КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1342
УДК 004.75: 004.056.2

Орленко Вікторія Сергіївна
к.т.н., доцент
Національна академія внутрішніх справ України, Київ, Україна
ORCID: 0000-0001-9601-1916
vorlenko80@ukr.net

Толюпа Сергій Васильович
д.т.н., професор,
професор кафедри кібербезпеки та захисту інформації
Київський національний університетіменіТараса Шевченка, Київ, Україна
ORCID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

Черниш Леся Григорівна
к.т.н, доцент
Державний науково-дослідний інституту технологій кібербезпеки та захисту інформації, Київ, Україна
ORCID: 0009-0004-9264-8863
l.chernysh@ws.cip.gov.ua

Кулько Андрій Аркадієвич
аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID:0009-0006-1185-0774
kulko452@gmail.com

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ БЕЗДРОТОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ ДІЇ ЗАВАД ТА КІБЕРВПЛИВУ

Анотація. Зростає обсяг інформації, яку передають люди. Більше людей користуються мобільними телефонами. Технології змінюються. Важливо, щоб бездротові інформаційно-комунікаційні системи (ІКС) працювали безперервно. Забезпечити це можна, якщо зберігати високу стійкість до перешкод, деструктивних завад та цілеспрямованого кібервпливу. Також важливо, щоб зв'язок був завжди доступний і не переривався. Це потрібно, навіть коли з'являються зовнішні або внутрішні проблеми, включаючи кібератаки на елементи мережі. Метою роботи є створення підходу для покращення бездротових інформаційно-комунікаційних систем, навіть коли є перешкоди та загрози інформаційній безпеці. В роботі показано сучасні підходи до підвищення функціональної стійкості бездротових інформаційно-комунікаційних систем шляхом комплексного використання методів балансування навантаження, адаптивного керування ресурсами мережі, завадостійкого кодування, інтелектуального аналізу параметрів каналів передачі, засобів виявлення кібератак та сучасних мережевих архітектур. Ідея в тому, щоб використовувати технології програмно-керованих мереж, периферійних обчислень та алгоритмів машинного навчання для оптимізації процесів передавання інформації та виявлення кібератак у комунікаційних системах. Розглянуто основні речі, які впливають на роботу бездротових мереж. Проаналізовано існуючі методи оцінювання ризиків втрати доступу до комунікаційних послуг через завади та кібернапади. І запропоновано комплексний підхід, щоб краще використовувати мережеві ресурси та протидіяти загрозам. Застосування цих підходів на практиці дасть можливість підвищити доступність комунікаційних послуг, зменшити вплив різноманітних завад і кібератак, оптимізувати використання каналів передавання інформації та забезпечити належний рівень надійності та захисту сучасних інформаційно-комунікаційних систем.

Ключові слова: завадостійкість, передавання інформації, балансування навантаження, функціональна стійкість, інформаційна безпека, кібервплив, кібератаки, адаптивне керування, якість обслуговування, мережеві ресурси.

ВСТУП

Сьогодні майже всі галузі нашого життя залежать від сучасних технологій. Це стосується бізнесу, управління країною, виробництва, охорони здоров'я, освіти та оборони. Більшість важливих послуг використовують мобільний інтернет, що дозволяє людям рухатися вільно, швидко отримувати інформацію та розширювати можливості зв'язку.

Паралельно зі збільшенням кількості користувачів значно зростають обсяги інформаційного трафіку. Сьогодні ми бачимо, як усе більше технологій Інтернету, індустріального Інтернету, систем штучного інтелекту, автономного транспорту, хмарних сервісів використовуються. Це призводить до того, що наш Інтернет стає переповненим. За таких умов особливо важливо, щоб наші інформаційно-комунікаційні системи працювали стабільно. Вони повинні мати можливість швидко адаптуватися до змін, реагувати на проблемні ситуації, витримувати зовнішні кібервпливи та підтримувати належний рівень якості передачі інформації [1]

Сучасні бездротові системи працюють у умовах, коли навколишнє середовище постійно змінюється, а загрози безпеці зростають. На якість передачі інформації впливають електромагнітні завади, багатопроменеве поширення сигналів, перевантаження окремих сегментів мережі, обмеженість спектрального ресурсу, зміна топології мережі, висока мобільність користувачів, значна кількість одночасних сеансів зв'язку, а також цілеспрямовані кібератаки, такі як відмова у обслуговуванні (DDoS) [2], підробка маршрутів або створення навмисних радіозавад. Вплив всіх цих факторів може призводити до втрати пакетів даних, збільшення затримок, зменшення пропускної здатності каналів передачі, компрометації даних та погіршення показників доступності комунікаційних сервісів [3-4]

У сучасних умовах недостатньо забезпечити лише високу швидкість передачі інформації або простий захист від завад. Саме тому сучасні інформаційно-комунікаційні системи активно використовують адаптивні алгоритми маршрутизації [5], інтелектуальні методи керування ресурсами, механізми автоматичного балансування навантаження, засоби прогнозування стану мережі та підсистеми протидії кібератакам.

Важливу роль у забезпеченні функціональної стійкості та кіберзахисту відіграють сучасні технології програмно-керованих мереж, віртуалізації мережевих функцій, периферійних обчислень, а також використання алгоритмів машинного навчання для прогнозування перевантажень мережі, виявлення аномалій, обумовлених кібервпливом, та автоматичного прийняття рішень щодо перерозподілу мережевих ресурсів. Такі технології дозволяють зробити роботу мереж більш ефективною та захищеною, навіть коли передається великий об’єм даних в умовах активних дій зловмисників [6].

