В.А.ФЕДОРЕНКО[1], А.Д.МОСЬКО[2]

АДАПТИВНОЕ ОБНАРУЖЕНИЕ СЕТЕВЫХ АНОМАЛИЙ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ СОВОКУПНОГО АНАЛИЗА ПРИЗНАКОВ ТРАФИКА

[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, начальник цикла кафедры связи
[2]Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, курсант

Рост взаимосвязанности инфокоммуникационных систем расширяет поверхность атаки: согласно ENISA Threat Landscape 2026, развитие взаимозависимостей цифровых сервисов повышает требования к постоянному мониторингу и устойчивости инфраструктуры. При этом шифрование трафика ограничивает применение методов, основанных на анализе полезной нагрузки, поэтому возрастает значение признаков потока и статистики пакетов. Цель исследования – разработать компактный метод обнаружения сетевых аномалий, пригодный для применения в системах и сетях инфокоммуникаций без расшифровки передаваемых данных.

В качестве базового подхода предложено совместно анализировать интенсивность трафика и энтропийные характеристики адресов и портов. Такой выбор согласуется с результатами исследований, где сетевые аномалии выявляются по изменению распределений признаков трафика, а также с современными методами, использующими flow-level статистику. Научная новизна состоит в использовании единого адаптивного балла, объединяющего разнотипные признаки и правило подтверждения аномалии в соседних окнах, что снижает зависимость решения от одного показателя.

Для каждого 60-секундного окна рассчитываются четыре признака: λ – число пакетов в секунду; D – число уникальных адресатов; Hdst и Hport – энтропии распределений адресов назначения и номеров портов. Энтропия Шеннона определяется выражением:

$$H = -\Sigma_i p_i \log_2 p_i,$$

где p_i – относительная частота i-го значения признака. Для сопоставимости величины нормируются относительно профиля штатного трафика. Для j-го признака вычисляется z-оценка:

$$z_j(t) = |x_j(t) - \mu_j| / (\sigma_j + \varepsilon).$$

Итоговый индикатор аномалии формируется как взвешенная сумма:

$$A(t) = 0{,}35z\lambda + 0{,}25zHdst + 0{,}20zHport + 0{,}20zD.$$

Сигнал тревоги формируется при A(t) > 2,5 в двух соседних окнах. Порог и веса в работе рассматриваются как исходная конфигурация для моделирования и могут адаптироваться по статистике конкретного сегмента сети.



Рисунок 1 – Предлагаемая схема адаптивного обнаружения сетевых аномалий

Для оценки работоспособности проведено моделирование 180 последовательных окон: 120 штатных, 30 с признаками низкоскоростного сканирования и 30 с признаками DDoS-нагрузки. Модель не обучалась на атакующих окнах; параметры μ и σ определялись только по первым 120 штатным окнам. Для сравнения использован однофакторный критерий $\lambda > \mu\lambda + 3\sigma\lambda$.

Таблица 1 – Сравнение методов обнаружения

Метод	Точность, %	Полнота, %	F1, %	Ложные тревоги / 120
Порог по λ	100,0	51.7	68.1	0
Совокупный A(t)	100,0	98.3	99.2	0

Моделирование показало, что порог по одному показателю λ пропускает значительную часть низкоскоростного сканирования: полнота составляет 51,7 %. Предложенный показатель A(t) обнаружил 59 из 60 атакующих окон, при этом на штатной выборке ложных тревог не зафиксировано; точность равна 100 %, полнота – 98,3 %, F1 – 99,2 %. На рисунке 2 видно, что рост балла проявляется уже при сканировании, хотя рост интенсивности еще не достигает уровня, характерного для DDoS.

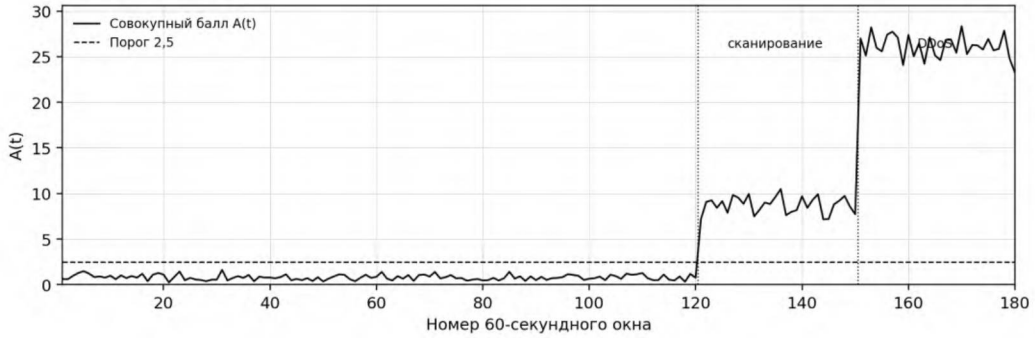


Рисунок 2 – Динамика совокупного балла аномалии при моделировании

Таким образом, совокупный статистический профиль позволяет повысить чувствительность обнаружения при сохранении простой вычислительной процедуры. Практически метод может использоваться как вычислительно простой уровень предварительного отбора событий перед СОВ/СОПВ более высокой сложности. Преимущество подхода состоит в том, что он не требует анализа содержимого пакетов и потому сохраняет работоспособность при шифровании полезной нагрузки. Дополнительное подтверждение аномалии в соседнем окне уменьшает вероятность реакции на кратковременный штатный всплеск. Для дальнейшего развития целесообразно проверить модель на реальных NetFlow/flow-записях, заменить фиксированные веса на адаптивные и исследовать устойчивость к дрейфу штатного профиля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ENISA Threat Landscape 2026. European Union Agency for Cybersecurity, 2026. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026 (дата обращения: 05.10.2026).

2. Sattar S., Khan S., Khan M.I. et al. Anomaly detection in encrypted network traffic using self-supervised learning // Scientific Reports. 2025. Vol. 15. Art. 26585. DOI: 10.1038/s41598-025-08568-0.

3. Аль-Тамими М.М.А., Алзагир А.А.Х., Аль-Свейти М.А.М. Комплексный обзор глубокого обучения в системах обнаружения вторжений // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 72–86. DOI: 10.31854/1813-324X-2025-11-3-72-86.

4. Котенко И.В., Ичетовкин Е.А. Методика защиты систем обнаружения вторжений от состязательных атак на основе шумоподавляющих автоэнкодеров // Правовая информатика. 2025. DOI: 10.24412/1994-1404-2025-1-110-120.

5. Network Intrusion Detection System Using Anomaly Detection Techniques // 2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP). 2024. DOI: 10.1109/ICCP63557.2024.10793023.

6. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.

7. Gu Y., McCallum A., Towsley D. Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation // Proceedings of the 5th ACM SIGCOMM Internet Measurement Conference. 2005.