянь для дослідження цих процесів практично не використовується. Більше того, реалії сьогодення свідчать про активне ведення кіберборотьби на усіх етапах сучасного збройного конфлікту. Аналіз досвіду кіберборотьби [9] свідчить про те, що деякі параметри марковського процесу, яким вона може бути описана носять виражений характер малих флуктуацій (підлягають впливу шумів), а сам процес є дифузійним у розумінні положень теорії випадкових процесів.

Мета статті. Розробити математичну модель визначення ймовірнісних станів інформаційно-комунікаційної системи в умовах ведення кіберборотьби як випадкового дифузійного марковського процесу.

Виклад основного матеріалу дослідження

Кіберпростір є середовищем, утвореним сукупністю систем електронних комунікацій усього спектру об'єктів суспільної діяльності (фінансових, урядових, інформаційних, медіа, енергетичних, та зокрема військових тощо) у результаті їхнього сумісного функціонування та передачі (обміну) даними за допомогою мережі Інтернет та/або інших глобальних мереж. Незважаючи на те, що наразі офіційне визначення поняття «кібердомен» відсутнє, провідні держави світу активно просувають у своїх збройних силах концепцію мультидоменних операцій, згідно з якою останній є одним із шести основних доменів бойового простору. Фізично кібердомен є сегментом кіберпростору, середовищем ведення воєнних дій у ньому, які, у свою чергу, прийнято називати кіберборотьбою.

Об'єктами кіберборотьби є військові системи електронних комунікацій різного цільового призначення, серед яких: автоматизовані системи управління військами та зброєю, системи ситуаційної обізнаності, системи службового електронного документообігу та ін. Здебільшого, названі та інші типові об'єкти, які функціонують у кібердомені мають схожий принцип дії та архітектуру побудови, що дає змогу узагальнити їх як інформаційно-комунікаційні системи (далі – ІКС). Як правило, на кожному пункті управління незалежно від ланки (рівня) та в кожному інформаційно-комунікаційному вузлі окремої військової частини розгорнуто принаймні одну ІКС, стала робота якої забезпечує оперативний склад пункту управління, командування і штаб військової частини зв'язком й доступом до інформаційних сервісів.

Зважаючи на те, що ІКС функціонує у кіберпросторі, та з урахуванням його «природи» (рис. 1), будемо розглядати ІКС як складну систему, підсистемами (рівнями) якої є [10]:

1. Фізичний рівень: програмно-апаратні вузли ІКС (сервери, автоматизовані робочі місця, маршрутизатори, програмовані комутатори та їх програмне забезпечення).

2. Логічний рівень: комунікації (мережевий трафік) та дані, що циркулюють в ІКС.

3. Рівень кіберперсони: облікові дані та облікові записи допущених до роботи в ІКС користувачів, з відповідними правами доступу.

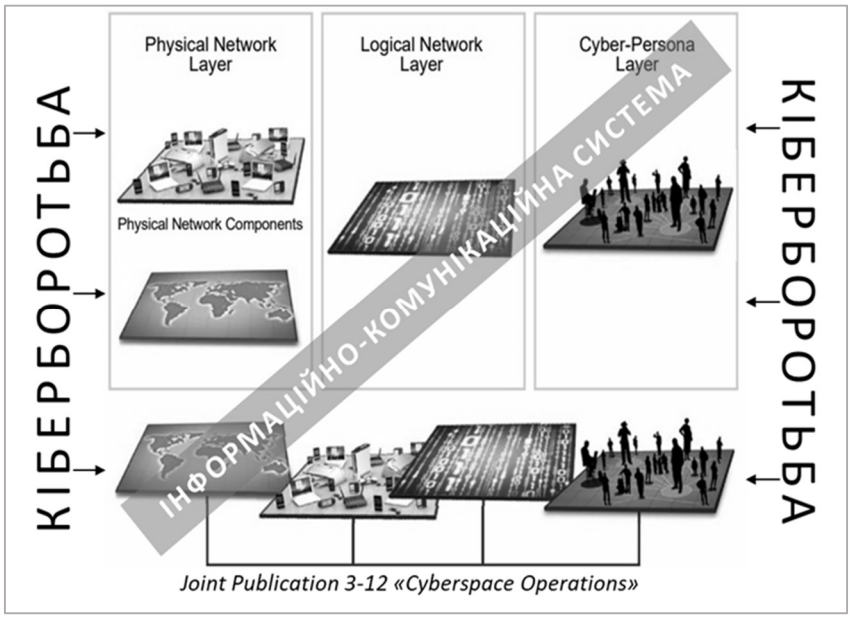

Рисунок 1 – Рівні кіберпростору [10]

