УДК 004.77 **doi: 10.26906/SUNZ.2026.1.214**

М. М. Суровицький, Т. В. Філімончук, С. О. Партика, О. М. Севостьянова

Харківський національний університет радіоелектроніки, Харків, Україна

МОДЕЛЬ ОПТИМІЗАЦІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗАКЛАДУ ВИЩОЇ ОСВІТИ НА ОСНОВІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ

Анотація. Актуальність дослідження зумовлено стрімким розвитком інформаційних технологій та цифровізацією освітнього процесу, що робить належну організацію комп'ютерної мережі у закладі вищої освіти критично важливою. Сучасні мережі закладів вищої освіти стикаються з викликами функціонального розділення сегментів, потребою захищати критично важливі данні від гостьового доступу, а також вимогами до масштабованості, гнучкості та відмовостійкості інфраструктури. У зв'язку з цим, набуває актуальності розробка математичної моделі, яка формалізує структурні та функціональні особливості мультисегментної мережі закладa вищої освіти з фокусом на відмовостійкості та політиці безпеки. **Об'єктом дослідження** виступає комп'ютерна мережа закладу вищої освіти, що охоплює її структуру, технічні засоби та процеси функціонування. **Предметом дослідження** виступають методи, моделі та технології оптимізації роботи цієї мережі на основі сучасних технологій передачі даних. **Результатом роботи** є удосконалнена математична модель функціонування комп'ютерної мережі закладу вищої освіти, що поєднує сім ключових вимог: побудову ієрархічної архітектури, забезпечення високої пропускної здатності й швидкодії, підтримку відмовостійкості та резервування, гарантування безпеки й контролю доступу, раціональне управління ресурсами, можливість масштабування й адаптивності, а також врахування потреб користувачів. Проведені експериментальні випробування засвідчили результативність запропонованих механізмів. **Висновки.** Запропонована модель ефективно формалізує багатоаспектну інфраструктуру компютерної мережі закладу вищої освіти та здатна кількісно оцінювати надійність через ймовірність відмови критичних компонентів, що дозволяє створювати масштабовані, гнучкі та безпечні мережні рішення, які мінімізують ризики для критичних даних та забезпечують безперервність освітнього процесу.

Ключові слова: комп'ютерна мережа закладу вищої освіти, математична модель, мультисегментна система, відмовостійкість, резервування, VLAN, політика безпеки, міжмережний екран.

Вступ

Постановка проблеми. В умовах стрімкого розвитку інформаційних технологій та цифровізації навчання [1] належна організація комп'ютерної мережі у закладі вищої освіти (ЗВО) є критично важливою для забезпечення ефективного та продуктивного освітнього процесу. Мережа ЗВО використовується як для надання здобувачам освіти необхідних навчальних ресурсів та інструментів, так і для проведення викладачами лекцій та практичних занять. Однак, сучасні мережі ЗВО стикаються з низкою викликів, зокрема необхідністю забезпечити:

- функціональне розділення мережі на сегменти для різних цілей (навчання, адміністрація, зберігання даних, відеоспостереження);
- безпеку та ізоляцію критично важливих сегментів (управління даними ЄДЕБО/ДЕКАНАТ та адміністративний сегмент) від гостьового доступу;
- масштабованість, гнучкість, відмовостійкість інфраструктури через механізми резервування даних, каналів та дублювання маршрутизаторів.

Традиційні підходи до побудови комп'ютерних мереж (КМ) часто потребують складного ручного налаштування та не завжди забезпечують необхідну гнучкість для швидкого реагування на зміну потреб [2]. У зв'язку з цим набуває актуальності впровадження нового підходу до формування мереж ЗВО, починаючи з етапу планування складових математичної моделі, який передбачає використання інтелектуальних технологій автоматизованого проєктування, віртуалізації та програмно-конфігурованих мереж (SDN). Такий підхід дозволяє моделювати мережну інфраструктуру як єдину адаптивну систему, у якій топологія, політики безпеки, маршрутизація та розподіл ресурсів визначаються програмно, а не лише фізичною архітектурою. Завдяки цьому забезпечується: динамічна масштабованість мережі при зростанні кількості користувачів або сервісів, автоматизоване керування та спрощене адміністрування мережних пристроїв, підвищення надійності та безпеки завдяки централізованому контролю доступу та моніторингу, оптимізація продуктивності за рахунок інтелектуального розподілу трафіку та ресурсів, інтеграція з хмарними та віртуальними середовищами для розгортання навчальних та адміністративних сервісів.

Таким чином, нове покоління мереж ЗВО розглядається не лише як набір з'єднань між пристроями, а як керована, масштабована та самоналаштовувана система, яка побудована на основі математичних моделей, що враховують реальні параметри, навантаження та вимоги користувачів.

Аналіз останніх досліджень і публікацій. Аналіз досліджень та публікацій зосереджений на структурній та функціональній оптимізації комп'ютерних мереж закладів вищої освіти (КМ ЗВО). Найчастіше мережа ЗВО розглядається як складна мультисегментна система, що вимагає впровадження спеціальних механізмів для забезпечення надійності та безпеки.

Дослідження [3] зосереджується на аналізі структурних особливостей мереж закладів вищої освіти (ЗВО), приділяючи особливу увагу принципам їх побудови та функціональному поділу. Представлена робота є особливо релевантною для формування цілісного уявлення про те, яким чином варто організовувати захист мережі установи. Стаття

присвячена критично важливій темі – розробці та впровадженню комплексної технології (методики, моделі) для забезпечення інформаційної та кібербезпеки у специфічному секторі ЗВО України. Запропоновані технічні рішення забезпечують логічну ізоляцію трафіку, підвищує рівень безпеки, створють можливості для масштабування інфраструктури та полегшують управління мережею в умовах зростання потреб користувачів та сервісів.

Дослідження [4] логічно доповнює структурний аналіз мереж, оскільки зосереджується на оптимізації ієрархічної організації комунікаційної інфраструктури. У роботі виділено три ключові рівні ієрархії (магістральний, зональний та внутрішній), кожен із яких виконує свою функціональну роль у забезпеченні ефективної передачі даних та управління навантаженнями. Особливу увагу приділено побудові математичної моделі, яка дає змогу визначати оптимальну конфігурацію структури мережі з урахуванням пропускної здатності, затримок, надійності та вартості обладнання. Завдяки такому підходу дослідження демонструє, що архітектура мережі ЗВО повинна розглядатися як багаторівнева система, де кожен рівень не лише виконує власні функції, а й взаємодіє з іншими для забезпечення цілісності та масштабованості інфраструктури, що підкреслює важливість комплексного моделювання при проєктуванні сучасних мереж ЗВО та дозволяє досягти збалансованості між продуктивністю, надійністю та економічною доцільністю.

