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 ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У ЛОКАЛЬНИХ МЕРЕЖАХ

МРА 02.22.214.02.ПЗ

Виконав:
студент групи 214-КМТ-Д24
спеціальності 273 «Залізничний транспорт»
Освітньої програми «Комп’ютерні мережеві технології» (роботу виконано самостійно відповідно до принципів академічної доброчесності)

 Артур САЛАЩЕНКО

Керівник:
професор кафедри, доктор техн. наук

Сергій ПАНЧЕНКО

Рецензент:
доцент кафедри, канд. техн. наук, доцент

Василь СОТНИК

Харків − 2026 р.

АНОТАЦІЯ

Актуальність роботи. Стрімке зростання кількості кіберзагроз та ускладнення мережевих атак зумовлюють необхідність підвищення рівня захисту локальних комп'ютерних мереж. Сучасні організації дедалі більше залежать від стабільної та безпечної роботи інформаційних систем, тому питання своєчасного виявлення та запобігання кібератакам набуває особливої актуальності. Найбільш поширеними є атаки типу DoS/DDoS та різноманітні flood-атаки, які здатні призводити до порушення доступності сервісів і втрати даних. У зв'язку з цим дослідження методів детекції атак та практичної реалізації систем виявлення вторгнень у локальних мережах є важливим завданням.

Ключові слова: кібербезпека, IDS, кібератаки, локальні мережі, DoS, DDoS, flood-атаки, мережевий трафік, виявлення вторгнень.

Об'єкт дослідження: процеси виявлення та запобігання кібератакам у локальних комп'ютерних мережах.

Мета роботи: процеси виявлення та запобігання кібератакам у локальних комп'ютерних мережах.

Структура та обсяг роботи: робота викладена у вигляді пояснювальної записки та складається зі вступу, трьох розділів, висновків, переліку умовних позначень і списку використаних джерел. У роботі наведено 24 рисунків, 17 таблиць та 22 джерела літератури, що відображають результати теоретичних і практичних досліджень.

У **першому розділі** розглянуто теоретичні основи кібератак, їх класифікацію, а також основні методи та засоби виявлення мережевих вторгнень.

У **другому розділі** проаналізовано методи виявлення мережевої топології та засоби їх реалізації, що є необхідною складовою для коректної роботи систем детекції атак.

У **третьому розділі** виконано проєктування та реалізацію системи IDS у віртуальному та реальному середовищі, проведено експериментальні дослідження

її ефективності та проаналізовано отримані результати.

Методи дослідження: виконано проєктування та реалізацію системи IDS у віртуальному та реальному середовищі, проведено експериментальні дослідження її ефективності та проаналізовано отримані результати.

Рекомендації щодо використання та результати впровадження. Отримані результати можуть бути використані під час проєктування та експлуатації систем захисту локальних комп'ютерних мереж, а також у навчальному процесі при підготовці фахівців у галузі кібербезпеки та комп'ютерних мереж.

ABSTRACT

Relevance of the work. The rapid growth in the number of cyber threats and the increasing complexity of network attacks necessitate a higher level of protection for local computer networks. Modern organizations are increasingly dependent on the stable and secure operation of information systems; therefore, timely detection and prevention of cyberattacks is of particular importance. The most common threats include DoS/DDoS attacks and various flood attacks, which can lead to service unavailability and data loss. In this context, the study of attack detection methods and the practical implementation of intrusion detection systems in local networks is an important task.

Keywords: cybersecurity, IDS, cyberattacks, local networks, DoS, DDoS, flood attacks, network traffic, intrusion detection.

Object of the processes of detection and prevention of cyberattacks in local computer networks.

The purpose of the research: processes of detection and prevention of cyberattacks in local computer networks.

Structure and scope of the work the thesis is presented in the form of an explanatory report and consists of an introduction, three chapters, conclusions, a list of abbreviations, and a list of references. The work contains 24 figures, 17 tables, and 22 literature sources reflecting the results of theoretical and practical research.

The first chapter considers the theoretical foundations of cyberattacks, their classification, as well as the main methods and tools for detecting network intrusions.

The second chapter analyzes methods for detecting network topology and the tools for their implementation, which are a necessary component for the correct operation of attack detection systems.

The third chapter presents the design and implementation of an IDS in virtual and real environments, experimental studies of its effectiveness, and an analysis of the obtained results.

Research methods: design and implementation of an IDS in virtual and real

environments, experimental evaluation of its effectiveness, and analysis of the obtained results.

Recommendations for use and implementation results. The obtained results can be used in the design and operation of protection systems for local computer networks, as well as in the educational process for training specialists in the fields of cybersecurity and computer networks.

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. Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. 5th ed., Upper Saddle River: Pearson Prentice Hall, 2011.

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. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. Bernet, D., & Vasilenko, A. Understanding and Configuring VPNs with IPsec. O'Reilly Media, 2017. – 384 p.

16. Gil, P., & Duro, R. Cryptographic Protocols in Networking: The Security of IPsec. Wiley, 2019. – 432 p.

17. Kaufman, C., & Dierks, T. IPSec: The Next Generation Internet Protocol Security. Addison-Wesley, 2002. – 528 p.

18. Raddatz, J., & Bozdag, D. An Introduction to Network Security: For Corporate Systems and Data. Springer, 2016. – 550 p.

19. Perrin, E., & Henson, R. IPSec: The Internet Protocol Security Handbook. Elsevier, 2019. – 400 p.

20. Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2017. – 288 p.

21. Easttom, C. Network Defense and Countermeasures: Principles and Practices. Pearson Education, 2020. – 640 p.

22. Rescorla, E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley Professional, 2001. – 624 p.