КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1024
УДК 004.056.55

Абрамов Вадим Олексійович
кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук
Київський столичний університет ім. Б. Грінченка, Київ, Україна
ORCID: 0000-0002-8026-1475
v.abramov@kubg.edu.ua

Глушак Оксана Михайлівна
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-9849-1140
o.hlushak@kubg.edu.ua

Абрамов Сергій Вадимович
Ph.D., системний адміністратор
Київський столичний університет ім. Б. Грінченка, Київ, Україна.
ORCID: 0000-0002-5145-2782
s.abramov.asp@kubg.edu.ua

ІНТЕГРАЦІЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Анотація. Збільшення обсягу переданої інформації, поява нових типів пристроїв та сервісів, а також збільшення вимог до безпеки та надійності комп'ютерних мереж визначають необхідність застосовувати нові технології і нові технічні засоби. У статті розглянуто сучасні тенденції та перспективні напрями розвитку комп'ютерних мереж, зокрема інтеграцію штучного інтелекту (AI), автономних систем і інших технологій (AIOps, SDN, NFV) в управління мережами. Дуже перспективним є використання технологій самовідновлення для збільшення надійності роботи мереж. Розглянуто перспективи продовження переходу до мереж п'ятого покоління та створення мереж шостого покоління (5G/6G) і їх де-які особливості, а також розвиток постквантової криптографії для забезпечення кібербезпеки в умовах появи квантових комп'ютерів. Пропонується для перспективного використання криптосистема CSIDH на ізогеніях еліптичних кривих Едвардса з додатковою модернізацією. Завдяки модернізації швидкодія відносно повільної криптосистеми зростає на три порядки. Особливу увагу приділено промисловим мережам управління технологічними процесами (IIoT) та ролі хмарних і периферійних обчислень у підвищенні ефективності, надійності та масштабованості мережевих рішень. Велику перспективу мають сенсорні мережі з використанням різних каналів і інтерфейсів. Розглянуто перспективи створення квантових і оптичних каналів зв'язку. Зазначено, що поєднання інтелектуальних алгоритмів, безпечних криптографічних протоколів і розподілених архітектур створює основу для цифрової економіки нового покоління.

Ключові слова: комп'ютерні мережі, перспективні технології, штучний інтелект, AIOps, 5G, 6G, постквантова криптографія CSIDH, крива Едвардса, ізогенія, IIoT, хмарні обчислення, периферійні обчислення, інтеграція технологій, квантові і оптичні мережі.

ВСТУП

У XXI столітті розвиток комп'ютерних мереж стає визначальним чинником для всіх сфер цифровізації – від економіки й промисловості до державного управління. Постійне збільшення трафіку, нове обладнання та технології, підвищення вимог до стабільності комунікацій потребують необхідності упровадження сучасних технологій. Відповідно цьому в Україні було схваленом Стратегію розвитку сфери електронних

комунікацій на період до 2030 року [1], в якої вказані перспективні шляхи розвитку комп'ютерних мереж.

Сучасні комп'ютерні мережі пройшли шлях від базової аналогової локальної структури до складної, багаторівневої, гібридної архітектури [2-5]. Мережеві технології розвиваються настільки динамічна, що розробники часто не встигають освоювати нові стандарти й методи, унаслідок чого створені системи нерідко морально застарівають уже під час їхнього розгортання. Молодим науковцям і фахівцям важливо орієнтуватися у ключових напрямах розвитку як власної галузі, так і суміжних сфер, оскільки це дозволяє правильно визначати тематику досліджень і розуміти вектор еволюції мережевих технологій. Тому періодичний аналіз стану та перспектив розвитку комп'ютерних мереж є невід'ємною складовою наукової та інженерної діяльності.

Дослідження сучасних трендів у телекомунікаціях має практичне значення під час побудови й оптимізації інфраструктури, розроблення сервісів та управління цифровими послугами. Метою даної роботи є аналіз провідних напрямів еволюції комп'ютерних мереж, що спрямовані на підвищення їхньої продуктивності, керованості та захищеності.

У 2025 році в усьому світі продовжуються активні дослідження та впровадження інноваційних мережевих технологій, які знаходять застосування у провідних секторах промисловості. Стандарт 5G активно розвивається: він забезпечує високу швидкість передавання даних (до 10 Гбіт/с), мінімальну затримку, масове підключення IoT-пристроїв, гарантує реалізацію критично важливих сервісів, а також підтримку управління технологічними процесами [6]. Паралельно створюються технологічні засади мереж шостого покоління – 6G, які обіцяють швидкості на рівні терабіт за секунду, інтеграцію штучного інтелекту, квантового зв'язку, підтримку голографічних і тактильних інтерфейсів, а також інших сучасних технологій [7]. Все ширше впроваджується протокол IPv6 – на сьогодні ним користується понад 40% глобального інтернет-трафіку [8]. Водночас продовжується розвиток оптичних технологій (FTTx, GPON), що забезпечують десятки гігабіт пропускної здатності для корпоративного та побутового сегментів [9].

Основні тенденції розвитку комп'ютерних мереж. Кожен рік з'являється велика кількість нових технічних рішень і удосконалюються відомі технології. Розглянути їх у невеликій статті досить складно, тому зосередимось на основних тенденціях технологій мереж, які відображені у Таблиці 1.

Таблиця 1

Основні сучасні тенденції розвитку цифрових мереж

	Основні тенденції розвитку	**Основні технології**	**Властивості**
1.	Глобалізація та збільшення пропускної спроможності мереж. Об'єднання обчислювальних і комунікаційних засобів.	5G, 6G (нові діапазони частот, оптичні мережі), Big Data, Global Gnoseology Graph, MPLS, Massive MIMO.	Загальне охоплення планети системами зв'язку різної фізичної природи. На планеті не залишиться недоступних місць та кордонів національних систем. Мітки MPLS збільшують пропускну здатність. Multiple Input Multiple Output.
2.	Масовізация	IoT, IIoT, IoE, Big Data	Охоплення всіх джерел та користувачів інформації.
3.	Інтер-операбельність	MPLS, спільні стандарти, протоколи, інтерфейси, формати даних.	Дозволяє різним технологіям, програмним компонентам, базам даних та файлам працювати разом без будь-яких обмежень доступу.