Посібник [5] присвячений огляду технологій захисту інформації та розробленню політики безпеки, що безпосередньо пов’язані з критично важливими вимогами до сегментації й захисту мережної інфраструктури. Автори детально розглядають механізми логічного поділу мережі на ізольовані віртуальні сегменти, що дає змогу мінімізувати вплив небажаного трафіку та локалізувати потенційні загрози. Зокрема, підкреслюється, що ізоляція трафіку між сегментами досягається завдяки коректному налаштуванню VLAN (Virtual Local Area Network), що унеможливлює пряме взаємне бачення пристроїв різних підмереж та підвищує рівень керованості. Посібник акцентує увагу на розмежуванні доступу та впровадженні політик безпеки шляхом використання міжмережних екранів, які контролюють міжсегментні з’єднання, що дозволяє гнучко регулювати правила взаємодії між різними частинами мережі, запроваджувати фільтрацію трафіку, здійснювати моніторинг та виявлення аномалій. Таким чином, комплексне застосування VLAN та міжмережних екранів розглядається як ключовий інструмент забезпечення захищеної, керованої та масштабованої мережної архітектури, що є особливо актуальним для інфраструктури ЗВО з великою кількістю користувачів та різнорідних сервісів.

У роботі [6] розглянуто комплексні підходи до забезпечення відмовостійкості та катастрофостійкості в корпоративних мережах, акцент зроблено на поєднанні технічних та архітектурних рішень, які мінімізують ризики простоїв та втрати даних. Автори детально аналізують сучасні механізми резервування, серед яких особливе місце займають технології MultiWAN, системи дублювання мережевого ядра та методи підвищення надійності зберігання інформації. Зокрема, підкреслюється, що відмовостійкість мережного ядра та його каналів досягається шляхом використання дубльованих маршрутизаторів, які працюють у режимах автоматичного перемикання або балансування навантаження. Технологія Multi-WAN забезпечує паралельне підключення до кількох провайдерів, що дозволяє підтримувати доступність зовнішнього каналу навіть у разі відмови одного з них, а також оптимізувати маршрутизацію трафіку. Для зберігання даних в дослідженні пропонується використання RAID-масивів, які забезпечують захист від виходу з ладу фізичних носіїв, та на використанні механізмів реплікації в реальному часі, що дозволяють створювати синхронні копії критично важливої інформації на резервних серверах або у віддалених дата-центрах. Такий підхід формує багаторівневу модель надійності, у якій збереженість даних та безперервність роботи сервісів підтримується навіть у випадках серйозних технічних збоїв.

Поглиблюючи аспект мережної стійкості, у статті [7] проаналізовано підходи до оптимізації алгоритмів функціонування комп’ютерних мереж підвищеної живучості ще на етапі їх проєктування. Автори акцентують увагу на необхідності врахування потенційних зовнішніх впливів, збоїв та структурних змін мережної інфраструктури, що можуть виникати в процесі її експлуатації. Саме тому ключовою метою роботи є розробка критерію живучості, який дозволяє кількісно оцінити здатність мережі адаптуватися до непередбачуваних умов, зберігати працездатність та забезпечувати мінімально необхідний рівень сервісів. У статті підкреслено, що критерій живучості охоплює як параметри стійкості топології, так і ефективність алгоритмів перебудови маршрутизації та перерозподілу навантажень. Він дозволяє моделювати поведінку мережі в умовах часткових відмов, аналізувати часові характеристики відновлення та визначати оптимальні стратегії резервування. Такий підхід є особливо значущим для побудови корпоративних мереж ЗВО, де високий рівень доступності сервісів, стійкість до зовнішніх впливів та можливість оперативної реконфігурації інфраструктури мають критичне значення.

Для теоретичного обґрунтування концепції живучості мереж особливо важливими є фундаментальні напрацювання у цій галузі. Зокрема, у дослідженні [8] сформульовано базові підходи до розуміння живучості інформаційних систем як здатності продовжувати функціонування в умовах зовнішніх впливів, часткових відмов чи деградації окремих компонентів. Автори пропонують універсальні принципи аналізу стійкості, що охоплюють як структурні, так і функціональні властивості систем, а також визначають загальні критерії, за якими можна оцінювати рівень їхньої здатності до відновлення та адаптації. Наведені положення формують методологічну основу, яку можна застосувати до телекомунікаційних та корпоративних мереж, зокрема до інфраструктури ЗВО.

Доповненням до цього підходу є робота [9], у якій об'єктом дослідження виступають ієрархічні телекомунікаційні мережі. Автори зосереджуються на методах кількісної оцінки живучості таких мереж, пропонуючи формальні метрики, що враховують багаторівневу організацію, динаміку відмов елементів різної критичності та поведінку мережі при перебудові топології. Завдяки цьому підхід дозволяє визначити, наскільки ефективно мережа зберігає працездатність за умов часткових пошкоджень, а також оцінити оптимальність впроваджених механізмів резервування.

Автор роботи [10] детально розглядає принципи організації систем зберігання даних та резервного копіювання в IT-інфраструктурах, що працюють із персональними даними, яка потребує підвищеного рівня захисту, надійності та контролю доступу. У дослідженні аналізуються сучасні підходи до побудови сховищ, включно з використанням мережних накопичувачів, систем централізованого зберігання, а також багаторівневої архітектури резервного копіювання. Значну увагу приділено питанням відповідності правовим та нормативним вимогам щодо обробки персональних даних, зокрема забезпеченню цілісності, конфіденційності та доступності інформації. У роботі підкреслюється, що резервне копіювання є критичною складовою будь-якої системи управління даними, оскільки саме воно гарантує можливість відновлення інформації у разі технічних збоїв, помилок користувачів або зовнішніх кіберзагроз. Автор розглядає різні стратегії резервування (повне, інкрементне, диференційоване) та моделі зберігання копій як локально, так і на віддалених майданчиках. Окремий акцент зроблено на автоматизації процесів резервування та використанні політик зберігання, які дозволяють підтримувати баланс між безпекою, продуктивністю та ефективністю використання ресурсів. Робота [11] присвячена комплексному математичному моделюванню мережного трафіку та оцінці продуктивності в мультисервісних мережах, що характеризуються різнорідністю переданих даних, різними вимогами до затримок, пропускної здатності та надійності. Автори пропонують системний підхід до опису процесів маршрутизації, обробки та передачі трафіку, базований на апараті теорії масового обслуговування, стохастичних процесів і мережевих моделей. У роботі детально формалізовано структурні елементи мережі, включно з вузлами комутації, каналами зв'язку, сервісними чергами й потоками трафіку різних класів. Окрему увагу приділено врахуванню пропускної здатності каналів зв'язку, затримок різних типів (маршрутизаційних, комутаційних, транспортних) та механізмів управління чергами, що дає можливість проводити аналіз якості обслуговування (QoS), оцінювати й оптимізувати продуктивність мережі під час роботи з великими обсягами даних та множиною сервісів. Важливим аспектом дослідження є також методи оцінювання надійності мультисервісних мереж, у тому числі через моделювання механізмів резервування каналів та вузлів. Автори розглядають варіанти забезпечення стійкості мережної інфраструктури до відмов, дозволяючи кількісно оцінити вплив резервування на загальну доступність системи.