Наразі, у сфері кібербезпеки та, зокрема, кіберборотьби виокремлено три основні її складові: кіберзахист, кіберрозвідка та кібервплив [1; 4; 6]. ІКС військового призначення, а особливо ті, у яких здійснюється обмін інформацією з обмеженим доступом до прийняття їх на озброєння та введення в експлуатацію в обов'язковому порядку проходять сертифікацію на рівень кіберзахищеності. Втім, навіть найнадійніші системи не здатні забезпечити абсолютну безпеку, так як форми і способи проведення кіберрозвідки та кібервпливу постійно удосконалюються. Тому під час функціонування відлагодженої та сертифікованої ІКС постійно проводиться «активний» кіберзахист власної кіберінфраструктури та моніторинг трафіку комп'ютерної мережі. Будемо вважати описаний вище стан функціонуванням ІКС у сталому режимі.

Тим не менш, кіберрозвідка ІКС, з досвіду ведення кіберборотьби у воєнних конфліктах сучасності загалом, та російсько-української війни зокрема [9], проводиться безупинно та, принципово, може призвести до виявлення вразливостей у відносно кіберзахищеній системі. Найчастіше такими вразливостями є недосконалості програмного забезпечення програмного-апаратних вузлів ІКС та налаштувань безпеки операційних систем, які дають змогу противнику безперешкодно оперувати з ними. На цьому етапі можливими є всього два варіанти розвитку подій: перший – системою кіберзахисту буде оперативно виявлено проведену противником кіберрозвідку і вжито заходів з активного кіберзахисту, усунення виявленої вразливості та відновлення ІКС до сталого режиму функціонування; другий – нанесення противником кібервпливу та ураження програмно-апаратного вузла/вузлів ІКС, що безумовно призведе до виведення ІКС із режиму сталого функціонування.

На відміну від першого варіанту, який переведе систему у режим відновлення, другий не вичерпує можливості противника із завдання кібервпливу відносно ІКС. Виведення з ладу вузлів фізичного рівня відкриває шлях до потенційного ураження логічного рівня та, як наслідок, отримання доступу до облікових записів посадових осіб, допущених до роботи в ІКС (рівень кіберперсони). Реалістичним є перехід у стан відновлення режиму сталого функціонування ІКС, за умови проведення вчасного та ефективного кіберзахисту, на стадії коли противником уражено лише фізичний або фізичний і логічний рівні, проте з ураженням кожного наступного рівня ІКС, ймовірність такого переходу зменшується за геометричною прогресією. Відновлення ж в умовах втрати/часткової втрати доступу до облікових записів посадових осіб, ураження програмно-апаратних вузлів ІКС, а також перехоплення та/або знищення даних файлової системи, вимагатиме значно більшого часу, протягом якого система буде виведеною з режиму сталого функціонування.

З огляду на вище зазначене можна стверджувати, що стан ІКС змінюється в часі у випадковому, заздалегідь непередбачуваному порядку під дією зазначених вище заходів з кіберборотьби. Звідси випливає те, що кіберборотьба, яка ведеться відносно системи, протікає як марківський випадковий процес з дискретними станами та неперервним часом (зміна стану ІКС може відбутися в будь-який попередньо невідомий момент часу).

Невід'ємними системоутворюючими складовими кіберборотьби є кіберзахист, кіберрозвідка та кібервплив, під дією яких у заздалегідь невідомі моменти часу змінюються стани, в яких може перебувати ІКС. Позначимо ІКС системою S, яка може перебувати в таких станах:

S_1 – функціонує у сталому режимі;

S_2 – кіберрозвідка (виявлено вразливість кіберінфраструктури та здійснено проникнення в ІКС);

S_3 – уражено програмно-апаратний вузол (вузли) ІКС;

S_4 – уражено логічний рівень ІКС (комунікації між вузлами та/або дані, що передаються);

S_5 – уражено рівень кіберперсони (отримано несанкціонований доступ до облікових записів користувачів, допущених до роботи в ІКС);

S_6 – відновлення сталого режиму функціонування ІКС.

