УДК 004.056

**Д. В. Довгалюк**

# АНАЛІЗ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Вінницький національний технічний університет

**Анотація**

*У роботі представлено підхід до аналізу подій інформаційної безпеки в комп'ютерних мережах, що базується на адаптивній моделі поведінки мережевих вузлів та механізмі кореляції подій. Підхід спрямований на зменшення кількості хибних спрацювань та підвищення ефективності систем моніторингу інформаційної безпеки.*

**Ключові слова:** інформаційна безпека, комп'ютерні мережі, аналіз подій безпеки, виявлення аномалій, кореляція подій, поведінковий аналіз.

**Abstract**

*The work presents an approach to analyzing information security events in computer networks, based on an adaptive model of network node behavior and an event correlation mechanism. The approach is aimed at reducing the number of false positives and increasing the efficiency of information security monitoring systems.*

**Keywords:** information security, computer networks, security event analysis, anomaly detection, event correlation, behavioral analysis.

## Вступ

Сучасні комп'ютерні мережі є складними інформаційними системами, які щоденно обробляють значні обсяги даних та мережевого трафіку. Зі зростанням кількості кіберзагроз підвищується потреба у створенні ефективних засобів моніторингу подій інформаційної безпеки. Традиційні системи аналізу подій безпеки часто базуються на статичних правилах і сигнатурах атак, що обмежує їх здатність виявляти нові або модифіковані типи загроз [1].

Одним із перспективних напрямів підвищення ефективності систем безпеки є використання методів аналізу подій, які дозволяють автоматично визначати аномальну поведінку мережевих вузлів та користувачів. Такі системи здатні враховувати статистичні характеристики роботи мережі та виявляти відхилення від нормальної поведінки [2].

Підхід базується на формуванні адаптивної моделі поведінки мережевих вузлів та використанні механізму кореляції подій інформаційної безпеки. Аналіз взаємозв'язку між різними подіями дозволяє підвищити точність виявлення потенційних загроз та зменшити кількість помилкових спрацювань системи.

## Математична модель аналізу подій безпеки

Формула (1) описує послідовність подій інформаційної безпеки, що відбуваються у комп'ютерній мережі. Кожен елемент послідовності відповідає окремій події, наприклад спробі входу в систему, мережевому запиту або зверненню до ресурсу. Така послідовність використовується як основа для подальшого аналізу поведінки системи [3].

$$S = \{e_1, e_2, e_3, \dots, en\} \quad (1)$$

де $s_t$ – множина подій інформаційної безпеки;

$e_i$ – окрема подія безпеки (запит доступу, мережеве з'єднання, автентифікація тощо);

$n$ – кількість зафіксованих подій.

Формула (2) визначає умовну ймовірність появи певної події після конкретного контексту попередніх подій. Ймовірність обчислюється як відношення кількості поява цієї події після заданого контексту до загальної кількості поява цього контексту. Це дозволяє оцінити, наскільки типова або очікувана дана подія для системи [3]:

$$P(s_t \mid s_{t-1}) = \frac{C(s_{t-1}, s_t)}{C(s_{t-1})} \quad (2)$$

де $P(e_i \mid C)$ – умовна ймовірність появи події $e_i$ після контексту С;

$N(C, e_i)$ – кількість появ події $e_i$ після контексту $C$;

$N(C)$ – загальна кількість появ контексту.

Формула (3) використовується для визначення рівня аномальності події. Чим менша ймовірність появи події у певному контексті, тим більшим буде значення коефіцієнта аномальності. Таким чином можна визначити події, які відхиляються від нормальної поведінки системи [3]:

$$A(e) = 1 - P(e_i \mid C) \quad (3)$$

де $A(e_i)$ – рівень аномальності події;

чим більше значення $A(e_i)$, тим вища ймовірність того, що подія є підозрілою.

Формула (4) визначає правило класифікації подій. Якщо значення коефіцієнта аномальності перевищує встановлений поріг, подія розглядається як потенційна загроза інформаційній безпеці. Це дозволяє автоматично виявляти підозрілу активність у мережі [3].

$$A(e_i) > \theta \quad (4)$$

подія класифікується, як потенційна загроза інформаційній безпеці.

Отримані математичні залежності дозволяють формалізувати процес аналізу подій інформаційної безпеки в комп'ютерних мережах. Запропонована модель враховує послідовність подій та їх контекст, що дає змогу оцінювати ймовірність появи подій у системі. Використання коефіцієнта аномальності дозволяє визначати відхилення від нормальної поведінки мережевих вузлів. Введення порогового значення забезпечує автоматичну класифікацію підозрілих подій. Створюється основа для побудови інтелектуальної системи моніторингу інформаційної безпеки.

## Висновок

Таким чином, в роботі описано підхід до аналізу подій інформаційної безпеки в комп'ютерних мережах, який базується на використанні адаптивної моделі поведінки мережевих вузлів та механізму кореляції подій. Реалізація такого підходу дозволяє підвищити точність виявлення аномалій у роботі мережі та зменшити кількість хибних спрацювань системи безпеки. Отримані результати можуть бути використані при розробці систем моніторингу та аналізу подій інформаційної безпеки.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Системний аналіз інформаційної безпеки: сучасні методи управління :: Державний університет інформаційно-комунікаційних технологій. Державний університет інформаційно-комунікаційних технологій. URL: https://duikt.edu.ua/ua/lib/1/category/2404/view/2230 (дата звернення: 10.05.2026).
2. NIST Technical Series Publications. NIST. URL: https://www.nist.gov/nist-research-library/nist-publications (дата звернення: 10.05.2026).
3. Bishop M. Computer Security: Art and Science, Boston: Addison-Wesley, 2018. 1024 p.



**Довгалюк Дмитрій Валентинович** – студент групи КІТС-25м, факультет менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: dimadovgaljuk123@gmail.com

*Науковий керівник:* **Зоря Ірина Сергіївна** − асистент кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету, м. Вінниця

**Dovhaliuk Dmytrii V. –** student of group KITS-25m, Faculty of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: dimadovgaljuk123@gmail.com

*Supervisor:* **Zoria Iryna S. –** Assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University