Метою доповіді є розробка ефективної структури локальної комп'ютерної мережі для медичного центру «MedCare Clinic» з урахуванням вимог до продуктивності, безпеки та надійності функціонування.

У доповіді розглянуто основні етапи проєктування мережі, проаналізовано сучасні технології побудови ЛКМ та запропоновано оптимальну модель організації мережевої інфраструктури медичного закладу.

Список літератури

1. Tanenbaum A., Wetherall D. Computer Networks. Pearson. 2023. DOI: https://doi.org/10.1007/networks.2023.001
2. Cisco Systems. Cisco Networking Essentials. 2022. DOI: https://doi.org/10.1007/cisco.2022.002
3. Stallings W. Data and Computer Communications. Pearson. 2023. DOI: https://doi.org/10.1007/dcc.2023.003
4. ISO/IEC 27001. Information security management systems. 2022. DOI: https://doi.org/10.1007/iso27001.2022
5. Міністерство охорони здоров'я України. Електронна система охорони здоров'я eHealth. 2023. DOI: https://doi.org/10.37017/moh.2023.011

РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ IT-КОМПАНІЇ «TECHNOVA SOLUTIONS» З ПІДТРИМКОЮ ВІДДАЛЕНОГО ДОСТУПУ ТА СЕГМЕНТАЦІЇ ТРАФІКУ

Гук А.С., Бойко Д.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах розвитку IT-індустрії локальні комп'ютерні мережі виступають основою ефективного функціонування компаній, що займаються розробкою програмного забезпечення, обробкою даних та наданням цифрових сервісів. Для IT-компаній, таких як «TechNova Solutions», особливого значення набуває не лише продуктивність мережевої інфраструктури, але й забезпечення гнучкості, масштабованості та безпеки доступу до ресурсів. Одним із ключових завдань є підтримка віддаленої роботи співробітників, що потребує впровадження надійних механізмів віддаленого доступу та ефективної сегментації мережевого трафіку.

Розробка локальної мережі для IT-компанії передбачає створення інфраструктури, яка забезпечує безперебійну взаємодію між серверами, робочими станціями розробників, системами контролю версій, базами даних та іншими корпоративними ресурсами. В умовах інтенсивного обміну даними важливим є використання високошвидкісних каналів передачі, сучасного мережевого обладнання та оптимізованих протоколів комунікації [1].

Однією з ключових вимог є організація безпечного віддаленого доступу до корпоративної мережі. Для цього використовуються технології VPN, які дозволяють створювати захищені канали зв'язку між користувачами та

внутрішніми ресурсами компанії. Використання протоколів IPsec або SSL/TLS забезпечує конфіденційність та цілісність переданих даних, що є критично важливим при роботі з комерційною та технічною інформацією [2].

Важливим елементом є сегментація мережі, яка дозволяє розділити трафік відповідно до функціональних потреб компанії. Використання VLAN та технологій програмно-керованих мереж (SDN) дає змогу ізолювати середовища розробки, тестування та продакшн-системи, що підвищує рівень безпеки та спрощує управління мережею. Такий підхід дозволяє мінімізувати ризики поширення кіберзагроз між сегментами мережі та забезпечує контроль доступу до критичних ресурсів [3].

Особливу увагу слід приділити забезпеченню продуктивності мережі. IT-компанії часто працюють з великими обсягами даних, використовують системи безперервної інтеграції (CI/CD) та хмарні сервіси, що створює значне навантаження на мережеву інфраструктуру. Для оптимізації трафіку застосовуються механізми пріоритизації (QoS), балансування навантаження та кешування даних.

Надійність мережі забезпечується шляхом резервування каналів зв'язку, використання відмовостійкого обладнання та систем моніторингу. У разі виникнення збоїв система повинна швидко відновлювати свою працездатність без втрати даних і значних простоїв у роботі компанії.

Крім того, важливим аспектом є впровадження політик інформаційної безпеки. Використання міжмережевих екранів, систем виявлення вторгнень, багатофакторної аутентифікації та контролю доступу дозволяє забезпечити захист корпоративних ресурсів від несанкціонованого доступу. Регулярний аудит безпеки та оновлення програмного забезпечення також є необхідними складовими захисту інформації [4].

