**УДК 004.046** DOI: 10.25045/jpit.v10.i1.08

***Шыхалиев Р.Г.***
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

# О МЕТОДЕ ИЗВЛЕЧЕНИЯ КЛАССИФИКАЦИОННЫХ ПРИЗНАКОВ СЕТЕВЫХ ТРАФИКОВ НА ОСНОВЕ АНАЛИЗА СИГНАЛОВ

*Современные сетевые трафики имеют множество признаков и динамических свойств, которые отражают поведение сети и активность пользователей. Признаки сетевых трафиков играют важную роль в их классификации. Однако традиционно используемые признаки не отражают сложный нелинейный характер сетевых трафиков и не обеспечивают высокую точность классификации. Известно, что сетевые трафики имеют нестационарный характер и нелинейные динамические характеристики, такие, как самоподобия, мультифрактальность, долговременная зависимость и периодичность. Поэтому очень актуально извлечение новых робастных классификационных признаков, которые повысят точность классификации сетевых трафиков. Для решения этой проблемы наиболее перспективным методом является спектральный анализ сигналов сетевых трафиков. В работе для спектрального анализа сигналов сетевых трафиков предлагается использовать вейвлет-преобразование, через которое можно определить энергетические характеристики сигналов сетевых трафиков, используемых в качестве классификационных признаков.*

***Ключевые слова:*** *сетевые трафики, классификация сетевых трафиков, извлечения классификационных признаков, спектральный анализ сигналов, вейвлет-преобразование, энергетические характеристики сигналов.*

## Введение

Сегодня в Интернете имеются множества различных P2P (*англ. Peer-to-Peer*) приложений, социальных сетей, сервисов видеопотока, онлайн-игр и т.д. Эти приложения являются очень популярными и их использует большое количество интернет-пользователей. В результате объем интернет-трафика чрезмерно увеличивается и меняется его характер, что приводит к трудностям по обеспечению необходимого уровня производительности и безопасности компьютерных сетей (КС), а также QoS (*англ. Quality of Service*) для сетевых приложений и сервисов.

Для обеспечения нормальной и безопасной работы КС необходим эффективный мониторинг, который требует точной идентификации сетевых трафиков. Идентификация сетевых трафиков является неотъемлемой частью процесса классификации сетевых трафиков, поскольку без идентификации сетевых трафиков их нельзя классифицировать [1]. Обычно для идентификации сетевых трафиков используются методы, основанные на анализе признаков сетевых трафиков. К этим признакам относятся некоторые атрибуты пакетов, такие, как номера портов, IP-адреса отправителя и получателя, виды приложений и протоколов, а также содержание пакетов, различные статистические характеристики трафиков и т.д.

Однако с появлением новых приложений сущность этих признаков меняется, также статистические характеристики не могут отражать сложный нелинейный характер сетевых трафиков, что может влиять на точность идентификации сетевых трафиков.

Известно, что сегодня идентификация сетевых трафиков на основе номеров портов малоэффективна. Это в основном связано с появлением множества приложений и сервисов, использующих нестандартные TCP-порты, а также с широким использованием виртуальных частных сетей и P2P-приложений. В результате некоторые приложения вовсе не могут идентифицироваться.

В работе [2] авторами показано, что точность идентификации трафиков на основе номеров портов составляет не более 50–70%.

Сегодня одной из важных областей исследования по идентификации сетевых трафиков является классификация сетевых трафиков. Целью классификации является построение классификационной модели для прогнозирования неизвестных сетевых трафиков на основе изучения обучающего набора данных, состоящего из признаков сетевых трафиков.

В общем, классификация сетевых трафиков является процессом извлечения необходимой информации из большого набора признаков сетевых трафиков. При этом точность и быстродействие классификации зависят от объема и робастности извлеченных из сетевых данных признаков.

Точная и эффективная классификация сетевых трафиков является очень важной задачей для эффективного мониторинга и управления, а также безопасности КС. Например, классификация сетевых трафиков позволит провайдерам интернет-услуг (ISP) и сетевым администраторам определить структуру трафиков и назначить приоритеты для трафиков сервисов и приложений, требующих высокой пропускной способности (например, передача голоса по IP (VoIP) и видеоконференции). Классификация сетевых трафиков также необходима для определения и блокировки нежелательных трафиков или трафиков атак к безопасности КС, а также аномалий.

