https://doi.org/10.31891/2219-9365-2025-81-22
УДК 004.9

ПРОКОПЕНКО Андрій
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0009-7227-3458
e-mail: imnelliel98@gmail.com
ТРЕНЬОВ Микита
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0002-8459-0599
e-mail: nekatrenov@gmail.com

# БАГАТОРІВНЕВЕ МОДЕЛЮВАННЯ ТА ІДЕНТИФІКАЦІЯ СТАНУ ВУЗЛІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ ПІДСИСТЕМОЮ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*У статті розглянуто багаторівневий підхід до аналізу складних технічних систем для моделювання небезпечних і критичних подій інформаційної безпеки (ІБ) в елементах та вузлах інформаційно-телекомунікаційних мереж (ІТКМ). Запропоновано методологію підвищення ефективності підсистеми моніторингу ІБ на різних логічних рівнях структури ІТКМ. Використано методи загальної теорії систем, теорії ігор, теорії надійності, теорії нечітких множин, теорії ймовірностей і математичної статистики, теорії класифікації та теорії графів. Запропоновано багаторівневу модель настання критичної події ІБ для всієї системи та її окремих елементів. Розроблено ймовірнісний граф реалізації несанкціонованого доступу, що враховує різні типи порушників. Аналітично описано чотири класи станів ІБ з урахуванням помилок контролю першого і другого роду. Отримано математичні вирази для оцінювання ймовірностей розкриття мережі та її нормального функціонування. Запропонований підхід дає змогу оцінювати рівень захищеності ІТКМ навіть за умов неповної інформації про порушника. Враховано вплив загроз на різних рівнях системи без прив'язки до конкретної точки входу.*

*Ключові слова: інформаційна безпека, моніторинг, інформаційно-телекомунікаційна мережа, критична подія, ймовірнісний аналіз, багаторівневе моделювання.*

PROKOPENKO Andrii, TRENOV Mykyta
State University of Information and Communication Technology

# MULTILEVEL MODELING AND STATE IDENTIFICATION OF NODES IN PUBLIC INFORMATION AND TELECOMMUNICATION NETWORKS USING AN INFORMATION SECURITY MONITORING SUBSYSTEM

*The article examines a multilevel approach to analyzing complex technical systems for modeling hazardous and critical information security (IS) events in the elements and nodes of public information and telecommunication networks (ITN). A methodology is proposed to enhance the effectiveness of the IS monitoring subsystem at various logical levels of the ITN structure. Methods of general systems theory, game theory, reliability theory, fuzzy set theory, probability theory, mathematical statistics, classification theory, and graph theory are utilized to formalize the processes of threat modeling and risk assessment. A multilevel model of critical IS events is proposed for both the entire system and its individual components. The model considers attack scenarios, threat propagation, and vulnerabilities that can be exploited by adversaries with different levels of capability and intent. A probabilistic graph of unauthorized access realization is developed, accounting for different types of intruders, including external and internal actors with varying degrees of privilege escalation. The study analytically describes four IS state classes, considering Type I and Type II control errors, and introduces a refined classification of IS incidents based on their severity and impact on network functionality. Mathematical expressions for evaluating the probabilities of network compromise, system resilience, and normal operation under different threat conditions are derived. The proposed approach enables the assessment of ITN security levels even under incomplete information about the intruder's strategies and available resources. The impact of threats at different system levels is considered without linking to a specific entry point, which allows for a more comprehensive analysis of network resilience. Additionally, practical recommendations are provided for improving IS monitoring through adaptive security policies and automated response mechanisms. The effectiveness of the proposed methodology is validated through simulation experiments, demonstrating its applicability in real-world network environments. The findings contribute to the development of proactive IS strategies aimed at minimizing risks and ensuring ITN stability under various cyber threat conditions.*

*Keywords: information security, monitoring, information and telecommunication network, critical event, probabilistic analysis, multilevel modeling.*

## ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сформулювати багаторівневий підхід до опису складних технічних систем для обґрунтування моделювання небезпечних і критичних подій інформаційної безпеки в елементах та вузлах інформаційно-телекомунікаційних мереж загального користування.

Підвищити ефективність функціонування підсистеми моніторингу інформаційної безпеки інформаційно-телекомунікаційної системи на різних логічних рівнях її структури. Методи аналізу, загальної

теорії систем, теорії ігор, теорії надійності, теорії нечітких множин, теорії ймовірностей і математичної статистики, теорії класифікації та теорії графів.

Запропоновано багаторівневу модель настання критичної події інформаційної безпеки як для всієї інформаційно-телекомунікаційної системи, так і для окремих її елементів. Розроблено ймовірнісний граф реалізації несанкціонованого доступу порушником (як випадковим, так і цілеспрямованим) до елементів мережі. Аналітично обґрунтовано та описано чотири класи стану ІБ з урахуванням помилок контролю першого і другого роду. Отримано математичні вирази для оцінювання ймовірностей розкриття та нормального функціонування інформаційно-телекомунікаційної мережі. Запропонований метод оцінювання інформаційної безпеки дає змогу визначити кількісні показники захищеності мережі за умов неповної інформації про порушника та його можливості. Завдяки багаторівневому підходу враховуються впливи загроз на різних логічних рівнях системи без прив'язування до конкретної точки входу.

## АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Сучасні інформаційно-телекомунікаційні мережі (ІТКМ) і мережі загального користування, в яких постійно нарощуються можливості проведення кібервпливів, як з боку організованих міжнародних терористичних угруповань, так і з боку ймовірного супротивника (порушника) [1-4], являють собою концепцію організації та побудови елементів (вузлів), які взаємодіють між собою і зовнішнім середовищем. Застосування технологій вимірювання, передавання, оброблення та ідентифікації даних зумовлює потребу у створенні різноманітних підсистем контролю та моніторингу стану елементів мережі з погляду інформаційної безпеки (ІБ), спрямованих на нейтралізацію небезпечного або критичного стану внаслідок впливу зовнішніх, а також внутрішніх дестабілізуючих чинників або загроз.

## ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті: моделювання небезпечних і критичних подій інформаційної безпеки інформаційно-телекомунікаційної системи. При цьому під небезпечною подією на кожному логічному рівні ІТКМ розуміють вплив загрози ІБ на її елемент, що не призвів до компрометації його вхідних і вихідних величин, а під критичною подією - вплив, який призвів до компрометації його вхідних і вихідних величин, що спричиняє підвищення ймовірності розкриття сусідніх елементів інформаційного тракту ІТКМ.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

### Багаторівневий підхід до побудови структури ІТКМ

Ефективність забезпечення нормального стану (функціонування) ІТКМ багато в чому залежить від реалізації комплексного підходу до побудови мережевої інфраструктури на основі відповідного моделювання загроз ІБ, вибору адекватних засобів захисту вузлів (елементів) і каналів зв'язку, методів моніторингу та управління на мережі тощо. [5-9]. Оскільки відомо, що сучасні ІТКМ працюють на глобальному, регіональному та локальному рівнях, для моделювання її інформаційного тракту (ІТ) використовуємо багаторівневий підхід до побудови захисту територіально-розподіленої системи. Так, на рис. 1 наведено логічну схему функціонування ІТКМ у вигляді інформаційного тракту доступу з локальної обчислювальної мережі (локальний рівень - ЛОМ) до глобальної комп'ютерної мережі (глобальний рівень - ГКМ «Інтернет»). На наведеній схемі показано, що доступ до того чи іншого вузла ІТКС здійснюється по ІТ, через сусідні її вузли, що мають зв'язність із ним і розташовані на сполучуваних логічних рівнях («локальний-регіональний», «регіональний-глобальний"). При цьому на рисунку показано: I - логічний рівень, на якому забезпечується доступ користувачів до ІТКМ (до її ресурсів) під час розв'язання прикладних завдань; II - логічний рівень, що займає проміжну ланку між ЛОМ і ГКМ, розв'язує завдання комутації та маршрутизації; III - логічний рівень сполучення з ГКМ.

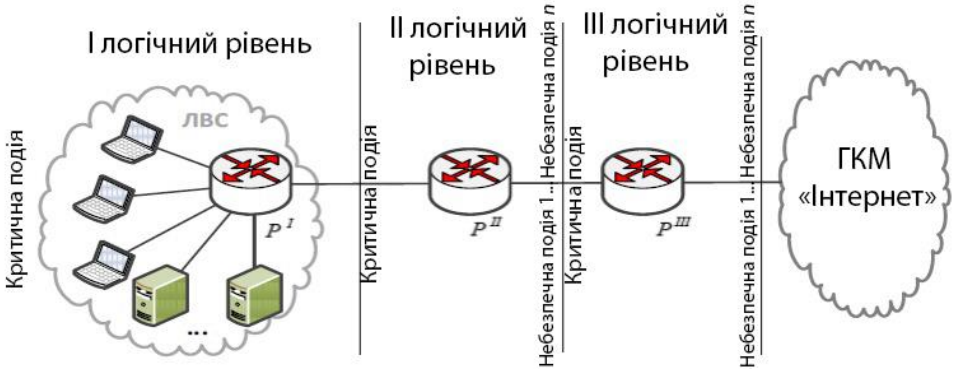


**Рис. 1. Логічна структура функціонування інформаційного тракту ІТКМ**

З аналізу цієї схеми видно, що будь-яка атака, проведена на першому логічному рівні ІТКМ, є критичною подією, оскільки фактично порушник працює всередині ЛОМ (є внутрішнім порушником) системи. Атаки на об'єкти ІІ і ІІІ логічних рівнів ІТ ІТКМ є очікуваними, зважаючи на територіальну розподіленість системи, це дає можливість здійснення ретельнішої підготовки організаційних і технічних заходів щодо забезпечення їхньої інформаційної безпеки. Залежно від цілей реалізації загроз інформаційній безпеці, а також їхнього місця проведення, є можливість вибору та реалізації заходів захисту й оцінювання ступеня їхньої небезпеки або критичності.