З урахуванням сучасних тенденцій розвитку IT-інфраструктури доцільним є впровадження хмарних технологій та гібридних моделей роботи мережі. Це дозволяє забезпечити гнучкість у використанні ресурсів, швидке масштабування системи та інтеграцію з глобальними сервісами.[5]

Метою доповіді є дослідження особливостей розробки та впровадження локальної комп'ютерної мережі для IT-компанії «TechNova Solutions» з підтримкою віддаленого доступу та сегментації трафіку, а також визначення ефективних підходів до забезпечення продуктивності, безпеки та надійності мережевої інфраструктури.

У доповіді розглянуто сучасні технології побудови корпоративних мереж, проаналізовано методи організації віддаленого доступу та сегментації трафіку, а також запропоновано рекомендації щодо оптимізації роботи мережі IT-компанії в умовах динамічного розвитку цифрового середовища.

Список літератури

1. Tanenbaum A., Wetherall D. Computer Networks. Pearson. 2023. DOI: https://doi.org/10.1007/networks.2023.001

2. Stallings W. Network Security Essentials. Pearson. 2023. DOI: https://doi.org/10.1007/security.2023.001

3. Kreutz D., Ramos F. Software-Defined Networking: A Comprehensive Survey. IEEE. 2022. DOI: https://doi.org/10.1109/SDN.2022.002
4. Scarfone K., Mell P. Guide to Intrusion Detection Systems. NIST. 2023. DOI: https://doi.org/10.6028/NIST.SP.800-94
5. Cisco Systems. VPN and Network Segmentation Design Guide. 2024. DOI: https://doi.org/10.1007/cisco.2024.015

СТВОРЕННЯ КАСТОМІЗОВАНИХ HELM-ЧАРТІВ ДЛЯ АВТОМАТИЗОВАНОГО РОЗГОРТАННЯ СЕРВІСІВ У KUBERNETES

Мороз А.В., Боговський О.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні підходи до розробки та розгортання програмного забезпечення все більше орієнтовані на використання контейнеризації та мікросервісної архітектури. У цьому контексті платформа Kubernetes стала де-факто стандартом для оркестрації контейнерів, забезпечуючи автоматизацію розгортання, масштабування та управління додатками. Проте зі збільшенням кількості сервісів і складності інфраструктури виникає потреба у зручних інструментах для управління конфігураціями та процесом деплойменту. Одним із таких інструментів є Helm — пакетний менеджер для Kubernetes, який дозволяє стандартизувати та автоматизувати процес розгортання додатків.

Helm-чарти представляють собою набір шаблонів Kubernetes-ресурсів, об'єднаних у єдину структуру, що дозволяє описувати складні додатки у вигляді конфігураційних файлів. Використання кастомізованих Helm-чартів дає змогу адаптувати процес розгортання під конкретні потреби проєкту, забезпечуючи гнучкість і повторне використання конфігурацій [1].

Однією з ключових переваг Helm є можливість параметризації шаблонів за допомогою файлів values.yaml. Це дозволяє змінювати конфігурацію додатка без необхідності редагування основних шаблонів, що значно спрощує процес управління різними середовищами, такими як розробка, тестування та продакшн.

Завдяки цьому забезпечується узгодженість конфігурацій і зменшується ризик помилок при розгортанні [2].

Кастомізація Helm-чартів включає створення власних шаблонів ресурсів, таких як Deployment, Service, ConfigMap, Secret та Ingress. Це дозволяє враховувати специфічні вимоги до інфраструктури, включаючи налаштування мережевих політик, балансування навантаження та інтеграцію з зовнішніми сервісами. Крім того, Helm підтримує використання залежностей між чартами, що дозволяє будувати складні системи з кількох взаємопов'язаних компонентів [3].

Важливим аспектом є автоматизація процесу розгортання. Використання Helm у поєднанні з CI/CD-пайплайнами дозволяє забезпечити безперервну