ANALYSIS OF METHODS FOR DETECTING SECURITY THREATS IN COMPUTER NETWORKS

Boymatov Mexrojiddin No'monjon o'g'li, *Assistent Professor,*
E-mail: boymatovmexrojiddin99@gmail.com,
Sharda University of Uzbekistan
Jaxparov Azizbek Muxibullayevich, *Master's student,*
E-mail: azizjaxparov@gmail.com,
Andijan Branch of Sharda University of Uzbekistan

Abstract. *This article presents a comprehensive analysis of the current state of methods for detecting factors that threaten information security in computer networks. Signature-based, anomaly-based, hybrid, and artificial intelligence–based threat detection methods are comparatively examined. Based on scientific studies and international reports published between 2019 and 2024, the dynamics of cyberattacks, the effectiveness of IDS/IPS systems, and detection accuracy are analyzed. The research results demonstrate the necessity of applying intelligent and adaptive approaches to enhance computer network security.*

Annotatsiya. *Ushbu maqolada kompyuter tarmoqlarida axborot xavfsizligiga tahdid soluvchi omillarni aniqlash usullarining hozirgi holatining keng qamrovli tahlili keltirilgan. Imzo asosidagi, anomaliya asosidagi, gibrid va sun'iy intellektga asoslangan tahdidlarni aniqlash usullari qiyosiy jihatdan o'rganilgan. 2019 va 2024 yillar oralig'ida nashr etilgan ilmiy tadqiqotlar va xalqaro hisobotlar asosida kiberhujumlar dinamikasi, IDS/IPS tizimlarining samaradorligi va aniqlash aniqligi tahlil qilingan. Tadqiqot natijalari kompyuter tarmog'i xavfsizligini oshirish uchun aqlli va moslashuvchan yondashuvlarni qo'llash zarurligini ko'rsatadi.*

Аннотация. *В данной статье представлен всесторонний анализ современного состояния методов обнаружения факторов, угрожающих информационной безопасности в компьютерных сетях. Проведено сравнительное исследование методов обнаружения угроз на основе сигнатур, аномалий, гибридных методов и методов, основанных на искусственном интеллекте. На основе научных исследований и международных отчетов, опубликованных в период с 2019 по 2024 год, проанализированы динамика кибератак, эффективность систем обнаружения вторжений (IDS/IPS) и точность обнаружения. Результаты исследования демонстрируют необходимость применения интеллектуальных и адаптивных подходов для повышения безопасности компьютерных сетей.*

Keywords: *computer networks, information security, cyber threats, IDS, IPS, anomaly, artificial intelligence, machine learning.*

Kalit so'zlar: *kompyuter tarmoqlari, axborot xavfsizligi, kibertahdidlar, IDS, IPS, anomaliya, sun'iy intellekt, mashinani o'rganish.*

Ключевые слова: *компьютерные сети, информационная безопасность, киберугрозы, IDS, IPS, аномалии, искусственный интеллект, машинное обучение.*

Today, the number of devices connected to the global Internet exceeded 30 billion in 2024, of which approximately 40 percent are considered insufficiently protected [1]. While the expansion of computer networks has accelerated information exchange, it has also significantly increased the risk of cyberattacks.

According to statistical data, the economic damage caused by cyberattacks worldwide amounted to USD 8.4 trillion in 2023 [2]. Therefore, early detection and prevention of security threats in computer networks is considered a relevant scientific and practical task.

Classification of Security Threats in Computer Networks.

Security threats encountered in computer networks can be divided into the following groups:

- **External threats** – attacks carried out via the Internet.
- **Internal threats** – actions performed by authorized users.
- **Accidental threats** – configuration errors and technical failures.

According to data from the *Kaspersky Security Report* 2024, the distribution of major cyberattacks in computer networks is presented in Table 1 [3].

