МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами X Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:

ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

20 грудня 2024 року

Полтава 2024

Запропонований метод інтеграції аналізу графів та алгоритмів машинного навчання дозволяє ефективно прогнозувати інциденти у соціальних мережах. Подальші дослідження мають бути спрямовані на оптимізацію вилучення ознак та адаптацію моделі до динамічно змінюваних даних.

ЛІТЕРАТУРА:

1. Shafiq M., Tian Z., Sun Y., Du X., Guizani M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city // Future Gener. Comput. Syst. – 2020. – Vol. 107. – P. 433–442.

2. Shafiq M., Tian Z., Bashir A.K., Du X., Guizani M. CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques // IEEE Internet Things J. – 2020. – Vol. 8. – P. 3242–3254.

3. Radivilova T., Kirichenko L., Ageiev D., Bulakh V. Classification methods of machine learning to detect DDOS attacks // Proc. of the 10th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – Metz, France, 2019. – P. 207–210. – doi: 10.1109/IDAACS.2019.8924406.

4. Popoola S.I., Adebisi B., Hammoudeh M., Gui G., Gacanin H. Hybrid deep learning for botnet attack detection in the internet-of-things networks // IEEE Internet Things J. – 2020.

5. Alothman Z., Alkasassbeh M., Al-Haj Baddar S. An efficient approach to detect IoT botnet attacks using machine learning // J. High Speed Netw. – 2020.

INTEGRATED APPROACH TO SOCIAL NETWORK ANALYSIS AND MACHINE LEARNING FOR INTERNAL INCIDENT DETECTION

***V. Pantielieiev**, Postgraduate Student*
Kharkiv National University of Radio Electronics

УДК 621.39

***С.В. Індик**, к.т.н., доцент,*
***В.В. Панич**, магістрант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ПРОЄКТУВАННЯ РОЗПОДІЛЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Розподілені корпоративні мережі є основою для забезпечення ефективної роботи сучасних підприємств, які мають численні підрозділи та офіси в різних регіонах. Вони дозволяють забезпечити обмін даними, доступ до інформаційних ресурсів та забезпечити високий рівень безпеки при взаємодії віддалених користувачів. Оскільки вимоги до таких мереж постійно зростають у зв'язку з глобалізацією, мобільністю співробітників і збільшенням обсягів даних — питання їх проєктування та оптимізації набуває особливої актуальності.

Об'єктами дослідження є корпоративні мережі, що охоплюють різні географічні локації та мають потребу в обміні даними між віддаленими офісами, філіями та віддаленими користувачами. Основними характеристиками таких мереж є: масштабованість, безпека, надійність і продуктивність. У дослідженні використано методи моделювання, аналізу топологій, а також технічні засоби моніторингу та оптимізації мережевих процесів. Для розв'язання завдань з підвищення продуктивності мережі застосовуються методи балансування навантаження, технології оптимізації трафіку та системи управління якістю обслуговування. Основним інструментом дослідження є аналіз різних архітектурних рішень та технічних засобів для забезпечення безпечного та ефективного обміну даними в умовах розподіленої мережі.

Результати дослідження показали, що для ефективного функціонування розподілених корпоративних мереж необхідно враховувати кілька основних аспектів. По-перше, вибір топології мережі, який залежить від розміру компанії та географічної поширеності її підрозділів, відіграє ключову роль у досягненні оптимальної продуктивності. Зокрема, топології "зірка", "дерево" та "кільце" демонструють різні переваги й недоліки в залежності від конкретних потреб бізнесу. Для малих та середніх компаній оптимальною є топологія зірка, яка забезпечує централізоване управління і простоту в налаштуванні, однак для великих корпорацій з численними підрозділами краще застосовувати деревоподібну топологію, що дозволяє покращити надійність і масштабованість мережі.

По-друге, для забезпечення безпеки в розподілених мережах необхідно застосовувати багатофакторну аутентифікацію, шифрування трафіку, а також використання віртуальних приватних мереж. Важливим компонентом є протокол IPsec (Internet Protocol Security), який забезпечує шифрування, цілісність і аутентифікацію даних, створюючи захищені тунелі для передачі між сегментами мережі. IPsec підтримує сучасні алгоритми шифрування, такі як Advanced Encryption Standard, і є надійним рішенням для захисту корпоративного трафіку. Впровадження систем моніторингу та засобів для відстеження аномалій у мережевому трафіку також є важливим аспектом у забезпеченні безпеки.

По-третє, дослідження показали, що застосування технології Software-Defined WAN (SD-WAN) є перспективним методом для оптимізації використання каналів зв'язку та управління трафіком. Це дає змогу знижувати витрати на передачу даних між віддаленими офісами і при цьому підвищувати продуктивність за рахунок гнучкого налаштування маршрутизації. Застосування таких технологій дозволяє ефективно керувати мережею, знижуючи ризики відмов та забезпечуючи високу швидкість обміну інформацією в умовах великих навантажень.

Ще одним важливим результатом є те, що застосування методів балансування навантаження дає змогу збільшити ефективність роботи мережі, зменшуючи ймовірність перевантаження окремих елементів інфраструктури. Це дозволяє забезпечити стабільність і доступність мережевих ресурсів навіть у періоди пікового навантаження.

Сучасні тенденції в проєктуванні корпоративних мереж орієнтовані на застосування новітніх технологій, таких як 5G, хмарні обчислення, штучний інтелект та Інтернет речей. Інтеграція цих технологій у розподілені мережі дозволяє значно збільшити швидкість обміну даними, забезпечити безпеку на новому рівні, а також оптимізувати використання ресурсів.

Дослідження вказують на важливість комплексного підходу до проєктування розподілених корпоративних мереж, що враховує як вимоги безпеки, так і ефективність використання ресурсів. Розробка оптимальних топологій, впровадження систем безпеки, а також технологій для управління трафіком і балансування навантаження дозволяє значно покращити продуктивність і надійність таких мереж. Отримані результати можуть бути використані для проєктування мереж у компаніях, що мають потребу в безпечному та ефективному обміні даними між віддаленими підрозділами, а також для подальших досліджень у сфері оптимізації мережевих архітектур у великих організаціях.

ЛІТЕРАТУРА:

1. Kent S., Seo K. Security Architecture for the Internet Protocol (RFC 4301) [Електронний ресурс] / Internet Engineering Task Force. – 2005. – Режим доступу: https://www.ietf.org/rfc/rfc4301.txt.

2. Kosiur D. IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. – Prentice Hall, 2000. – 320 с.

3. Cisco Systems. Cisco IPsec VPN Design Guide [Електронний ресурс] / Cisco Systems, Inc. – 2018. – Режим доступу: https://www.cisco.com.

DESIGN OF A DISTRIBUTED CORPORATE NETWORK

***S. Indyk**, PhD (Engineering), Associate Professor,*
***V. Panych**, Master's Student*
National University "Yuri Kondratyuk Poltava Polytechnic"

УДК 620.91:621.311.243

***М.В. Обілець**, магістрант,*
***Р.В. Захарченко**, к.т.н., доцент*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ДВОСТОРОННІХ СОНЯЧНИХ ПАНЕЛЕЙ НА ПРАКТИЧНОМУ ДОСЛІДІ

Сонячні панелі широко увійшли в нашу буденність. Вони використовуються в домашніх приладах (світильниках, калькуляторах) слугують доповненням для портативних джерел електроенергії (повербанки, зарядні станції) а також відіграють чималу роль в енергетиці.