Исходя из вышесказанного, можно прийти к выводу, что сегодня очень актуальна разработка методов извлечения классификационных признаков сетевых трафиков, обеспечивающих высокую точность их классификации.

Целью данной статьи является разработка метода извлечения робастных к различным условиям функционирования КС классификационных новых признаков сетевых трафиков, который позволит эффективно идентифицировать их. Извлечение признаков – это процесс извлечения информации из сигнала сетевых трафиков, который используется для классификации сетевых трафиков.

Для извлечения классификационных признаков сетевых трафиков очень важна характеризация описывающих их сигналов, что требует определения волновой структуры этих сигналов, эффективным методом которой является спектральный анализ.

Потому в работе предлагается использовать методы спектрального анализа сигналов, а именно вейвлет-преобразование, чтобы извлекать признаки из сигнала сетевых трафиков. Так как все же определяющим в достижении высокой точности и производительности классификации сетевых трафиков является не выбор самого лучшего алгоритма классификации, а извлечения робастных классификационных признаков.

**Связанные работы**

В последние два десятилетия в литературе было предложено большое количество методов идентификации и классификации сетевых трафиков. Сегодня для идентификации и классификации сетевых трафиков широко используются методы машинного обучения (МО) [3–5]. При этом для классификации сетевых трафиков используются различные статистические признаки, такие, как атрибуты пакетов, статистические характеристики потоков трафиков и т.д.

Однако классификация сетевых трафиков методами МО на основе традиционных признаков сетевых трафиков все еще является не очень точной, поскольку используемые признаки являются не столь робастными признаками классификации.

Для решения этой задачи в работе [6] предлагается новый подход к извлечению и выбору классификационных признаков сетевых трафиков, который заключается в том, что для описания потоков трафиков сначала используется мультифрактальный формализм вейвлет-лидеров (*англ. Wavelet Leaders Multifractal Formalism – WLMF*), затем из потоков

трафиков извлекаются мультифрактальные признаки. После этого для устранения нерелевантных и излишних признаков к извлеченным мультифрактальным признакам применяется метод анализа главных компонентов (*англ. Principal Component Analysis – PCA*).

В работе [7] был предложен новый подход к идентификации сетевых трафиков, который основывается на мультифрактальном анализе энергетического спектра сигналов и классификации с помощью нейронных сетей. Предложенный подход заключается в том, что сначала осуществляется мультифрактальный анализ выборок потоков, соответствующих различным приложениям, и с помощью дискретного вейвлет-преобразования (*англ. Discrete Wavelet Transform – DWT*) оцениваются коэффициенты их энергетических спектров. Далее, используя модель комбинированных нейронных сетей, осуществляется классификация этих коэффициентов.

Таким образом, предложенный подход позволяет добиться идентификации трафиков различных приложений на основе классификации коэффициентов энергетического спектра сигналов, извлеченных из исходного трафика.

Идентификация P2P-трафиков является одним из основных направлений классификации сетевых трафиков, и были предложены множества подходов, основанные на анализе статистических характеристик потоков сетевых трафиков. Однако извлеченные с помощью традиционных методов признаки потоков сетевых трафиков являются неточными и неполными, что делает идентификацию сетевых трафиков неточной. Кроме того, P2P-трафики имеют очень много статистических признаков, которые делают задачу классификации сложной в плане времени и пространства. Для решения этой задачи в работе [8] авторы предлагают сначала на основе декомпозиции вейвлет-пакетов сигнала (*англ. wavelet packet decomposition*) извлечь микропризнаки и комбинировать их с традиционными признаками. После этого для уменьшения количества признаков предлагают алгоритм, основанный на методе анализа главных компонентов.