З розвитком мереж з’являються кращі способи передавати інформацію без помилок і захищати її від перехоплення чи спотворення. Дуже часто застосовують адаптивні методи кодування, різні способи модуляції, керування потужністю, алгоритми завадостійкості та криптографічний захист, які добре використовують спектр та забезпечують цілісність даних [7].

Їх комплексне застосування дозволяє суттєво підвищити ймовірність правильного приймання інформації навіть у складних умовах функціонування бездротових мереж та під час кібератак [8]

Незважаючи на значну кількість наукових досліджень у сфері забезпечення завадостійкості та інформаційної безпеки, питання комплексного поєднання методів балансування навантаження, адаптивного керування ресурсами, оцінювання ризиків функціонування, виявлення кібератак та сучасних технологій інтелектуального управління залишаються недостатньо дослідженими. Особливо це стосується високонавантажених інформаційно-комунікаційних систем, в яких одночасно потрібно забезпечувати високу продуктивність, мінімальні затримки передачі даних, надійність, стійкість до різних видів завад та захищеність від кібервпливу [9]

У цьому випадку потрібно знайти нові способи зробити бездротові інформаційно-комунікаційні системи більш ефективними та безпечними. Для цього потрібно створити комплексні моделі. Ці моделі поєднують традиційні методи оцінювання завадостійкості з сучасними засобами керування мережевими ресурсами та аналізу загроз кібербезпеці. Також потрібно використовувати інтелектуальні алгоритми. Ці інтелектуальні алгоритми допомагають приймати рішення в умовах завад і кібератак. Ці моделі повинні бути такими, щоб вони могли адаптуватися до різних ситуацій. Вони повинні забезпечувати стабільну роботу систем. Це дуже важливе завдання, оскільки бездротові інформаційно-комунікаційні системи використовуються майже скрізь і часто стають ціллю для кібернападів [10].

Проблематика забезпечення ефективного та захищеного функціонування бездротових інформаційно-комунікаційних систем протягом останніх років залишається одним із ключових напрямів розвитку сучасних телекомунікаційних технологій.

Українські та зарубіжні науковці зробили фундаментальний та прикладний внесок у розробку методів протидії навмисним завадам, виявлення кібератак і підвищення пропускної здатності бездротових

мереж (зокрема спеціального та подвійного призначення): Олександр Зеленський, Володимир Поповський, Валерій Безрук, Олександр Лемешко, Олександр Кузнецов, Ігор Рубан, Володимир Бурячок, Олександр Корченко, Сергій Євсеєв, Михайло Климаш, Андрій Лунтовський, Клод Шеннон, Бернард Відроу, Ендрю Вітербі, H. Vincent Poor Andrea Goldsmith, David Tse та інші.

Результати численних наукових досліджень свідчать, що традиційні методи побудови інформаційно-комунікаційних мереж уже не забезпечують необхідного рівня ефективності та безпеки в умовах інтенсивного інформаційного навантаження та активного кібервпливу [11]. Разом із цим суттєво збільшується складність управління мережевими ресурсами та захисту даних. За умов високої мобільності користувачів, постійної зміни структури інформаційних потоків, нерівномірного розподілу навантаження та наявності потенційних кібератак виникає необхідність застосування інтелектуальних алгоритмів підтримки прийняття рішень [12].

Ці інтелектуальні алгоритми підтримки прийняття рішень повинні бути здатними прогнозувати зміну стану мережі та виявляти аномалії трафіку ще до виникнення критичних перевантажень або успішного здійснення кібератаки. Завдяки цьому можна запобігти проблемам у роботі мережі, нейтралізувати кібервплив та забезпечити її стабільну роботу [13]. Такі інтелектуальні алгоритми підтримки прийняття рішень можуть бути дуже корисними для мобільних мереж. Вони можуть допомогти передбачити проблеми, ідентифікувати кібератаки та вирішити їх до того, як вони стануть серйозними. Таким чином, застосування інтелектуальних алгоритмів підтримки прийняття рішень може бути дуже важливим для забезпечення стабільності та захищеності мережі. Даною проблематикою займалися та займаються вітчизняні науковці та закордонні.

Після аналізу стало зрозуміло, що найперспективніший напрям розвитку бездротових інформаційно-комунікаційних систем полягає у поєднанні класичних методів забезпечення стабільності та завадостійкості з сучасними технологіями адаптивного керування ресурсами мережі та засобами протидії кібервпливам. Це включає автоматичне балансування навантаження, виявлення кібератак, прогнозування стану мережі та інтелектуальну підтримку прийняття рішень. Якщо поєднати ці підходи, можна створити продуктивні, надійні, захищені і масштабовані інформаційно-комунікаційні системи нового покоління [14].

Проведений аналіз сучасного стану розвитку бездротових інформаційно-комунікаційних систем свідчить, що збільшення кількості користувачів, розширення спектра інформаційних сервісів, зростання кількості кіберзагроз та впровадження нових телекомунікаційних технологій супроводжується суттєвим зростанням вимог до якості та безпеки функціонування мережевої інфраструктури. Зростає кількість інформації, яка проходить через мережу. Структура мережі стає складнішою. Тому більше ймовірність, що деякі частини мережі будуть перенавантажені або піддадуться кібератакам особливо це стосується критичної інфраструктури [15].

Саме вирішенню зазначеної наукової проблеми присвячено дане дослідження. Метою цієї статті є підвищення ефективності функціонування бездротових інформаційно-комунікаційних мереж в умовах дії завад та кібервпливу. Це відбувається шляхом з'єднання різних методів: оцінки ризиків, які можуть призвести до відмови зв’язку або порушення безпеки, алгоритмів, які розподіляють навантаження, способів, як керувати мережевими ресурсами, аналізу загроз кібербезпеці і нових технологій, щоб інформація передавалася без помилок та була захищена.