Слід зауважити, що думка провідних науковців за напрямом дослідження проблем кібербезпеки та досвід ведення кіберборотьби у воєнних конфліктах сучасності зводяться до того, що саме людина та людський фактор є «найслабшою» ланкою в ІКС військового призначення. Враховуючи це, було б логічним, що стан ураження рівня кіберперсони ІКС (S_5) має передувати ураженню фізичного (S_3) та логічного (S_4) рівнів. Втім, математична модель визначення ймовірнісних станів ІКС розроблена за принципом результату дії, а не способу дії. Тобто, для моделі не важливо яким саме способом (методом) було досягнуто певного стану ІКС. Важливим є те, що без ураження фізичного рівня ІКС не можливе ураження логічного та рівня кіберперсони, а відповідно, отримання несанкціонованого доступу до рівня кіберперсони можливе лише за умови ураження логічного рівня ІКС. Розмічений граф станів функціонування ІКС подано на рис. 2 (розроблено автором).

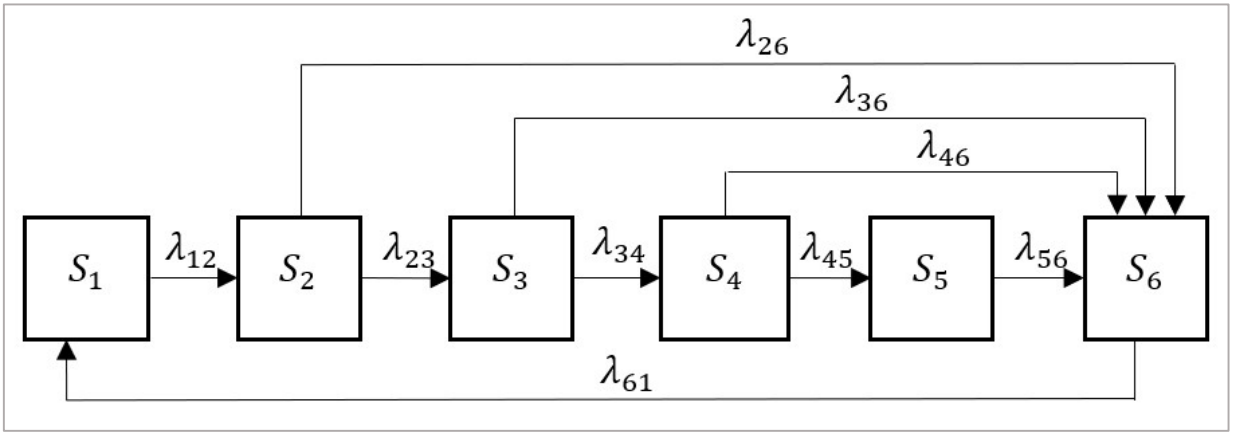

Рисунок 2 – Граф станів функціонування інформаційно-комунікаційної системи

Відповідно, система диференціальних рівнянь Колмогорова для визначення ймовірностей станів ІКС матиме вигляд:

$$\begin{cases} \frac{dp_1}{dt} = -\lambda_{12}p_1 + \lambda_{61}p_6; \\ \frac{dp_2}{dt} = -\lambda_{23}p_2 - \lambda_{26}p_2 + \lambda_{12}p_1; \\ \frac{dp_3}{dt} = -\lambda_{36}p_3 + \lambda_{23}p_2 - \lambda_{34}p_3; \\ \frac{dp_4}{dt} = -\lambda_{46}p_4 - \lambda_{45}p_4 + \lambda_{34}p_3; \\ \frac{dp_5}{dt} = -\lambda_{56}p_5 + \lambda_{45}p_4; \\ \frac{dp_6}{dt} = -\lambda_{61}p_6 + \lambda_{26}p_2 + \lambda_{36}p_3 + \lambda_{46}p_4 + \lambda_{56}p_5, \end{cases} \quad (1)$$

де, p_i – початкова ймовірність перебування системи S в i-му стані, $i = \overline{1,n}$, $\sum_{i=1}^{n} p_i = 1$, $n = 6$;

λ_{ij} – інтенсивність переходу системи S з i-го в j-ий стан, $i = \overline{1,n}$, $j = \overline{1,n}$, $n = 6$, $\lambda_{ij} \in \mathbb{R}$, $\lambda_{ij} > 0$.

t – час.