Продовження таблиці 1

4.	Конвергенція	IMS (IP Multimedia Subsystem)	Об'єднує функції телефона, телебачення, IoT, передавання даних и тексту.
5.	Автоматизація на основі Штучного Інтелекту	AI, AIOps AR/VR	Оптимізація, адаптація, самоналаштування, прокладання маршрутів, покращення якості обслуговування. Підтримка нових користувацьких технологій. Підтримка всіх типів реальності.
6.	Децентралізація інформаційних процесів	MEC, хмарні та периферійні обчислення: cloud-, fog, edge -computing	Використання мобільних периферійних обчислень (MEC) та «хмарних» технологій (cloud, туманних -fog, кордонних -edge для швидкої ефективної обробки та зберігання даних).
7.	Централізація управління архітектурою	SDN, SD-WAN.	Більша гнучкість мережі, адаптивність. Програмне-управління (SDN) з оптимальним та пріоритетним трафіком.
8.	Віртуалізація функцій	NFV	Оптимізація трафіку та спрощене розгортання послуг.
9.	Гіперзв'язність	IoT, IoE, IIoT, 5G, 6G.	Створення єдиного та всеосяжного середовища з надлишковою кількістю зв'язків між елементами, для надійності системи.
10.	Масовий перехід до захищених методів шифрування	FIPS 203 (Кібер), FIPS 204 (Ділітій), FIPS 205 (СФІНКС+), CSIDH, Zero Trust, QKD, Zero Trust	Реалізація квантових обчислень та постквантових методів шифрування і цифрового підпису. Забезпечує безпеку обміну ключами та шифрування даних в умовах перешкод, кібератак та нестабільного середовища. Нульова довіра
11.	Концепція надання послуг	NaaS, Network Slicing	Мережа надає послуги (NaaS) та надає в оренду свої фрагменти (Network Slicing) для спеціалізованих ізольованих додатків.
12.	Автономність, зменшення енергоспоживання	LPWA, BLE, Sigfox, LoRaWAN, LTE-M и NB-IoT, Zero-Power Communication.	Надійна, безпечна робота та малопотужне енергоспоживання. NB-IoT і LTE-M охоплюватимуть понад 60% з 3,6 млрд підключень до мереж LPWA.
13.	Інтеграція мережевих технологій	SD-WAN, LAN/WAN, IoT, IIoT, 5G/6G, edge та хмарних платформ	Поєднання у єдину цифрову екосистему. Універсальні протоколи, зокрема OPC UA, MQTT, REST, забезпечують інтероперабельність та стандартизацію процесів.
14.	Використання нових технологій		Голографічний, тактильний, голографічна телепортація, голосові помічники, високоточна синхронізація, мережева архитектура Many Networks, зворотна сумісність, вбудована програмованість.

Поряд із розвитком традиційних технологій, у першу чергу, створюються бездротові мережі, розвиваються програмно-керовані мережі та здійснюється віртуалізація мережевих функцій, які підвищують гнучкість і масштабованість систем [10-11]. Водночас, значно збільшуються розміри трафіка і кількість вбудованих IoT-пристроїв, які викликають перевантаження мережевих систем і каналів зв'язку, а також потребують нових методів управління трафіком.

Значно зростає кількість атак на мережі, наближається загроза квантових атак, які зроблять неефективними велику частину методів захисту інформації і шифрування. У

відповідь створюються і стандартизуються постквантові алгоритми шифрування, які здатні забезпечити стійкість до атак нового типу [10]. Усі зазначені інновації реалізуються в технологіях, кожна з яких має власні переваги та обмеження, а загалом вони визначають напрями розвитку інфраструктури майбутнього. Реалізація цих тенденцій здійснюється розробкою нових технологій, з яких найбільш досконалими і популярними є вказані у таблиці 2.

Таблиця 2

Перспективні технології комп'ютерних мереж

№	Технологія	Основні переваги	Основні недоліки
1	Бездротові мережі 5G	• Висока швидкість передачі даних • Мала затримка (до 1 мс) • Масове підключення пристроїв	• Складність інфраструктури • Велике енергоспоживання • Вразливість до кібератак • Нерівномірне покриття
2	SDN (Software Defined Networking)	•Централізоване управління мережею • Гнучке і швидке налаштування •Спрощене впровадження нових сервісів	• Одна точка відмови (контролер) •Складність інтеграції зі старими системами •Потребує високої кваліфікації персоналу
3	NFV (Network Function virtualization)	• Зниження затрат на обладнання •Масштабування і гнучкість •Можливість автоматизації	• Залежність від програмних платформ •Зниження якості в порівнянні з «апаратом» •Складність моніторингу і налаштування
4	Мережі Інтернету речей IIoT)	• Інтеграція «розумних» пристроїв •Автоматизація процесів • Збір і аналіз даних в реальному часі	• Слабка безпека пристроїв • Проблеми масштабування •Обмежені ресурси (пам'ять, харчування) •Залежність від стабільного з'єднання
5	MEC технології	• Доступність ресурсів за запитом •Зменшення витрат на фізичну інфраструктуру •Простота масштабування	• Ризик втрати даних •Залежність від провайдера (вендор-блокування) •можлива затримки при доступі до хмари
6	Оптичні мережі (FTTH, DWDM)	•Висока пропускна здатність • Малий рівень перешкод • Довговічність кабелів	• Висока вартість установки •Складність ремонту та обслуговування •Крихкість оптичних волокон
7	Квантові комунікації (QKD)	•Абсолютна теоретична безпека передачі •Перспектива захисту від квантових атак	•Обмежена дальність передачі •Висока вартість обладнання •Відсутність стандартів та інфраструктури
8	Постквантові мережі (ML-KEM (раніше Kyber), CSIDH)	• Стійкість до квантових атак • Можливість інтеграції в класичні мережі	• Більші розміри ключів і повідомлень • Більш висока обчислювальне навантаження • Недоліки стандартизації
9	Штучний інтелект AI, (AIOps, NaaS)	• Автоматичне управління та діагностика • Прогнозування збоїв • Оптимізація трафіку	• Непрозорість рішень II • Можливість помилок при навчанні • Ризикові маніпуляції алгоритмами

1. Збільшення швидкості і кількості кінцевих пристроїв. Значний потенціал збільшення продуктивності закладено у технологіях покоління G5, які не усі ще реалізовано. Але на горизонті з'явилося нове покоління G6, яке очікується буде мати майже фантастичні можливості [11, 12].