Сучасні бездротові інформаційно-комунікаційні системи характеризуються високим рівнем складності, багаторівневою архітектурою та значною кількістю взаємопов'язаних компонентів, що забезпечують процеси передавання, маршрутизації, оброблення, захисту та зберігання інформації. Вони повинні мати деякі важливі характеристики [16]. До них належать велика здатність передавати інформацію, мінімальна затримка передачі інформації, ефективне використання частот, можливість розширення, надійність роботи, захист інформації від кібервпливу та можливість адаптуватися до змін умов використання та загрозового середовища. Виконання цих вимог є необхідним для забезпечення якісної та безпечної роботи інформаційних сервісів, критично важливих об'єктів інфраструктури, систем автоматизованого управління, промислових мереж, транспортних комплексів та інших сучасних цифрових платформ [17].

Одним із наиболее перспективних напрямів розвитку сучасних інформаційно-комунікаційних систем є застосування концепції програмно-керованих мереж (Software Defined Networking). Основною особливістю такого підходу є відокремлення площини передавання інформації від площини керування мережею [18].

Централізований контролер SDN знає абсолютно все про стан усіх мережевих вузлів, а також про поточні ризики кібербезпеки. Він аналізує, яким чином навантажуються канали зв'язку, дивиться на параметри інформації, яка передається, аналізує трафік на наявність ознак кібератак і створює найкращі правила для того, щоб дані рухались найбільш оптимальним та безпечним шляхом. Це означає, що

контролер може дуже швидко реагувати на зміни мережі, завади чи виявлений кібервплив. Це значно краще, ніж традиційні системи, де кожен вузол сам вирішує, куди відправляти інформацію і як захищатися.

Програмно-керовані мережі мають багато переваг. Вони дозволяють швидко перенаправляти інформацію між різними частинами мережі, якщо це потрібно, зокрема для ізоляції уражених кібератакою вузлів. Вони можуть автоматично шукати альтернативні маршрути, якщо основний шлях зайнятий або перебуває під дією радіозавад чи DDoS-атаки. Вони швидко виявляють вузли, які перевантажені інформацією або атакуються зловмисниками, і допомагають використовувати канали зв'язку найефективніше. Це робить мережу дуже гнучкою, безпечною і здатною швидко адаптуватися до змін [19].

Додатковою перевагою SDN є можливість інтеграції із системами машинного навчання, що дозволяє прогнозувати розвиток мережевої ситуації, виявляти складні аномалії трафіку, характерні для кібератак, та приймати рішення ще до виникнення критичних перевантажень чи порушень безпеки [20].

Зростання обсягів інформаційного трафіку та потреби в локальному аналізі загроз призводить до збільшення затримок під час взаємодії із централізованими хмарними сервісами. Одним із найбільш ефективних шляхів вирішення цієї проблеми є використання технології периферійних обчислень.

Основною ідеєю периферійних обчислень є перенесення частини процесів оброблення інформації та аналізу безпеки максимально близько до джерела її виникнення. Це дозволяє істотно скоротити час передавання даних, зменшити навантаження на магістральні канали зв'язку, швидше виявляти локальні кібератаки та підвищити швидкодію інформаційної системи.

Особливо добре працює використання периферійних обчислень у тих випадках, коли потрібно миттєво реагувати, наприклад, у автономному транспорті, промислових мережах, медичних інформаційних системах та інфраструктурі Інтернету, а також при відбитті кібератак у реальному часі. Це тому, що системи периферійних обчислень можуть обробляти інформацію та перевіряти її безпеку прямо там, де вона з'являється, без потреби відправляти її до центру для обробки.

Коли поєднати периферійні обчислення з програмно-керованими мережами, можна створити дуже гнучку та захищену систему керування ресурсами. У цій системі локальні рішення та первинна фільтрація шкідливого трафіку приймаються прямо на периферії мережі, тобто там, де знаходяться пристрої, які збирають інформацію. А центральний контролер займається стратегічним плануванням і глобальною безпекою, тобто визначає загальні цілі, напрямки та правила протидії кібервпливам. Це дозволяє зробити управління мережею та її кіберзахист більш ефективним і швидким.

Забезпечення високого рівня функціональної стійкості та безпеки бездротових інформаційно-комунікаційних систем потребує комплексного врахування значної кількості факторів, що впливають на процес передачі інформації. До таких факторів належать інтенсивність інформаційного трафіку, рівень електромагнітних та деструктивних завад, наявність і тип кібератак (DDoS, підробка даних, впровадження хибних вузлів), характеристики каналів зв'язку, завантаженість мережевих вузлів, імовірність відмов обладнання, якість маршрутизації та ефективність використання мережевих ресурсів [21].

На відміну від традиційних моделей, що орієнтовані на аналіз окремих характеристик мережі, запропонований підхід базується на комплексному оцінюванні функціонального стану та рівня безпеки системи, що дозволяє врахувати взаємозалежність між окремими параметрами, виявляти кібервплив та своєчасно реагувати на зміну умов функціонування.

Першим етапом моделювання є визначення інтегрального показника функціональної ефективності та безпеки системи, який враховує вплив факторів ризику (включаючи ризики кібератак) на доступність інформаційно-комунікаційних сервісів.

