УДК 004.77
DOI: https://doi.org/10.53920/ITS-2024-2-3

Андрій Вікторович ЛЕМЕШКО,
доктор філософії, доцент,
Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0001-8003-3168
Ольга Миколаївна ТКАЧЕНКО,
доктор технічних наук, професор,
Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0001-7983-9033
Артем Васильович АНТОНЕНКО,
кандидат технічних наук, доцент
Національний університет біоресурсів і природокористування України
ORCID ID: 0000-0001-9397-1209
Микола Анатолійович ЛЯШУК,
викладач, Заклад вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая»
ORCID ID: 0009-0007-2910-4160

ВПРОВАДЖЕННЯ ПРИСТРОЇВ І СИСТЕМ ДЛЯ ПІДВИЩЕННЯ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПРИВАТНИХ ПІДПРИЄМСТВ

У роботі досліджено сучасні підходи до забезпечення безпеки інфокомунікаційних мереж, зокрема локальної мережі підприємства. Проаналізовано переваги та недоліки різних пристроїв та архітектур безпеки, а також їх вплив на захист інформаційних систем від кіберзагроз. За допомогою Cisco Packet Tracer змодельовано мережеві інфраструктури для оцінки ефективності інтеграції міжмережевих екранів, систем IDS/IPS та VPN-з'єднань. Розглянуто концепції нульової довіри та сегментації мережі.

Результати дослідження дають уявлення про найбільш ефективні стратегії зменшення ризиків у локальній мережі. Крім того, розглядаються проблеми впровадження та найкращі практики розгортання заходів безпеки в реальних умовах підприємства, підкреслюється важливість постійного моніторингу та регулярного оновлення протоколів безпеки для забезпечення стійкості до нових загроз. Крім того, дослідження підкреслює роль навчання та обізнаності працівників у підтримці мережевої безпеки. Інтегруючи передові рішення з безпеки та розвиваючи культуру безпеки, підприємства можуть значно посилити свої захисні механізми. Нарешті, результати дослідження свідчать про те, що багаторівневий підхід до безпеки має вирішальне значення для надійного захисту від кіберзагроз.

Ключові слова: *мережа, топологія, ієрархічна модель, брандмауер, системи безпеки, персоналізація, штучний інтелект, онлайн-освіта, е-освіта.*

Andrii LEMESHKO,
Doctor of Philosophy, associate Professor,
Taras Shevchenko National University of Kyiv
Olha TKACHENKO,
Doctor of technical sciences, professor
Taras Shevchenko National University of Kyiv
Artem ANTONENKO,
Candidate of technical sciences, associate professor
National University of Life and Environmental Sciences of Ukraine
Mykola LIASHUK,
Teacher, Higher Education Institution «Academician Yuriy Bugay International Scientific and Technical University»

IMPLEMENTATION OF DEVICES AND SYSTEMS TO ENHANCE THE PROTECTION OF THE NETWORK INFRASTRUCTURE OF PRIVATE ENTERPRISES

The paper investigates modern approaches to ensuring the security of information and communication networks, in particular, the local enterprise network. The advantages and disadvantages of various security devices and architectures, as well as their impact on the protection of information systems from cyber threats, are analysed. Using Cisco Packet Tracer, network infrastructures are modelled to assess the effectiveness of the integration of firewalls, IDS/IPS systems and VPN connections. The concepts of zero trust and network segmentation are considered.

The results of the study provide insight into the most effective strategies for mitigating risks in a local network. In addition, it discusses the challenges of implementing and best practices for deploying security measures in real-world enterprise environments, and emphasises the importance of continuous monitoring and regular updates to security protocols to ensure resilience to new threats. The study also highlights the role of employee training and awareness in maintaining network security. By integrating advanced security solutions and developing a security culture, enterprises can significantly strengthen their defences. Finally, the study's findings suggest that a layered approach to security is crucial to ensure that businesses are well protected against cyber threats.

Keywords: *network, topology, hierarchical model, firewall, security systems, personalisation, artificial intelligence, online education, e-education.*

Постановка проблеми. У сучасному цифровому світі бізнесу необхідна стабільна та надійна мережева інфраструктура. Відмова в ро-

боті мережі може призвести до серйозних проблем, простоїв та втрати прибутку. Тому проблема забезпечення відмовостійкості мереж актуальна і важлива для підприємств. Забезпечення відмовостійкості мереж є ключовим завданням для успішної роботи підприємства.