Мережі шостого покоління (6G) орієнтовані на надвисокі швидкості передачі (до 1 Тбіт/с), дуже малі затримки та підтримку інтелектуальних сервісів. Ключові технології 6G: терагерцова передача даних, штучний інтелект у керуванні мережею, хмарні

радіоінтерфейси (Cloud-RAN), підтримка технології XR (розширена реальність), енергоефективні протоколи [13].

Мережі мають також підтримувати великі, швидкісні потоки неоднорідних даних від багатьох джерел (Big Data). А також технології і інструменти для роботи з цими даними. Необхідно забезпечити розподілену обробку цих даних багатьма серверами у реальному часі, а також їх безпеку і захист.

Ефективний метод збільшення пропускної здатності для різних даних є технологія міток MPLS. Разом із адресою пакетам надається мітка, яка відповідає певному маршруту і всі пакети з однією міткою слідують одним маршрутом. MPLS може працювати майже з будь-яким протоколом (звідси й назва «багатопротокольний»). Не має значення, як відформатовано решту пакета, головне, щоб маршрутизатор міг зчитувати мітки MPLS на початку пакета. Маршрутизатор не витрачає час на пошук адресата у своїх великих таблицях, но швидко знаходить метку и відправляє пакеті по заданому маршруту. Цій метод також забезпечує добрий захист и надійність мережі – чужа метка не пройде.

У сучасному світі значно збільшується кількість підключених до мережі вбудованих кінцевих пристроїв: IoT-мережі, мільйони давачів, актуаторів, контролерів, автомобілів і т.і. Головні вимоги до пристроїв низьке енергоспоживання, надійна передача даних, масштабованість, безпека. Зменшення енергозатрат кінцевих пристроїв бездротових мереж здійснюється завдяки застосуванню енергоефективних технологій IoT і мереж LPWAN (Low-Power Wide Area Network), LoRaWAN, NB-IoT, Sigfox, LTE-M. Ці технології забезпечують зв'язок на великих відстанях при мінімальному енергоспоживанні, що дозволяє збирати дані навіть у віддалених зонах [14].

Одна з технологій обслуговування великої кількості приладів (давачів і актуаторів) є сенсорна мережа. Це розподілена система пристроїв, що взаємодіють між собою і з центральним вузлом для збору, передачі та аналізу інформації з навколишнього середовища. Пристрої транслюють сигнали один одного до центрального вузла. Мережа має розподілену, стійку до відмови структуру, що самоорганізується. Мережа створена на ґрунті технології ближнього радіозв'язку 802.15.4/ZigBee і має високу енергоефективність – вузли можуть працювати роками на одній батареї. Мережа має високу масштабованість – легко додати нові пристрої [15]. Мережі вийшли за межі землі, технології Starlink, OneWeb, Kuiper працюють на низькоорбітальних супутниках (LEO), що забезпечує інтернет у будь-якій точці Землі, на швидкості до сотень Мбіт/с та затримці 20-40 мс.

2. Децентралізована обробка даних. Швидкість обробки даних у комп'ютерах вже наблизилася до своєї фізичної межі. Подальше збільшення ефективності можливе тільки шляхом розподіленої і паралельної обробки даних. Для мереж IoT це, у першу чергу, технології Edge і Fog Computing. Edge Computing це обчислення на локальних пристроях і серверах, а Fog Computing включає ширшу мережу розподілених обчислювальних вузлів. Таким чином обробка наближається до місць виникнення та зберігання інформації, що збільшує швидкодію системи, знижує затримки і зменшує навантаження на дата-центри. Така децентралізація дуже важлива для автономного транспорту, IoT, технологій AR/VR і розумного виробництва. Здійснюється миттєве прийняття рішень при аварійних ситуаціях [16]. Пакетна обробка значно підвищує ефективність управління мережею та даними. Внаслідок інтеграції локальної інфраструктури та хмар отримуємо нові технології Hybrid Cloud Networking AWS, Azure, GCP [15].

Концепція прикордонної хмари Edge Cloud останнім часом набуває все більшого поширення. Якщо раніше хмарним дата-центром називали, в основному, великий стаціонарний дата-центр, з інженерною інфраструктурою, резервним живленням тощо, то тепер дата-центри «дрібніють» у розмірах. Їх можна розміщувати в легких транспортних контейнерах та інших модульних конструкціях. Такі дата-центри можна розташовувати значно ближче до точок отримання даних у мережі доступу, зокрема з давачами та сенсорами IoT. Саме тому таку хмару з невеликих дат-центрів називають прикордонною хмарою Edge Cloud. Кордони між локальними і хмарними сервісами поступово зникають і створюється гібридна інфраструктура (Hybrid Cloud Infrastructure).

Автономні мережі (Autonomous Networks) – це наступний етап еволюції SDN, коли система здатна самостійно приймати рішення щодо конфігурації, безпеки й обслуговування. Використовується аналітика на основі даних, цифрові двійники (Digital Twins) і алгоритми глибинного навчання для оптимізації ресурсів. Обробку інформації краще виконувати децентралізовано, але для управління мережею найбільш ефективними є централізовані. Технологія централізованого програмного управління SDN (Software-Defined Networking) або SD-WAN здійснює управління мережею через програмне забезпечення. При цьому покращується маршрутизація, автоматизація управління та оптимізація трафіку, здійснюється перенесення мережевих функцій (фаєрвол, брандмауер, NAT, балансування навантаження) у віртуальні технології (NFV Network Function Virtualization) [8 ,9].