Для оцінювання ризику системи підвищення доступності послуг та якості функціонування комунікаційної системи в умовах завад і кібервпливу використовують величину середньозваженого модуля відхилення ризику доступності R (при $\sum_{i=1}^{n} p_i = 1$):

$$R = \sum_{i=1}^{n} p_i K_{d,i} \, | \upsilon_i - \bar{\upsilon} |, \quad (1)$$

де: p_i - ймовірність небажаного впливу каналу передачі інформації (що враховує як рівень природних і навмисних завад, так і ймовірність здійснення кібератаки на i- й канал);

$K_{d,i}$ - коефіцієнт доступності;

υ_i - величина втрат каналу передачі (включаючи втрати даних від дій зловмисників);

$\bar{\upsilon}$ - середнє значення показника втрат.

Показник, визначений співвідношенням (1), дозволяє отримати узагальнену оцінку функціонального стану мережі та визначити ступінь впливу окремих факторів, завад і кібератак на ефективність передавання інформації. Його використання забезпечує можливість кількісного порівняння різних варіантів побудови та захисту інформаційно-комунікаційної системи та вибору найбільш ефективної й безпечної конфігурації.

Наступним етапом дослідження є оцінювання ризику втрати доступності інформаційних сервісів залежно від параметрів функціонування мережі та рівня кіберзагрози.

$$R_{loss} = f(p_i, K_{d,i}, \upsilon_i) \quad . \quad (2)$$

Отримана залежність дозволяє встановити кількісний взаємозв'язок між характеристиками інформаційного середовища, інтенсивністю кібервпливу та ймовірністю виникнення критичних ситуацій у процесі функціонування мережі. Аналіз отриманих результатів свідчить, що навіть незначне збільшення інтенсивності інформаційного навантаження або здійснення локальної кібератаки за відсутності механізмів адаптивного керування та захисту може призводити до суттєвого погіршення показників доступності інформаційних сервісів.

Для оцінювання впливу параметрів каналів зв'язку та загрозового середовища на загальну ефективність функціонування інформаційно-комунікаційної системи використовується наступне співвідношення.

Якщо врахувати коефіцієнт доступності та негативні відхилення від запланованого значення параметра $K_{d,i}$, то ступінь доступності та функціонування захисту інформації в умовах завад і кібератак оцінюється показником варіації V:

$$V = \frac{\sqrt{\sum_{i=1}^{n} p_i \delta_i (K_{d,i} - \bar{K}_d)^2}}{}, \quad (3)$$

де δ_i – індикатор несприятливих відхилень доступності комунікаційної системи, якому відповідають: для сприятливого відхилення $\delta_i = 0$, для несприятливого (викликаного завадами чи кібератакою) $\delta_i = 1$; $\bar{K}_d$ – середнє заплановане значення коефіцієнта доступності.

Використання співвідношення (3) дозволяє оцінити зміну ефективності функціонування та рівня захисту мережі залежно від характеристик каналу передавання інформації, рівня зовнішніх завад та наявності кібервпливів. Практичні результати моделювання показують, що найбільш суттєвий вплив на функціональну стійкість системи мають перевантаження окремих мережевих вузлів, цілеспрямовані кібератаки на виведення з ладу елементів мережі, нестабільність характеристик бездротового середовища та недостатня ефективність алгоритмів балансування навантаження і захисту.

Завершальним етапом математичного опису базової моделі є визначення інтегрального показника оцінювання ефективності та безпеки функціонування інформаційно-комунікаційної системи E_{int}:

$$E_{\text{int}} = \frac{\Delta^+}{\Delta^-},$$

де: Δ^+ - ймовірна величина сприятливих відхилень доступності;

Δ^- - ймовірна величина несприятливих відхилень доступності (спричинених завадами, деструктивним кібервпливом та перевантаженнями).

Це інший підхід, ніж той, який використовується в окремих місцевих випадках. Інтегральний показник дозволяє брати до уваги вплив різних факторів, включаючи завади і кібератаки, і давати загальну оцінку стану та захищеності мережі. Це дає змогу застосовувати методи адаптивного керування ресурсами та кіберзахисту. Це також дозволяє автоматично приймати рішення про зміну параметрів роботи системи зв’язку та активацію засобів протидії загрозам.

З метою адаптації запропонованої моделі до сучасних бездротових мереж доцільно врахувати коефіцієнт використання мережевих ресурсів K_{res}:

$$K_{res} = \frac{B_{used}}{B_{total}},$$

де: B_{used} - поточний обсяг використаної пропускної здатності (включаючи аналіз частки аномального трафіку кібератак);

B_{total} - загальна доступна пропускна здатність мережі.

Запропонований коефіцієнт дозволяє оцінити рівень завантаженості інформаційно-комунікаційної системи, виявити аномальні сплески трафіку при DDoS-атаках та визначити момент переходу мережі до режиму критичного навантаження.

Наступним важливим показником є інтегральний коефіцієнт якості та безпеки функціонування Q:

$$Q = \alpha_1 P_{succ} + \alpha_2 K_d - \alpha_3 P_{loss} - \alpha_4 P_{cyber},$$

де: P_{succ} - імовірність успішного та коректного передавання пакета;

K_d - нормований показник доступності сервісу;

P_{loss} - коефіцієнт втрати пакетів;

P_{cyber} - ймовірність реалізації загрози кібервпливу на каналі;

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ - вагові коефіцієнти, що визначають значущість відповідних параметрів.

Цей показник розглядає кілька характеристик одночасно, поєднуючи параметри якості обслуговування та рівень кібербезпеки.

Для кращого балансування навантаження та виявлення аномального перерозподілу трафіку під час кібератак варто використовувати коефіцієнт нерівномірності використання мережевих вузлів K_{unev}:

$$K_{unev} \frac{\sigma L}{L},$$

де: σ_L - середньоквадратичне відхилення навантаження між вузлами мережі;

L - середнє навантаження мережі.