Розв'язуються такі рівняння відомими чисельними методами, знаючи інтенсивності переходу системи зі стану в стан [8]. Втім, фізичному змісту кіберборотьби притаманна параметрична невизначеність, яка прямо впливає на адекватність математичної моделі визначення ймовірнісних станів ІКС у її варіанті з детермінованою постановкою (1). Результати, отримані з дослідження процесів кіберборотьби виключно як найпростіших потоків, не будуть реалістичними і матимуть узагальнений характер. Згадана параметрична невизначеність зводиться до неможливості чітко передбачити хід та результати проведення кібердій, маючи вихідними даними склад власних сил і засобів і противника, їх навченість, досвід, злагодженість та ін. Наприклад, неможливо сказати напевне, що буде знайдено принаймні одну вразливість ІКС під час ведення кіберрозвідки на інтервалі часу $t \to \infty$, так як і немає підстав стверджувати, що навіть ретельно спланована кібероперація із залученням значного комплекту сил і засобів не може бути зірвана вчасно проведеним активним кіберзахистом. Це пов'язано, в першу чергу, з особливостями інформаційно-комунікаційних технологій та їх прикладного використання у складних системах військового призначення.

З описаного вище випливає, що інтенсивності переходу ІКС з одного стану до іншого під впливом заходів з кіберборотьби мають бути змінними величинами, розподіленими за показниковим (експоненційним) законом. Для розроблення математичної моделі визначення ймовірнісних станів

ІКС необхідно визначити, які саме інтенсивності переходів зі стану в стан є стохастичними за означенням, підлягають впливу шумів та, власне, природу цих шумів (адитивну або мультиплікативну).

Зважаючи на те, що кіберборотьба у воєнних конфліктах сучасності ведеться постійно, можемо припустити, що сканування ІКС на вразливості проводиться зі сталою інтенсивністю та є процесом детермінованим. Обидва переходи зі стану S_2 також будемо вважати детермінованими, адже якщо було знайдено вразливість ІКС, а заходів активного кіберзахисту не проводилося або вони були недостатніми, та залежно від виду знайденої вразливості, з деякою сталою інтенсивністю система перейде до стану S_3.

Проте, подальші переходи зі стану S_3 у стан S_4, із S_4 в S_5 та з S_5 у стан S_6, підлягають мультиплікативному впливу шумів, які носять характер вінерівського випадкового процесу (з нульовим математичним сподіванням та одиничною дисперсією). Обґрунтуванням накладанню впливу таких шумів є вкрай значна кількість і різноплановість умов, які мають виконатися для настання події, що переведе ІКС до станів S_4, S_5 або S_6. Більш того, остаточний перелік згаданих умов переходу системи до станів S_4 – S_6 є невідомим до початку ведення кіберборотьби, він формується динамічно залежно від подій, які передували входженню системи у стан S_3, S_4 та S_5 відповідно.

А саме, стохастичність переходу ІКС зі стану S_3 у стан S_4 породжується необхідністю виконання таких умов, як: можливість ураження логічного рівня ІКС за допомогою виявленої вразливості фізичного рівня; достатній рівень ураження програмно-апаратного вузла/вузлів ІКС для впливу на логічний рівень; не здатність системи кіберзахисту вчасно відновити режим сталого функціонування ІКС, а також низки інших умов.

Перехід зі стану ураження логічного рівня ІКС (S_4) у стан S_5 також є стохастичним, що обумовлюється таким: а) чи було отримано доступ до даних автентифікації облікових записів посадових осіб ПУ ОСУВ; б) рівень кібергігієни особового складу, допущеного до роботи в ІКС; в) які протоколи шифрування даних (Transport Layer Security, Secure Sockets Layer тощо) було закладено під час розробки програмного забезпечення ІКС, та чи є вони взаємно сумісними; г) ціль кібероперації: знищити/перехопити дані або отримати несанкціонований доступ до облікових записів тощо.