В работе [9] для определения аномалий сетевых трафиков используется метод анализа сигналов. При этом анализируются четыре класса сетевых аномалий, такие, как сбои (*англ. outages*), резкое увеличение трафика (*англ. flash crowds*), атаки (*англ. attacks*) и неудачи измерения (*англ. measurement failures*). Авторы используют частотно-временные характеристики IP-потоков и SNMP (*англ. Simple Network Management Protocol*) данных, собранных на граничном маршрутизаторе сети, а для анализа – вейвлет-фильтры.

Исключение ложных тревог является важным показателем эффективности алгоритмов обнаружения инцидентов трафиков, которые должны иметь возможность извлекать из трафиков робастные признаки инцидентов. Для решения этой проблемы в работе [10] предложена эффективная модель извлечения признаков трафиков с использованием дискретного вейвлет-преобразования (*англ. Discrete Wavelet Transform – DWT*) и линейного дискриминантного анализа (*англ. Linear Discriminant Analysis – LDA*). В основном DWT применяется к необработанным («сырым») данным трафиков, а коэффициенты максимального разрешения, представляющие случайные флуктуации трафика, отбрасываются. После этого LDA применяется к фильтрованному сигналу для дальнейшего извлечения признаков и уменьшения размерности задачи. Результаты LDA используются в качестве входных данных для нейронной сети, чтобы обнаружить инциденты трафиков.

В работе [11] на основе вейвлет-анализа предложен подход для анализа долгосрочной зависимости в трафиках и полупараметрической оценки связанного с ней коэффициента Херста. Показано, что оценка является объективной в общих условиях и эффективна при гауссовских допущениях. Также проводится анализ фрактальности и стационарности по коэффициенту Херста и детерминированным тенденциям.

Чтобы определить нормальный TCP-трафик, в работе [12] предлагается метод спектрального анализа сетевого трафика, который позволит обнаруживать атаки типа «отказ в обслуживании» (*англ. Denial of Service – DoS*). Для спектрального анализа авторы в качестве сигнала используют потоки пакетов, поступающие в определенные интервалы времени. Затем оценивается спектральная плотность мощности сигнала, по которой определяется периодичность или непериодичность сигнала. Нормальный TCP-поток должен проявлять явную периодичность в течение времени передачи и подтверждения приема (round-trip time) в обоих направлениях потока, тогда как потоки атак обычно не проявляют явную периодичность.

В работе [13] авторы для извлечения признаков вредоносных программ применили методологию спектрального анализа, поскольку вредоносные программы используют различные шаблоны сканирования, которые включают выбор IP-адресов назначения, и многие из этих колебаний имеют естественную периодичность. Используя эти шаблоны сканирования, авторы предложили новую концепцию извлечения признаков вредоносных программ и метод их анализа.

**Характеризация аномалий сетевых трафиков**

В данной работе задача классификации сетевых трафиков представляется как идентификация аномальных сетевых трафиков, для решения которой требуется определение признаков, указывающих на наличие в них аномалий. Для классификации сетевых трафиков предлагается следующий метод, который представлен на рисунке 1.

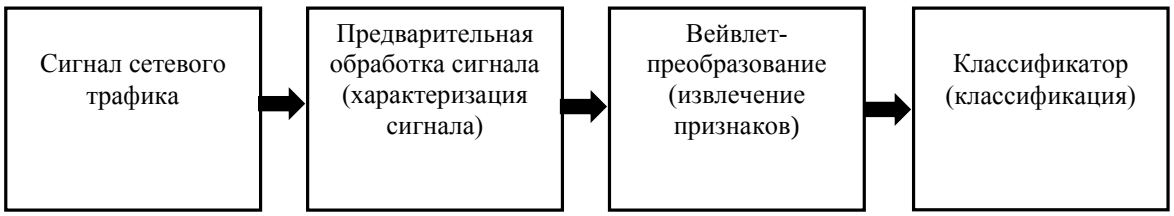


Рис.1. Процесс классификации сетевых трафиков

Известно, что сетевые трафики являются суперпозицией многих трафиков, которые генерируются различными протоколами, сетевыми сервисами и приложениями [14]. В литературе для моделирования сетевых трафиков предложены различные подходы и в каждой модели используются различные характеристики сетевых трафиков [15]. При этом для характеризации сетевых трафиков могут быть использованы различные статистические характеристики, такие, как временные интервалы между поступлениями пакетов, распределение размера пакетов, интенсивность задержки и потери пакетов, статистические характеристики потоков и т.д. [16, 17]. Однако в последнее время с быстрым развитием коммуникационных и сетевых технологий характеристики сетевых трафиков резко изменились и указанные статистические характеристики не могут достаточно полно отражать характер сетевых трафиков.