Для досягнення цього необхідно використовувати спеціалізовані апаратно-програмні засоби, які забезпечують високий рівень безпеки, здійснюють моніторинг комп'ютерної системи в режимі реального часу, захищати дані від зовнішніх і внутрішніх атак, а також своєчасно реагувати на спроби несанкціонованого доступу [1].

Аналіз останніх досліджень і публікацій. Оскільки обсяги інформації, що передається в електронному вигляді, постійно зростає, важливо враховувати безпеку під час функціонування локальної мережі. Незважаючи на те, що велика увага приділяється безпроводовим мережам і віддаленому доступу до них, важливо враховувати масштаб мережі, а саме:

- невелику домашню мережу, яка з'єднує кілька комп'ютерів один з одним та з глобальною мережею Інтернет;
- малий офіс, що дозволяє завдяки комп'ютеру підключатися до корпоративної мережі чи отримувати доступ до централізованих, спільних ресурсів з метою забезпечення роботи офісу;
- мережу середнього та великого розмірів можуть охоплювати декілька локацій із сотнями або тисячами з'єднаних комп'ютерів;
- глобальну мережу Інтернет, що з'єднує сотні мільйонів комп'ютерів.

Необхідність врахування масштабу мережі під час обрання інструментів для її захисту зумовлено тим, що навіть найпоширеніші типи мережевих інфраструктур (локальні мережі та глобальні мережі) суттєво відрізняють за: площею; кількості під'єднаних користувачів; діапазоном і послугами; сферою відповідальності [2].

Мета цієї статті. Дослідження сучасних підходів до забезпечення безпеки інфокомунікаційних мереж, та запропонувати апаратно-програмні рішення що, гарантують максимальну відмовостійкість.

Виклад основного матеріалу дослідження.

Типи мережних інфраструктур.

Інтернет – це всесвітнє об'єднання взаємопов'язаних локальних (LAN) і глобальних мереж (WAN). Локальні мережі з'єднуються між собою за допомогою глобальних мереж, що беруть на себе функцію обміну інформації між локальними мережами (Рис. 1).

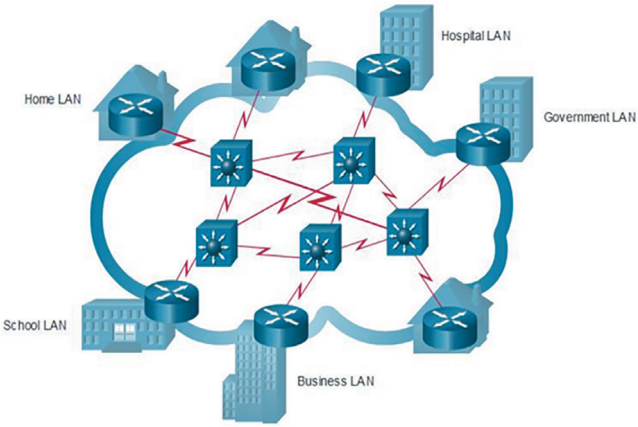

Рис. 1. Приклад мереж LAN, підключених до мережі WAN

Джерело: [5]

Інтернет ще можна назвати «конвергентною мережею» що складається з публічних та приватних мереж де публічна мережа забезпечує переміщення цифрового трафіку між приватними мережами (Рис. 2).

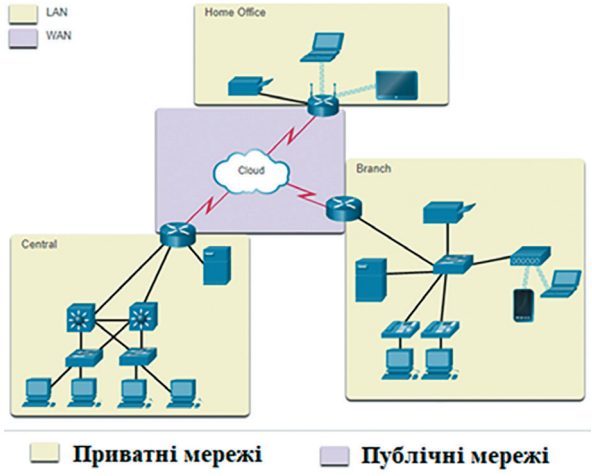

Рис. 2. Приватні мережі LAN, підключені до публічної мережі WAN

Джерело: [5]

Така назва пов'язана з тим, що в публічній мережі використовується пул публічних IP, а в приватних відповідно використовують пул приватних IP це стосується в першу чергу мереж які функціонують на базі протоколу IPv4. Результати порівняння мереж занесено в (табл. 1).