Етап переходу ІКС до відновлення (S_6) зі стану ураження рівня кіберперсони (S_5) є найскладнішим для реалізації з огляду на те, що він передбачає часткову або повну втрату доступу до всіх рівнів функціонування системи. Переведення системи на відновлення у такій ситуації потребуватиме ведення дій з кіберзахисту в умовах «присутності» противника в системі. Особливої стохастичності інтенсивності саме цього переходу додає те, що, на відміну від попередніх, немає можливості сформулювати хоча б орієнтовний алгоритм дій персоналу з кіберзахисту для виходу на відновлення ІКС зі стану S_5 через безліч можливих варіантів розвитку подій.

Означена вище параметрична невизначеність процесу ведення кіберборотьби зумовлює перехід від системи лінійних диференціальних рівнянь Колмогорова (1) до системи диференціальних рівнянь у стохастичній постановці такого вигляду:

$$\begin{cases} \frac{dp_1}{dt} = -\lambda_{12}p_1 + \lambda_{61}p_4; \\ \frac{dp_2}{dt} = -\lambda_{23}p_2 - \lambda_{26}p_2 + \lambda_{12}p_1; \\ \frac{dp_3}{dt} = -\lambda_{36}p_3 + \lambda_{23}p_2 - \sigma_{34}p_3\omega_t; \\ \frac{dp_4}{dt} = -\lambda_{46}p_4 - \sigma_{45}p_4\omega_t + \sigma_{34}p_3\omega_t; \\ \frac{dp_5}{dt} = -\sigma_{56}p_5\omega_t + \sigma_{45}p_4\omega_t; \\ \frac{dp_6}{dt} = -\lambda_{61}p_4 + \lambda_{26}p_2 + \lambda_{36}p_3 + \lambda_{46}p_4 + \sigma_{56}p_5\omega_t, \end{cases} \quad (2)$$

де, $\omega_t \sim \sqrt{\Delta t}N(0,1)$ – одновимірний вінерівський процес;

$N(0,1)$ – нормальний розподіл із нульовим середнім та одиничною дисперсією;

σ_{34}, σ_{45}, σ_{56} – інтенсивності переходів, які підлягають впливу вінерівського процесу ω_t.

Задачу Коші для системи (2), з огляду на відсутність точних початкових даних, пропонується розв'язувати за допомогою відомого чисельного методу Ейлера-Маруями, що дає змогу отримати сімейство траєкторій розподілу ймовірностей станів у якості слабких розв'язків системи стохастичних диференціальних рівнянь. Як відомо, метод Ейлера-Маруями математично формалізується у вигляді рекурсії. Для наочності процесу визначення ймовірнісних станів ІКС в умовах ведення кіберборотьби за допомогою цього методу сформулюємо вираз для знаходження ймовірності перебування ІКС у стані S_3:

$$\begin{gathered} y_{k+1} - y_k = -\lambda_{36}p_3\Delta t + \lambda_{23}p_2\Delta t - \sigma_{34}p_3\sqrt{\Delta t}\Delta w_k; \\ \Delta w_k = w_{t_{k+1}} - w_{t_k}; \\ \Delta t = \frac{T}{n}, \end{gathered} \quad (3)$$

де, y_k – наближене значення ймовірності перебування ІКС у стані S_3 на кроці інтегрування k, $k = 0,1,\dots,n-1$;

T – загальний час інтегрування, $T \in \mathbb{R}$, $T > 0$;

n – кількість кроків інтегрування, $n \in \mathbb{N}$.

Розв'язання задачі Коші системи (2) передбачає наявність початкових даних – інтенсивностей переходів між станами та попередніх ймовірностей станів. Аналіз та узагальнення передового досвіду ведення кіберборотьби у воєнних конфліктах сучасності [9] дав змогу отримати принаймні

наближені апроксимовані числові значення інтенсивностей переходів ІКС зі стану в стан (табл. 1).

Таблиця 1

Інтенсивність переходів інформаційно-комунікаційної системи зі стану в стан

Інтенсивність переходу	Числове значення
λ_{12}	5
λ_{26}	2,5
λ_{23}	1,3
λ_{36}	0,75
σ_{34}	0,5
λ_{46}	0,5
σ_{45}	0,2
σ_{56}	0,05
λ_{61}	2

Аналогічним чином було отримано узагальнені початкові числові показники ймовірностей перебування ІКС у відповідних станах (табл. 2).