У руслі моделювання трафіку та аналізу продуктивності мереж дослідження [12] приділяє значну увагу системам управління трафіком, що забезпечують стабільність та ефективність роботи мережної інфраструктури в умовах змінних навантажень. У роботі детально розглянуто методи QoS, які дозволяють гарантувати пріоритетність окремих типів трафіку та забезпечити відповідний рівень якості обслуговування для критичних сервісів. Крім того, досліджується застосування механізмів traffic shaping, які спрямовано на згладжування пікових навантажень та запобігання перевантаженню каналів зв'язку, а також load balancing – балансування навантаження між маршрутизаторами, серверами або каналами з метою підвищення продуктивності й стійкості системи в цілому. Представлені методи є ключовими для підтримки оптимальної пропускної здатності, мінімізації затримок та стабільного функціонування мережі ЗВО, яка обслуговує велику кількість користувачів та різнорідних сервісів. У доповнення до цього у роботі [13] розглядається застосування графових моделей як універсального інструменту для аналізу структурних та функціональних характеристик комп'ютерних мереж. У таких моделях вузли графа відображають маршрутизатори, комутатори чи інші мережні елементи, тоді як ребра описують канали зв'язку. Вага ребра, що визначає пропускну спроможність каналу або затримку, дозволяє точно формалізувати параметри інфраструктури та виконувати розрахунки, необхідні для оптимізації мережі. Особливе значення має можливість обчислення максимального потоку між вузлами за допомогою класичних алгоритмів, таких як метод Форда-Фалкерсона, що створює основу для кількісної оцінки пропускної здатності окремих сегментів мережі, виявлення «вузьких місць» та визначення потенційних напрямів модернізації інфраструктури. Використання графових моделей також дозволяє аналізувати живучість мережі через оцінку альтернативних шляхів, виявлення критичних зв'язків та моделювання сценаріїв відмов.

Проведений аналіз підтверджує актуальність напрямку розробки математичної моделі, що формалізує структурні та функціональні особливості мультисегментної мережі ЗВО з фокусом на відмовостійкості та політиці безпеки. В рамках процесу моделювання «наповненості» КМ ЗВО слід орієнтуватися на методи, які спрямовані на забезпечення структурної та функціональної оптимізації. В даному напрямку дослідження мережу ЗВО слід розглядати як складну мультисегментну систему, ядро якої формується з основного маршрутизатора, до якого підключені сегменти через комутатори та маршрутизатори. В якості складових такої мережі можливо розглядати:

- комп'ютерні класи для здійснення навчальної діяльності;
- систему управління даними (ЄДЕБО та ДЕКАНАТ) для зберігання персональних даних здобувачів освіти та викладачів;

- систему відеоспостереження;
- адміністративний сегмент, орієнтований на управління фінансовими та кадровими аспектами;
- гостьовий доступ для користувачів, який відокремлений від внутрішньої мережі;
- підсистему зберігання та резервування даних.

Критично важливими вимогами, які висуваються до цих складових є:

- ізоляція трафіку між сегментами, що забезпечується використанням VLAN [14];
- резервування даних (використання RAID-масивів, реплікація в реальному часі);
- відмовостійкість ядра та каналів (дублювання маршрутизаторів та MultiWAN);
- захищеність від атак.

Взаємодія між складовими мережі відбувається через її ядро за допомогою кореневих комутаторів та маршрутизаторів [15], а міжсегментні з'єднання проходять через міжмережні екрани для розмежування доступу та забезпечення політики безпеки [16].

Метою цієї роботи є удосконалення математичної моделі функціонування КМ ЗВО, яка формалізує її ключові структурні елементи (сегменти, вузли, зв'язки), механізми відмовостійкості (резервування), а також політику безпеки та конфігурацію трафіку (VLAN, пропускна здатність).

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– проаналізувати сучасні складові моделей функціонування КМ ЗВО та виявити їх переваги та обмеження;

– удосконалити математичну модель шляхом розширення її складових, що дозволить інтегрувати політику безпеки та кількісно оцінювати показники надійності через ймовірність відмови;

– виконати експериментальні дослідження та за їх результатами провести порівняльний аналіз базової та модифікованої моделі КМ ЗВО з позиції гнучкості, ефективності та масштабованості.

Основна частина

За попереднім аналізом сучасного стану інфраструктури (апаратно-програмного забезпечення, мережної архітектури, інформаційно комунікаційної системи ЗВО) можливо зробити висновок, що КМ ЗВО є багаторівневою ієрархічною системою, що може включати ядро мережі, розподільчий рівень та рівень доступу до кінцевих пристроїв. Математично таку мережу можливо представити як неорієнтований або орієнтований граф (1), де кожне ребро графа може бути охарактеризовано набором параметрів (затримка передачі, пропускна здатність каналу, коефіцієнт надійності):

$$M = \{N, C\}, \quad (1)$$

де N (Nodes) – вузли КМ, C (Channels) – канали зв'язку між вузлами.

Щоб мережа ЗВО була продуктивною, надійною та безпечною, вона має відповідати певним технічним, організаційним та структурним вимогам: мати ієрархічну архітектуру, високу пропускну здатність та швидкодію, бути відмовостійкою, оперувати політиками безпеки, бути гнучкою та масштабованою, а також надавати можливість ефективного управління ресурсами мережі, орієнтуючись на потреби користувачів. КМ, що побудована на основі кортежу (1), на жаль не оперує поняттями, що перелічено вище, тому було вирішено розширити цю модель за рахунок додавання необхідних складових:

$$M = \{N, C, HA, BC, FR, SA, RM, SG, UB\}, \quad (2)$$

де N (Nodes) – вузли КМ, C (Channels) – канали зв'язку між вузлами, HA (Hierarchical Architecture) – ієрархічна архітектура, BC (Bandwidth & Capacity) – пропускна здатність та швидкодія, FR (Fault Tolerance & Redundancy) – відмовостійкість та резервування, SA (Security & Access Control) – безпека та контроль доступу, RM (Resource Management) – ефективне управління ресурсами, SG (Scalability & Flexibility) – масштабованість та гнучкість, UB (User-Based Requirements) – потреби користувачів.

КМ ЗВО буде продуктивною лише, тоді коли вона буде мати ієрархічну архітектуру, тобто буде поділена на декілька рівнів:

- рівень ядра, який забезпечує високу швидкість передавання даних між основними сегментами, мінімальну затримку та високу пропускну здатність;
- розподільчий рівень, який відповідає за маршрутизацію між VLAN, політики доступу, балансування навантаження;
- рівень доступу, який відповідає за підключення користувачів, лабораторій, серверів, відеосистем тощо.

Для реалізації такого підходу пропонується розширити складову, що відповідає за архітектуру:

$$HA = \{CL, DL, AL\}, \quad (3)$$

де CL (Core Layer) – рівень ядра (висока швидкість передавання даних, мінімальна затримка), DL (Distribution Layer) – розподільчий рівень (маршрутизація між VLAN, політики доступу, балансування навантаження), AL (Access Layer) – рівень доступу (підключення користувачів, лабораторій, серверів).