Таблиця 1. Порівняння LAN та WAN

LAN	WAN
З'єднує кінцеві пристрої на обмеженій території.	З'єднує локальні мережі на значних географічних відстанях.
Адмініструється окремою організацією або особою.	Зазвичай адмініструється кількома провайдерами послуг.
Забезпечує високошвидкісну пропускну здатність для внутрішніх кінцевих пристроїв та проміжних пристроїв.	Зазвичай створюють повільніші канали зв'язку між локальними мережами.

Джерело: [5]

Ієрархічні моделі приватних мереж.

У середніх за розмірами і кількістю користувачів проводових локальних мереж для виокремлення у мережній топології груп модулів або рівнів пропонується застосовувати ієрархічну модель (Рис. 3).

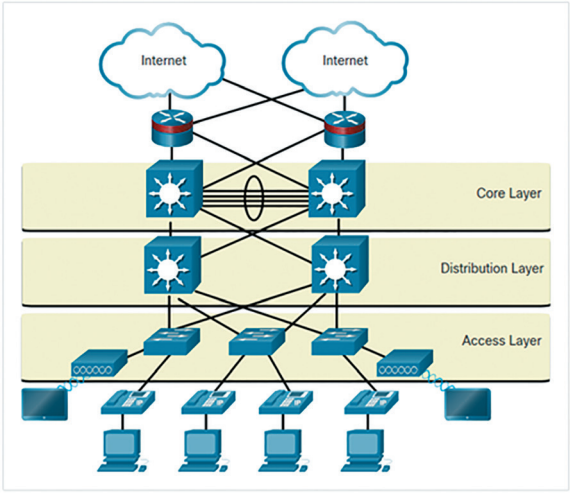

Рис. 3. Ієрархічна модель дизайну

Джерело: [5]

Ієрархічне проектування LAN містить три рівні:

1. Доступ – надає кінцевим точкам і користувачам прямий доступ до мережі.

2. Розподіл – агрегує рівні доступу та забезпечує підключення до служб.

3. Ядро – забезпечує підключення між рівнями розподілу для великих локальних середовищ.

Хоча ієрархічна модель має три рівні, деякі невеликі корпоративні мережі можуть реалізовувати дворівневу ієрархічну структуру (рис. 4).

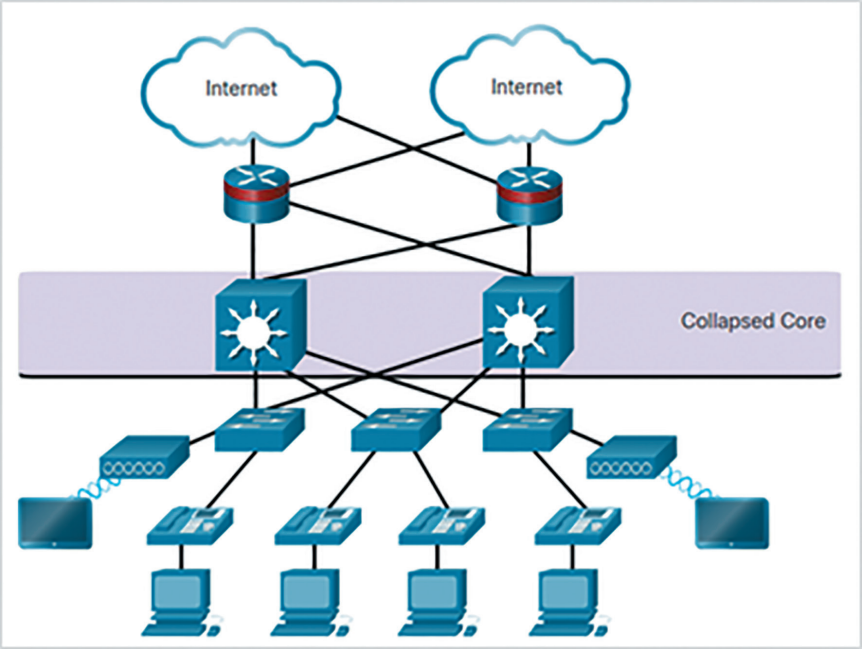

Рис. 4. Згорнуте ядро

Джерело: [5]

При використанні даної дворівневої ієрархічної структури, базовий та розподільний рівні об'єднуються в один рівень, що зменшує вартість та складність.

