УДК 004.056.5+004.6
DOI: https://doi.org/ 10.17721/3041-2323.2024.214-225

Андрій ЛЕМЕШКО, канд техн. наук, доц.
ORCID ID: 0000-0001-8003-3168
e-mail: andrii.lemeshko@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Ольга ТКАЧЕНКО, д-р техн. наук, проф.
ORCID ID: 0000-0001-7983-9033
e-mail: olga.tkachenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ: ВПРОВАДЖЕННЯ ПРИСТРОЇВ І СИСТЕМ ДЛЯ ПІДВИЩЕННЯ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

Досліджено сучасні підходи до забезпечення безпеки інфокомунікаційних мереж, зокрема локальної мережі підприємства. Проведено аналіз переваг і недоліків архітектур та пристроїв, що забезпечують кібербезпеку, виконано порівняльний аналіз щодо впливу на ефективність захисту. Використано середовище Cisco Packet Tracer для моделювання мережевої інфраструктури й оцінювання ефективності інтеграції брандмауерів, систем IDS/IPS і VPN-з'єднань. Розглянуто концепції нульової довіри та сегментації мережі.

Ключові слова: ***онлайн-освіта, штучний інтелект, персоналізація, е-освіта.***

Вступ

Захист інформації в сучасних інфокомунікаційних мережах є одним із визначальних пріоритетів. Серед основних загроз – викрадення конфіденційної інформації, знищення даних, спотворення інформації та виведення з ладу комп'ютерних систем. Це лише частина потенційних ризиків, що виникають під час експлуатації та використання прикладних інформаційних систем. Ефективна система безпеки має бути комплексною і забезпечувати захист від різноманітних загроз, включаючи контроль за

© Лемешко Андрій, Ткаченко Ольга, 2024

діяльністю працівників, які мають доступ до внутрішніх ресурсів автоматизованої інформаційної системи.

Результати

Постановка задачі. Для досягнення захисту від різноманітних загроз необхідно використовувати спеціалізовані апаратно-програмні засоби, які забезпечують високий рівень безпеки, а також здійснювати моніторинг комп'ютерної системи в режимі реального часу, захищати дані від зовнішніх і внутрішніх атак, а також своєчасно реагувати на спроби несанкціонованого доступу.

Оскільки кількість 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 із метою забезпечення роботи офісу;

• мережу середнього та великого розмірів можуть охоплювати кілька 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 відрізняються: за площею; кількістю під'єднаних користувачів; діапазоном і послугами; сферою відповідальності.

Аналіз готових рішень. З іншого боку, більшість локальних, а також глобальних мереж побудовано за принципом згорнутої магістралі з використанням комутаторів другого чи третього рівня (рис. 1).

Недолік указаної побудови мережі такий: якщо комутатор або маршрутизатор вийшов із ладу через збій живлення, то сегмент чи вся мережа може припинити роботу до відновлення живлення або заміни обладнання, що вийшло з ладу внаслідок збою. Такий вихід із ладу обладнання є дуже поширеним явищем під час

стабілізаційних відключень електроенергії в об'єднаній енергетичній системі України внаслідок воєнних дій. У деяких випадках збій мережі є результатом вірусної атаки на вторинне сховище, що призводить до втрати даних.

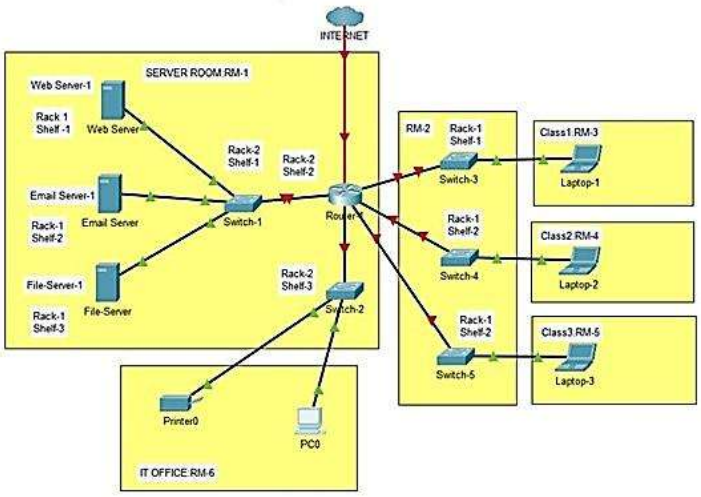

Рис. 1. *Приклад мережі LAN, підключеної до мережі WAN*

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

З огляду на це, актуальним завданням є розроблення способів удосконалення безпеки корпоративної мережі, зокрема і 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, варто враховувати такі важливі фактори, як складність

упровадження, 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 і нові виклики, пов'язані з масштабованістю мереж і цифровізацією бізнесу.