В литературе имеются работы, посвященные анализу влияния аномалий на статистические характеристики сетевых трафиков и определения профилей нормальных и аномальных трафиков. В работе [18] для анализа влияния аномалий на статистические характеристики сетевых трафиков предлагается моделировать сетевые трафики на основе использования стохастических негауссовских процессов. Экспериментально показано, что модель достаточно универсальна и позволяет статистически описать обычные сетевые трафики, а также трафики с аномалиями.

В работах [19, 20] для обнаружения аномалий в сетевых трафиках были использованы традиционные методы анализа временных рядов, такие, как экспоненциальное сглаживание и авторегрессионный процесс. Использование этих методов требует, чтобы трафики были стационарными, однако сетевые трафики фактически являются нестационарными и демонстрируют некоторые нелинейные динамические характеристики, такие, как самоподобия, мультифрактальность, долговременная зависимость и периодичность.

Кроме того, статистические показатели сетевых трафиков имеют определенную случайность и могут изменяться в зависимости от сетевых масштабов и условий использования. Поэтому традиционные методы анализа временных рядов не могут быть эффективными для обнаружения аномалий в сетевых трафиках.

Сигналы современных сетевых трафиков в нормальных условиях демонстрируют большие флуктуации и колебания пропускной способности в разных временных масштабах, а также разброс разных временных характеристик. Эти характеристики сетевых трафиков могут быть описаны в терминах самоподобия [21], мультифрактальности [22], долговременной зависимости (*англ. long-range dependence – LRD*) [23]. Анализ характеристик мультифрактальности, самоподобия, долговременной зависимости и периодичности сигналов сетевых трафиков позволит извлечь признаки, которые могут быть использованы для их классификации.

Самоподобия сетевых трафиков заключаются в том, что независимо от анализируемых временных масштабов статистическое распределение характеристик трафика является аналогичным. Другими словами, сетевые трафики являются фрактальными и выглядят статистически одинаковыми во всех масштабах.

Наличие в сетевых трафиках LRD означает, что трафики сильно коррелированы, и поэтому предыдущие состояния трафиков сильно влияют на их дальнейшие состояния.

В данной работе для характеризации аномалий предлагается использовать спектральные характеристики сетевых трафиков. Потому предполагается, что появление в сетевых трафиках тех или иных аномалий приводит к изменению спектральных характеристик сетевых трафиков.

**Извлечения классификационных признаков сетевых трафиков**

Учитывая вышеприведенные доводы, можно сказать, что сегодня одним из наиболее перспективных методов извлечения новых робастных признаков классификации сетевых трафиков является спектральный анализ сигналов сетевых трафиков. При этом основная проблема заключается в выборе таких характеристик, которые позволят характеризовать изменение спектра сигналов сетевых трафиков и определять аномалии.

В литературе широко рассмотрены вопросы спектрального анализа сигналов, основанные на преобразовании Фурье [24]. Однако используемые в рядах Фурье базисные функции (синус, косинус) не могут представлять сигналы с разрывами, скачками и мгновенными изменениями, каковыми являются сетевые трафики. Кроме того, бесконечное число членов в ряде Фурье усложняет вычисления, а ограничение их числа может привести к большим погрешностям.

Для решения этой проблемы могут быть использованы вейвлеты и вейвлет-преобразование, которые позволят характеризовать сигналы сетевых трафиков. Вейвлет-преобразование используется для извлечения коэффициентов преобразования, которые могут быть использованы в качестве признаков сетевых трафиков [25].