Аналіз готових рішень

З іншого боку, більшість локальних мереж, як і глобальні мережі розроблено як згорнуті магістральні мережі за допомогою комутатора рівня 2 або 3 (рис. 5).

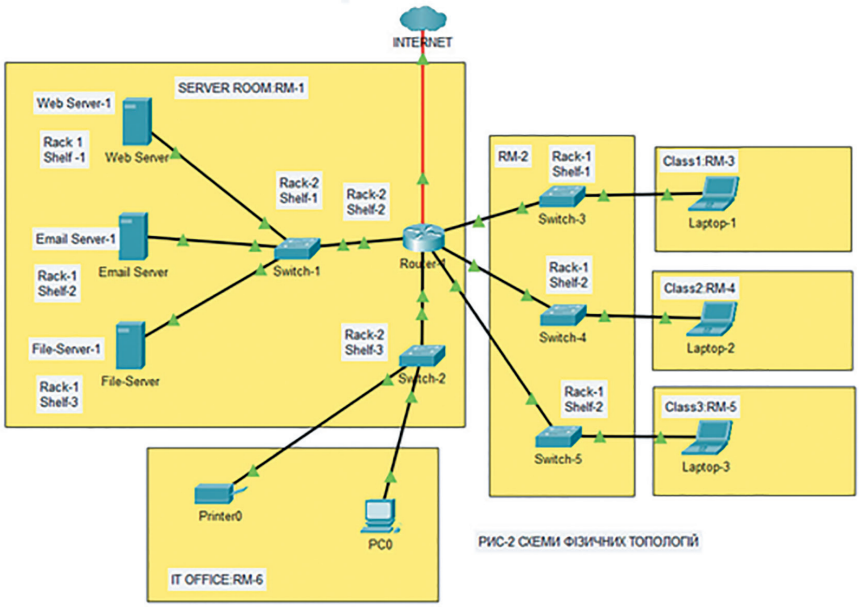

Рис. 5. Приклад мережі LAN, підключеної до мережі WAN

Джерело: [5]

Недоліком такої побудови мережі є те, що, якщо комутатор або маршрутизатор вийшов з ладу через збій живлення, сегмент або вся мережа може припинити роботу до відновлення живлення або заміни обладнання, що вийшло з ладу внаслідок збою. Такий вихід з ладу обладнання є дуже поширеним явищем під час стабілізаційних відключень електроенергії в об'єднаній енергетичній системі України внаслідок військових дій. У деяких випадках збій мережі є результатом вірусної атаки на вторинне сховище, що призводить до втрати даних.

У зв'язку з тим, що традиційні моделі безпеки комп'ютерних мереж поступово втрачають свою ефективність, виникає нагальна потреба у розробленні та впровадженні нових підходів для забезпе-

чення захисту автоматизованих інформаційних систем від сучасних кіберзагроз, що ставить перед організаціями завдання пошуку досконаліших методів захисту, які б відповідали вимогам сучасних корпоративних сервісів і продуктів.

З огляду на це, актуальним завданням є розроблення способів удосконалення безпеки корпоративної мережі, зокрема підвищення ефективності захисту її операційних середовищ, даних і вузлів. Важливо, щоб нові підходи враховували специфіку сучасних кіберзагроз, зростаючу складність атак, а також обмеженість ресурсів, доступних для імплементації рішень.

Тому, для знаходження ефективного шляху реалізації захисних заходів, необхідно враховувати такі важливі фактори, як складність впровадження, вартість рішень, а також обмежені технічні та фінансові ресурси, що є типовими для більшості організацій.

Сучасні тренди забезпечення мережевої безпеки швидко змінюються через зростаючі кіберзагрози, розвиток технологій та нові виклики, пов'язані з масштабованістю мереж і цифровізацією бізнесу.

Як-от, концепція Zero Trust передбачає, що жоден користувач або пристрій не вважають надійним, навіть якщо він знаходиться всередині корпоративної мережі, тому для доступу до ресурсів необхідна постійна перевірка ідентифікації користувача, пристрою та дій, що виконує цей користувач.

Новим викликом є використання штучного інтелекту та машинного навчання для виявлення загроз та автоматизації процесів безпеки. Ці технології аналізують великі обсяги даних для виявлення аномалій і кібератак на ранніх стадіях. Їх також використовують для автоматизації відповіді на інциденти.