Розгортання КМ ЗВО з орієнтацією на ієрархічну архітектуру (3) спрощує у майбутньому адміністрування, підвищує масштабованість та надійність системи в цілому.

Складова, що відповідає за пропускну здатність та швидкодію (BC) – це ключовий показник ефективності комп'ютерної мережі ЗВО (4). Вона визначає, наскільки швидко дані можуть передаватися між користувачами, серверами, навчальними ресурсами та зовнішніми мережами. Щоб мережа задоволняла цим потребам, слід дотримуватися правил:

- ядро мережі повинно працювати з пропускною здатностью 1 Гбіт/с та більше, що забезпечує швидке обслуговування трафіку між корпусами, серверними кімнатами, дата-центрами та адміністративними сегментами;
- розподільчий рівень – бажано не менше 100 Мбіт/с, з можливістю агрегування каналів (Link Aggregation, LACP);
- рівень доступу – 100 Мбіт/с на робочу станцію, а для комп'ютерних класів або лабораторій з високим навантаженням повинна бути закладена підтримка 1 Гбіт/с Ethernet;

- для міжкорпусних з'єднань слід застосовувати оптоволоконні лінії, які забезпечують мінімальні втрати та затрим-ку сигналу.

$$BC = \{TO, LD, LB, MDT, SO, PM\}, \quad (4)$$

де TO (Traffic Optimization) – оптимізація трафіку, LD (Low Delay) – зменшення затримок, LB (Load Balancing) – балансування навантаження, MDT (Modern Data Transmission Technologies) – сучасні технології передачі даних, SO (Server Optimization) – оптимізація серверної інфраструктури, PM (Performance Monitoring) – моніторинг продуктивності.

Кортеж (4) формально описує основні елементи, що впливають на пропускну здатність та швидкодію комп'ютерної мережі ЗВО. Оптимізація трафіку в мережі (ТО) передбачає ефективне керування потоками даних з метою забезпечення стабільної роботи сервісів та раціонального використання ресурсів:

$$TO = \{QoS, DR, PC, SLB\}, \quad (5)$$

де QoS (Quality of Service) – вибір пріорітетного трафіку, DR (Dynamic Routing) – динамічна маршрутизація, PC (Proxy Caching) – кешування Proxy, SLB (Server Load Balancing) – балансування серверного навантаження.

Одним із ключових інструментів для цього є використання технології QoS, яка пріоритезує трафік відповідно до його важливості. Зокрема, найвищий пріоритет надається навчальним сервісам, таким як Moodle, Zoom, Meet та Microsoft Teams, оскільки вони забезпечують безпосередню підтримку освітнього процесу. Трафік службового або адміністративного призначення отримує середній пріоритет, що гарантує стабільну роботу внутрішніх інформаційних систем. Гостьовий доступ, який не є критичним для основної діяльності, має найнижчий рівень пріоритету, аби не перевантажувати основні канали зв'язку.

Для підвищення ефективності передачі даних слід застосовувати динамічну маршрутизацію (DR) за допомогою протоколів OSPF, EIGRP або BGP, що дозволяє автоматично обирати найоптимальніші шляхи руху трафіку залежно від стану мережі.

Важливим елементом оптимізації трафіку в мережі є використання технологій кешування через Proxy-сервери (PC), які зберігають копії даних, що часто використовуються. Такий підхід зменшує обсяг зовнішнього трафіку, прискорює доступ до ресурсів та знижує навантаження на зовнішні канали зв'язку

У комплексі всі заходи, шо зазначено у кортежі (5) створюють умови для стабільної, швидкої та надійної роботи мережної інфраструктури, особливо в середовищі з великою кількістю користувачів та критично важливими онлайн-сервісами. Додавання складової, що слідкує за зменшенням затримок у мережі (LD) є важливим аспектом підвищення її продуктивності та якості роботи корис-тувачів:

$$LD = \{L3S, MH, DNSC, CDN\}, \quad (6)$$

де L3S (Layer 3 Switching) – високошвидкісні комутатори L3, MH (Minimum Hops) – мінімізація «стрибків» між вузлами, DNSC (DNS Caching) – локальний DNS-кеш, CDN (Content Delivery Net-work) – мережа доставки контенту.

Основною метою цього процесу є скорочення часу, який витрачається на передачу даних між пристроями та сервісами. Для досягнення мінімальної затримки використовуються високошвидкісні комутатори третього рівня (L3S), які здатні обробляти трафік безпосередньо на апаратному рівні. Такий підхід забезпечує прискорення процесів маршрутизації, оскільки обробка пакетів здійснюється апаратно, а не програмно, що значно скорочує час їхнього проходження через мережу. Ще одним важливим чинником є мінімізація кількості «стрибків» між вузлами (MH), тобто зменшення кількості проміжних пристроїв, через які проходять дані на шляху від відправника до одержувача. Оптимальною вважається глибина маршруту у 2-3 переходи, що дозволяє уникати зайвих затримок, пов'язаних із перенаправленням трафіку між численними проміжними точками.

Великий вплив на швидкість доступу до ресурсів має оптимізація DNS-сервісів. Впровадження локального DNS-кешування (DNSC) дозволяє значно скоротити час пошуку потрібних адрес, що забезпечує швидший доступ до вебресурсів, які часто використовуються та зменшує навантаження на канали зв'язку.

Крім того, ефективним засобом зниження затримок є використання мереж доставки контенту (CDN). Завдяки цій технології освітні платформи, навчальні матеріали та інші ресурси зберігаються на серверах, розташованих географічно ближче до користувачів, що дозволяє значно прискорити завантаження контенту, покращити стабільність з'єднання та забезпечити комфортну роботу з навчальними онлайн-сервісами навіть при великій кількості одночасних підключень.

У сукупності всі заходи, що зазначено у кортежі (6) сприяють зниженню затримок у передачі даних, підвищенню швидкодії мережі та поліпшенню загальної якості досвіду користувача.

Балансування навантаження є важливою складовою забезпечення стабільної та ефективної роботи мережної інфраструктури (LB), особливо в умовах великої кількості користувачів та високих навантажень на сервери чи канали зв'язку. Основна мета цього процесу полягає в рівномірному розподілі запитів та трафіку між наявними ресурсами, що дозволяє уникнути перевантаження окремих вузлів і забезпечує безперервність роботи сервісів:

$$LB = \{SLB, NLB, MWS\}, \quad (7)$$

де SLB (Server Load Balancing) – серверне балансування навантаження, NLB (Network Load Balan-cing) – мережне балансування навантаження, MWS (MultiWAN support) – одночасне підключення до декількох провайдерів.

Одним із ключових напрямів є серверне балансування навантаження (SLB), яке передбачає розподіл запитів користувачів (наприклад, запитів здобувачів освіти до навчальних порталів чи БД) між кількома веб- або прикладними серверами. Завдяки цьому кожен сервер отримує лише частину загального навантаження, що запобігає його перевантаженню та підвищує стабільність функціонування всієї системи. Такий механізм дозволяє ефективно використовувати обчислювальні ресурси, забезпечує швидку обробку

запитів та підвищує загальну доступність освітніх сервісів, навіть у разі зростання кількості користувачів або тимчасового виходу з ладу одного з серверів.