Чим менше значення K_{unev}, тим більш рівномірно розподіляється інформаційне навантаження і тим краще використовуються наявні ресурси мережі, що також знижує вразливість системи до кібератак на окремі вузли.

Ця модель може стати основою для створення розумних систем підтримки прийняття рішень, які можуть автоматично керувати мережевими ресурсами та засобами кіберзахисту, навіть якщо навколишнє середовище змінюється дуже швидко і відбуваються постійні кібернапади.

Таким чином, на основі досліджень та аналізу методів підвищення доступності комунікаційних послуг завадостійкими та захищеними бездротовими каналами передачі даних інформаційно-комунікаційних систем, можливо зробити висновок, що завдання підвищення доступності послуг при оптимальному та якісному захисті потоків даних полягає у використанні всіх властивостей таких корисних сигналів, завад, факторів кібервпливу та каналів передачі для підвищення доступності комунікаційних послуг, ймовірності їх правильного прийому та захищеності від викривлення чи перехоплення. Для збільшення доступності комунікаційних послуг та ймовірності правильного, завадостійкого і безперебійного їх прийому має бути проведене попереднє оброблення таких сигналів та фільтрація трафіку, що забезпечує значне збільшення відношення сигналів та завад і відсікання шкідливого кібервпливу. Завадостійкі та захищені бездротові канали передачі інформації застосовують нові технології, які дозволяють у режимі роботи в реальному часі гарантувати підвищення доступності комунікаційних послуг для якісної, вірогідної та безпечної передачі потоків даних в умовах впливу різнотипних завад і кібератак. Це забезпечує необхідні значення показників вірогідності завадостійкої та захищеної передачі, що здійснюється за рахунок використання необхідного виду та типу кодування, криптографічного захисту та динамічного аналізу трафіку. Знаючи всі властивості сигналів, завад, ознаки кібератак, види та типи комунікаційних послуг, можна встановити певні відмінності між ними і використати їх для розроблення способів та методів забезпечення завадостійкої і безпечної передачі для доступності таких послуг. Застосування подібних методів, способів та засобів побудови сучасних

завадостійких і кіберстійких каналів бездротових інформаційно-комунікаційних систем в умовах дії завад та кібервпливу дозволить будувати надійні канали передачі даних та підвищити доступність послуг.

Як критерії ефективності використовувалися показники доступності інформаційних сервісів, середній час передавання пакетів, коефіцієнт втрати інформації, рівень використання пропускної здатності каналів зв'язку, показники виявлення та нейтралізації кібератак та інтегральний показник функціональної стійкості і безпеки системи. Такий підхід дозволяє комплексно оцінити роботу інформаційно-комунікаційної системи в умовах змінних параметрів середовища та наявності загроз інформаційній безпеці.

Проведений аналіз показує, що при невисокому рівні навантаження та відсутності кібератак ефективність функціонування традиційних і вдосконалених алгоритмів практично не відрізняється. Це пояснюється достатнім резервом пропускної здатності мережі та незначною кількістю конфліктів під час передавання інформації.

Проте зі збільшенням інтенсивності інформаційних потоків та виникненням дій зловмисників (кібератак чи навмисних радіозавад) ситуація істотно змінюється. У традиційних мережах спостерігається нерівномірне використання окремих вузлів, що призводить до виникнення локальних перевантажень, уразливості до точкових кібервпливів, збільшення часу очікування пакетів у чергах та зростання ймовірності повторного передавання інформації або відмови обслуговування. Ефективність використання мережевих ресурсів зменшується з часом, а сервіси стають менш доступними і захищеними.

Комплексний підхід дозволяє вчасно бачити, де мережа перенавантажена або піддається кібератаці, і автоматично перенаправляти дані на інші, безпечні шляхи. Це допомагає більш рівномірно використовувати мережу, зменшити кількість перенавантажених та уразливих точок і зробити доставку інформації швидшою та надійною.

Особливе значення має використання інтегрального показника функціональної ефективності та безпеки, який дозволяє одночасно враховувати кілька взаємопов'язаних характеристик мережі, включаючи фактори ризику кіберзагроз. На відміну від традиційних підходів, які базуються лише на одному критерії оцінювання, ця система забезпечує більш об'єктивне відображення поточного стану та захищеності інформаційно-комунікаційної системи. Це значно полегшує прийняття ефективних рішень щодо зміни режимів її функціонування та активації методів кіберзахисту. Крім того, ця система має ще одну перевагу. Вона дозволяє легко інтегруватися із сучасними технологіями програмно-керованих мереж.

Централізований контролер цієї системи отримує інформацію про стан усіх мережевих вузлів та наявність аномалій, характерних для кібератак. Після цього він оцінює рівень їх завантаження та безпеки, прогнозує можливі перевантаження чи наслідки кібервпливу та автоматично змінює правила маршрутизації інформаційних потоків і конфігурацію захисту. Це робить її дуже корисною для різних застосувань. Це забезпечує скорочення часу реакції системи на зміну умов функціонування та дії кіберзловмисників і підвищує ефективність використання наявних ресурсів.

Використання технологій периферійних обчислень також добре впливає на загальну продуктивність та безпеку системи. Коли частина інформації та первинний аналіз аномалій трафіку обробляються прямо біля джерела її виникнення, навантаження на магістральні канали зв'язку зменшується, а кібератаки локалізуються на ранніх стадіях. Затримки передавання інформації скорочуються, а швидкість реагування інформаційно-комунікаційної системи на зовнішні події та кібернапади підвищується.