Таблиця 2

Середні значення ймовірностей станів інформаційно-комунікаційної системи

Ймовірність стану	Числове значення
P_1	0,5
P_2	0,15
P_3	0,06
P_4	0,05
P_5	0,04
P_6	0,2

З метою підкреслення концептуальної відмінності рішення отриманого внаслідок розв'язання системи диференціальних рівнянь Колмогорова у детермінованій постановці (1) від отриманого рішення задачі Коші для системи диференціальних рівнянь у стохастичній постановці (2) наведемо сімейства траєкторій розподілу ймовірнісних станів ІКС, які відображають результати чисельного інтегрування на відрізку часу $T = 1$, з кроком інтегрування $\Delta t = 0{,}01$ (кількість реалізацій моделі – 25) на рис. 3 та рис. 4 відповідно.

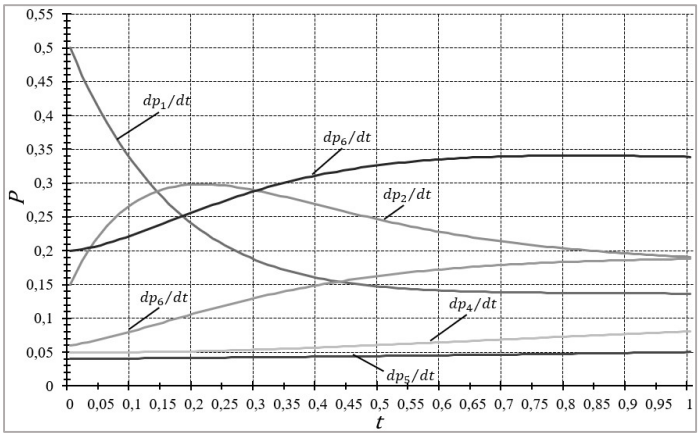

Рисунок 3 – Траєкторії розподілу ймовірнісних станів інформаційно-комунікаційної системи у детермінованій постановці (1)

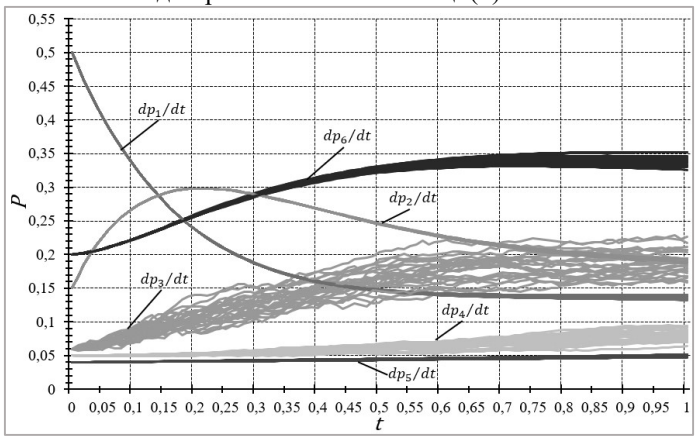

Рисунок 4 – Траєкторії розподілу ймовірнісних станів інформаційно-комунікаційної системи у стохастичній постановці (2)

Рисунок 4 дає зрозуміти, що математична модель визначення ймовірнісних станів ІКС в умовах ведення кіберборотьби у стохастичній постановці, на відміну від детермінованого варіанту (рис. 3), дає змогу враховувати випадкові фактори, що притаманні досліджуваному процесу. З діаграми видно, що при заданих у табл. 1 та табл. 2 початкових умовах найбільшої невизначеності набуде розподіл

ймовірності стану S_3 «ураження фізичного рівня ІКС» (математичне сподівання $\widetilde{M} = 0{,}188$, дисперсія $\widetilde{D} = 0{,}0003126$), що в цілому відповідає фізичному змісту процесу кіберборотьби та особливостям функціонування ІКС в умовах її ведення.

Саме математичні сподівання ймовірностей перебування ІКС у визначених станах та дисперсії розподілів цих ймовірностей пропонується використовувати як показники ефективності функціонування ІКС в умовах ведення кіберборотьби. Числові значення показників ефективності, отримані в результаті чисельного інтегрування системи (2) методом Ейлера-Маруями за попередньо наданих початкових даних наведено в табл. 3.

