УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Факультет «Інформаційно-керуючі системи та технології»

Кафедра «Транспортний зв'язок»

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи магістра

на тему:

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ З УРАХУВАННЯМ АНАЛІЗУ ТРАФІКУ

МРА 02.24.214.04.ПЗ

Виконав:
студент групи 214-КМТ-Д23
спеціальності 273 «Залізничний транспорт»
Освітньої програми «Комп'ютерні мережеві технології» (роботу виконано самостійно відповідно до принципів академічної доброчесності)

 Сенік МІРЗОЯН

Керівник:
доцент кафедри, канд. техн. наук

 Сергій ІНДИК

Рецензент:
доцентка кафедри АТ, докторка філософії

Олена ЩЕБЛИКІНА

Харків − 2025 р.

АНОТАЦІЯ

Актуальність роботи. У сучасних умовах цифровізації корпоративні мережі виступають важливим компонентом діяльності будь-якої організації. Водночас збільшення обсягів даних, розвиток технологій, хмарних сервісів та дистанційної роботи супроводжується зростанням ризику кіберзагроз. Це вимагає застосування сучасних підходів до захисту інформаційних систем, одним із яких є аналіз мережевого трафіку для виявлення загроз, вторгнень та аномальної активності. Оскільки традиційні системи безпеки часто виявляються недостатньо ефективними перед сучасними атаками, важливим є впровадження нових підходів до моніторингу та аналізу трафіку, які враховують розвиток статистичних і машинних методів. Це робить дане дослідження актуальним як у науковій, так і в практичній площинах.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ВИЯВЛЕННЯ ЗАГРОЗ, ПРОТОКОЛИ БЕЗПЕКИ, МЕРЕЖЕВИЙ ЕКРАН, АНАЛІЗ ПОВЕДІНКИ КОРИСТУВАЧІВ, СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Об'єктом дослідження є корпоративна мережа як комплексна інформаційно-технологічна інфраструктура, що забезпечує передачу, обробку та зберігання даних в організаціях.

Мета роботи: Метою роботи є дослідження методів моніторингу, аналізу мережевого трафіку та виявлення вторгнень у корпоративних мережах для розробки ефективної системи захисту, яка забезпечить високий рівень безпеки та надійності функціонування мережевої інфраструктури.

Структура та обсяг роботи. Об'єм даної роботи становить: 68 сторінок друкованого тексту, містить 11 рисунків, 7 таблиць, 22 літературних джерела. Робота містить вступ, 3 розділи, висновки та список використаних джерел.

Розділи кваліфікаційної роботи:

У першому розділі розглянуто теоретичні основи функціонування корпоративних мереж, їх структура, перспективи розвитку та основи аналізу трафіку.

У другому розділі досліджено методи моніторингу та фільтрації трафіку, а також аналіз існуючих систем виявлення атак.

У третьому розділі проведено розробку системи виявлення атак, обґрунтовано вибір методів та оцінено їх ефективність.

Методи дослідження. У роботі застосовано комплексний підхід до вирішення поставлених завдань. Використано теоретичний аналіз наукових праць та технічної документації, моделювання для оцінки ефективності обраних методів, а також експериментальне тестування програмних рішень у віртуальному середовищі для порівняння ефективності систем виявлення атак.

Рекомендації щодо використання та результати впровадження. Результати роботи можуть бути використані в організаціях, які потребують підвищення рівня інформаційної безпеки корпоративних мереж. Розроблені рекомендації дозволяють покращити ефективність виявлення атак та зменшити кількість хибних спрацьовувань у системах моніторингу. Впровадження запропонованих рішень забезпечить підвищення точності аналізу трафіку, оптимізацію використання ресурсів центрального процесора та масштабованість системи в умовах багатоядерного середовища.

ABSTRACT

Relevance of the work. In today's digitalized environment, corporate networks are a critical component of any organization's operations. At the same time, the growing volume of data, advancements in technologies, cloud services, and remote work are accompanied by an increased risk of cyber threats. This necessitates the adoption of modern approaches to protecting information systems, one of which is traffic analysis to detect threats, intrusions, and anomalous activity. Since traditional security systems often prove insufficient against modern attacks, it is essential to implement new approaches to traffic monitoring and analysis that incorporate advancements in statistical and machine-learning methods. This makes the study relevant both in scientific and practical dimensions.