Концепція, наприклад Zero Trust, передбачає, що жоден користувач або пристрій не вважають надійним, навіть якщо він розміщений усередині корпоративної мережі, тому для доступу до ресурсів необхідна постійна перевірка ідентифікації користувача, пристрою та дій, які 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 застосовують 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 хмарову платформу. SASE дозволяє захистити віддалений доступ до корпоративних ресурсів, незалежно від місця перебування користувачів.

Зі зростанням поширеності хмарових сервісів з'являються нові виклики у сфері безпеки. Організації фокусуються на захисті хмарової цифрової інфраструктури, використовуючи хмарові міжмережеві екрани, багатофакторну автентифікацію, 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.

Через зростання кількості IoT-пристроїв важливим аспектом стає їхній захист. IoT-пристрої часто вразливі через недостатні можливості для оновлення та слабкий рівень захисту. Нові рішення спрямовано на моніторинг цих пристроїв і 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 в усі етапи розроблення програмного забезпечення, що дозволяє виявляти і виправляти вразливості на ранніх етапах розроблення, завдяки чому знижуються загальні ризики.

Мультифакторна автентифікація стає стандартом для захисту облікових записів і зменшення ризику несанкціонованого доступу до мереж і систем. Використання кількох факторів автентифікації, 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, хмарові рішення для безпеки, а також рішення для моніторингу віддалених робочих середовищ.

Справді, мережева безпека стає дедалі складнішою, і підприємства мають адаптуватися до нових викликів через упровадження 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 і 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 і сегментацію мережі, що сприяють підвищенню рівня захисту без значного збільшення витрат. Детальний аналіз цих компонентів допоможе знайти оптимальні шляхи для впровадження захисних заходів у типову інфраструктуру мережі з урахуванням поточних ресурсних обмежень і технічних вимог.

Архітектури безпеки. Дизайн брандмауера полягає, передусім, в інтерфейсах пристроїв, що дозволяють чи забороняють трафік за джерелом, призначенням і типом трафіка. Розглянемо три типи брандмауера.

1) Публічний і приватний: загальнодоступна / публічна мережа (зовнішня мережа) − ненадійна мережа, приватна мережа (внутрішня мережа) − надійна мережа (рис. 2).

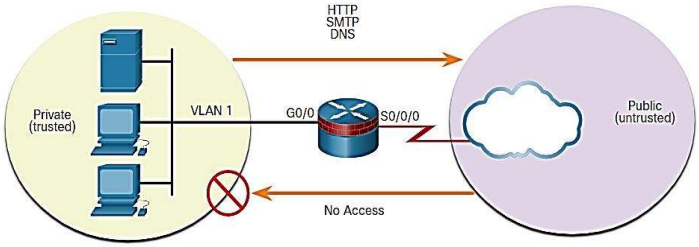

Рис. 2. *Захист приватної мережі*

2) Демілітаризована зона (DMZ), в якій тип брандмауера передбачає таке.

• Внутрішній інтерфейс, підключений до приватної мережі.

• Зовнішній інтерфейс, підключений до загальнодоступної мережі.

• Інтерфейс DMZ (рис. 3).

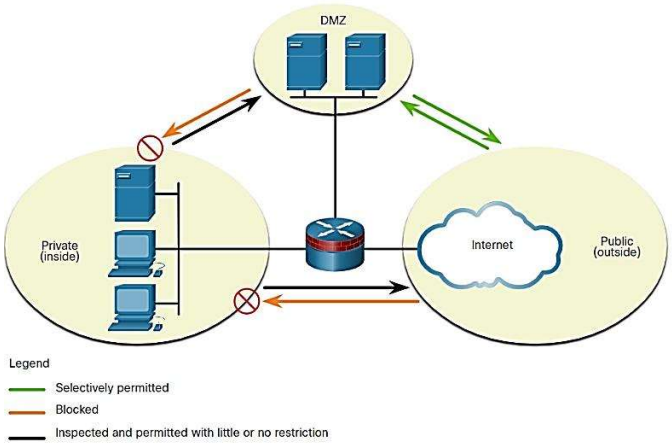

Рис. 3. *Демілітаризована зона (DMZ)*

3) Міжмережеві екрани на базі зональних політик. ZPF використовують концепцію зон, щоб забезпечити додаткову гнучкість. Зона – це група з одного чи кількох інтерфейсів, які мають схожі функції або характеристики. Зони допомагають зазначити, де слід застосовувати правило чи політику міжмережевого екрана (рис. 4).