Вейвлет-преобразование сигналов является разложением их по базису путем масштабных изменений и переносов. В качестве базиса используются функции, которые также называются вейвлетами, обладающими определенными свойствами, которые характеризуют как определенную пространственную частоту, так и ее локализацию в физическом пространстве:

$$s(t) = \sum_k C_k \psi_k(t),$$

где $C_k$ – коэффициенты разложения; а $\psi_k(t)$ – базисные функции.

Сегодня используются различные вейвлет-функции $\psi(t)$, такие, как вейвлеты «мексиканская шляпа» (Mexican hat – MHAT-вейвлеты), вейвлеты Морле, вейвлет Хаара, вейвлеты Добеши и т.д.

Вейвлет-преобразование имеет такие свойства, как частотно-временная локализация сигналов, многократная фильтрация сигналов, пространственно-масштабный и многомасштабный анализы сигналов. При этом частотно-временная локализация сигналов заключается в получении сигналов в определенный отрезок времени или частоты, многократная фильтрация − в дифференциации сигналов с различными частотами, а пространственно-масштабный анализ сигналов − в извлечении признаков сигналов в различных пространствах и масштабах.

Следовательно, используя эти свойства, из входных сигналов можно извлечь признаки, которые характеризуются определенными локальными свойствами во времени и в пространстве.

Для того чтобы идентифицировать аномалии в сетевых трафиках, предлагается через вейвлет-преобразование определить их энергетические характеристики. При этом применение вейвлет-преобразования позволит определить распределение энергетических характеристик сигналов сетевых трафиков в частотной области.

Полная энергия сигнала $s(t)$ через вейвлет-преобразование может быть записана в следующем виде:

$$E_s = \int s^2(t)dt = C_\psi^{-1} \iint W^2(a,b) \frac{dadb}{a^2}.$$

При этом энергетический уровень сигнала $s(t)$ в пространстве $(a,b)$ характеризуется плотностью энергии $E_W(a,b) = W^2(a,b)$, где $a$ – масштаб и $b$ – время. Используя плотность энергии сигнала $E_W(a,b)$, с помощью окна можно определить локальную плотность энергии в точке $b_0$ (или $t_0$):

$$E_\xi(a,t_0) = \int E_W(a,b)\xi\left[\frac{b-t_0}{a}\right]db,$$

где $\xi$ является оконной функцией и удовлетворяет равенству $\int \xi(b)db = 1$. Если в качестве оконной функции $\xi$ использовать функцию Дирака, то локальный спектр сигнала будет иметь следующий вид:

$$E_\delta(a,t_0) = W^2(a,t_0).$$

Глобальный спектр энергии сигнала определяется распределением полной энергии по масштабам в соответствии с глобальным спектром энергии коэффициентов вейвлет-преобразования и имеет следующий вид:

$$E_W(a) = \int W^2(a,b)db = E_W(a,b)db,$$

он также называется дисперсией вейвлет-преобразования.

Степень неравномерности распределения энергии сигнала по масштабам определяется использованием меры локальных отклонений от среднего поля спектров на каждом масштабе:

$$I_W(a,t) = \frac{E_W(a,t)}{\langle E_W(a,t)\rangle_t}.$$

Для определения в сигналах незначительных изменений, например, для выявления слабых вибраций в сигналах на фоне масштабной структуры, используется так называемая мера контрастности, которая определяется следующим образом:

$$C_W(a,t) = \frac{E_W(a,t)}{E'_W(a,t)};\ E'_W(a,t) = \int_{a'=0}^{a'=a} E_W(a',t)da'.$$

Использование энергетических характеристик в качестве классификационных признаков позволит идентифицировать аномалии в сетевых трафиках, то есть аномальные трафики могут быть отделены от обычных трафиков.

**Заключение**

В данной статье исследуется проблема извлечения новых робастных классификационных признаков сетевых трафиков. Для этого предлагается использовать вейвлет-преобразование, которое позволяет осуществлять спектральный анализ сигналов сетевых трафиков. Вейвлет-преобразование используется для извлечения коэффициентов преобразования, которые могут быть применены в качестве признаков сетевых трафиков. Вейвлет-преобразование имеет свойства частотно-временной локализации сигналов, многократной фильтрации сигналов, пространственно-масштабного и многомасштабного анализов сигналов.