Управління мережами. Розглянуті технології комп'ютерних мереж забезпечують високу швидкість, надійність та безпеку, а також пропонують гнучкість у керуванні мережею. Технології управління мережами постійно удосконалюється забезпечуючи підвищення продуктивності та надійності передавання інформації [17]. Управління суттєво залежить від технологій, що використовуються для створення мережі. У Таблиці 3 показані основні властивості технологій, які впливають на управління мережею.

Основою хмарних мереж та центрів обробки даних (ЦОД) стають технології SDN – (Software-Defined Networking), де керування мережею здійснюється централізовано через програмні контролери та NFV. Віртуалізація мережевих функцій, здійснюється на серверах мережі [11]. Ці технології дозволяють віртуалізувати функції керування і гнучко керувати мережею. Одне з важливих властивостей SD-WAN це інтеграція с хмарними сервісами. Ця технологія забезпечує оптимізоване та безпечне з'єднання з хмарними платформами и сервісами, такими як AWS, Google Cloud и Microsoft Azure. Технологія SD-WAN забезпечує оптимізацію трафіку та автоматичне перемикання між каналами зв'язку для забезпечення найкращої продуктивності та надійності.

Таблиця 3

Результати впровадження сучасних технологій мереж

Технологія	Результат впровадження
Високошвидкісний зв'язок 5G/6G	Швидка реакція системи і зниження затримок
Квантові і оптичні лінії	Висока швидкість та фізичний захист
Штучний інтелект AI	Автоматичне прийняття рішень з питань управління
Край/Туман Edge/Fog computing	Децентралізована обробка даних в реальному часі
Постквантова криптографія PQC	Ефективний захист даних
Програмне управління і віртуалізація SDN/NFV	Централізоване управління збільшує гнучкість і керованість інфраструктури.
IoT + 5G	Масштабованість і мобільність систем IoT
Wi-Fi (HaLow)	Оптимізація параметрів мережі IoT.

Технологія Intent-Based Networking (IBN) здійснює управління на основі описання бізнес задач (намірів) на природній мові які транслюються у мережеві політики і створює оптимальні конфігурації мережі [18]. Для динамічної оптимізації QoS (якості обслуговування) використовується аналітика великих даних.

У промисловості впроваджуються мережі управління технологічними процесами (ICS/SCADA, DCS, IIoT), де центральну роль відіграють програмовані логічні контролери. Підключення таких систем до хмарних платформ (наприклад, Azure IoT Hub) забезпечує збір даних, оптимізацію управління, випереджаюче обслуговування обладнання та інтеграцію з аналітичними сервісами [19]. Здійснюється автоматизація рутинних завдань управління та розгортання мережевих сервісів для підвищення ефективності та зниження витрат. Сучасні мережі дедалі більше орієнтовані на інтеграцію різних технологій – AI, IoT, централізованого керування SDN, хмарних і периферійних обчислень. Таке об'єднання створює інтелектуальну екосистему, де мережа сама аналізує стан трафіку, реагує на кібератаки, оптимізує маршрути та забезпечує мінімальні затримки для критичних додатків. Перспективними напрямами є створення мережевого цифрового двійника, який дозволяє моделювати роботу мережі та прогнозувати проблеми. У цьому напрямку частіше використовують мультихмарні інфраструктури (multi-cloud), поєднуючи AWS, Azure, Google Cloud та локальні рішення для резервування. Використання штучного інтелекту та машинного навчання у сфері управління мережами (технології AIOps) [20] дозволяє автоматично виявляти несправності, прогнозувати перевантаження каналів і оптимізувати трафік у режимі реального часу. Такі системи забезпечують самоналаштування та самовідновлення мережі без втручання оператора.

Перспективні технології комп'ютерних мереж формують основу для нової цифрової ери, у якій ключову роль відіграють інтелектуальні алгоритми, безпечні протоколи та висока автоматизація. Реалізується перехід до автономних, інтелектуальних та квантово-захищених мереж нового покоління. При цьому у глобальних мережах на фізичному рівні зберігаються тенденції розвитку квантових і оптичних ліній. В мережах IIoT та IoE керування часто здійснюється на рівні каналів, які визначають властивості відповідної мережі (таблиця 4).

Таблиця 4

Властивості сучасних каналів для IoT

Технологія	Частота	Даль-ність	Швид-кість	Енерго-споживання	Тип мережі	Властивості
LoRaWAN	433 / 868 915 МГц (без ліцензії)	до 15 км	до 50 кбіт/с	Дуже Низьке	LPWAN	далекий зв'язок, зручно для сільського господарства.
NB-IoT	LTE/ліцензія	до 10 км	до 250 кбіт/с	Низьке	Стільник ова	операторська мережа для сенсорів із глибокою проникністю
Sigfox	868/902 МГц	до 50 км	до 100 біт/с	Надто Низьке	LPWAN	Охоронні системи
Wi-Fi (HaLow)	900 МГц 2.4 / 5 ГГц	до 1 км	до 78 Мбіт/с	Середнє	Локальна	швидкісна передача для локальних систем
(Bluetooth Low Energy(BLE)	2.4 ГГц	до 100 м	до 2 Мбіт/с	Дуже Низьке	PAN	пристрої, маячки, що носять
5G (mMTC / URLLC)	>3 ГГц	до 5 км	до 10 Гбіт/с	Середнє / високо	Стільник ова	Автономний транспорт, дрони
Zigbee/Thread	868 / 915 2.4 ГГц	100-200 м (між вузлами)	до 250 кбіт/с	Низьке	Mesh	Мала дальність, низьке енергоспоживання

У мережах 5G існує три компоненти: eMBB, URLLC и mMTC. Перша дає високу швидкість передачі даних (до 1 Гбіт/с). Компонента mMTC забезпечує розгортання мереж IoT, які мають дуже велику кількість малопотужних пристроїв, які передають невеликі пакети даних на відстані до 10 км. Ці автономні IoT пристрої мають бути дуже енергоекономічними і відповідно великий термін служби пристрою живлення (до 10 років). URLLC. Важливий компонент мереж 5G, якій забезпечує передачу даних з затримкою менше 1 мс та високою надійністю до 99,999%. Компонент використовується у дуже критичних областях (автономний транспорт, роботизація, медицина).