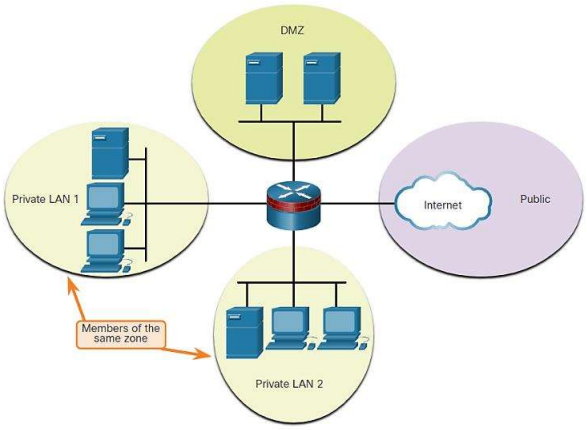

Рис. 4. *Міжмережеві екрани на базі зональних політик*

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

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

Переваги та недоліки міжмережевих екранів представлено у табл. 1.

Зміна парадигми мережевої архітектури вимагає захисту від швидкоплинних еволюціонуючих атак, що вимагає застосування економічно ефективних систем, таких як-от: системи виявлення вторгнень (IDS); системи запобігання вторгненням (IPS); архітектура мережі інтегрує ці рішення до вхідних і вихідних точок мережі. Технології IPS та IDS можуть доповнювати одна одну. Рішення щодо того, який варіант упроваджувати, приймають з урахуванням безпекових цілей організації та переваг і недоліків технологій IPS та IDS (табл. 2).

Таблиця 1

Переваги та недоліки міжмережевих екранів

Переваги міжмережевого екрана	Недоліки міжмережевого екрана
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 екрана для отримання матеріалу блокування, що відкриває мережу для потенційної атаки
Знижує складність управління безпекою	Продуктивність мережі може знижуватися

Таблиця 2

Переваги та недоліки технологій IPS і IDS

Реалізація	Переваги	Недоліки
IDS	Відсутній вплив на мережу (затримка, джитер) Відсутній вплив на мережу під час виходу 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 трафіка	Проблеми із сенсором можуть вплинути на мережевий трафік Перевантаження сенсора впливає на мережу Наявний певний вплив на мережу (затримка, джитер)

Врахувавши переваги й недоліки різних пристроїв і архітектур безпеки можна прийняти рішення щодо вдосконалення сегментів мережі LAN (рис. 1) із 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 зображено на рис. 5.

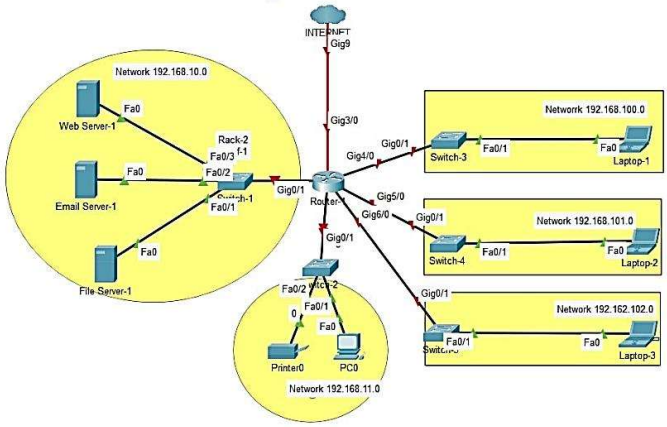

Рис. 5. *Приклад удосконаленого сегмента мережі LAN, підключеної до мережі WAN*

Cisco Packet Tracer як потужний інструмент для симуляції мережевих інфраструктур надав можливість побудувати та проаналізувати сегментацію мережі, упровадження міжмережевих екранів, систем IDS/IPS для виявлення та запобігання вторгненням, а також налаштування безпечних VPN-з'єднань. Досліджено різні архітектурні підходи, зокрема й 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 трафіка 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.