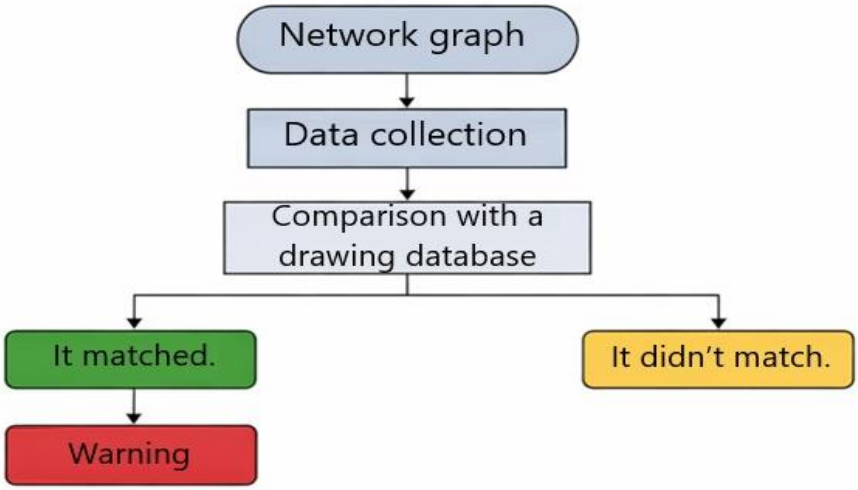
Table 1

Classification of Security Threats

Type of attack	Share, %
DDoS	32
Phishing	28
Malware	21
Brute-force	11
Others	8

Signature-Based Threat Detection Method

The signature-based detection method is considered the most widely used traditional approach in IDS (Intrusion Detection System) systems. In this method, network traffic is compared with previously known attack patterns (signatures) (Block Diagram 1).

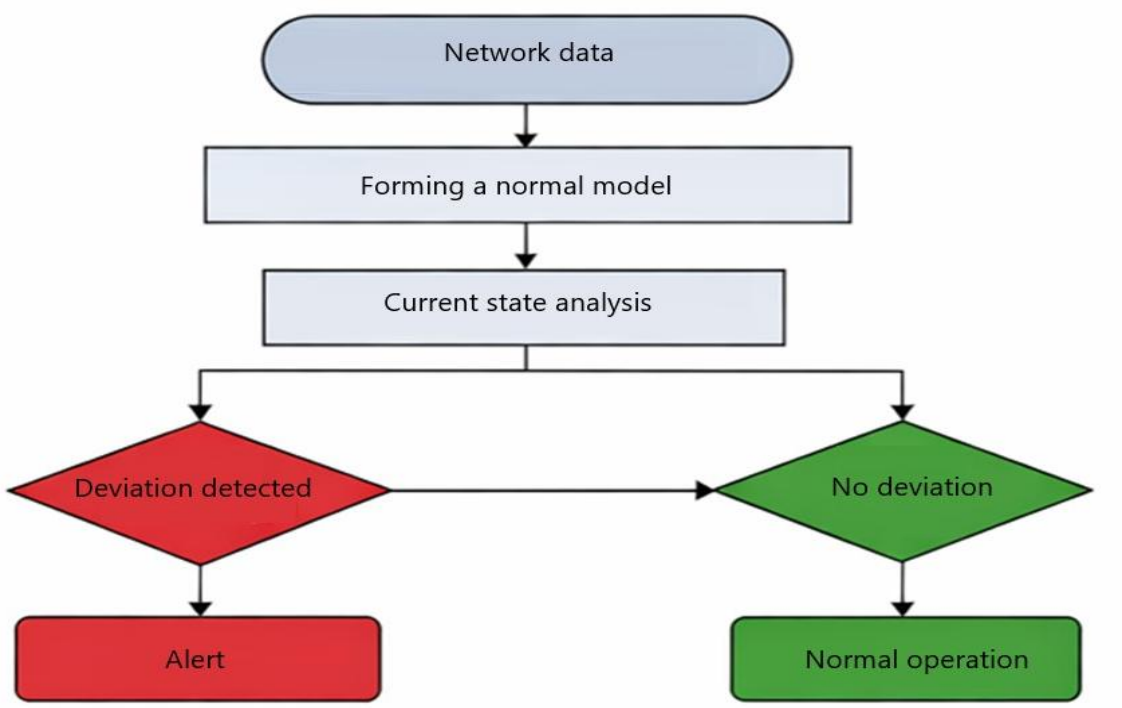


Block Diagram 1. Algorithm of Signature-Based IDS

The accuracy of the signature-based IDS algorithm is 90–95%, with its main limitation being the inability to detect zero-day attacks [4].

Anomaly-Based Threat Detection Methods

In the anomaly-based method, a normal operating profile of the network is established, and deviations from this profile are assessed as threats. Research indicates that anomaly-based methods achieve 70–85% effectiveness in detecting new attacks (Block Diagram 2) [5].



Block Diagram 2. Anomaly-Based Detection Process

Hybrid Threat Detection Methods

Hybrid methods combine signature-based and anomaly-based approaches. These methods demonstrate the highest effectiveness in practice. A comparative analysis of the detection methods is presented in Table 2.