Таблиця 3

Числові значення показників ефективності функціонування інформаційно-комунікаційної системи

	p_1	p_2	p_3	p_4	p_5	p_6
$\widetilde{M}$	0,137	0,191	0,188	0,081	0,050	0,339
$\widetilde{D}$	0,000 0043	0,000 0033	0,000 3126	0,000 0723	0,000 0011	0,000 0446

Висновки й перспективи подальших досліджень

Отже, у статті було висвітлено основні положення розробленої математичної моделі визначення ймовірнісних станів інформаційно-комунікаційної системи в умовах ведення кіберборотьби. Науковою новизною запропонованої математичної моделі є використання математичного апарату теорії стохастичних диференціальних рівнянь для аналітичного моделювання кіберборотьби як дифузійного марковського процесу та слабкого методу Ейлера-Маруями для чисельного інтегрування системи диференціальних рівнянь у стохастичній постановці, що описує функціонування інформаційно-комунікаційної системи.

Напрямом подальшого дослідження за цим напрямом є пошук та апроксимація представницької статистики ведення кіберборотьби, дані з якої були б придатними для використання у якості параметрів (початкових даних) математичної моделі визначення ймовірнісних станів інформаційно-комунікаційної системи.

Список бібліографічних посилань

1. Горгуленко В. А. Військово-теоретичне обґрунтування рекомендацій стосовно розвитку термінологічного апарату в сфері кіберборотьби. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 3(51). С. 41–50. DOI: https://doi.org/10.33099/2311-7249/2024-51-3-41-50.

2. Мазулевський О. Є., Жолобович Н. В. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 3(51). С. 34–40. DOI: 10.33099/2311-7249/2024-51-3-34-40. **3. Park J., Kim D., Shin D.** Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness). *Journal of the Korea Institute of Information Security & Cryptology*. 2019. Vol. 29. № 2. P. 465–472. DOI: 10.13089/JKIISC.2019.29.2.465. **4. Грищук Р. В., Даник Ю. Г.** Основи кібернетичної безпеки: моногр. Житомир : ЖНАЕУ, 2016. 636 с. **5. Бутвін Б. Л., Машкін О. О., Соломицький О. І.** Використання модифікованих рівнянь динаміки середніх для оперативного прогнозування ходу та результатів бойових дій. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2019. № 2(35). С. 115–120. DOI: 10.33099/2311-7249/2019-35-2-115-120. **6. Богданович В. Ю., Грищук Р. В., Левченко О. В.** Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: Військові та технічні науки*. 2017. № 4(74). С. 21–37. **7. Hryshchuk R.** Example of Differential Transformations Application in Cybersecurity. *ISecIT*. 2021. P. 223–227. URL: https://ceur-ws.org/Vol-3200/paper31.pdf (accessed: 12 February 2025). **8. Машкін О. О.** Особливості чисельного вирішення диференційних рівнянь моделей ланчестерського типу у стохастичній постановці. *Системи обробки інформації*. 2020. № 1(160). С. 67–72. DOI: 10.30748/soi.2020.160.08. **9. Горгуленко В. А.** Кіберборотьба у воєнних конфліктах сучасності: передовий досвід, тенденції та закономірності розвитку. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 2(50). С. 11–28. DOI: 10.33099/2311-7249/2024-50-2-11-28. **10. Joint Publication 3-12 «Cyberspace Operations».** J7 Directorate for Joint Force Development. 2018. URL: https://irp.fas.org/doddir/dod/jp3_12.pdf (accessed: 10 March 2025).

A MATHEMATICAL MODEL FOR DETERMINING PROBABILISTIC STATES OF AN INFORMATION AND COMMUNICATION SYSTEM IN THE CONDITIONS OF CYBERWARFARE

HORHULENKO Vladyslav, Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine, https://orcid.org/0000-0001-6382-5075

Formulation of the problem in general. *Science has no substantiated system of indicators and cyber warfare effectiveness evaluation criteria. Mathematical modelling of cyber warfare, as a relatively new and innovative area of the Armed Forces of Ukraine activity, is undoubtedly essential and will allow for a comprehensive investigation of the issue of assessing the effectiveness of its conduct, which has not yet received sufficient attention.*

Research methods. *Methods of formalisation and mathematical modelling were used in this research. By the formalisation method, cyber warfare was represented as a diffusion Markov process, in sense of the stochastic processes theory, as well as a set of typical cyber warfare targets were generalised as an information and communication system by the structural feature (most of cyber warfare targets consists of physical, logical and cyber-persona layers). The*

method of mathematical modelling was used to develop a mathematical model for determining probabilistic states of an information and communication system in the conditions of cyberwarfare.

