

1 **Исаев, А. В.** Спектрально-импульсные методы измерения сопротивления межвитковой изоляции электрических машин со вспынной обмоткой и приборы на их основе : дис. ... канд. техн. наук : 05.11.01 / А. В. Исаев [Место защиты: БНТУ]. – Минск, 2024. – 140 с.

2 **Галушко, В. Н.** Метод неразрушающего контроля состояния однофазных и трёхфазных трансформаторов на основе частотных характеристик / В. Н. Галушко, И. Л. Громыко // Приборы и методы измерений. – 2025. – Т. 16, № 2. – С. 158–167. – DOI: 10.21122/2220-9506-2025-16-2-158-167.

3 **Мирош, Д. В.** Технология применения нейронных сетей для диагностики межвитковых замыканий в трансформаторах и асинхронных двигателях / Д. В. Мирош, В. М. Овчинников, И. Е. Монархович // Вестник БелГУТа: Наука и транспорт. – 2024. – № 1 (48). – С. 24–29.

Получено 27.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 004.056.5

О. А. БАКИЕВ, П. А. ЖДАНОВ (ЭМ-21)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. С. ТАТУР

АНАЛИЗ СЕТЕВОГО ТРАФИКА С ПОМОЩЬЮ WIRESHARK, ZUI, ZEEK

Обосновывается трехуровневая методология анализа сетевого трафика, основанная на каскадном применении инструментов Zeek, ZUI и Wireshark. Показано, что традиционный подход Full Packet Capture (FPC) сталкивается с проблемой экспоненциального роста объемов данных, делающей хранение и ручной анализ терабайтных дампов экономически нецелесообразным. Предложенная архитектура базируется на принципе семантической компрессии. Доказано, что интеграция инструментов в единый континуум абстракции преодолевает фундаментальные ограничения каждого из них в отдельности.

Современные информационно-телекоммуникационные инфраструктуры генерируют колоссальные объемы данных, которые превращают сетевой трафик в ключевой источник для мониторинга безопасности и диагностики сбоев.

Традиционная парадигма полного захвата пакетов (Full Packet Capture, FPC) является «золотым стандартом» криминалистики, сталкивается с критическими ограничениями: на высокоскоростных каналах суточные объемы дампов достигают терабайт, что делает их хранение экономически нецелесообразным, а ручной поиск аномалий в них – практически невозможным.

В то же время упрощенный Flow-анализ хотя и решает проблему объема,

создает «информационную слепоту», не раскрывает контекст передаваемых данных. Усложнение киберугроз, таких как целевые атаки (АРТ) и скрытые каналы эксфильтрации, диктует необходимость разработки многоуровневых методологий, сочетающих высокую скорость обработки больших данных с возможностью детальной пакетной экспертизы [1].

Научная новизна выполненной работы заключается в обосновании и систематизации трехуровневой архитектуры анализа трафика, базирующейся на принципе каскадной дистилляции данных. Доказано, что последовательное применение Zeek (для семантической компрессии), ZUI (для интерактивной навигации и корреляции) и Wireshark (для микроскопической верификации) формирует замкнутый цикл расследования. Такой подход преодолевает фундаментальные ограничения каждого инструмента в отдельности и трансформирует хаотичный поток битов в упорядоченную систему знаний.

Практическая ценность предложенной методологии определяется следующими факторами:

- 1 Радикальная оптимизация ресурсов: переход от хранения полных PCAP-дампов к структурированным логам Zeek позволяет сократить занимаемый объем данных на 98–99,5 %, делая долгосрочное архивирование трафика финансово доступным для организаций любого масштаба.

- 2 Ускорение реагирования на инциденты: использование языка конвейерных запросов ZEDL в среде ZUI сокращает время локализации угрозы с часов до минут, исключая необходимость ручного перебора гигабайтов текстовых файлов или дампов.

- 3 Реализация технологического моста: функция pivot to PCAP в ZUI элегантно решает проблему масштабируемости Wireshark. Она позволяет извлекать из многогигабайтных архивов только те пакеты, которые относятся к конкретному идентификатору сессии (UID), передавая аналитику файл объемом в несколько мегабайт вместо терабайтного дампа [2].

- 4 Устойчивость к повсеместному шифрованию: методология обеспечивает выявление аномалий в зашифрованном трафике (TLS 1.3, QUIC) посредством JA3/JA4-фингерпринтинга и анализа временных интервалов (таймингов), что критически важно в условиях, когда ретроспективное дешифрование невозможно из-за Perfect Forward Secrecy [3].

Сравнительный анализ демонстрирует, что данные инструменты образуют единый континуум абстракции, каждый из которых решает свой класс задач:

- 1 Zeek оперирует семантическими событиями (нагрузка CPU-bound), извлекая смысл из протоколов и формируя базу знаний о поведении сети.

- 2 ZUI занимает мета-уровень навигации (нагрузка I/O-bound), обеспечивая мгновенную корреляцию разрозненных логов и визуализацию топологии связей.

- 3 Wireshark работает с первичными битами (нагрузка RAM-bound) и высту-

пает беспристрастным арбитром для декодирования протоколов и реконструкции потоков данных.

Ни один из инструментов не является самодостаточным: их истинная мощь раскрывается исключительно при экосистемной интеграции.

Выявленные ограничения связаны с агрессивным ростом доли сквозного шифрования (включая Encrypted Client Hello), которое скрывает не только полезную нагрузку, но и часть метаданных. Дальнейшее развитие данной методологии требует интеграции алгоритмов машинного обучения для поведенческого анализа структурированных логов Zeek, а также стандартизации форматов ZNG и ZEDL в качестве де-факто протоколов обмена данными между платформами классов SIEM, SOAR и XDR.

Основные выводы исследования:

1 Эффективный сетевой мониторинг в современных условиях должен строиться по каскадному принципу «от общего к частному»: генерация метаданных (Zeek) – гипотезирование и поиск (ZUI) – доказательная верификация (Wireshark).

2 Метаданные Zeek представляют собой не урезанную копию трафика, а семантически обогащенную модель, достаточную для выявления сложных поведенческих паттернов без обращения к исходным пакетам.

3 ZUI выполняет критически важную роль технологического моста, ликвидирующего разрыв между масштабируемостью хранения данных и глубиной их пакетного анализа.

4 Wireshark сохраняет незаменимый статус инструмента финальной криминалистической экспертизы и обеспечивает юридически значимую достоверность выводов за счет работы с первичными, неизменными данными.

Таким образом, внедрение комплексной методологии на базе триады Zeek – ZUI – Wireshark обеспечивает переход от реактивного разбора инцидентов к проактивному мониторингу, что делает её высокоэффективной для центров мониторинга безопасности (SOC), служб цифровой криминалистики и профильных учебных лабораторий.

СПИСОК ЛИТЕРАТУРЫ

1 TheHive Project Documentation : [site]. – StrangeBee SAS, 2026. – URL: <https://thehive-project.org/> (date of access: 06.04.2026).

2 Cortex Documentation // StrangeBee. – URL: <https://cortex.thehive-project.org/> (date of access: 06.04.2026).

3 MISP Project : [site]. – URL: <https://www.misp-project.org/> (date of access: 06.04.2026).

Получено 28.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