Як розглянуто в багатьох роботах [1-9] програмно-апаратні засоби елементів ІТКМ у глобальному кіберпросторі постійно піддаються деструктивним впливам, що мають навмисний або випадковий характер. При цьому на різні елементи і вузли ІТКМ, типу ПЕОМ, сервер, маршрутизатор, комутатор тощо, діють відповідні види загроз інформаційної безпеки [10]. Важливо зазначити, що однакові види загроз на різних елементах ІТКМ та її логічних рівнях мають різний ступінь критичності їхніх реалізацій щодо нанесення шкоди як самій ІТКМ, так і її системі управління. Відповідно, одна й та сама загроза ІБ, що діє на різних логічних рівнях ІТКМ матиме різний рівень небезпеки (критичності). Тому й методи захисту логічного рівня або всієї системи загалом від різних загроз ІБ мають відрізнятися. Для вибору адекватних заходів захисту ІТКМ від загроз ІБ на різних її логічних рівнях необхідно здійснити моделювання настання критичної події ІБ, а також оцінювання ймовірності її відсутності (нормального функціонування системи). Далі розглянемо питання моделювання критичних подій ІБ на ІТКМ та її логічних рівнях.

**Багаторівневе моделювання критичного стану ІТКМ**

У предметній області забезпечення ІБ пропонується велика кількість рішень з побудови, як моделей атак, моделей порушника, так і моделей об'єктів захисту [1-8]. Причому критичні події ІБ зазвичай уявляють сукупністю декількох небезпечних або причинних подій [11], які відбуваються на доступних порушнику різних логічних рівнях ІТКМ (рис. 1). Для здійснення оцінки ймовірності реалізації таких подій проводять їхню ієрархічну декомпозицію за рівнями інформаційного тракту ІТКМ.

На рис.1 у вигляді $P^{\mathrm{I}}$, $P^{\mathrm{II}}$ і $\mathrm{P}^{\mathrm{III}}$ позначено ймовірності настання критичної події, відповідно на I, II і III логічних рівнях інформаційного тракту ІТКМ, які дорівнюють:

$$P^{\mathrm{I}} = 1 - (1 - P^{\mathrm{II}})(1 - P_{1.1})(1 - P_{1.2}) \dots (1 - P_{1n})$$
$$P^{\mathrm{II}} = 1 - (1 - P^{\mathrm{III}})(1 - P_{1.1})(1 - P_{1.2}) \dots (1 - P_{1n})$$
$$P^{\mathrm{III}} = (1 - P_{1.1})(1 - P_{1.2}) \dots (1 - P_{1n})$$

де $P_{1.1}, P_{1.2}, \dots, P_{1n}$ - імовірності впливу деструктивних загроз на елементи ІТКМ, а n - кількість їхніх видів, які можливі до застосування в інформаційному тракті ІТКМ.

Тоді, використовуючи математичний апарат загальної теорії надійності [12], для переходу порушника з одного на інший логічний рівень ІТКМ із врахуванням протидії підсистеми моніторингу ІБ ІТКМ на кожному з логічних рівнів (I, II, III), мають виконуватися необхідні умови, що характеризують цю ймовірність. Так, імовірність переходу порушника з III логічного рівня ІТКМ на II логічний рівень матиме вигляд:

$$P_1^{\mathrm{III}} = (1 - (1 - P_{1.1})(1 - P_{1.2}) \dots (1 - P_{1n}))P_{\mathrm{н}}^{\mathrm{III}}\overline{P_{\mathrm{м}}^{\mathrm{III}}} \quad (1)$$

а ймовірність переходу порушника від першого до наступного елемента логічного рівня (II):

$$P_1^{\mathrm{II}} = (1 - (1 - P_1^{\mathrm{III}})(1 - P_{1.1})(1 - P_{1.2}) \dots (1 - P_{1n}))P_{\mathrm{н}}^{\mathrm{II}}\overline{P_{\mathrm{м}}^{\mathrm{II}}} \quad (2)$$

При цьому, фінальну ймовірність розкриття інформаційного тракту ІТКМ виразимо як:

$$P_{\text{вскр.}} = P_1^{\mathrm{I}}(1 - (1 - P_1^{\mathrm{II}})(1 - P_{1.1})(1 - P_{1.2}) \dots (1 - P_{1n}))P_{\mathrm{ц}}^{\mathrm{I}}\overline{P_{\mathrm{м}}^{\mathrm{II}}} \quad (3)$$

Під час переходу за ієрархією до нижчого логічного рівня інформаційного тракту ІТКМ критичний стан (подія) поточного рівня може розглядатися або як небезпечна подія наступного логічного рівня, або як критична подія всієї ІТКМ. Також, будь-яка з небезпечних подій з деякою ймовірністю може призвести до критичної події на даному логічному рівні ІТ ІТКМ, однак може і не виключати появи наступних *n*-х небезпечних подій для розглянутого мережевого елемента. Це свідчить про те, що небезпечні події для елемента логічного рівня ІТ ІТКМ є спільними.