Іншим напрямом є мережне балансування навантаження (NLB), яке полягає в оптимізації розподілу вихідного трафіку між кількома інтернет-каналами. У системах з підтримкою MultiWAN (MW) така технологія дозволяє одночасно використовувати декілька підключень до різних провайдерів, що підвищує пропускну здатність та надійність мережі. У разі збою або перевантаження одного з каналів трафік автоматично перенаправляється через інший, забезпечуючи безперервність роботи користувачів та сервісів.

Завдяки поєднанню серверного та мережного балансування (7) досягається високий рівень відмовостійкості, стабільності та продуктивності мережної інфраструктури, що є особливо важливим для навчальних середовищ, де безперервний доступ до онлайн-ресурсів має критичне значення.

Впровадження в мережу ЗВО сучасних технологій передачі даних (MDT) суттєво підвищує швидкодію, надійність та ефективність мережної інфраструктури:

$$MDT = \{EC, SDN, IPV6, WIFI\}, \quad (8)$$

де EC (EtherChannel) – об'єднання кількох фізичних ліній в один канал, SDN (Software Defined Networ-king) – централізоване керування мережею, IPV6 (In-ternet Protocol v6) – маршрутизація та адресація, WIFI (Wi-Fi Standards) – стандарти бездротових ліній зв'язку.

Одним із таких рішень є EtherChannel з використанням протоколу LACP, що дозволяє об'єднувати кілька фізичних ліній у один логічний канал. Цей підхід забезпечує збільшення пропускної здатності між комутаторами чи серверами, підвищує відмовостійкість мережі та дозволяє розподіляти навантаження між декількома фізичними кабелями, мінімізуючи ризик перевантаження окремого каналу.

Ще одним важливим інструментом є SDN, який забезпечує централізоване керування всією мережею. Завдяки цій технології адміністратори можуть динамічно оптимізувати маршрути трафіку, контролювати пріоритети даних і швидко адаптувати мережу до змінних умов, що особливо важливо для великих освітніх або корпоративних середовищ із високою активністю користувачів.

У комплексі всі технології, що наведено у кортежі (8) створюють високо продуктивну, надійну та масштабовану мережну інфраструктуру, здатну підтримувати сучасні освітні процеси та інтенсивне використання цифрових ресурсів.

Впровадження в мережу механізмів, що орієнтовані на оптимізацію серверної інфраструктури (SO), має на меті підвищення продуктивності, надійності та гнучкості обчислювальних ресурсів:

$$SO = \{VIRT, NVMe, RAID\}, \quad (9)$$

де VIRT (Virtualization) – віртуалізація, NVMe (High-speed NVMe storage) – швидкісні накопичувачі, RAID – масиви зберігання даних.

Один із ключових підходів, що спрямовані на оптиізації серверної інфрастуктури, полягає у використанні віртуалізованих серверів на платформах таких як VMware, Proxmox або Hyper-V. Віртуалізація дозволяє динамічно розподіляти ресурси між різними віртуальними машинами залежно від навантаження, що забезпечує ефективніше використання апаратного забезпечення та дозволяє швидко масштабувати обчислювальні потужності під потреби користувачів.

Для забезпечення одночасної високої швидкодії та надійності зберігання даних використовуються RAID-масиви, зокрема конфігурації RAID 10 або RAID 6. RAID 10 поєднує переваги дзеркалювання та смугування даних, що забезпечує швидкий доступ до інформації та одночасно високу відмовостійкість, тоді як RAID 6 дозволяє витримати вихід з ладу кількох накопичувачів без втрати даних. Такі рішення гарантують безперервність роботи сервісів та захист критично важливої інформації навіть у разі апаратних збоїв. У сукупності заходи, які представлено кортежем (9) забезпечують високу продуктивність, надійність та гнучкість серверної інфраструктури, що є критично важливим для сучасних освітніх та корпоративних систем. Застосування у комп'ютерній мережі механізмів, що допомогають здійснювати моніторинг продуктивності та серверної інфраструктури (PM) є критично важливим для забезпечення стабільної та ефективної роботи систем в цілому:

$$PM = \{NM, MPD, AN\}, \quad (10)$$

де NM (Network Monitoring) – мониторінг мережі, MPD (Monitoring of Performance Data) – набір систем моніторингу, AN (Alert Notifications) – механізм оповіщення про проблеми у роботі.

Наявність механізму маниторвнгу (NM) у мережі передбачає безперервний контроль швидкості передачі даних, навантаження на сервери та мережні вузли за допомогою спеціалізованих систем, таких як PRTG Network Monitor, Zabbix, Nagios або SolarWinds NPM. Цей набір інструментів дозволяє в реальному часі виявляти вузькі місця, де продуктивність мережі або серверів обмежується надмірним навантаженням чи технічними обмеженнями.

У комплексі моніторинг продуктивності (10) забезпечує прозорість роботи систем, своєчасне виявлення потенційних проблем та дозволяє планувати оптимізацію мережі та серверної інфраструктури на основі реальних даних.

Впровадження складової, що слідкує за відмовостійкістю системи та резервуванням інформації, якою вона оперує (FR), є ключовим аспектом забезпечення стабільної та безперебійної роботи мережної та серверної інфраструктури:

$$FR = \{BRD, TP, VRRP, MW, BCP\}, \quad (11)$$

де BRD (Backup Routers & Devices) – резервне обладнання, TP (Tree Protocol) – нбір технологій для уникнення петель, VRRP (Virtual Router Redundancy Protocol) – протокол для забезпечення дублювання шлюзів, MW (MultiWAN Channels) – розподіл трафіку між каналами та автоматичне переключення на резервний канал, BCP (Backup & Cloud Replication) – резервне копіювання.

Основною метою заходів, що зазначено у кортежі (11), є гарантування безперервного доступу до сервісів навіть у разі виходу з ладу окремих компонентів або каналів зв'язку. Для цього в мережах передбачають наявність резервних маршрутизаторів, комутаторів та

каналів зв'язку (BRD), які можуть автоматично підміняти основні вузли та лінії при їхньому збою, забезпечуючи безперервність передачі даних.

Для запобігання проблемам у топології мережі застосовуються технології STP та RSTP, які дозволяють уникати утворення петель та забезпечують стабільну маршрутизацію трафіку. Дублювання шлюзів реалізується за допомогою протоколів VRRP або HSRP, що дозволяє резервним шлюзам автоматично брати на себе функції основного у разі його відмови. У випадку підключення до кількох провайдерів використовується MultiWAN, що забезпечує розподіл трафіку між каналами та автоматичне переключення на резервний канал при збоях основного. Важливим елементом відмовостійкості є регулярне резервне копіювання даних (BCP), що досягається через використання RAID-масивів, які забезпечують збереження інформації навіть при виході з ладу окремих накопичувачів, а також через реплікацію даних у хмарі, що дозволяє мати актуальні резервні копії поза межами локальної інфраструктури. У результаті поєднання резервних пристроїв, дублікації каналів та шлюзів, а також систем резервного копіювання створюється комплексна система відмовостійкості, яка забезпечує надійну, безперебійну та стійку роботу мережі та серверів навіть у разі технічних збоїв чи перевантажень.