Відомим підходом є SASE (Secure Access Service Edge), що означає об'єднання мережевих технологій і функцій безпеки, таких як SD-WAN, VPN, міжмережеві екрани в одну хмарну платформу. SASE дозволяє захистити віддалений доступ до корпоративних ресурсів, незалежно від місця перебування користувачів.

Зі зростанням поширеності хмарних сервісів з'являються нові виклики у сфері безпеки. Організації фокусуються на захисті хмарної цифрової інфраструктури, використовуючи хмарні міжмережеві екрани, багатофакторну аутентифікацію, шифрування даних у хмарі.

Застосовують нині Endpoint Detection and Response (EDR), що передбачає активний моніторинг і виявлення загроз на кінцевих пристроях, таких як комп'ютери, мобільні пристрої або сервери. Системи

EDR не тільки ідентифікують загрози, але й дозволяють швидко реагувати на них для мінімізації шкоди [3].

Через зростання кількості IoT-пристроїв важливим аспектом стає їх захист. IoT-пристрої часто вразливі через недостатні можливості для оновлення та слабкий рівень захисту. Нові рішення спрямовано на моніторинг цих пристроїв та запобігання потенційним загрозам.

Технології аналізу ризиків у режимі реального часу дозволяють установам виявляти потенційні загрози на основі поточних даних і миттєво вживати заходів для захисту.

DevSecOps – це інтеграція безпеки у всі етапи розроблення програмного забезпечення, що дозволяє виявляти і виправляти вразливості на ранніх етапах розробки, що знижує загальні ризики.

Мультифакторна аутентифікація стає стандартом для захисту облікових записів і зменшення ризику несанкціонованого доступу до мереж і систем. Використання декількох факторів аутентифікації, таких як паролі, одноразові коди чи біометричні дані значно підвищує рівень безпеки.

Тому зі зростанням кількості віддалених співробітників багато компаній інвестують у рішення для забезпечення безпечного доступу до корпоративних ресурсів, таких як VPN, хмарні рішення для безпеки, та рішення для моніторингу віддалених робочих середовищ [4].

Дійсно, мережева безпека стає дедалі складнішою, і підприємства мають адаптуватися до нових викликів через впровадження сучасних технологій і стратегій.

У зв'язку з постійним розвитком кіберзагроз і технологій, необхідно обирати такі рішення, що не лише забезпечують високий рівень захисту, але й можуть бути ефективно впроваджені з урахуванням специфіки підприємства та доступних ресурсів, що вимагає ретельного аналізу наявних технологій та їхньої адаптації до потреб компанії.

Впровадження пристроїв та систем.

Розглянемо можливості використання апаратних і програмних засобів, таких як міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), VPN для безпечного з'єднання, а також архітектурні рішення, включаючи Zero Trust та сегментацію мережі, що сприяють підвищенню рівня захисту без значного збільшення витрат.

Таким чином, детальний аналіз цих компонентів допоможе знайти оптимальні шляхи для впровадження захисних заходів в типову інфраструктуру мережі з урахуванням поточних ресурсних обмежень та технічних вимог.

Архітектури безпеки.

Дизайн брандмауера полягає, передусім, в інтерфейсах пристроїв, що дозволяють чи забороняють трафік за джерелом, призначенням та типом трафіку. Три конструкції брандмауера є такими.

1. Публічний і приватний – це загальнодоступна/публічна мережа (зовнішня мережа) – ненадійна мережа, приватна мережа (внутрішня мережа) – надійна мережа (рис 6).

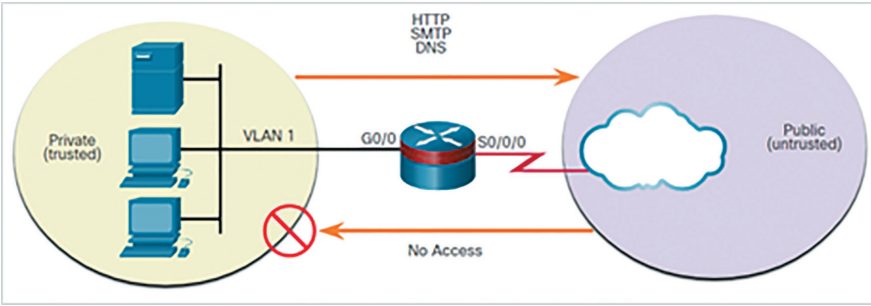

Рисунок 6. Захист приватної мережі

Джерело: [5]

2. Демілітаризована зона (DMZ), в якій конструкція брандмауера передбачає:

- внутрішній інтерфейс, підключений до приватної мережі.
- зовнішній інтерфейс, підключений до загальнодоступної мережі.
- інтерфейс DMZ (рис. 7).