Трансформація критичної події ІБ одного логічного рівня в небезпечну подію іншого рівня, або ж настання критичної події для всієї ІТ ІТКМ багато в чому залежить від місця виникнення несанкціонованого доступу (ВНД) порушника в ньому, технічної оснащеності обох зі сторін протиборства, а також застосовуваних технологій впливу на ІТКМ і доступних методів захисту елементів інформаційного тракту. При цьому важливо враховувати і цілі інформаційного впливу під час здійснення ВДН, а також ефективність функціонування підсистеми моніторингу ІБ ІТКМ під час виявлення ВНД.

З урахуванням вищевикладеного, розв'язання задачі оцінювання ефективності підсистеми моніторингу ІБ ІТКМ, запропоновано представити байєсівською грою з неповною інформацією про порушника та його передбачувані стратегії [13]. При цьому модель поведінки порушника з урахуванням

ідентифікації НСД підсистемою моніторингу ІБ ІТКМ наведено на рис. 2. Із чого видно, що в разі виникнення ВНД до елемента будь-якого логічного рівня ІТКМ існує ймовірність того, що доступ здійснено випадковим або цілеспрямованим порушником.

Оскільки відомо [1-4], що в ГКМ «Інтернет» злом інформаційних ресурсів став повсякденною проблемою і де-факто перевіркою на «професіоналізм» недбайливих початківців-користувачів, то в моделі вважатимемо «випадковим» порушником - порушника ІБ, що одержав доступ до елемента інформаційного тракту ІТКМ випадково (або з метою розв'язання своїх завдань на обчислювальних потужностях «потенційної жертви»), а «цілеспрямованим» порушником - порушника-професіонала (хакера), який володіє інформацією про цілі та завдання інформаційно-телекомунікаційної системи та її ресурсів.

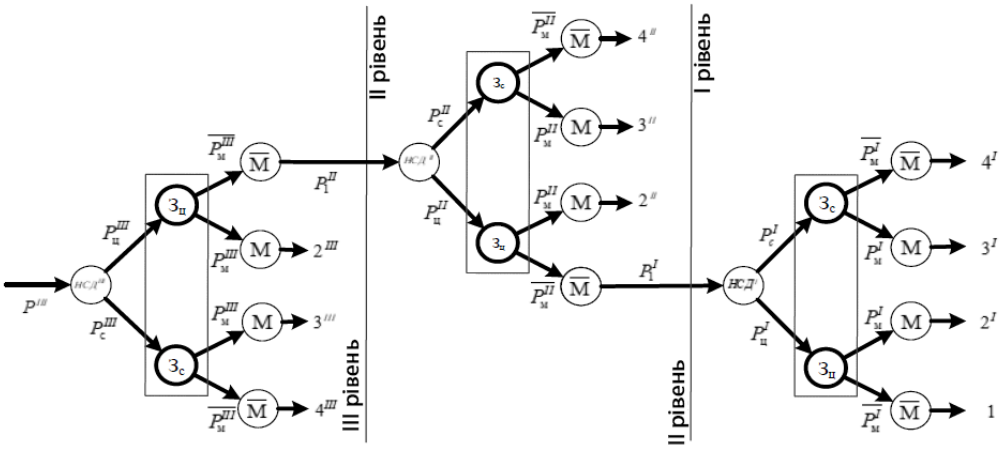


**Рис. 2. Модель ідентифікації критичного стану ІТКМ засобами підсистеми моніторингу**

Використовуючи підхід концепції теорії ігор [13], перший крок робить порушник. Водночас, нам невідомо «випадковий» чи «цілеспрямований» порушник здійснив ВНД. Отже, до інформаційної множини моделі, що розглядається, ми повинні включити обидва ці типи порушників через імовірності здійснення ВНД: $P_{\text{в}}$ і $P_{\text{ц}}$. Також на кожному з елементів ІТ ІТКС [14, 15] існує два стани системи моніторингу, що зводяться до фінальних імовірностей станів елемента на розглянутому логічному рівні: $P_{\text{м}}$ - коли система моніторингу виявляє ВНД; $\overline{P_{\text{м}}}$ - коли система моніторингу не змогла виявити ВНД. Відповідно, у моделі на рис. 2 виділено класи 1 - 4 стану елемента (вузла) інформаційного тракту ІТКМ розглянутого логічного рівня:

1 - елемент ІТ ІТКМ зламаний цілеспрямованим порушником, водночас підсистема моніторингу не повідомила про ВНД ($\overline{M}$), противник переходить на наступний логічний рівень;

2 - елемент зламаний цілеспрямованим порушником, підсистема моніторингу повідомила про факт порушення ІБ ($M$), своєчасно проводяться заходи протидії НСД;

3 - елемент зламаний випадковим порушником, підсистема моніторингу повідомила про факт порушення ІБ ІТ ІТКМ ($M$), своєчасно вживаються заходи протидії ВНД;

4 - елемент зламаний випадковим порушником, підсистема моніторингу не повідомила про факт порушення ІБ ($M$), порушник не переходить на наступний логічний рівень ІТКМ.