Важливою перевагою цього підходу є можливість використання алгоритмів машинного навчання для прогнозування майбутнього стану мережі та автоматичного виявлення нових типів кібератак. Аналіз статистичних даних щодо навантаження каналів зв'язку, інтенсивності інформаційних потоків, профілів трафіку та історії виникнення аномалій і перевантажень дозволяє робити прогнози щодо можливих змін параметрів функціонування системи та потенційних кіберзагроз. Це дозволяє своєчасно здійснювати необхідне балансування ресурсів та вживати превентивних заходів кіберзахисту.

Комплексне використання класичних математичних моделей оцінювання ризиків і сучасних інтелектуальних методів керування ресурсами та безпекою забезпечує істотне підвищення функціональної стійкості бездротових інформаційно-комунікаційних систем. При цьому найбільший ефект досягається саме під час високого навантаження та активного кібервпливу, коли звичайні алгоритми вже не дають необхідної продуктивності та захищеності.

Результати проведеного дослідження підтверджують доцільність використання інтегрованого підходу до керування та захисту бездротових інформаційно-комунікаційних систем. Поєднання оцінювання ризиків, адаптивного балансування навантаження, виявлення кібератак, прогнозування розвитку мережевої ситуації та інтелектуального керування ресурсами створило умови для побудови високопродуктивних і захищених інформаційних систем нового покоління. Вони можуть забезпечувати стабільне функціонування навіть тоді, коли відбувається значне інформаційне навантаження, дія зовнішніх завад та цілеспрямований кібервплив. Це дозволяє їм працювати без перебоїв у будь-яких

умовах. Таким чином, системи нового покоління стають ще надійнішими, безпечнішими та ефективними. Практична цінність запропонованого підходу полягає в можливості його застосування під час проектування, модернізації та експлуатації сучасних бездротових інформаційно-комунікаційних систем різного призначення. Розроблена математична модель може використовуватися як основа для створення програмних засобів підтримки прийняття рішень, що забезпечують автоматизоване керування мережевими ресурсами та заходами кіберзахисту в режимі реального часу.

Отримані результати можуть бути використані під час побудови корпоративних бездротових мереж, інформаційних систем органів державного управління, промислових телекомунікаційних комплексів, мереж Інтернету речей, транспортних інформаційних систем, а також телекомунікаційної інфраструктури критично важливих об'єктів, що є першочерговими мішенями для кібератак.

Запропонований підхід також може бути інтегрований у сучасні програмно-керовані мережі, що забезпечить автоматичну адаптацію параметрів функціонування та політик безпеки до зміни навантаження, характеристик каналів зв'язку, умов експлуатації та загроз кібербезпеці.

Крім того, результати дослідження можуть бути використані як теоретична основа для подальших наукових робіт, спрямованих на розроблення інтелектуальних методів керування та захисту бездротових мереж нового покоління, використання технологій штучного інтелекту для виявлення складних кібератак та побудову самокерованих і самозахищених інформаційно-комунікаційних систем.

ВИСНОВКИ ТА НАПРЯМКИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі проведено дослідження сучасних підходів до забезпечення ефективного та захищеного функціонування бездротових інформаційно-комунікаційних систем. Під час дослідження встановлено, що ефективність функціонування сучасних інформаційно-комунікаційних систем залежить не тільки від окремих характеристик каналів передавання інформації, а й від комплексної взаємодії параметрів мережевого навантаження, структури інформаційних потоків, рівня електромагнітних завад, загрозового середовища кібербезпеки, ефективності алгоритмів маршрутизації та механізмів адаптивного керування ресурсами і кіберзахистом. Тому використання локальних критеріїв оцінювання без урахування чинників кібервпливу не забезпечує достатньої точності під час аналізу функціонального стану та надійності мережі.

На основі результатів дослідження запропоновано підхід до підвищення ефективності та безпеки функціонування бездротових інформаційно-комунікаційних систем. Це поєднання класичних математичних моделей оцінювання ризиків із сучасними технологіями програмно-керованих мереж, периферійних обчислень, адаптивного балансування навантаження, засобів виявлення кібератак та інтелектуального керування мережевими ресурсами. Це дозволяє своєчасно виявляти потенційні перевантаження та кібернапади, прогнозувати зміну стану мережі та автоматично змінювати параметри її функціонування й конфігурацію захисту відповідно до поточної інформаційної ситуації.

Проведений аналіз підтвердив, що використання адаптивних механізмів балансування навантаження та інтелектуального аналізу загрозового стану забезпечує більш ефективне використання пропускної здатності каналів зв'язку, скорочує середній час передавання інформації, зменшує ймовірність втрати пакетів, нейтралізує наслідки кібервпливів та підвищує загальну доступність інформаційних сервісів. Найбільший ефект досягається за умов високого навантаження та наявності деструктивних зовнішніх впливів, коли традиційні алгоритми маршрутизації та захисту вже не забезпечують необхідної продуктивності та безпеки.

Перспективним напрямом подальших досліджень є розроблення інтелектуальних алгоритмів самоорганізації та самозахисту бездротових мереж із використанням технологій штучного інтелекту, цифрових двійників телекомунікаційних систем, предиктивної аналітики загроз та механізмів автономного керування мережевими ресурсами й кіберзахистом у реальному масштабі часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Al-Jawad, A., Shah, P., Toseef, U. (2021). Deep reinforcement learning for dynamic routing in software-defined networks. IEEE Access, 9, 122818–122833.
2. Толюпа С.В. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз / Лукова-Чуйко Н.В., С.В. Толюпа, В.С. Наконечний, Браіловський М.М.: монографія - К.: Формат, 2021. – 407 с.
3. Swain, S., Sahoo, K. S., Mishra, A., Jhanjhi, N. Z., Humayun, M. (2023). Intelligent traffic engineering with security enforcement in Software Defined Networks. IEEE Access, 11, 23410–23425.

