Устройство обнаружения аномалий трафика

Регистрационный номер 230293 от 26.11.2024 (ПМ)

Аннотация

Разработана система обнаружения аномалий трафика, относящаяся к области информационной безопасности. Устройство выявляет и классифицирует сетевые отклонения на основе вейвлет-преобразования, что повышает точность обнаружения угроз и защищает от несанкционированного доступа.

Конкурентные преимущества

В отличие от сигнатурных и статистических методов, система анализирует структуру трафика, выявляя ранее неизвестные атаки. Использование вейвлет-коэффициентов снижает количество ложных срабатываний и не требует предварительного обучения.

Технологический результат

Повышена эффективность обработки трафика за счёт точной идентификации структур аномалий. Сравнение вейвлет-коэффициентов с эталонными значениями обеспечивает достоверное выявление угроз в режиме реального времени.

Область применения

Система предназначена для корпоративных сетей и дата-центров, особенно актуальна при анализе зашифрованного или нестабильного трафика.

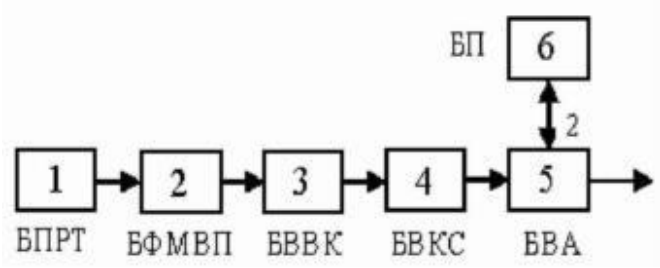

Рис. 1 Блок-схема устройства обнаружения аномалий трафика

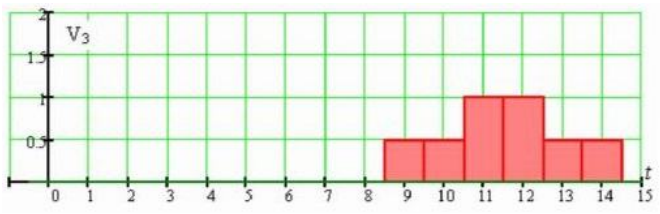

Рис. 3 Вейвлет-коэффициенты третьего ряда матрицы контрольного трафика

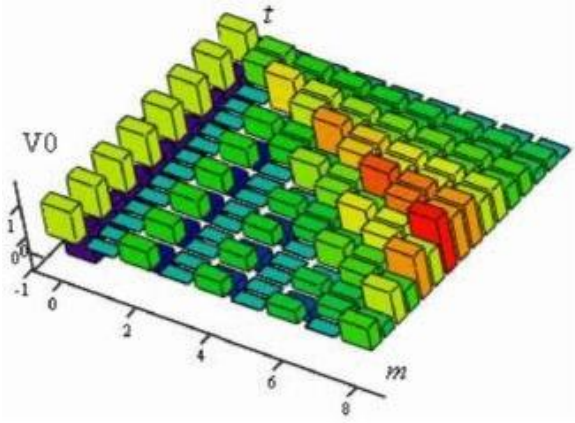

Рис. 2 Матрица вейвлет-коэффициентов контрольного трафика