Властивості мережі значно покращуються при інтеграції різнорідних мережевих технологій у єдину інфраструктуру. Тобто об'єднання ШІ, Edge AI для децентралізованого аналізу даних у вузлах, тотального шифрування і створення єдиного цифрового простору.

Метою інтеграції є забезпечення ефективного обміну інформацією, підвищення ефективності управління ресурсами та створення адаптивної платформи для цифрової трансформації техногенного середовища.

Одночасно зростання обсягів трафіку, масове впровадження IoT-пристроїв, а також збільшення частоти кібератак створюють додаткові виклики для систем управління мережею.

Використання штучного інтелекту (AI). Технології AI (Artificial Intelligence) та ML (machine learning) є основою автоматизації управління, оптимізації і захисту мережі. Вони забезпечують мережам самостійно адаптуватися до умов, що змінюються, прогнозувати проблеми і автоматично усувати їх, підвищуючи загальну продуктивність і надійність.

AI використовується як для обробки інформації так і для управління мережею, аналізу даних, машинного навчання, виявлення та усунення проблем, оптимізації продуктивності та підвищення безпеки мережі. Наприклад, технології AIOps (Artificial Intelligence for IT Operations) використовуються для підвищення ефективності виконання операцій IT. Основна мета AIOps – оптимізація управління IT-послугами, скорочення часу та зусиль, необхідних для управління IT-операціями. AIOps виконує попереджувальну аналітику IT-операцій, обробку великих даних та інші дії для автоматизації та вдосконалення IT-операцій [20]. Ці технології дозволять мережі незалежно відстежувати, аналізувати та реагувати на мережні стани в режимі реального часу.

Розроблено ряд платформ ONOS, OpenDaylight, які здатні забезпечувати стійкість до відмов і здійснюють балансування навантаження. Self-Healing Networks – Технології Cisco DNA Center та Juniper Mist AI дозволяють мережам автоматично виявляти та усувати несправності без участі адміністратора [21],[22]. Системи на базі штучного інтелекту (наприклад, Darktrace, Palo Alto Cortex XSIAM) аналізують мережевий трафік у реальному часі та прогнозують неполадки і атаки на мережу.

Мережа, що самовідновлюється – це дуже перспективний тип мережі, здатний усувати проблеми без участі людини. Цей процес в основному спирається на функції резервування, що активуються при виявленні збою. Використовуються алгоритми штучного інтелекту та машинного навчання, які виявляють, діагностують та усувають аномальні режими мережі (технології AIOps і принципи автономних мереж.) [22].

Сучасна мережа має ефективно підтримувати одну з популярних сучасних технологій XR. Тобто групу технологій нової реальності (virtual reality (VR), augmented reality (AR, доповнена реальність) та mixed reality (MR, змішана реальність). Зараз XR

все частіше зустрічається у повсякденності, знаходячи нові різноманітні застосування. XR ще вчора називалося "технологією далекого майбутнього", а сьогодні ці технології проникли в різні сфери нашого життя і ще більше будуть розвиватися завтра, особливо в інтеграції з мережами і AI [16].

Квантові і постквантові технології. По всьому світу йде активна розробка квантових комп'ютерів, квантових мереж і квантової криптографії (QKD), які дуже добре захищені від несанкціонованого втручання. Розробляються квантові проекти мереж: Китай (QUESS), ЄС (OpenQKD), США (Quantum Network Testbed). [23]-[24]. Через деякий час квантовий зв'язок стане таким же обов'язковим елементом цифрової архітектури, як антивірус і криптографія.

Квантові технології базуються на використанні квантових станів фотонів і заплутаності. Технологія Quantum Key Distribution (QKD) забезпечує абсолютну безпеку каналів зв'язку [23].

У квантових мережах (наприклад, Відень, Делфт, Пекін) сьогодні використовують QKD-протоколи BB84 (Bennett & Brassard, 1984) і E91 [25]. BB84 найперший протокол квантового розподілу ключів. У ньому використовуються фотони із двома базисами поляризації (0 і 45 градусів). Протокол E91 (Ekert, 1991) створено на основі квантової заплутаності фотонів [25].

Однак квантові технології дуже специфічні і складні, тому звичайні комп'ютери і технології, а також звичайні канали зв'язку будуть використовуватись ще довго. Наразі продовжують розвиватися оптичні мережі, їх ефективність залежить від швидкодії електронних схем накачки лазерів, а також чистоти і прозорості оптичного волокна. Ці технології мають ще багато резервів розвитку і тому оптичні лінії будуть ще довго здатні передавати дані з пропускною здатністю понад 1 Тбіт/с на міжконтинентальних відстанях.

З появою незабаром квантових комп'ютерів класичні криптосистеми (наприклад, RSA, ECC) стають вразливими. Один із способів підвищення кібербезпеки в звичайних мережах в умовах існування квантових комп'ютерів є стійке до квантових атак асиметричне шифрування, яке дозволяє двом сторонам створити загальний секретний ключ по відкритому каналу зв'язку.

Цей ключ використовується для шифрування і подальшого обміну даними за допомогою симетричних алгоритмів. Але вже в даний час конче необхідно застосувати постквантові криптографічні алгоритми. Тому що незважаючи на те що квантові комп'ютери ще не створені перехоплення даних вже наразі здійснюється, а коли стане можливим, ці дані будуть розшифровані.

Перспективними напрямками розвитку постквантових алгоритмів обміну ключами є, алгоритми ML-KEM і CSIDH. ML-KEM (раніше Kyber) вже стандартизований NIST [26] як механізм інкапсуляції ключів (KEM) завдяки високій швидкодії та надійності.

Комбіновані алгоритми, наприклад KDF (ECDH_key || ML-KEM_key), забезпечують гібридну стійкість до майбутніх квантових атак. Алгоритм CSIDH знаходиться на стадії розробки та дослідження, які показують, що его ефективність не гірша ніж у ML-KEM. Порівняння постквантових протоколів ML-KEM і CSIDH показано у Таблиці 5.