Analysis of the latest research findings. *The latest research results in this area highlight only partial indicators of the separate components of cyber warfare (cyber defence, cyber intelligence, and cyber influence) productivity. Such indicators are usually based on the volume of intercepted, modified or destroyed data (information) and its importance, which, in turn, can only be assessed by experts, which a priori generates subjectivity of the cyber warfare effectiveness assessment.*

Presenting the main results. *The main result of the research is the developed mathematical model for determining probabilistic states of an information and communication system in the conditions of cyberwarfare, based on a mathematical apparatus of the stochastic differential equations theory.*

An element of scientific novelty. *The developed mathematical model, unlike existing ones, allows for obtaining probabilistic parameters of the information and communication system, which function as effective indicators of cyber warfare. Such parameters are the mathematical expectations of the information and communication system probabilities of being in determined states and the dispersions of these probability distributions.*

Theoretical and practical significance of the article. *The theoretical importance of the obtained scientific results is the applied use of the powerful mathematical apparatus of the theory of stochastic differential equations for analytical mathematical modelling of cyberspace actions, which are characterised by uncertainty and randomness. The practical significance of the research results is the possibility of using the mathematical model to determine the probabilistic states of the information and communication system software implementation to predict the course and results of cyber warfare.*

Conclusion and the perspectives of future research. *Therefore, the article highlighted the main provisions of the mathematical model for determining probabilistic states of an information and communication system in the conditions of cyberwarfare. The direction of further research in this area is the search and approximation of representative statistics of cyber warfare, the data from which would be suitable for use as parameters (initial data) of the developed mathematical model.*

Keywords: *cyber defence, cybersecurity, cyberspace, cyber warfare, diffusion stochastic processes, Markov chain, mathematical model, stochastic differential equations.*

References

1. Horhulenko, V. A., (2024). Military-theoretical justification of recommendations for the development of terminological apparatus in the sphere of cyber warfare. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 3(51), 41–50. DOI: https://doi.org/10.33099/2311-7249/2024-51-3-41-50.

2. Mazulevskyi, O. Ye., Zholobovych, N. V., (2024). Assessment of the current state of cyber resilience, taking into account the situation in cyberspace. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 3(51), 34–40. DOI: 10.33099/2311-7249/2024-51-3-34-40. **3. Park, J., Kim, D., Shin, D.,** (2019). Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness). *Journal of the Korea Institute of Information Security & Cryptology*. 29(2), 465–472. DOI: 10.13089/JKIISC.2019.29.2.465. **4. Hryschuk, R. V., Danyk, Yu. H.,** (2016). *Fundamentals of cyber security*: a monograph. Zhytomyr: ZhNAEU. **5. Butvin, B. L., Mashkin, O. O., Solomytskyi, O. I.,** (2019). The modified equation of the medium dynamics for operative forecasting of the course and results of the combat actions. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony.* 2(35), 115–120. DOI: 10.33099/2311-7249/2019-35-2-115-120.

6. Bohdanovych, V. Yu., Hryshchuk, R. V., Levchenko, O. V., (2017). System of criteria and indicators for assessing the effectiveness of the information security system. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia: Viiskovi ta tekhnichni nauky*. 4(74), 21–37. **7. Hryshchuk, R.,** (2021). Example of Differential Transformations Application in Cybersecurity [online]. *ISecIT*. 223–227. Available at: https://ceur-ws.org/Vol-3200/paper31.pdf [Accessed: 12 February 2025]. **8. Mashkin, O. O.,** (2020). Features of numerical solution of differential equations of Lanchester-type models in stochastic production. *Systemy obrobky informatsii*. 1(160), 67–72. DOI: 10.30748/soi.2020.160.08. **9. Horhulenko, V. A.,** (2024). Cyber warfare in modern military conflicts: experience, trends and regularities of development. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 50(2), 11–28. DOI: 10.33099/2311-7249/2024-50-2-11-28. **10. Joint Publication 3-12 «Cyberspace Operations».** J7 Directorate for Joint Force Development [online]. 2018. Available at: https://irp.fas.org/doddir/dod/jp3_12.pdf [Accessed: 10 March 2025].

Рукопис надійшов до редакції *28.02.2025*
Рукопис прийнято до друку після рецензування *25.03.2025*
Дата публікації *30.04.2025*