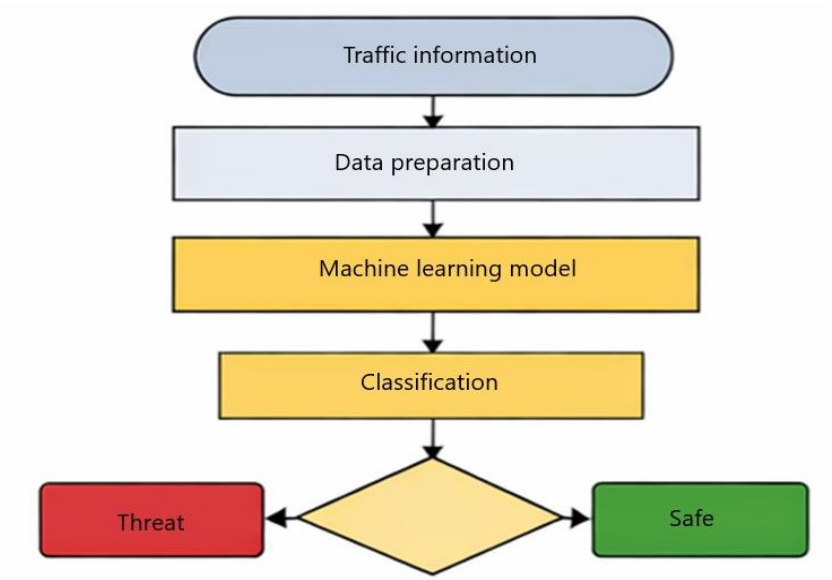
In recent years, IDS systems have been developed using neural networks, SVM, Random Forest, and Deep Learning models. According to IBM research, AI-based IDS systems have increased the speed of attack detection by 60% (Block Diagram 3) [6].

Table 2

Comparative analysis of the detection methods is presented in

Method Type	Accuracy	Zero-Day Detection	Resource Requirement
Signature-Based	High	No	Low
Anomaly-Based	Medium	Yes	Medium
Hybrid	High	Yes	High

Artificial Intelligence and Machine Learning–Based Threat Detection.



Block Diagram 3. AI-Based IDS Architecture

The analysis shows that traditional methods still hold significant value, but AI-based systems demonstrate superiority in combating modern cyberattacks. However, their implementation requires high computational power and quality training data.

According to the research results, hybrid and AI-based methods are the most promising for detecting security threats in computer networks. In the future, implementing adaptive and intelligent algorithms in the development of IDS/IPS systems will significantly enhance network security.

Machine Learning-Based Detection

In recent years, artificial intelligence technologies have been widely applied in network security. Machine learning algorithms analyze large volumes of network traffic and distinguish between normal and abnormal behavior patterns.

Advantages:

- Ability to detect new (unknown) threats
- Capability to operate in real-time environments
- Reduction in the number of false positives

Commonly used algorithms:

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- Neural Networks
- Deep Learning models

SIEM Systems

SIEM (Security Information and Event Management) systems collect log data from various sources (servers, routers, firewalls, applications) and analyze them in a centralized manner.

Advantages:

- Comprehensive monitoring
- Real-time alerting
- Forensic analysis capabilities

Zero Trust Security Model

The Zero Trust model is based on the principle of "never trust, always verify." Every user and device must undergo authentication and authorization before accessing resources.

Key components:

- Multi-Factor Authentication (MFA)
- Micro-segmentation
- Continuous monitoring

Behavioral Analysis

This method monitors the activities of users and devices within a network. If a deviation from normal behavior is detected, the system generates an alert.

For example:

- An employee usually works from 9:00 a.m. to 6:00 p.m., but system access is detected late at night.
- A large volume of data is downloaded or transferred within a short period of time.

Comparative Analysis of Threat Detection Methods

Method	Advantages	Disadvantages
Signature-based	**Fast and accurate**	**Cannot detect new threats**
Anomaly-based	**Detects unknown attacks**	**May generate many false positives**
ML-based	**High accuracy**	**Requires significant computational resources**
SIEM	**Centralized monitoring and control**	**Complex configuration**
Zero Trust	**High level of security**	**High implementation cost**

Conclusion. Methods for detecting security threats in computer networks are continuously evolving. Traditional signature-based approaches are no longer sufficient in the face of modern cyberattacks. Emerging technologies such as artificial intelligence, machine learning, SIEM systems, and the Zero Trust model are significantly enhancing the level of security.

The most effective approach is the implementation of a multi-layered and comprehensive security system. In the future, automated and self-learning systems are expected to become the dominant trend in the field of network security.

References

1. Global Internet Devices Statistics, 2024.
2. Cybersecurity Economic Impact Report, 2023.
3. Kaspersky Security Report, 2024.
4. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST.
5. Patcha, A., & Park, J.-M. (2007). *An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends*. Computer Networks, 51(12), 3448–3470.
6. IBM Security Intelligence. (2022). *AI in Intrusion Detection Systems: Enhancing Cybersecurity with Machine Learning*.