4. В.М Джулій, Ю.П. Кльоц, В.С. Орленко [та ін.] / Підвищення функціональності і стабільності завадостійких бездротових інформаційно-комунікаційних систем // Вісник Хмельницького національного університету. Технічні науки. – 2021. – №1. – С. 12-16.
5. Лемешко, О. В., Єременко, О. С., Невзорова, О. С. (2021). Модель адаптивної маршрутизації в Software-Defined Networks з дотриманням вимог щодо якості обслуговування. Телекомунікаційні та інформаційні технології, (1), 45–56/
6. Tang, F., Mao, B., Zubair, M., & Kato, N. (2021). Joint power and resource allocation for ultra-reliable low-latency communication in 6G: A deep reinforcement learning approach. IEEE Wireless Communications, 28(2), 24–31.
7. Shah S. D. A., Gregory M. A., Bouhafs F., Den Hartog F. Artificial Intelligence-Defined Wireless Networking for Computational Offloading and Resource Allocation in Edge Computing Networks // IEEE Open Journal of the Communications Society. 2024. Vol. 5. P. 2039–2057.
8. Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 24(2), 767–809.
9. Лемешко, О. В., Єременко, О. С., Baavenko, А. В. (2022). Комплексна модель адаптивної маршрутизації та забезпечення живучості телекомунікаційних мереж при кібератаках. Захист інформації, 24(2), 89–101.
10. Поповський, В. О., Лошаков, В. А., Кляпчук, М. В. (2021). Інтелектуальні методи управління ресурсами в умовах деструктивних впливів та завад. Телекомунікаційні та інформаційні технології, (3), 12–23
11. Руслан Політанський, Валентин Лесінський, Сергій Галюк, Андрій Кулько. Методи визначення рівноважного стану мережі із заданими потоками у вузлах інформаційних мереж кіберфізичних систем. (2025). Безпека інформаційних систем і технологій, *1*(9), 93-101. https://doi.org/10.17721/ISTS.2025.9.93-101.
12. Alhashimi, H. F., Hindia, M. N., Nguyen, Q. N. (2023). A survey on resource management for 6G heterogeneous networks: Current research, future trends, and challenges. Electronics, 12(3), 647.
13. Наталія Лукова-Чуйко, Сергій Толюпа, Іван Пархоменко. Методи виявлення вторгнень у сучасних системах IDS. (2021). Безпека інформаційних систем і технологій, *1*(5), 19-26. https://doi.org/10.17721/ISTS.2021.1.17-24.
14. Лемешко, О. В., Єременко, О. С., Родіонов, А. В. (2021). Модель забезпечення живучості та завадостійкості бездротових мереж зв'язку в умовах деструктивних впливів. Телекомунікаційні та інформаційні технології, (4), 15–28.
15. Сергій Толюпа, Анатолій Шевченко, Андрій Кулько Особливості забезпечення безпеки критичних інфраструктур. (2024). Безпека інформаційних систем і технологій, *1*(7), 11-23. https://doi.org/10.17721/ISTS.2024.7.11-23.
16. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Siamwalla, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.
17. Al-Jawad, A., Shah, P., Toseef, U. (2021). Deep reinforcement learning for dynamic routing in software-defined networks. IEEE Access, 9, 122818–122833.
18. Беркман, Л. Н., Захарченко, М. В., & Скрипник, О. В. (2022). Моделі та засоби підвищення безпеки та стійкості програмно-конфігурованих мереж. Захист інформації, 24(1), 35–46.
19. Юрій Кравченко, Олена Фісун. Метод забезпечення функціональної стійкості програмно-керованих мереж в умовах впливу кібератак. (2025). Безпека інформаційних систем і технологій, 2(10), 83-95. https://doi.org/10.17721/ISTS.2025.10.83-95.
20. Verma S., Rodrigues T. K., Kawamoto Y., Fouda M. M., Kato N. A Survey on Multi-AP Coordination Approaches over Emerging WLANs: Future Directions and Open Challenges. 2023. arXiv:2306.04164.
21. Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Simpson, S., White, Y., & Mauthe, A. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8), 1245–1265.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Viktoriia Orlenko
Ph.D. in Technical Sciences, Associate Professor
National Academy of Internal Affairs of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-9601-1916
vorlenko80@ukr.net

Serhii Toliupa
Doctor of Technical Sciences, Professor
Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

Lesia Chernysh
PhD in Technical Sciences, Associate Professor
State Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
ORCID: 0009-0004-9264-8863
l.chernysh@ws.cip.gov.ua

Andrii Kulko
Postgraduate Student of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0009-0006-1185-0774
kulko452@gmail.com

IMPROVING THE EFFICIENCY OF WIRELESS INFORMATION AND COMMUNICATION SYSTEMS IN THE FACE OF INTERFERENCE AND CYBERATTACKS

Abstract. The volume of information transmitted by people is growing. More people are using mobile phones. Technology is changing. It is important that wireless information and communication systems (ICS) operate continuously. This can be ensured by maintaining high resilience to interference, destructive disruptions, and targeted cyberattacks. It is also important that communication remains constantly available and uninterrupted. This is necessary even when external or internal problems arise, including cyberattacks on network components. The aim of this work is to develop an approach for improving wireless information and communication systems, even in the presence of interference and threats to information security. This work presents modern approaches to enhancing the functional resilience of wireless information and communication systems through the integrated use of load balancing methods, adaptive network resource management, error-correcting coding, intelligent analysis of transmission channel parameters, cyberattack detection mechanisms, and modern network architectures. The idea is to use software-defined networking technologies, edge computing, and machine learning algorithms to optimize information transmission processes and detect cyberattacks in communication systems. The paper examines the key factors that influence the operation of wireless networks. Existing methods for assessing the risks of losing access to communication services due to interference and cyberattacks are analyzed. A comprehensive approach is proposed to make better use of network resources and counter threats. The practical application of these approaches will make it possible to improve the availability of communication services, reduce the impact of various interferences and cyberattacks, optimize the use of information transmission channels, and ensure an adequate level of reliability and security for modern information and communication systems.