При цьому класи стану ІТКС «2» - «4» є внутрішньорівневими, а клас стану «1» дає змогу цілеспрямованому порушнику перейти на наступний рівень ІТКМ. У зв'язку з чим, варіаційний ряд переваги фінальних станів, застосовний для розглянутого мережевого елемента або для ІТКМ загалом має вигляд: 3→2→4→1, тобто критичним (найменш бажаним) класом стану ІБ ІТКМ буде клас «1».

Аналітично фінальні ймовірності для елемента логічного рівня ІТКС можна записати у вигляді:

$$P^*_{\text{"1"}} = P^* P^*_{\text{ц}} \overline{P^*_{\text{м}}};\ P^*_{\text{"2"}} = P^* P^*_{\text{ц}} P^*_{\text{м}};\ P^*_{\text{"3"}} = P^* P^*_{\text{с}} P^*_{\text{м}};\ P^*_{\text{"4"}} = P^* P^*_{\text{ц}} \overline{P^*_{\text{м}}} \qquad (4)$$

де - $P_{\text{м}}$ вірогідність ідентифікації ВНД підсистемою моніторингу ІБ ІТКМ, * - номер логічного рівня ІТКМ.

**Моделювання подій інформаційної безпеки на логічних рівнях ІТКМ**

Імовірності проведення деструктивного впливу на елементи інформаційного тракту ІТКМ - $P_{1.1}, P_{1.2}, \ldots, P_{1.n}$ - залежать від багатьох чинників як внутрішнього стану елемента ІТКС, властивостей підсистеми ІБ, ефективності підсистеми моніторингу, так і можливостей потенційного порушника ІБ (видів загроз ІБ елементів ІТКМ та методів захисту, які використовуються від них). При цьому підсистема моніторингу фактично реалізує поетапну процедуру контролю ІБ на кожному з логічних рівнів ІТКМ, коли

на першому етапі відбувається виявлення ВНД (небезпечної події), а на другому - розпізнавання критичної події.

На рис. 3 позначено класи критичного стану елементів ІТ ІТКМ, де: О - виявлення небезпечної події ІБ ІТКМ, $O = 1 - \overline{O}$ ; $P_1$ - апріорна ймовірність факту нормального функціонування ІТКМ ($\overline{O}$), $P_1 = 1 - P_2$; $P_2$ - апріорна ймовірність факту розкриття ІТКМ (О); $\overline{K}$ - нормальний стан ІБ ІТКМ; К - критичний стан ІБ ІТКМ; α - помилка першого роду «помилкова тривога про ВНД» $(\alpha = 1 - \bar{\alpha})$; β - помилка другого роду «невиявлений ВНД» $(\beta = 1 - \bar{\beta})$; “1” - ІТКМ функціонує нормально, хибне виявлення ВНД не розпізнано; “2” - ІТКМ розкрито, небезпечну подію виявлено, але не розпізнано; «3» - ІТКМ функціонує нормально, хибне виявлення ВНД і розпізнавання; “4” - ІТКМ розкрито, небезпечна подія виявлена та розпізнана; “5” - ІТКМ функціонує нормально, визнана працездатною; “6” - ІТКМ розкрито, але ВНД не виявлено. На рис. 3 також наведено ймовірності виявлення і розпізнавання критичного стану ІБ ІТ ІТКМ.

Схема заміщення ймовірнісного графа (за рис. 3) інформаційного тракту ІТКМ з урахуванням логічного рівня підсистеми моніторингу, у функціонуванні якої також можуть спостерігатися помилки першого α і другого роду β, наведено на рис. 4.