Таблиця 5

Порівняння криптосистем CSIDH и ML-KEM

Критерій	CSIDH	ML-KEM
Назва	Commutative Supersingular Isogeny Diffie–Hellman	CRYSTALS-ML-KEM
Тип	Схема обміну ключами (Diffie–Hellman-подобна)	Схема шифрування/обміну ключами (KEM)
Математична основа	Ізогенії між суперсингулярними еліптичними кривими	Задача на гратах — Learning With Errors (LWE)
Захист від квантових атак	Захищена від квантових атак на основі ізогеній	Захищена від квантових атак на основі решіток
Стандартизація і використання	Находиться на дослідницькому етапі	Прийнята NIST (2022) як стандартна постквантова схема KEM для OpenSSL, liboqs Використовується у TLS, VPN,
Розмір ключей	Дуже малий (біля 64–96 байт)	Великий публічний ключ (800–1500 байт)
Швидкість роботи	Велика (для модернізованих систем)	Дуже велика (при апаратній оптимізації)
Тип алгоритма	Діффі-Хелман-подібний протокол (обмін ключами), є варіант CSIKE з інкапсуляцією ключів.	KEM (Key Encapsulation Mechanism) - механізм інкапсуляції ключів
Переваги	Малі ключі, комутативність, значно підвищена швидкість дії модернізованих криптосистем	Швидкодія, стійкість, промислова підтримка
Недоліки	Підлеглість до атаки по сторонньому каналу	Великий розмір ключів и шифротексту Підлеглість атакам по стороннім каналам

Постквантова криптосистема ML-KEM розроблена на основі математичні теорії грат, які вважаються стійкими до відомих квантових алгоритмів злому. Розмір ключів криптосистеми ML-KEM512 близько 800 байт, цей рівень безпеки дорівнює AES-128 [25].

Постквантовий протокол обміну ключами CSIDH створений на основі криптосистеми Діффі-Хельмана і використовує ізогенії суперсингулярних еліптичних кривих [27]- [30]. Ізогенія – це особисті відображення між еліптичними кривими, які зберігають їх структуру. Задача побудови ізогенії або находження шляху між кривими вважається складною навіть для квантових комп’ютерів.

Обидві системи є асиметричними, відкритими та публічними. Вони розроблені для захисту від атак із використанням квантових комп'ютерів, які можуть легко зламати існуючі криптосистеми.

CSIDH досить повільній в порівнянні з алгоритмами на гратах (ML-KEM, Dilithium), але він дає компактні ключі, строгу математичну основу і активно розвивається. Тому його розглядають як перспективне рішення для: IoT, супутникових мереж, квантово-гібридних мереж, тривалого зберігання та захисту даних (архіви, блокчейн).

У процесі досліджень системи CSIDH створені ефективні модифікації цього криптоалгоритма на ізогеніях суперсингулярних кривих у формі Едвардса [23]. Отримані нижні оцінки збільшення швидкості модифікованих алгоритмів. Найбільш значимі результати отримані при виборі класів нециклічних кривих Едвардса [29 ,30], при використанні квадратичних пар кручення, замість циклічних повних кривих

Едвардса, а також використанні методу рандомізації алгоритму в якості альтернативного методу захисту від атаки по стороннім каналам «Constant time CSIDH».

В системі CSIKE (Commutative Supersingular Isogeny Key Encapsulation), яка є модифікацією CSIDH, запропоновано відмовитися від зайвого обчислення ізогенної функції та створити оптимізацію розподілу ступенів ізогенії. Запропонований також оригінальний і швидкий алгоритм інкапсуляції ключа, який є єдиним відкритим ключем алгоритму, замість двох, що дає підвищення безпеки [29]. В цьому алгоритмі існують дві незалежні криптосистеми з можливістю паралельних обчислень. Інтегральні нижні оцінки приросту продуктивності модифікованого алгоритму CSIKE отримані на рівні $1,5 \times 2^{9}$. Існування двох ізоморфних криптосистем з можливістю паралельних обчислень ліквідує загрозу атаки по стороннім каналам і підвищує продуктивність алгоритму.

При використанні несуперсингулярних кривих виникає 4 незалежних криптосистеми з можливістю паралельних обчислень і підвищення продуктивності. Усі ці модифікації дозволили збільшити швидкість модифікованого алгоритма маже у 2^{10} раз, що відповідає параметрам алгоритма ML-KEM і стане основою для створення криптосистем майбутнього.

ВИСНОВКИ

Поки ще не створено технологій, які не мають недоліків. Усунення недоліків комунікаційних мереж потребує інтеграції нових технологій на межах основних направлень розвитку.

Сучасні тенденції показують, що розвиток і вдосконалення мереж відбувається шляхом інтеграції штучного інтелекту, децентралізації обробки інформації і централізації управління, використання квантових технологій і постквантової криптографії, а також енергоефективних рішень. Технології розвіваються у напрямку створення розподілених, гнучких, інтелектуальних, адаптивних, автономних, швидкісних та програмно-визначених мереж шостого покоління (6G), де безпека є складовою частиною архітектури.

Розвиток стандартів зв'язку – одне з головних завдань технологічного прогресу. Швидкість і надійність обміну даними є важливими параметрами систем зв'язку. Інтернет речей, розумні агломерації, транспорт, децентралізовані сервіси, медицина,– все це отримає швидкого розвитку із впровадженням технології 5G. А з появою 6G, з'являться принципово нові можливості: інтеграція с квантовими технологіями, приєднання великої кількості сенсорних мереж,

Наразі найбільше враження складають такі основні тенденції: всеохоплююче шифрування та розвиток методів квантової і постквантової технологій, використання методів штучного інтелекту при керуванні мережами, інтеграція хмарних та мобільних технологій. Вражаючим є створення глобальних гібридних мереж (земля+супутники+квантові канали+штучний інтелект), інтеграція квантового зв'язку та AI у виробничих мережах, використання цифрових двійників (Digital Twin) та випереджаюче обслуговування мереж.