3. Міжмережеві екрани на базі зональних політик. ZPF використовують концепцію зон, щоб забезпечити додаткову гнучкість. Зона – це група з одного чи декількох інтерфейсів, які мають схожі функції або характеристики. Зони допомагають зазначити, де слід застосовувати правило чи політику міжмережевого екрану (рис. 8).

Пристрої безпеки.

Міжмережевий екран (Firewall) – це система або група систем, яка забезпечує реалізацію політики контролю доступу між мережами. Загальні характеристики міжмережевих екранів є такі:

- стійкість до атак на мережу;
- забезпечення виконання політики контролю доступу.

Переваги та недоліки міжмережевих екранів занесено у таблицю (табл. 2).

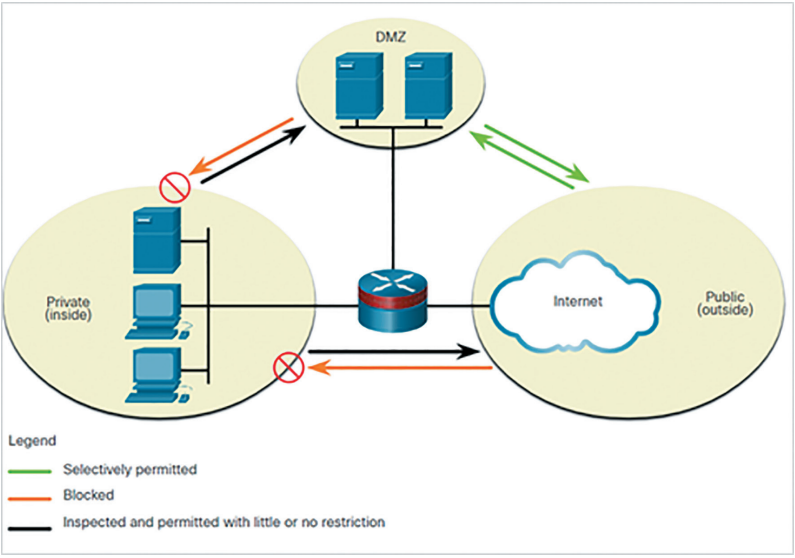

Рис. 7. Демілітаризована зона (DMZ)

Джерело: [5]

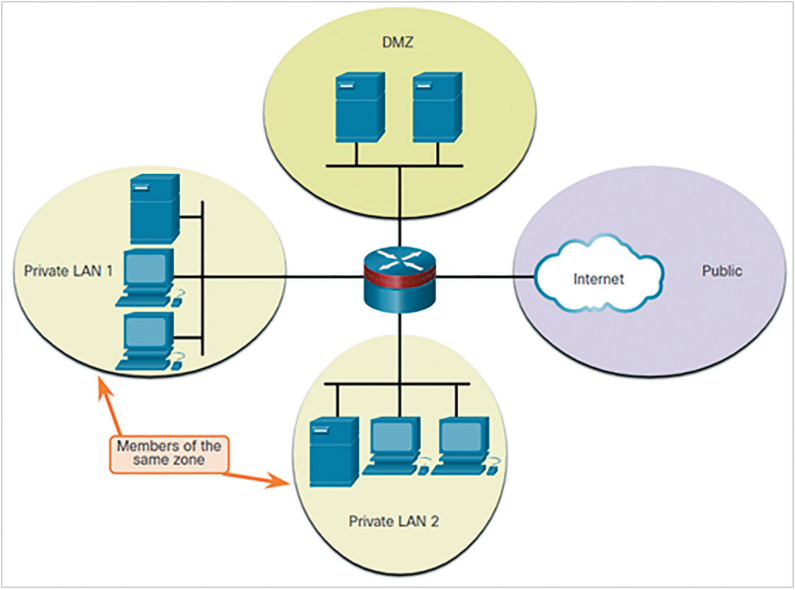

Рис. 8. Міжмережеві екрани на базі зональних політик

Джерело: [5]