Отже, 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.

Дискусія і висновки

У процесі дослідження та вдосконалення сегмента мережі локальної мережі (LAN) враховано сучасні виклики у сфері кібербезпеки й обмеження ресурсів, з якими стикаються організації. Використання штучного інтелекту, нейронних мереж і методів машинного навчання у системах мережевої безпеки забезпечує проактивне виявлення загроз, автоматичне реагування на аномалії та підвищення рівня захисту мережевої інфраструктури шляхом постійного самонавчання й адаптації до нових типів атак (Приймак та ін., 2024; Ткаченко, & Сосновий, 2022; Anitha, Kavitha, & Kavitha, 2022, Li et al., 2019). 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 й архітектури безпеки, що забезпечують захист від сучасних кіберзагроз.

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

Зважаючи на переваги та недоліки різних рішень, вирішено вдосконалити сегмент мережі LAN у 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 тестувати такі рішення, як міжмережеві екрани, системи IDS/IPS і VPN-з'єднання, а також застосувати архітектурні підходи, що включають сегментацію мережі та концепції Zero Trust.

Список використаних джерел

Приймак, Є. О., Зайцев, Є. О., Лемешко, А. В., & Антоненко, А. В. (2024). Дослідження можливостей оптимізації процесу обробки даних в державних

інформаційних системах із використанням штучного інтелекту. *ITSynergy*, 1, 6–15. https://doi.org/10.53920/ITS-2024-1-1

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

Anitha, S., Kavitha, S., & Kavitha, P. (2022). Machine learning for operating systems security. *International Journal of Scientific & Engineering Research,* 13(2), 243–246.

Li, J., Sun, L., Wang, Q., Wang, Z., & Liu, Y. (2019). Deep learning for network security intrusion detection: Reviews, challenges, and solutions. *IEEE Access,* 7, 10113–10165. https://doi.org/10.1109/ACCESS.2019.2895334

References

Anitha, S., Kavitha, S., & Kavitha, P. (2022). Machine learning for operating systems security. *International Journal of Scientific & Engineering Research,* 13(2), 243–246.

Li, J., Sun, L., Wang, Q., Wang, Z., & Liu, Y. (2019). Deep learning for network security intrusion detection: Reviews, challenges, and solutions. *IEEE Access, 7*, 10113–10165. https://doi.org/10.1109/ACCESS.2019.2895334

Pryimak, Y. O., Zaitsev, Y. O., Lemeshko, A. V., & Antonenko, A. V. (2024). Research on optimization of data processing in government information systems using artificial intelligence. *ITSynergy*, 1, 6–15 [in Ukrainian]. https://doi.org/10.53920/ITS-2024-1-1

Tkachenko, O. M., & Sosnovyi, V. O. (2022). A model for predicting network security using neural networks. *ITSynergy*, 2, 43–54 [in Ukrainian]. https://doi.org/10.53920/ITS-2022-2-4

Отримано редакцією журналу / Received: 16.09.24
Прорецензовано / Revised: 26.09.24
Схвалено до друку / Accepted: 01.10.24

Andrii LEMESHKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-8003-3168
e-mail: andrii.lemeshko@gmail.com
Taras Shevchenko National University of Kyiv, Ukraine

Olha TKACHENKO, DSc (Engin.), Prof.
ORCID ID: 0000-0001-7983-9033
e-mail: olga.tkachenko@knu.ua
Taras Shevchenko National University of Kyiv, Ukraine

ENSURING NETWORK SECURITY: IMPLEMENTATION OF DEVICES AND SYSTEMS TO ENHANCE THE NETWORK INFRASTRUCTURE PROTECTION

This paper explores modern approaches to ensuring network security, particularly in the context of the local area network of the enterprise LLC. It analyzes the advantages and disadvantages of various security devices and architectures, as well as their impact on protecting information systems from cyber threats. Using the Cisco Packet Tracer network infrastructures modeled to evaluate the effectiveness of integrating firewalls, IDS/IPS systems and VPN connections. The concepts of Zero Trust and network segmentation discussed.

Keywords*: network, topology, hierarchical model, architecture, firewall, security systems.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.