Велике значення набули постквантові технології шифрування, які потребують негайної імплементації. Лідерами є технології з використанням теорії грат і ізогеній еліптичних кривих. Технологія ML-KEM – стандартизується NIST як кандидат для масового впровадження в корпоративні мережі. ML-KEM стане одним із стандартів для

постквантової криптографії у мережевих протоколах. Але використання ізогеній залишається дуже перспективним напрямом. Вже з'явилися стійкіші схеми (наприклад, CSIDH на ізогеніях кривих Едвардса та його модифікації). CSIDH – цікавий там, де важлива компактність ключів і строга математика (IoT, супутники, гібрид QKD + PQC). Теоретично порівняти технології Кібер (ML-KEM) з модернізованим CSIDH є досить складним. Вони мають різні математичні основі але схожий принцип дії та функції. Остаточний висновок зробить експериментальне випробування. Ймовірно, досить ефективними стануть гібридні схеми шифрування (ML-KEM + ECDHE, ML-KEM + CSIDH).

Проблемами всіх сучасних мереж є постійне зростання енергоспоживання; сумісність старих та нових протоколів; зростання складності адміністрування та моніторингу; відсутність єдиних стандартів і протоколів; висока вартість апаратної складової та модернізації інфраструктури. Тому важливими напрямками майбутнього розвитку мереж буде подолання їх сучасних недоліків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cabinet of Ministers of Ukraine. (2023). *On approval of the strategy for the development of electronic communications until 2030*. https://zakon.rada.gov.ua
2. Cisco Systems. (2024). *Global networking trends report 2025*. Cisco Press.
3. Stetsenko, V. P., & Titova, I. (2022). *Modern network technologies*. Uman State Pedagogical University named after Pavlo Tychyna.
4. Zhurakovskyi, B. Yu., & Zeniv, I. O. (2020). *Computer networks*. Igor Sikorsky Kyiv Polytechnic Institute.
5. Roslyakov, A. (n.d.). Network 2030: ITU-T vision for the future of fixed communication networks. https://www.lastmile.su/files/article_pdf/8/article_8861_92.pdf
6. International Telecommunication Union. (2022). *Recommendation ITU-T Y.3100: Framework of the IMT-2020 network*.
7. 6G Flagship. (2023). *Key drivers and research challenges for 6G ubiquitous wireless intelligence*. University of Oulu.
8. Orlov, R. (n.d.). Introduction to IPv6 compared to IPv4. https://4te.me/post/vvedenie-v-ipv6-na-praktike
9. Sukhorukova, H. (n.d.). Drivers of fiber-optic internet development: What to expect from the technology. https://hub.kyivstar.ua/author/ganna-suhorukova
10. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.
11. Shalahinov, A. (2025). Migration from 4G to 5G using network function virtualization (NFV). https://shalaginov.com/2023/03/13/4g-to-5g-nfv-migration
12. European Telecommunications Standards Institute. (2023). *Network function virtualisation (NFV): Management and orchestration (ETSI GR NFV-EVE 012)*.
13. Stallings, W. (2022). *Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud*. Pearson Education.
14. Jooby. (n.d.). How LPWAN networks work and why LoRaWAN stands out. https://jooby.eu/ru/blog/kak-rabotayut-lpwan-seti-i-pochemu-lorawan-vydelyaetsya-na-ih-fone/
15. Shalahinov, A. (2023). Edge cloud. https://shalaginov.com/2023/09/20/edge-cloud
16. TTT. (n.d.). The future of virtual reality: Where the industry is heading. https://www.ttt.ua/ua/articles-reviews/budushchee-virtualnoi-realnosti-kuda-dvizhetsia-industriia
17. Rolik, A. I., Telenyk, S. F., & Yasochka, M. V. (2018). *Management of corporate IT infrastructure*. Naukova Dumka.
18. Cisco Systems. (2025). Intent-based networking (IBN). https://www.cisco.com/site/us/en/solutions/intent-based-networking/index.html
19. Microsoft. (2025). *Azure IoT Hub documentation*. https://learn.microsoft.com/azure/iot-hub
20. Khazyka, S. (2025). Artificial intelligence for IT operations (AIOps). https://www.unite.ai/ru/what-is-aiops
21. Tang, F., Kawamoto, Y., & Kato, N. (2024). Future intelligent and autonomous 6G networks: AI-based self-optimization. *IEEE Network*, *38*(2), 12–21.

22. Sibanda, I. (2025, February 7). Self-healing networks: The next evolution in network management. *ComputerWeekly.com*.
23. Cobourne, S. (2025). *Quantum key distribution: Protocols and applications*. Royal Holloway, University of London.
24. Mattsson, J. P., et al. (2021). Quantum-resistant cryptography. *arXiv*. https://arxiv.org/abs/2112.00399
25. ML-KEM Network Crystal Legacy. (n.d.). Events, news and roadmap. https://coindar.org/en/coin/ML-KEM-network
26. National Institute of Standards and Technology. (2024). *Post-quantum cryptography standardization: Finalists and round 4 candidates*.
27. Jao, D., & De Feo, L. (2023). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (CSIDH). In *Post-Quantum Cryptography Conference Proceedings*.
28. Castryck, W., Lange, T., Martindale, C., Panny, L., & Renes, J. (2018). CSIDH: An efficient post-quantum commutative group action. In T. Peyrin & S. Galbraith (Eds.), *Advances in cryptology – ASIACRYPT 2018* (pp. 395–427). Springer.
29. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient switching algorithms for PQC on Edwards curve isogenies. *Cryptography, 8*, 38.
30. Bessalov, A. V., & Abramov, S. V. (2023). PQC CSIKE algorithm on non-cyclic Edwards curves. *Cybernetics and Systems Analysis, 59*, 3–18.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Vadym Abramov
PhD in Technical Sciences, Associate Professor
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-8026-1475
v.abramov@kubg.edu.ua

Oksana Hlushak
PhD in Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-9849-1140
o.hlushak@kubg.edu.ua

