УДК 004.75:004.056

А.А. Мурсалова

МЕТОДИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ АТАК

Вінницький національний технічний університет

Анотація

У роботі розглянуто основні методи аналізу мережевого трафіку для виявлення кібернетичних атак. Проаналізовано сучасні підходи до моніторингу мережевої активності та виявлення аномалій у роботі інформаційних систем. Описано особливості використання систем аналізу трафіку та засобів виявлення вторгнень. Показано, що ефективне забезпечення кібербезпеки можливе лише за умови комплексного застосування методів аналізу мережевих даних.

Ключові слова: мережевий трафік, кібербезпека, аналіз трафіку, IDS, мережеві атаки, виявлення загроз.

Abstract

The paper considers the main methods of network traffic analysis for cyberattack detection. Modern approaches to monitoring network activity and detecting anomalies in information systems are analyzed. The features of using traffic analysis systems and intrusion detection tools are described. It is shown that effective cybersecurity can be achieved only through the comprehensive application of network data analysis methods.

Keywords: network traffic, cybersecurity, traffic analysis, IDS, network attacks, threat detection.

Вступ

Сьогодні комп’ютерні мережі є основою функціонування більшості інформаційних систем у сфері освіти, бізнесу, державного управління та промисловості. Разом із розвитком цифрових технологій зростає і кількість кібернетичних загроз, які можуть призводити до витоку інформації, порушення роботи систем або несанкціонованого доступу до даних. Одним із найефективніших способів своєчасного виявлення таких загроз є аналіз мережевого трафіку.

Мережевий трафік містить значну кількість інформації про роботу системи та взаємодію між її компонентами. Аналізуючи потоки даних, можна виявляти підозрілу активність, ознаки атак та аномалії у функціонуванні мережі. Це дозволяє оперативно реагувати на інциденти безпеки та мінімізувати можливі наслідки.

Метою роботи є дослідження сучасних методів аналізу мережевого трафіку для виявлення кібернетичних атак та визначення їх ефективності в умовах сучасних інформаційних систем.

Результати дослідження

Наразі аналіз мережевого трафіку є одним із ключових напрямів забезпечення кібербезпеки. Основним завданням такого аналізу є виявлення підозрілих дій, які можуть свідчити про спроби несанкціонованого доступу або проведення атак на інформаційну систему.

Одним із найбільш поширених методів є сигнатурний аналіз. Його суть полягає у порівнянні мережевого трафіку з відомими шаблонами атак. Цей підхід використовується в багатьох системах IDS/IPS та дозволяє ефективно виявляти вже відомі загрози [1]. Проте сигнатурний метод має обмеження, оскільки не здатний розпізнавати нові або модифіковані атаки.

Іншим важливим підходом є поведінковий аналіз, який базується на виявленні аномалій у мережевій активності. У цьому випадку система формує модель нормальної поведінки мережі та визначає відхилення від неї. Такий метод дозволяє виявляти нові типи атак, однак може створювати хибні спрацювання через нестандартну, але легітимну активність користувачів [2].

Для аналізу трафіку широко використовуються спеціалізовані програмні засоби, зокрема Wireshark, Snort та Suricata. Вони дозволяють здійснювати моніторинг мережі, аналіз пакетів даних та автоматичне виявлення підозрілої активності у режимі реального часу.

Однією з найнебезпечніших загроз для мережевих систем залишаються DDoS-атаки, шкідливе програмне забезпечення та спроби перехоплення даних. Для протидії таким атакам застосовуються системи фільтрації трафіку, механізми виявлення аномалій та засоби машинного навчання [3].

Сучасні технології кібербезпеки дедалі частіше використовують алгоритми штучного інтелекту для автоматизованого аналізу великих обсягів мережевих даних. Використання методів машинного навчання дозволяє підвищити швидкість виявлення атак та зменшити навантаження на адміністраторів безпеки [4].

Таким чином, аналіз мережевого трафіку є важливим компонентом сучасних систем кібербезпеки. Поєднання сигнатурних, поведінкових та інтелектуальних методів аналізу дозволяє значно підвищити ефективність виявлення кібернетичних загроз.

Висновки

У роботі розглянуто основні методи аналізу мережевого трафіку для виявлення кібернетичних атак. Проаналізовано сигнатурний та поведінковий підходи до моніторингу мережевої активності, а також особливості використання сучасних систем IDS/IPS. Визначено, що ефективне забезпечення кібербезпеки потребує комплексного використання методів аналізу трафіку та сучасних засобів виявлення загроз. Застосування інтелектуальних технологій і систем автоматизованого аналізу дозволяє підвищити рівень захисту інформаційних систем та своєчасно реагувати на кібернетичні атаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Boston : Pearson, 2021. – 816 p.
2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). – Gaithersburg : National Institute of Standards and Technology, 2022. – 127 p.
3. Easttom C. Network Defense and Countermeasures. – 3rd ed. – New York : Pearson IT Certification, 2020. – 552 p.
4. Wireshark User’s Guide. – Режим доступу: Wireshark Official Website (дата звернення: 09.05.2026).
5. NIST Cybersecurity Framework. – Режим доступу: NIST Official Website (дата звернення: 09.05.2026).
6.

Мурсалова Анастасія Андріївна – студентка групи 1КІТС-24б кафедри менеджменту та безпеки інформаційних систем факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, anastasia.mursalovaa@gmail.com

Науковий керівник – **Шелепало Галина Василівна** – кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Mursalova Anastasiia Andriivna – student of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, anastasia.mursalovaa@gmail.com

Supervisor – **Halyna Shelepalo** – Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.