Таблиця 2. Переваги та недоліки міжмережевих екранів

Переваги міжмережевого екрану	Недоліки міжмережового екрану
Запобігає зламу чутливих хостів, ресурсів і застосунків недовірливими користувачами.	Неправильно налаштований міжмережевий екран може мати серйозні наслідки для мережі, наприклад, стати єдиною точкою відмови.
Очищає потік протоколу, що запобігає використанню недоліків протоколу.	Дані з багатьох застосунків не можуть бути безпечно передані через міжмережеві екрани.
Блокує шкідливі дані від серверів і клієнтів.	Користувачі можуть активно шукати способи обходу захисту міжмережевого екрану для отримання матеріалу блокування, що відкриває мережу для потенційної атаки.
Знижує складність управління безпекою.	Продуктивність мережі може знижуватися.

Джерело: [5]

Зміна парадигми мережевої архітектури вимагає захисту від швидкоплинних еволюціонуючих атак, що вимагає застосування економічно ефективних систем, такі як-от: системи виявлення вторгнень (IDS); системи запобігання вторгненням (IPS); архітектура мережі інтегрує ці рішення до вхідних та вихідних точок мережі. Технології IPS та IDS можуть доповнювати одна одну. Рішення щодо того, який варіант впроваджувати, приймають із врахуванням безпекових цілей організації та переваг і недоліків технологій IPS та IDS що занесено в таблицю (табл. 3).

Таблиця 3. Переваги та недоліки технологій IPS і IDS

Реалізація	Переваги	Недоліки
IDS	Відсутній вплив на мережу (затримка, джитер). Відсутній вплив на мережу при виході з ладу сенсора. Немає впливу мережі, якщо є перевантаження сенсора.	Дія у відповідь не може зупинити пересилання пакетів. Необхідні правильні налаштування для дій у відповідь. Вразливіші до технік обходу засобів мережевої безпеки.
IPS	Зупиняє пересилання пакетів. Можна застосовувати техніки нормалізації потоків трафіку.	Проблеми з сенсором можуть вплинути на мережевий трафік. Перевантаження сенсора впливає на мережу. Наявний певний вплив на мережу (затримка, джитер).

Джерело: [5]

Врахувавши переваги та недоліки різних пристроїв і архітектур безпеки можна прийняти рішення щодо вдосконалення сегментів мережі LAN (рис. 1) з використанням програмного середовища Cisco Packet Tracer, що дозволило не лише моделювати можливі загрози, а й протестувати різні конфігурації захисту в умовах, наближених до реальних. Отриманий сегмент мережі наведено на рис. 9.

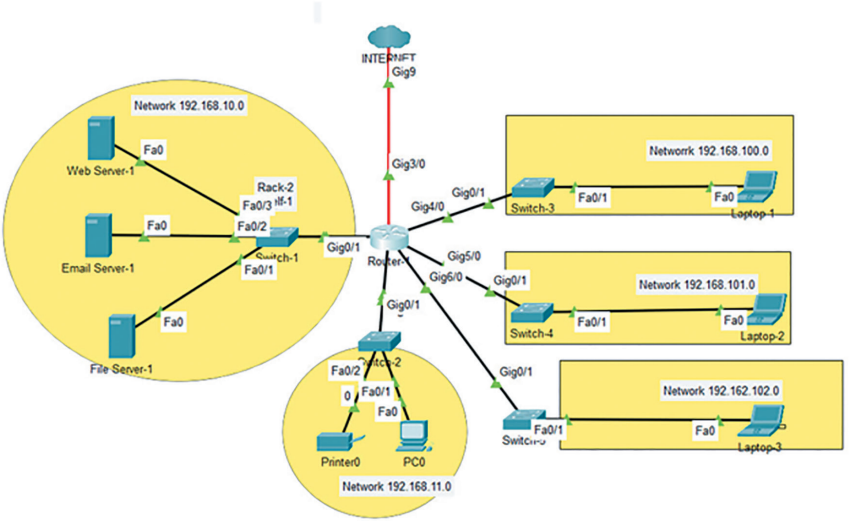

Рис. 9. Приклад удосконаленого сегмента мережі LAN, підключеної до мережі WAN

Джерело: [5]

Cisco Packet Tracer як потужний інструмент для симуляції мережевих інфраструктур надав можливість побудувати та проаналізувати сегментацію мережі, впровадження міжмережевих екранів, систем IDS/IPS для виявлення та запобігання вторгненням, а також налаштування безпечних VPN-з'єднань. Було досліджено різні архітектурні підходи, зокрема сегментацію мережі та Zero Trust архітектуру, що забезпечує контроль доступу на основі постійної верифікації користувачів і пристроїв.