Serhii Abramov
PhD, System Administrator
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-5145-2782
s.abramov.asp@kubg.edu.ua

INTEGRATION OF INTELLIGENT TECHNOLOGIES IN COMPUTER NETWORKS

Abstract. The increased need for transmitted information, the emergence of new types of devices and services, as well as the increased security and reliability of computer networks mean the need to develop new technologies and new technical features and solutions. The statistics examines current trends and promising developments of computer networks, including the integration of artificial intelligence (AI), autonomous systems (AIOps) and others technologies (SDN, NFV) in management of networks. It is important to use advanced self-innovation technology to increase the reliability of the measurement process. The transition to the fifth and sixth generations (5G/6G) and their power, as well as the development of post-quantum cryptography to ensure cybersecurity in the minds of quantum computing, is examined. The CSIDH cryptosystem on the isogenies of Edwards elliptic curves with additional modernization is being introduced for the upcoming development. With the recent modernization of the speed code, the increasingly comprehensive cryptosystem is growing by three orders of magnitude. Particular attention is paid to industrial process control measures (IIoT) and the role of cloud and peripheral calculations in the increased efficiency, reliability and scalability of process solutions. A significant perspective is the sensory networks from different channels and interfaces. The prospects for the creation of quantum and optical channels are examined. It is believed that the advent of smart algorithms, secure cryptographic protocols and partitioned architectures creates the basis for a new generation of digital economy.

Keywords: computer networks, advanced technologies, artificial intelligence, AIOps, 5G, 6G, post-quantum cryptography, CSIDH, Edwards curve, isogeny, IIoT, Edge/Fog computing, integration of technologies, quantum and optical networks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Cabinet of Ministers of Ukraine. (2023). *On approval of the strategy for the development of electronic communications until 2030*. https://zakon.rada.gov.ua
2. Cisco Systems. (2024). *Global networking trends report 2025*. Cisco Press.
3. Stetsenko, V. P., & Titova, I. (2022). *Modern network technologies*. Uman State Pedagogical University named after Pavlo Tychyna.
4. Zhurakovskyi, B. Yu., & Zeniv, I. O. (2020). *Computer networks*. Igor Sikorsky Kyiv Polytechnic Institute.

5. Roslyakov, A. (n.d.). Network 2030: ITU-T vision for the future of fixed communication networks. https://www.lastmile.su/files/article_pdf/8/article_8861_92.pdf
6. International Telecommunication Union. (2022). *Recommendation ITU-T Y.3100: Framework of the IMT-2020 network*.
7. 6G Flagship. (2023). *Key drivers and research challenges for 6G ubiquitous wireless intelligence*. University of Oulu.
8. Orlov, R. (n.d.). Introduction to IPv6 compared to IPv4. https://4te.me/post/vvedenie-v-ipv6-na-praktike
9. Sukhorukova, H. (n.d.). Drivers of fiber-optic internet development: What to expect from the technology. https://hub.kyivstar.ua/author/ganna-suhorukova
10. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.
11. Shalahinov, A. (2025). Migration from 4G to 5G using network function virtualization (NFV). https://shalaginov.com/2023/03/13/4g-to-5g-nfv-migration
12. European Telecommunications Standards Institute. (2023). *Network function virtualisation (NFV): Management and orchestration (ETSI GR NFV-EVE 012)*.
13. Stallings, W. (2022). *Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud*. Pearson Education.
14. Jooby. (n.d.). How LPWAN networks work and why LoRaWAN stands out. https://jooby.eu/ru/blog/kak-rabotayut-lpwan-seti-i-pochemu-lorawan-vydelyaetsya-na-ih-fone/
15. Shalahinov, A. (2023). Edge cloud. https://shalaginov.com/2023/09/20/edge-cloud
16. TTT. (n.d.). The future of virtual reality: Where the industry is heading. https://www.ttt.ua/ua/articles-reviews/budushchee-virtualnoi-realnosti-kuda-dvizhetsia-industriia
17. Rolik, A. I., Telenyk, S. F., & Yasochka, M. V. (2018). *Management of corporate IT infrastructure*. Naukova Dumka.
18. Cisco Systems. (2025). Intent-based networking (IBN). https://www.cisco.com/site/us/en/solutions/intent-based-networking/index.html
19. Microsoft. (2025). *Azure IoT Hub documentation*. https://learn.microsoft.com/azure/iot-hub
20. Khazyka, S. (2025). Artificial intelligence for IT operations (AIOps). https://www.unite.ai/ru/what-is-aiops
21. Tang, F., Kawamoto, Y., & Kato, N. (2024). Future intelligent and autonomous 6G networks: AI-based self-optimization. *IEEE Network, 38*(2), 12–21.
22. Sibanda, I. (2025, February 7). Self-healing networks: The next evolution in network management. *ComputerWeekly.com*.
23. Cobourne, S. (2025). *Quantum key distribution: Protocols and applications*. Royal Holloway, University of London.
24. Mattsson, J. P., et al. (2021). Quantum-resistant cryptography. *arXiv*. https://arxiv.org/abs/2112.00399
25. ML-KEM Network Crystal Legacy. (n.d.). Events, news and roadmap. https://coindar.org/en/coin/ML-KEM-network
26. National Institute of Standards and Technology. (2024). *Post-quantum cryptography standardization: Finalists and round 4 candidates*.
27. Jao, D., & De Feo, L. (2023). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (CSIDH). In *Post-Quantum Cryptography Conference Proceedings*.
28. Castryck, W., Lange, T., Martindale, C., Panny, L., & Renes, J. (2018). CSIDH: An efficient post-quantum commutative group action. In T. Peyrin & S. Galbraith (Eds.), *Advances in cryptology – ASIACRYPT 2018* (pp. 395–427). Springer.
29. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient switching algorithms for PQC on Edwards curve isogenies. *Cryptography, 8*, 38.
30. Bessalov, A. V., & Abramov, S. V. (2023). PQC CSIKE algorithm on non-cyclic Edwards curves. *Cybernetics and Systems Analysis, 59*, 3–18.

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 26.03.26