Механізми, які реалізують безпеку та рівень доступу у мережі (SA), є невід'ємними складовими сучасної мережної інфраструктури, що спрямовані на захист даних та забезпечення правильного розподілу прав користувачів:

$$SA = \{VLAN, FW, IPS, AC, ENC\}, \quad (12)$$

де VLAN (Segmentation of traffic) – VLAN сегментація, FW (Firewalls) – міжмережні екрани, IPS (Intru-sion Prevention System) – система запобігання несанкціонованих вторгнень, AC (Access Control) – система аутентифікації користувачів, ENC (Encryption) – захист переданих даних від перехоплення та несанкціонованого доступу.

Одним із основних заходів у цій сфері є сегментація мережі за допомогою VLAN, що дозволяє відокремлювати студентські, адміністративні та гостьові зони. Така організація забезпечує контрольоване обмеження доступу між різними групами користувачів та мінімізує ризик поширення загроз у мережі. Для захисту від кібератак використовуються міжмережні екрани (FW) та системи виявлення та запобігання вторгнень (IPS), які відстежують трафік, виявляють підозрілі дії та надають можливість блокувати потенційні загрози до того, як вони можуть вплинути на роботу мережі або сервісів. Контроль доступу до ресурсів реалізується через системи аутентифікації користувачів (AC), такі як RADIUS, LDAP або Active Directory, що дозволяють перевіряти права доступу та забезпечують централізоване управління обліковими записами. Такий підхід гарантує, що тільки авторизовані користувачі отримують доступ до відповідних ресурсів, а права та ролі можна налаштовувати відповідно до потреб організації.

Для захисту переданих даних від перехоплення та несанкціонованого доступу (ENC) застосовується шифрування трафіку. Використання VPN забезпечує безпечне віддалене підключення, HTTPS гарантує захищену передачу даних через вебсервіси, а сучасні стандарти Wi-Fi, такі як WPA3, підвищують безпеку бездротових підключень. У комплексі заходи, що впроваджено у скадову SA (12), забезпечують захист мережі, контроль за доступом до ресурсів та безпечну передачу даних, що особливо важливо в освітніх і корпоративних середовищах із великою кількістю користувачів та різнорівневими зонами доступу.

Ефективне управління ресурсами в сучасних мережних та серверних інфраструктурах за рахунок використання відповідного набору механізмів (RM) є ключовим фактором забезпечення стабільності, продуктивності та швидкого реагування на зміни навантаження чи потенційні проблеми (13):

$$RM = \{NMS, OEM, ACNF\}, \quad (13)$$

де NMS (Network Management Systems) – централізоване адміністрування, OEM (Operational Efficiency Monitoring) – моніторинг ефективності функціонування, ACNF (Automated Configuration) – автоматизація конфігурацій та оновлень.

Одним із основних підходів до досягнення цього є централізоване адміністрування за допомогою систем управління мережею (NMS). Централізоване адміністрування дозволяє контролювати всі вузли та пристрої мережі з одного інтерфейсу, відстежувати їхній стан, налаштовувати політики доступу, керувати конфігураціями та планувати масштабування ресурсів відповідно до потреб організації. Не менш важливим аспектом є моніторинг ефективності функціонування (OEM), який дає змогу відстежувати стан мережі та серверів у реальному часі. Застосування систем, таких як Nagios, Zabbix або PRTG, дозволяє контролювати завантаження каналів зв'язку, використання серверів пам'яті, затримки передачі даних та інші критичні параметри. Завдяки цьому адміністратори можуть своєчасно виявляти вузькі місця, потенційні проблеми та загрози, що дозволяє швидко реагувати та запобігати простою або зниженню продуктивності. Ще одним важливим елементом ефективного управління є автоматизація конфігурацій та оновлень (ACNF) за допомогою спеціалізованих інструментів, таких як Ansible або Cisco DNA Center. У результаті поєднання централізованого адміністрування, постійного моніторингу продуктивності та автоматиза-ції конфігурацій (13) досягається високий рівень ефективного управління ресурсами, що дозволяє підтримувати стабільну, безпечну та масштабовану мережну інфра-структуру навіть у складних і динамічних умовах експлуатації.

Масштабованість та гнучкість (SG) – це ключові характеристики освітньої мережної інфра-структури, які визначають здатність системи швидко адаптуватися до змінних потреб та зростання навантаження:

$$SG = \{NE, VRT, SDN, CT\}, \quad (14)$$

де NE (Network Expansion) – можливість розширення мережі, VRT (Virtualization) – підтримка віртуалізації, SDN (Software Defined Networking) – програмно-конфігуровані мережі, CT (Cloud Techno-logies) – хмарні технології.

Одним із проявів масштабованості є можливість легко розширювати мережу (NE) шляхом підключення нових корпусів, факультетів або лабораторій без необхідності повної перебудови існуючої інфраструктури. Такий підхід дозволяє організаціям ефективно реагувати на збільшення числа користувачів, нові освітні програми або технологічні проєкти, зберігаючи при цьому стабільність та продуктивність мережі.

Підтримка віртуалізації серверів та мережних елементів (VRT) є важливим інструментом досягнення гнучкості. У поєднанні з технологіями SDN, що дозволяють централізовано керувати потоками даних та змінювати маршрути передачі інформації у реальному часі, така інфраструктура стає максимально адаптивною та готовою до швидких змін.

Важливу роль у забезпеченні масштабованості таких систем відіграють хмарні технології (CT), які дозволяють зберігати великі обсяги даних, навчальні ресурси та резервні копії поза межами локальної інфраструктури. У сукупності масштабованість та гнучкість (14) дозволяють мережній та серверній інфраструктурі адаптуватися до умов освітнього процесу, які постійно змінюються, забезпечувати ефективне використання ресурсів та гарантувати безперервний доступ до сервісів навіть при різкому збільшенні кількості користувачів або розширенні функціональних потреб установи.

Орієнтація на потреби користувачів (UB) є ключовим принципом побудови сучасної освітньої мережної інфраструктури, оскільки саме комфорт та ефективність роботи кінцевих користувачів визначають успішність цифрових сервісів:

$$UB = \{SQ, WFC, GA\}, \quad (15)$$

де SQ (Service Quality) – висока якість обслуговування, WFC (Wi-Fi Coverage) – надійне покриття Wi-Fi, GA (Guest Access) – можливість гостьового доступу (ізольовані гостьові VLAN).