Keywords: INFORMATION SECURITY, THREAT DETECTION, SECURITY PROTOCOLS, FIREWALL, USER BEHAVIOR ANALYSIS, INFORMATION SECURITY STANDARDS.

The object of the study is the corporate network as a complex information and technology infrastructure that ensures the transmission, processing, and storage of data within organizations.

The purpose of the research is to research methods of traffic monitoring, analysis, and intrusion detection in corporate networks to develop an effective security system that ensures a high level of safety and reliability for the network infrastructure.

Structure and scope of the paper. This work consists of 68 pages of printed text. It contains of 11 figures, 7 tables, 22 literature sources. It includes an introduction, three chapters, conclusions, and a list of references.

Chapters of the qualification work:

The first chapter examines the theoretical foundations of corporate network operation, their structure, development prospects, and traffic analysis basics.

The second chapter explores traffic monitoring and filtering methods and analyzes existing intrusion detection systems.

The third chapter involves the development of an intrusion detection system, justification of the selected methods, and evaluation of their efficiency.

Research methods. The study employs a comprehensive approach to addressing the research objectives. It includes theoretical analysis of scientific literature and technical documentation, modeling to assess the efficiency of the selected methods, and experimental testing of software solutions in a virtual environment to compare the effectiveness of intrusion detection systems.

Recommendations for use and implementation results. The results of this study can be utilized by organizations requiring enhanced information security for their corporate networks. The proposed recommendations improve attack detection efficiency and reduce the number of false positives in monitoring systems. Implementing the suggested solutions ensures higher accuracy in traffic analysis, optimization of CPU resource usage, and scalability of the system in multi-core environments.

ЗМІСТ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kurose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach*. 8th ed., Boston: Pearson, 2020.

2 Stallings, William. *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Boston: Pearson, 2016.

3. Шнайер Б. Прикладна криптографія. Протоколи, алгоритми та вихідні тексти на С. – К.: Діалектика, 2020. – 784 с.

4. Ramaswami, Rajiv, and Kumar N. Sivarajan. *Optical Networks: A Practical Perspective*. 3rd ed., Burlington: Morgan Kaufmann, 2010.

5. Clemm, Alexander. *Network Management Fundamentals*. Indianapolis: Cisco Press, 2007.

6. Cisco Systems. *IP Multiservice Networking*. Indianapolis: Cisco Press, 2002.

7. Subramanian, Manohar. *Network Management: Principles and Practice*. Boston: Addison-Wesley, 2000.

8. Minoli, Daniel. *Telecommunications Technology Handbook*. 2nd ed., Boston: Artech House, 2003.

9. David D. Coleman, David A. Westcott. CWNA Certified Wireless Network Administrator Study Guide Exam CWNA 107 5th Edition. SYBEX. 2018. – 1024 p.

10. Стеклов В.К. Проектування телекомунікаційних мереж [Текст] / В.К. Стеклов, Л.Н. Беркман. – К.: Техніка, 2002. – 792 с.

11. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі [Текст] / В.К. Стеклов, Л.Н. Беркман. – К.: Техніка, 2001. – 392 с.

12. Shawn M. Jackman, Matt Swartz, Marcus Burton, Thomas W. Head. CWDP Certified Wireless Design Professional Official Study Guide: Exam PW0-250. SYBEX. 2011. – 864 p.

13. Батаєв О.П., Ковтун І.В., Корольова Н.А. Теорія електричного зв'язку: Навч. посібник. – Харків: УкрДАЗТ, 2010. - 630 с.

14. Адресації в IP-мережах: Теоретичні основи та приклади розв'язання задач

[Електронний ресурс]: навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка» / Д. І. Могилевич, І. В. Кононова; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 55 с.

15. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

16. Телекомунікаційні системи та мережі: навчальний посібник. [Текст] / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.

17. Довгий С.О. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання.[Текст] / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв, – К.: Азимут-Україна. – 2013. – 608.

18. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

19. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.

20. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (2nd ed.). Addison-Wesley.

21. Stalling, W. (2017). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

22. Gollmann, D. (2011). *Computer Security* (3rd ed.). Wiley.