Keywords: interference resilience, information transmission, load balancing, functional resilience, information security, cyber impact, cyberattacks, adaptive control, quality of service, network resources.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Al-Jawad, A., Shah, P., Toseef, U. (2021). Deep reinforcement learning for dynamic routing in software-defined networks. IEEE Access, 9, 122818–122833.
2. Toliupa, S.V. Intrusion Detection Systems and the Functional Resilience of Distributed Information Systems to Cyber Threats / Lukova-Chuyko, N.V., S.V. Tolyupa, V.S. Nakonechny, Brailovsky, M.M.: monograph. Kyiv: Format, 2021. – 407 pp.
3. Swain, S., Sahoo, K. S., Mishra, A., Jhanjhi, N. Z., Humayun, M. (2023). Intelligent traffic engineering with security enforcement in Software-Defined Networks. IEEE Access, 11, 23410–23425.
4. V. M. Dzhuliy, Yu. P. Klyots, B. C. Orlenko [et al.] / Improving the Functionality and Stability of Interference-Resistant Wireless Information and Communication Systems // Bulletin of Khmelnytskyi National University. Technical Sciences. – 2021. – No. 1. – pp. 12–16.
5. Lemeshko, O. V., Yeremenko, O. S., Nevzorova, O. S. (2021). A model of adaptive routing in Software-Defined Networks that meets quality-of-service requirements. Telecommunications and Information Technologies, (1), 45–56/
6. Tang, F., Mao, B., Zubair, M., Kato, N. (2021). Joint power and resource allocation for ultra-reliable low-latency communication in 6G: A deep reinforcement learning approach. IEEE Wireless Communications, 28(2), 24–31.
7. Shah S. D. A., Gregory M. A., Bouhafs F., Den Hartog F. Artificial Intelligence-Defined Wireless Networking for Computational Offloading and Resource Allocation in Edge Computing Networks // IEEE Open Journal of the Communications Society. 2024. Vol. 5. P. 2039–2057.
8. Pirayesh, H., Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 24(2), 767–809.
9. Lemeshko, O. V., Yeremenko, O. S., and Vaavenko, A. V. (2022). A comprehensive model of adaptive routing and ensuring the resilience of telecommunications networks against cyberattacks. Information Security, 24(2), 89–101.
10. Popovskyi, V. O., Loshakov, V. A., Klyapchuk, M. V. (2021). Intelligent methods for resource management under conditions of destructive influences and interference. Telecommunications and Information Technologies, (3), 12–23
11. Ruslan Politansky, Valentin Lesinsky, Serhiy Halyuk, Andriy Kulko. Methods for Determining the Equilibrium State of a Network with Given Flows at Nodes of Information Networks in Cyber-Physical Systems. (2025). Security of Information Systems and Technologies, 1(9), 93–101. https://doi.org/10.17721/ISTS.2025.9.93-101.
12. Alhashimi, H. F., Hindia, M. N., Nguyen, Q. N. (2023). A survey on resource management for 6G heterogeneous networks: Current research, future trends, and challenges. Electronics, 12(3), 647.
13. Natalia Lukova-Chuyko, Serhiy Tolyupa, Ivan Parkhomenko. Methods for Detecting Intrusions in Modern IDS Systems. (2021). Security of Information Systems and Technologies, 1(5), 19–26. https://doi.org/10.17721/ISTS.2021.1.17-24.
14. Lemeshko, O. V., Yeremenko, O. S., Rodionov, A. V. (2021). A Model for Ensuring the Survivability and Resilience of Wireless Communication Networks Under Destructive Influences. Telecommunications and Information Technologies, (4), 15–28.
15. Serhii Toliupa, Anatolii Shevchenko, Andrii Kulko. Features of Ensuring the Security of Critical Infrastructure. (2024). Security of Information Systems and Technologies, 1(7), 11–23.
16. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Siamwalla, S., Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.
17. Al-Jawad, A., Shah, P., Toseef, U. (2021). Deep reinforcement learning for dynamic routing in software-defined networks. IEEE Access, 9, 122818–122833.
18. Berkman, L. N., Zakharchenko, M. V., Skrypnyk, O. V. (2022). Models and methods for enhancing the security and resilience of software-configurable networks. Information Security, 24(1), 35–46.
19. Yuriy Kravchenko, Olena Fison. A Method for Ensuring the Functional Resilience of Software-Defined Networks Under Cyberattacks. (2025). Information Systems and Technology Security, 2(10), 83–95. https://doi.org/10.17721/ISTS.2025.10.83-95.
20. Verma S., Rodrigues T. K., Kawamoto Y., Fouda M. M., Kato N. A Survey on Multi-AP Coordination Approaches over Emerging WLANs: Future Directions and Open Challenges. 2023. arXiv:2306.04164.

21. Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Simpson, S., White, Y., & Mauthe, A. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 54(8), 1245–1265.

Отримано редакцією журналу / Received: 02.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 24.09.26