Одним із аспектів цього підходу є забезпечення високої якості обслуговування (SQ) для критичних застосунків, таких як ЄДЕБО, Moodle, Zoom, Meet та Microsoft Teams. Пріоритезація трафіку цих сервісів гарантує, що навчальні платформи, відеоконференції та електронні документообіги працюють стабільно та без затримок, що дозволяє здобувачам освіти та викладачам ефективно взаємодіяти та отримувати доступ до освітніх ресурсів у будь-який час без перебоїв або падіння продуктивності.

Ще одним важливим елементом орієнтації на користувача є надійне покриття Wi-Fi у всіх зонах перебування здобувачів освіти та співробітників. Мережа повинна забезпечувати стабільне та швидке з'єднання не лише у навчальних корпусах і лабораторіях, але й у інших громадських просторах на території установи. Такий підхід дає змогу користувачам залишатися підключеними до освітніх ресурсів та сервісів у будь-який момент, не знижуючи продуктивності освітнього процесу. Не менш важливою є можливість гостьового доступу (GA) до мережі, що дозволяє відвідувачам, гостям та стороннім користувачам підключатися без негативного впливу на безпеку та продуктивність внутрішньої мережі. Для цього застосовуються ізольовані гостьові VLAN та відповідні механізми контролю доступу, що гарантують захист критично важливих ресурсів та даних організації. У комплексі заходи, що зазначено у кортежі (15) дозволяють створити інфраструктуру, що орієнтована на кінцевого користувача, яка забезпечує стабільну роботу критичних сервісів, комфортний доступ до навчальних матеріалів та високий рівень безпеки, задовольняючи потреби здобувачів освіти, викладачів та гостей установи.

Результати та їх обговорення

На основі модифікованої моделі (2) та впроваджених функціональних механізмах (3-15), проведено ряд експериментів, що демонструють кількісне поліпшення ключових параметрів мережі ЗВО.

Зокрема експеремент, що визначає вплив (SQ) на затримку та продуктивність верифікує ефективність оптимізації трафіку (TO) та забезпечення потреб користувачів (UB) через механізм обирання пріорітетного трафіку QoS. Отже, в результаті проведення експерименту має бути сгенеровано критичний трафік (імітація відеоконференції (Meet, Zoom) та некритичний трафік (інтенсивне завантаження великих файлів), пічля чого слід виміряти середню затримку (RTT) критичного трафіку у двох режимах. Розглянемо докладніше ці два режими: перший режим (базова мережа) без застосування QoS, другий режим (оптимізована мережа) з активним QoS, де критичний трафік отримує найвищий пріоритет.

Результат генерації у першому режимі під впливом навантаження від некритичного трафіку: середня затримка критичного трафіку може сягати значень, більше 120 мс, що є неприйнятним для VoIP/Video. Перехід до другого режиму із застосуванням QoS призводить до суттєвого зниження RTT до декількох десятків мілісекунд, що підтверджує, що механізм QoS гарантує стабільне виділення смуги та високу якість обслуговування для пріоритетних навчальних сервісів (Meet, Zoom) та адміністративних систем (ЄДЕБО), відповідно до вимог UB.

Наступний експеремент описує можливості кількісної оцінки відмовостійкості (FR) та спрямований на визначення ефективності механізмів резервування, шляхом визначення часу відновлення сервісу (TTR) при моделюванні збоїв ключових компонентів. Розглянуто два критичні сценарії відмови: перший – це відмова основного шлюзу/маршрутизатора на розподільчому рівні, де активовано протоколи дуб-лювання шлюзів VRR; другий – це відмова основного інтернет-каналу, де використовуються резервування та розподіл трафіку MW (MultiWAN). У результаті при відмові основного шлюзу, перемикання на резервний шлюз за допомогою VRR відбувається менше ніж за 3 сек. При відмові основного зовнішнього каналу, переключення на резервний канал MultiWAN займає менше ніж 10 секунд. Отримані результати доводять, що реалізація механізмів (FR) забезпечує високий рівень відмовостійкості та мінімізує час простою мережі, що є критичним для безперервності роботи.

Мета третього експерименту підтвердити ефективність ізоляції критичних сегментів мережі, забезпечену VLAN сегментацією та міжмережними екранами (FW), як елементів безпеки та контролю доступу (SA). Розглянута спроба несанкціонованого доступу до «Адміністративного сегменту» мережі з гостьового та навчального сегментів. Отже, завдяки коректно налаштованим політикам (FW) та ізоляції, забезпеченій VLAN, всі спроби встановлення зв'язку (наприклад, Ping, Telnet) між ізольованими сегментами були заблоковані. Це підтверджує, що запропонована модель успішно реалізує вимогу безпеки та контролю доступу (SA), гарантуючи ізоляцію трафіку та захист критичних даних від неавторизованого доступу з інших сегментів мережі ЗВО.

Висновки

Проведений аналіз та експерименти показали, що запропонована модель функціонування комп'ютерної мережі ЗВО (2) ефективно формалізує багатоаспектну інфраструктуру, що є критично важливою для сучасного закладу освіти. Зазначена модель враховує необхідність функціонального розділення мережі на сегменти. Основними її перевагами є здатність інтегрувати політику безпеки та кількісно оцінювати надійність через ймовірність відмови, що дозволяє створювати масштабовані, гнучкі та безпечні мережні рішення, які мінімізують ризики для критичних даних та забезпечують безперервність освітнього процесу.

Проведений аналіз та розроблена математична модель функціонування КМ ЗВО успішно формалізують багатоаспектну інфраструктуру, що є критично важливою для сучасного закладу освіти.

Основними перевагами моделі є:

- формалізація структурних та функціональних вимог: запропонована модель (2) включає ключові структурні елементи (N, C) та сім основних функціональних вимог: ієрархічну архітектуру (HA), пропускну здатність та швидкодію (BC), відмовостійкість та резервування (FR), безпеку та контроль доступу (SA), управління ресурсами (RM), масштабованість та гнуч-кість (SG), орієнтацію на потреби користувачів (UB);

- сегментація та безпека: модель враховує необхід-ність функціонального розділення мережі на сегменти (VLAN) для різних цілей (навчання, адміністрація, зберігання даних, відеоспостереження), що дозволяє створювати безпечні мережні рішення, які мінімізують ризики для критичних даних (ЄДЕБО/ДЕКАНАТ) та забезпечують безперервність освітнього процесу;

- інтеграція відмовостійкості: основною перевагою моделі є її здатність інтегрувати механізми відмо-востійкості та резервування (FR), включаючи дублю-вання маршрутизаторів, шлюзів (VRRP) та MultiWAN, що дозволяє кількісно оцінювати надійність через ймовірність відмови критичних компонентів.