Используя эти свойства, из сигналов можно извлечь признаки, которые характеризуются определенными локальными свойствами во времени и в пространстве. При этом применение вейвлет-преобразования позволяет определить распределение энергетических характеристик сигналов в частотной области, которые вполне могут быть использованы для характеризации сигналов сетевых трафиков. Использование этих характеристик в качестве классификационных признаков позволит идентифицировать сетевые трафики.

**Литература**


1. Callado A., Kamienski C., Szabo G., et al. A Survey on Internet Traffic Identification // IEEE Communications Surveys & Tutorials, 2009, vol.11, no.3, pp.37−52.
2. Moore A.W., Panpagiannaki D. Toward the accurate identification of network application / Proceedings of the VI Passive and Active Measurement Workshop, 2005, pp.41–54.
3. Nguyen T., Armitage G. A Survey of Techniques for Internet Traffic Classification using Machine Learning // IEEE Communications Survey & Tutorials, 2008, vol.10, no.4, pp.56–76.
4. Singhal P., Mathur R., Vyas H. State of the Art Review of Network Traffic Classification based on Machine Learning Approach / International Conference on Recent Trends in Engineering & Technology, 2013, pp.12−15.
5. Williams N., Zander S., Armitage G. Evaluating Machine Learning Algorithms for Automated Network Application Identification. CAIA Technical Report 060410B, p.14.
6. Shi H., Li H., Zhang D., Cheng C., Wu W. Efficient and robust feature extraction and selection for traffic classification, Computer Networks, 2017, vol.119, no.4, pp.1−16.
7. Shi H., Liang G., Wang H. A novel traffic identification approach based on multifractal analysis and combined neural network // Annals of Telecommunications, 2014, vol.69, no.3−4, pp.155−169.
8. Du M., Chen X., and Tan J. An efficient method of P2P traffic identification based on wavelet packet decomposition and kernel principal component analysis // International Journal of Communication Systems, 2014, vol.27, no.10, pp.1476−1490.

9. Barford P., Kline J., Plonka D., and Ron A. A Signal Analysis of Network Traffic Anomalies / Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, 2002, pp.71−82.
10. Samant A., Adeli H. Feature Extraction for Traffic Incident Detection Using Wavelet Transform and Linear Discriminant Analysis // Computer-Aided Civil and Infrastructure Engineering, 2000, vol.15, no.4, pp.241−250.
11. Abry P. and Veitch D. Wavelet Analysis of Long-Range-Dependent Traffic // IEEE Transactions on Information Theory, 1998, vol.44, no.1, pp.2−15.
12. Cheng C.M., Kung H.T., Tan K.S. Use of Spectral Analysis in Defense Against DoS Attacks / Global Telecommunications Conference, 2002, pp.2143–2148.
13. Eto M., Sonoda K., Inoue D. Yoshioka K. and Nakao K. Fine-Grain Feature Extraction from Malware's Scan Behavior Based on Spectrum Analysis // IEICE Transactions on Information and Systems, 2010, vol.93, no.5, pp.1106−1116.
14. Шыхалиев Р.Г. Анализ и классификация сетевого трафика компьютерных сетей // İnformasiya texnologiyaları problemləri, 2010, №2, s.15−23.
15. Şıxəliyev R.H. Şəbəkə trafikinin modelləri haqqında // İnformasiya texnologiyaları problemləri, 2017, №2, s.98–104.
16. Dainotti A., Pescape A., and Ventre G. A Packet-level Characterization of Network Traffic / 11th International Workshop on Computer-Aided Modeling, Analysis and Design of Communication Links and Networks, 2006, pp.38−45.
17. Velan P., Medková J., Jirsík T., Celeda P. Network Traffic Characterisation Using Flow-Based Statistics / IEEE/IFIP Network Operations and Management Symposium, 2016, pp.907−912.
18. Scherrer A., Larrieu N., Owezarski P., Borgnat P., Abry P. Non Gaussian and Long Memory Statistical Characterisations for Internet Traffic with Anomalies // IEEE Transactions on Dependable and Secure Computing archive, 2007, vol.4, no.1, pp.56−70.
19. Kim H.J., Na J.C., Jang J.S. Network traffic anomaly detection based on ratio and volume analysis // International Journal of Computer Science and Network Security, 2006, vol.6, no.5, pp.190−194.
20. Wu, Q., Shao Z. Network anomaly detection using time series analysis / Proceedings of the Joint Int. Conference on Autonomic and Autonomous Systems and International Conference on Network and Services, 2005, pp. 42−47.
21. Smith R.D. The Dynamics of Internet Traffic: Self-Similarity, Self-Organization, and Complex Phenomena // Advances in Complex Systems, 2011, vol.14, no.6, pp.905−949.
22. Feldmann A., Gilbert A.C., and Willinger W. Data networks as cascades: Investigating the multifractal nature of internet wan traffic / ACM/SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communication, 1998, vol.28, no.4, pp.42−55.
23. Erramilli A., Narayan O., and Willinger W. Experimental queueing analysis with long-range dependent packet traffic // ACM/IEEE transactions on Networking, 1996, vol. 4, no.2, pp. 209−223.
24. Stoica P. and Moses R. Spectral Analysis of Signals, 2005, 427 p.
25. Liu C.L. A Tutorial of the Wavelet Transform, 2010, 71 p.