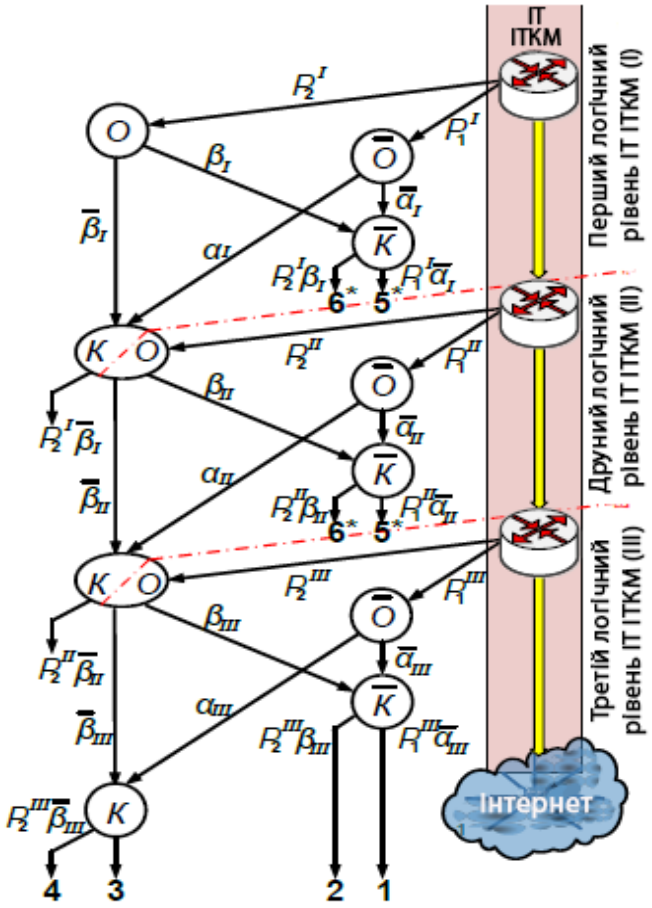


**Рис. 3. Ймовірнісний граф класифікації критичного стану ІТКМ**

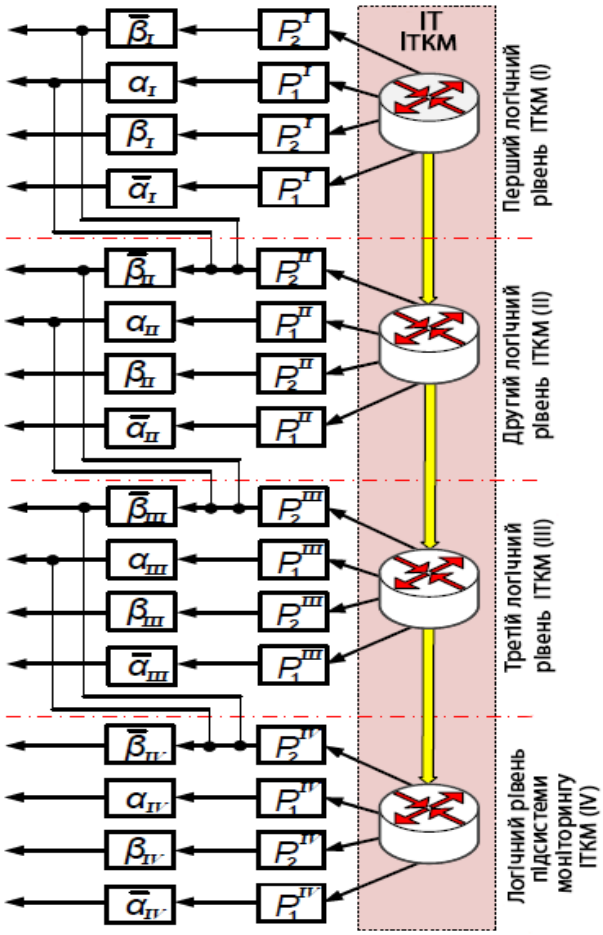


**Рис. 4. Схема надійності для заміщення ймовірнісного графа класифікації критичного стану ІТКМ**

Процедуру визначення фінальної ймовірності нормального функціонування (відсутності критичного стану ІБ) $P_{нф}$ ІТ ІТКМ із врахуванням помилок першого та другого роду подано на рис. 5, а процедура визначення фінальної ймовірності настання критичної події ІБ $P_{КМ}$ інформаційного тракту ІТКМ, відповідно, на рис. 6.

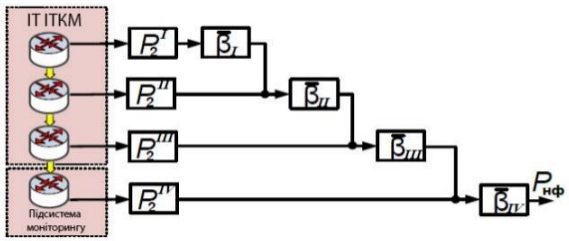


**Рис. 5. Процедура розрахунку підсумкової ймовірності нормального функціонування ($P_{нф}$) ІТКМ**

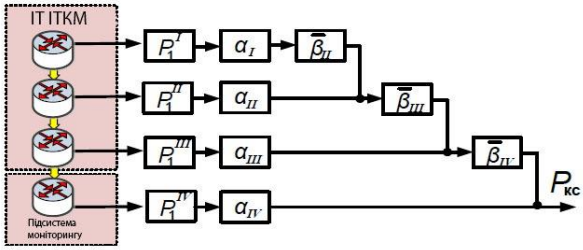


**Рис. 6. Процедура розрахунку підсумкової ймовірності настання критичного стану ($P_{КМ}$) ІБ ІТКМ**

Тоді математичні записи розрахунку $P_{нф}$ і $P_{км}$ з урахуванням помилок контролю ІБ мають вигляд:

$$P_{нф} = 1 - \left(1 - \bar{\beta}_{IV}\langle 1 - \left[\bar{\beta}_{III}\left\{1 - \left(1 - P_1^I \alpha_I \bar{\beta}_{II}\right)\left(1 - P_1^{II}\alpha_{II}\right)\right\}\right]\left[1 - P_1^{III}\alpha_{III}\right]\rangle\right)\left(1 - P_1^{IV}\alpha_{IV}\right) \quad (5)$$

$$P_{км} = \left(1 - \langle 1 - \bar{\beta}_{III}\left[1 - \bar{\beta}_{II}\left\{1 - \left(1 - P_2^I \alpha_I \bar{\beta}_I\right)\left(1 - P_2^{II}\right)\right\}\right]\left[1 - P_2^{III}\right]\rangle\langle 1 - P_2^{IV}\rangle\right)\bar{\beta}_{IV} \quad (6)$$

## ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У рамках запропонованого методу ідентифікації стану елементів (вузлів) інформаційно-телекомунікаційних мереж загального користування підсистемою моніторингу інформаційної безпеки реалізовано багаторівневий підхід «згори донизу». Такий підхід уможливлює всебічне врахування деструктивних впливів на різних логічних рівнях мережі незалежно від точки проникнення зловмисника. Запропонована модель у вигляді ймовірнісного графа передбачає чітку структурованість і водночас гнучкість, що дозволяє відстежувати та оцінювати вплив як «випадкового», так і «цілеспрямованого» порушника.

Завдяки врахуванню похибок контролю ІБ першого (хибна тривога) та другого (невиявлений несанкціонований доступ) роду вдається отримати достовірнішу оцінку рівня безпеки. Відсутність повної інформації про зловмисника й різноманітність можливих загроз компенсується залученням положень теорії ігор та методів імовірнісного моделювання. Таким чином, розроблений метод підвищує ефективність моніторингу інформаційної безпеки, забезпечує адаптивність системи захисту до змінних умов функціонування ІТКМ та дозволяє гнучко реагувати на широкий спектр сучасних кіберзагроз.

### Література

1. Zhang, Y., Lu, Y., Yang, G., & Luo, Z. (2022). Research on the Identification of Internet Critical Nodes Based on Multilayer Network Modeling. *Security and Communication Networks*. https://doi.org/10.1155/2022/2036370.
2. Hou, N., Wang, Z., Ho, D., & Dong, H. (2020). Robust Partial-Nodes-Based State Estimation for Complex Networks Under Deception Attacks. *IEEE Transactions on Cybernetics*, 50, 2793-2802. https://doi.org/10.1109/TCYB.2019.2918760.
3. Forti, N., Battistelli, G., Chisci, L., Li, S., Wang, B., & Sinopoli, B. (2018). Distributed Joint Attack Detection and Secure State Estimation. *IEEE Transactions on Signal and Information Processing over Networks*, 4, 96-110. https://doi.org/10.1109/TSIPN.2017.2760804.
4. Yang, W., Zheng, Z., Chen, G., Tang, Y., & Wang, X. (2020). Security Analysis of a Distributed Networked System Under Eavesdropping Attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67, 1254-1258. https://doi.org/10.1109/TCSII.2019.2928558.
5. Wan, L., Zhang, M., Li, X., Sun, L., Wang, X., & Liu, K. (2022). Identification of Important Nodes in Multilayer Heterogeneous Networks Incorporating Multirelational Information. *IEEE Transactions on Computational Social Systems*, 9, 1715-1724. https://doi.org/10.1109/TCSS.2022.3161305.
6. Wang, T., Li, Y., Chen, F., & Duan, S. (2022). Bayes-Based Distributed Estimation in Adversarial Multitask Networks. *IEEE Transactions on Aerospace and Electronic Systems*, 58, 4004-4019. https://doi.org/10.1109/TAES.2022.3158638.
7. Xi, B., Liu, H., Hou, B., Wang, Y., & Guo, Y. (2024). Stealing complex network attack detection method considering security situation awareness. *PLOS ONE*, 19. https://doi.org/10.1371/journal.pone.0298555.
8. Hu, D., Chen, Z., & Yin, F. (2021). Information Weighted Consensus With Interacting Multiple Model Over Distributed Networks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68, 1537-1541. https://doi.org/10.1109/TCSII.2020.3032963.
9. Cintuglu, M., & Ishchenko, D. (2019). Secure Distributed State Estimation for Networked Microgrids. *IEEE Internet of Things Journal*, 6, 8046-8055. https://doi.org/10.1109/JIOT.2019.2902793.
10. Gao, Q., & Xie, Z. (2024). Multi-Armed Bandit-Based User Network Node Selection. *Sensors (Basel, Switzerland)*, 24. https://doi.org/10.3390/s24134104.
11. Zhang, L., Wang, G., & Giannakis, G. (2018). Real-Time Power System State Estimation and Forecasting via Deep Unrolled Neural Networks. *IEEE Transactions on Signal Processing*, 67, 4069-4077. https://doi.org/10.1109/TSP.2019.2926023.
12. Ângelos, E., & Asada, E. (2016). Improving State Estimation With Real-Time External Equivalents. *IEEE Transactions on Power Systems*, 31, 1289-1296. https://doi.org/10.1109/PESGM.2016.7741743.
13. Monticelli, A. (2000). Electric power system state estimation. *Proceedings of the IEEE*, 88, 262-282. https://doi.org/10.1109/5.824004.