Експериментальні дослідження підтвердили ефективність механізмів, що було закладено у моделі. Подальші дослідження будуть зосереджені на кількісній оцінці впливу програмно-конфігурованих мереж (SDN) та віртуалізації (SG) на динамічну масштабованість мережі, а також розробці або модифікації алгоритмів автоматизованого керування політиками безпеки та маршрутизацією на основі даних, отриманих від систем моніторингу RM.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Використання засобів штучного інтелекту

Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

СПИСОК ЛІТЕРАТУРИ

1. Філімончук Т. В., Плюта А. О. Структура інформаційної системи, що орієнтована на онлайн-навчання. *Систнеми управління, навігації та зв'язку.* 2021. Вип. 4(66). С. 69–72. URL: https://doi.org/10.26906/SUNZ.2021.4.069
2. Жураковський. Б. Ю., Зенів І. О. Комп'ютерні мережі : навчальний посібник. Частина 1. Київ : КПІ ім. Ігоря Сікорського, 2020. 328 с. URL: https://ela.kpi.ua/items/55130022-a21a-474f-8047-028555236092
3. Нашинець-Наумова А. Ю., Бурячок В. Л., Коршун Н. В., Жильцов О. Б., Складанний П. М., Кузьменко Л. В. Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання.* 2020. Т. 77. № 3. С. 337–354. URL: https://doi.org/10.33407/itlt.v77i3.3424
4. Васянін В. О., Трофимчук О. М., Ушакова Л. П. Дослідження задачі оптимізації структури ієрархічної комунікаційної мережі при зміні її параметрів. *Екологічна безпека та природокористування.* 2024. Вип. 49 (1). С. 99–125. URL: https://doi.org/10.32347/2411-4049.2024.1.99-125
5. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. К. : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с. URL: https://ela.kpi.ua/items/8a692251-3210-4a77-b623-9db1af4fa5b2
6. Fahmi K., Leith D., Kucera S., Claussen H. Understanding MPTCP in Multi-WAN Routers: Measurements and System Design. 2021 IEEE 46th Conference on Local Computer Networks. 2021. URL: https://doi.org/10.1109/LCN52139.2021.9524976
7. Ткачов В. М., Коваленко А. А., Фесенко Т. Г. Оптимізація мережного алгоритму функціонування комп'ютерних мереж підвищеної живучості на мобільній платформі на етапі їх проектування. *Зв'язок, телекомунікації та радіотехніка.* 2021. Том 3 №65. С. 143–147. URL: https://doi.org/10.26906/SUNZ.2021.3.143
8. Коник Р. С. Живучість інформаційної системи та основні напрямки її підвищення. *Зв'язок.* №4, 2017. С. 21-23. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/808732

9. Бондаренко Л. О., Масесов М. О., Єфанова К. О., Садиков О. І. Оцінка живучості ієрархічних телекомунікаційних мереж військового призначення. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. Т. 31. №1. С. 61–67. URL: https://journals.indexcopernicus.com/search/article?articleId=1976195
10. Nelson S. Pro Data Backup and Recovery. New York: Apress, 2011. 296 p. URL: https://doi.org/10.1007/978-1-4302-2663-5
11. Поповський, В. В. та ін. Математичні основи теорії телекомунікаційних систем. Харків: Компанія СМІТ, 2006. 500 с. URL: https://opac.kntu.kr.ua/cgi-bin/koha/opac-detail.pl?biblionumber=4049
12. Лушпа Б. Є., Куриленко А. О., Янковський О. А. Управління трафіком мереж. Тринадцята міжнародна науково-технічна конференця «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». Баку-Харків-Жиліна-2023. Т. 2, секція 2. С. 103. URL: https://doi.org/10.32620/ICT.23.t2
13. Трасковецька Л., Боровик Л., Боровик О. Застосування графових моделей для дослідження характеристик комп'ютерних мереж. *Вісник Хмельницького національного університету.* 2023. Вип. 91(2). С. 185–191. URL: https://doi.org/10.32453/3.v91i2.1417
14. Jadah H. M. Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise. International Journal of Advanced Networking and Applications (IJANA). 2021. Vol. 12 Issue: 06. Pp: 4750-4762. URL: https://doi.org/10.35444/IJANA.2021.12604
15. Liu L.. Computer Network Routing Optimization Algorithm Based on Neural Network Model. Asia-Pacific Conf. on Image Processing, Electronics and Computers (IPEC). 2023. Pp. 490–493. URL: https://doi.org/10.1109/IPEC57296.2023.00091
16. Liu N., Fan W., Fan J., Zheng H. Fault-Tolerant Secure Routing Based on Trust Evaluation Model in Data Center Networks. *Security and Communication Networks*. Vol. 2022. Issue 1. 2022. https://doi.org/10.1155/2022/9339515

Received (Надійшла) 01.12.2025
Accepted for publication (Прийнята до друку) 11.02.2026
Publication date (Дата публікації) 27.02.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Суровицький Микола Миколайович – магістрант, Харківський національний університет радіоелектроніки, Україна;
Mykola Surovytskyi – master's student, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: mykola.surovytskyi@nure.ua; ORCID Author ID: https://orcid.org/0009-0009-4675-4354.

Філімончук Тетяна Володимирівна – кандидат технічних наук, доцентка, доцент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Tetiana Filimonchuk – PhD, Associate Professor of the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: tetiana.filimonchuk@nure.ua; ORCID Author ID: http://orcid.org/0000-0002-4380-504X;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57190949991.

Партика Станіслав Олександрович – старший викладач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Stanislav Partyka – Senior lecturer of the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: stanislav.partyka@nure.ua; ORCID Author ID: http://orcid.org/0000-0002-7376-8980;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57204560890.

Севостьянова Олена Миколаївна – старший викладач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Olena Sevostianova – Senior lecturer of the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: olena.sevostianova@nure.ua; ORCID: http://orcid.org/0009-0008-2595-5133.

Optimization model of a higher education institution's computer network based on data transmission technologies

Mykola Surovytskyi, Tetiana Filimonchuk, Stanislav Partyka, Olena Sevostianova

Abstract. The relevance of the study is determined by the rapid development of information technologies and the digitalization of the educational process, which makes the proper organization of a computer network in a higher education institution critically important. Modern higher education institution networks face challenges related to the functional segmentation of network segments, the need to ensure the security of critical data from guest access, and the requirements for infrastructure scalability, flexibility, and fault tolerance. In this regard, the development of a mathematical model that formalizes the structural and functional features of a multi-segment higher education institution network, focusing on fault tolerance and security policies, becomes relevant. **The object of the study** is the computer network of a higher education institution, encompassing its structure, technical means, and operational processes. **The subject of the study** is the methods, models, and technologies for optimizing the operation of this network based on modern data transmission technologies. **The result of the work** is an improved mathematical model for the functioning of an higher education institution computer network that combines seven key requirements: building a hierarchical architecture, ensuring high throughput and performance, supporting fault tolerance and redundancy, guaranteeing security and access control, rational resource management, enabling scalability and adaptivity, and considering user needs. The conducted experimental tests confirmed the effectiveness of the proposed mechanisms. **Conclusions.** The proposed model effectively formalizes the multi-faceted infrastructure of an higher education institution computer network and is capable of quantitatively assessing reliability through the probability of critical component failure. This allows for the creation of scalable, flexible, and secure network solutions that minimize risks to critical data and ensure the continuity of the educational process.

Keywords: computer network of a higher education institution, mathematical model, multi-segment system, fault tolerance, redundancy, VLAN, security policy, firewall.