**UOT 004.046**
**Şıxəliyev Ramiz H.**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az
**Siqnalların analizi əsasında şəbəkə trafiklərinin təsnifat əlamətlərinin çıxarılması metodu**
Müasir şəbəkə trafikləri şəbəkənin fəaliyyətini və istifadəçilərin aktivliyini əks etdirən çoxlu sayda əlamətlərə və dinamik xassələrə malikdirlər. Şəbəkə trafikləri əlamətlərinin çıxarılması onların təsnifatında vacib rol oynayır. Lakin ənənəvi istifadə edilən əlamətlər şəbəkə trafiklərinin mürəkkəb qeyri-xətti xarakterini əks etdirmir və yüksək təsnifat dəqiqliyi təmin etmirlər. Şəbəkə trafikləri qeyri-stationar xarakterə və multifraktallıq, uzunmüddətli asılılıq və periodiklik kimi qeri-xətti xarakteristikalara malik olduğu üçün şəbəkə trafiklərinin təsnifatının dəqiqliyini artıran yeni robast təsnifat əlamətlərinin çıxarılması çox aktualdır. Bu məsələnin həlli üçün ən perspektivli üsul şəbəkə trafiki siqnallarının spektral analizidir. İşdə şəbəkə trafiki siqnallarının spektral analizi üçün veyvlet çevirməsinin istifadəsi təklif edilir və onun vasitəsilə təsnifat əlamətləri kimi istifadə ediləcək şəbəkə trafikləri siqnallarının energetik xarakteristikaları müəyyən edilir.
***Açar sözlər**: şəbəkə trafiki, şəbəkə trafikinin təsnifatı, təsnifat əlamətlərinin çıxarılması, siqnalların spektral analizi, veyvlet çevrilməsi, siqnalların energetik xassələri*

**Ramiz H. Shikhaliyev**
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az
**On the method of extracting classification features of network traffic based on signal analysis**
Modern network traffic has many features and dynamic properties that reflect network behavior and user activity. Extraction of the network traffic features plays an important role in their classification. However, the traditional features do not represent the complex non-linear nature of network traffic and do not represent high classification accuracy. Since the network traffic is non-stationary and has non-linear dynamic characteristics, such as self-similarity, multifractality, long-range dependence and periodicity. Therefore, it is very relevant to extract new robust classification features that will improve the accuracy of the classification of network traffic. To solve this problem, the most promising method is the spectral analysis of network traffic signals. For the spectral analysis of network traffic signals, this study proposes the use of wavelet transform that determines the energy characteristics of network traffic signals, which can be used as classification features.
***Keywords**: network traffic, network traffic classification, classification features extraction, spectral analysis of signals, wavelet transform, energy characteristics of signals.*