У процесі моделювання в Cisco Packet Tracer виявлено, що використання поєднання традиційних міжмережевих екранів із сучасними підходами до контролю доступу і моніторингу трафіку значно

підвищує рівень захищеності мережі. Крім того, з урахуванням обмежених ресурсів, було протестовано варіанти з мінімально необхідними витратами, що забезпечують високий рівень захисту без значних фінансових вкладень.

Таким чином, удосконалений сегмент мережі в Cisco Packet Tracer дозволяє не тільки підвищити безпеку, але й адаптувати мережеву інфраструктуру до новітніх кіберзагроз, зберігаючи баланс між ефективністю та ресурсами.

Висновки та пропозиції. У процесі дослідження та вдосконалення сегмента мережі локальної мережі (LAN) було враховано сучасні виклики у сфері кібербезпеки та обмеження ресурсів, з якими стикаються організації. Важливо зазначити, що традиційні моделі безпеки комп'ютерних мереж втрачають актуальність, і для підвищення ефективності захисту інформаційних систем необхідно застосовувати нові підходи. Вивчаючи різні рішення, зосереджено увагу на впровадженні пристроїв безпеки та архітектури безпеки, що забезпечують захист від сучасних кіберзагроз.

Важливу роль у побудові безпечної мережі також відіграє вибір архітектури безпеки. Архітектура Zero Trust, яка передбачає постійну верифікацію користувачів і пристроїв незалежно від їхнього розташування в мережі, також була врахована для підвищення безпеки.

Зважаючи на переваги та недоліки різних рішень, було запропоновано вдосконалення сегменту мережі LAN в програмному середовищі Cisco Packet Tracer, що дозволило моделювати можливі загрози та тестувати різні сценарії впровадження захисних заходів у безпечному віртуальному середовищі. Cisco Packet Tracer надав можливість інтегрувати і протестувати такі рішення, як міжмережеві екрани, системи IDS/IPS та VPN-з'єднання, а також застосувати архітектурні підходи, що включають сегментацію мережі та концепції Zero Trust.

ЛІТЕРАТУРА

1. Ткаченко О. М., Сосновий В. О. (2022). Модель прогнозування безпеки мережі за допомогою нейронних мереж. *ITSynergy*, (2), 43–54. https://doi.org/10.53920/ITS-2022-2-4

2. S. Anitha, S. Kavitha, and P. Kavitha, "Machine Learning for Operating Systems Security," *International Journal of Scientific & Engineering Research*, Vol. 13, no. 2, Pp. 243-246, 2022.

3. Li, Sun, et al. (2019). Deep learning for network security intrusion detection: Reviews, challenges, and solutions. IEEE Access, 7, 10113-10165.

4. Приймак Є.О., Зайцев Є.О., Лемешко А.В., Антоненко А.В. Дослідження можливостей оптимізації процесу обробки даних в державних інформаційних системах із використанням штучного інтелекту. 2024, *ITSynergy*, (1), С. 6–15. DOI: https://doi.org/10.53920/ITS-2024-1-1.

5. https://www.netacad.com/courses/cyberops-associate?courseLang=en-US.

REFERENCES

1. Tkachenko O. M., Sosnovy V. AT. (2022). A network security prediction model using neural networks. *ITSynergy*, (2), 43–54. https://doi.org/10.53920/ITS-2022-2-4.

2. S. Anitha, S. Kavitha, and P. Kavitha, "Machine Learning for Operating Systems Security," *International Journal of Scientific & Engineering Research*, Vol. 13, No. 2, Pp. 243-246, 2022.

3. Li, Sun, et al. (2019). Deep learning for network security intrusion detection: Reviews, challenges, and solutions. IEEE Access, 7, 10113-10165.

4. Pryimak E.O., Zaitsev E.O., Lemeshko A.V., Antonenko A.V. Research on the possibilities of optimizing the data processing process in state information systems using artificial intelligence. 2024, *ITSynergy*, (1), С. 6–15. DOI: https://doi.org/10.53920/ITS-2024-1-1.

5. https://www.netacad.com/courses/cyberops-associate?courseLang=en-US.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 03.10.2024