14. Boiko, J., Druzhynin, V., Buchyk, S., Pyatin, I. & Kulko, A. (2024). Methodology of FPGA Implementation and Performance Evaluation of Polar Coding for 5G Communications. *CEUR Workshop Proceedings*, 3654, 15-24. urn:nbn:de:0074-3654-7.

15. Семенко, А. І., Бойко, Ю. М., Шпур, О. М., Стрелковська, І. В., Корчинський, В. В., & Яровий, Р. О. (2024). *Сучасні технології інфокомунікаційних та комп'ютерних мереж: Монографія* (А. І. Семенко, Ред.). Європейський університет, ФО-П Білецький Р. Г., 557 с. ISBN 978-617-853-009-9. https://elar.khmnu.edu.ua/handle/123456789/17381.

## References

1. Zhang, Y., Lu, Y., Yang, G., & Luo, Z. (2022). Research on the Identification of Internet Critical Nodes Based on Multilayer Network Modeling. *Security and Communication Networks*. https://doi.org/10.1155/2022/2036370.

2. Hou, N., Wang, Z., Ho, D., & Dong, H. (2020). Robust Partial-Nodes-Based State Estimation for Complex Networks Under Deception Attacks. *IEEE Transactions on Cybernetics, 50*, 2793-2802. https://doi.org/10.1109/TCYB.2019.2918760.

3. Forti, N., Battistelli, G., Chisci, L., Li, S., Wang, B., & Sinopoli, B. (2018). Distributed Joint Attack Detection and Secure State Estimation. *IEEE Transactions on Signal and Information Processing over Networks, 4*, 96-110. https://doi.org/10.1109/TSIPN.2017.2760804.

4. Yang, W., Zheng, Z., Chen, G., Tang, Y., & Wang, X. (2020). Security Analysis of a Distributed Networked System Under Eavesdropping Attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs, 67*, 1254-1258. https://doi.org/10.1109/TCSII.2019.2928558.

5. Wan, L., Zhang, M., Li, X., Sun, L., Wang, X., & Liu, K. (2022). Identification of Important Nodes in Multilayer Heterogeneous Networks Incorporating Multirelational Information. *IEEE Transactions on Computational Social Systems, 9*, 1715-1724. https://doi.org/10.1109/TCSS.2022.3161305.

6. Wang, T., Li, Y., Chen, F., & Duan, S. (2022). Bayes-Based Distributed Estimation in Adversarial Multitask Networks. *IEEE Transactions on Aerospace and Electronic Systems, 58*, 4004-4019. https://doi.org/10.1109/TAES.2022.3158638.

7. Xi, B., Liu, H., Hou, B., Wang, Y., & Guo, Y. (2024). Stealing complex network attack detection method considering security situation awareness. *PLOS ONE, 19*. https://doi.org/10.1371/journal.pone.0298555.

8. Hu, D., Chen, Z., & Yin, F. (2021). Information Weighted Consensus With Interacting Multiple Model Over Distributed Networks. *IEEE Transactions on Circuits and Systems II: Express Briefs, 68*, 1537-1541. https://doi.org/10.1109/TCSII.2020.3032963.

9. Cintuglu, M., & Ishchenko, D. (2019). Secure Distributed State Estimation for Networked Microgrids. *IEEE Internet of Things Journal, 6*, 8046-8055. https://doi.org/10.1109/JIOT.2019.2902793.

10. Gao, Q., & Xie, Z. (2024). Multi-Armed Bandit-Based User Network Node Selection. *Sensors (Basel, Switzerland), 24*. https://doi.org/10.3390/s24134104.

11. Zhang, L., Wang, G., & Giannakis, G. (2018). Real-Time Power System State Estimation and Forecasting via Deep Unrolled Neural Networks. *IEEE Transactions on Signal Processing, 67*, 4069-4077. https://doi.org/10.1109/TSP.2019.2926023.

12. Ângelos, E., & Asada, E. (2016). Improving State Estimation With Real-Time External Equivalents. *IEEE Transactions on Power Systems, 31*, 1289-1296. https://doi.org/10.1109/PESGM.2016.7741743.

13. Monticelli, A. (2000). Electric power system state estimation. *Proceedings of the IEEE, 88*, 262-282. https://doi.org/10.1109/5.824004.

14. Boiko, J., Druzhynin, V., Buchyk, S., Pyatin, I., & Kulko, A. (2024). Methodology of FPGA Implementation and Performance Evaluation of Polar Coding for 5G Communications. *CEUR Workshop Proceedings, 3654*, 15-24. urn:nbn:de:0074-3654-7.

15. Semenko, A. I., Boiko, Yu. M., Shpur, O. M., Strelkovska, I. V., Korchynskyi, V. V., & Yarovyi, R. O. (2024). Suchasni tekhnolohii infokomunikatsiinykh ta komp'iuternykh merezh: Monohrafiia (A. I. Semenko, Red.). *Yevropeiskyi universytet, FO-P Biletskyi R. H.*, 557 s. ISBN 978-617-853-009-9. https://elar.khmnu.edu.ua/handle/123456789/17381.