Современная наука и инновации. 2025. № 4. С. 37-46
ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Modern Science and Innovations. 2025;(4):37-46
TECHNICAL SCIENCE
INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Научная статья
УДК 004.75
https://doi.org/10.37493/2307-910X.2025.4.3

# Комплексная модель обнаружения аномалий в распределённых системах с применением спектральных и биометрических методов

**Игорь Владимирович Калиберда**[1*]

[1]Северо-Кавказский федеральный университет, Пятигорский институт (филиал) СКФУ, (д. 46, ул. Ермолова, 357500, г. Пятигорск, Россия)
[1] kaliberda-igor@yandex.ru; https://orcid.org/0009-0002-4186-7412
*Автор, ответственный за переписку

**Аннотация.** ***Введение.*** В статье рассмотрена интеграция спектрального анализа сетевого поведения и современных биометрических методов аутентификации. ***Цель.*** Целью исследования является повышение безопасности распределённых вычислительных систем. Перспективы дальнейших исследований включают использование вейвлет-преобразований для анализа нестационарных трафиков, адаптацию порогов обнаружения в зависимости от контекста пользователя. ***Материалы и методы.*** Модель включает использование рядов Фурье для анализа периодичности сетевых процессов, а также применение FaceNet, VGGFace и IrisCode для корректной идентификации пользователей. Представлена корреляционная модель, объединяющая биометрические и спектральные характеристики пользователя, позволяющая формировать интегральный показатель риска. ***Результаты и обсуждение.*** Проведён численный анализ, демонстрирующий возможность разделения нормальных пользователей и злоумышленников по спектральным характеристикам поведения. Графические результаты подтверждают эффективность предлагаемой модели. ***Заключение.*** По итогам проведенного исследования можно сделать вывод о том, что применение разложения в ряды Фурье позволяет формализовать поведенческий профиль пользователя в частотной области и выявлять высокочастотные компоненты, характерные для автоматизированных атак.

**Ключевые слова:** распределённые системы; безопасность; обнаружение аномалий; спектральный анализ; ряды Фурье; биометрическая аутентификация; FaceNet; VGGFace; IrisCode; поведенческий анализ; сетевой трафик; корреляционная модель риска; Fourier-спектр; IDS.
**Для цитирования:** Калиберда И. В. Комплексная модель обнаружения аномалий в распределённых системах с применением спектральных и биометрических методов // Современная наука и инновации. 2025. № 4. С. 37-46. https://doi.org/10.37493/2307-910X.2025.4.3
**Конфликт интересов:** автор заявляет об отсутствии конфликта интересов

Статья поступила в редакцию 01.01.2025;
одобрена после рецензирования 01.02.2025;
принята к публикации 01.03.2025.

© Калиберда И. В., 2025

Research article

# Comprehensive anomaly detection model for distributed systems using spectral and biometric methods

**Igor V. Kaliberda**[1*]

[1]North-Caucasus Federal University, Pyatigorsk Institute (branch) of NCFU (46, Ermolov Street, 357500, Pyatigorsk, Russia)
[1] kaliberda-igor@yandex.ru; https://orcid.org/0009-0002-4186-7412
*Corresponding author

**Abstract.** ***Introduction.*** The article discusses the integration of spectral analysis of network behavior and modern biometric authentication methods. ***Goal.*** The goal of the research is to improve the security of distributed computing systems. Further research prospects include the use of wavelet transformations for analyzing non-stationary traffic, and the adaptation of detection thresholds based on the user's context. ***Materials and methods.*** The model includes the use of Fourier series to analyze the periodicity of network processes, as well as the use of FaceNet, VGGFace, and IrisCode for the correct identification of users. A correlation model is presented that combines the biometric and spectral characteristics of a user, allowing for the formation of an integrated risk indicator. ***Results and discussion.*** A numerical analysis has been conducted to demonstrate the possibility of separating normal users and attackers based on the spectral characteristics of their behavior. The graphical results confirm the effectiveness of the proposed model. ***Conclusion.*** Based on the results of this study, it can be concluded that the use of Fourier series decomposition allows for the formalization of a user's behavioral profile in the frequency domain and the identification of high-frequency components characteristic of automated attacks.
**Key words:** Distributed systems, Fourier analysis, biometric authentication, FaceNet, IrisCode, VGGFace, spectral anomaly detection, network traffic modeling, intrusion detection systems, user behavior profiling, ROC optimization, information security.
**For citation:** Kaliberda IV. Comprehensive anomaly detection model for distributed systems using spectral and biometric methods. *Modern Science and Innovations*. 2025;(4):37-46. (In Russ.). https://doi.org/10.37493/2307-910X.2025.4.3

**Conflict of interest:** the authors declare no conflicts of interests.

The article was submitted 01.01.2025;
approved after reviewing 01.02.2025;
accepted for publication 01.03.2025.

**Введение.** Современные распределённые вычислительные системы характеризуются высокой динамичностью топологии, большим числом взаимодействующих узлов и неоднородностью сетевых протоколов, что усложняет обеспечение их информационной безопасности. Рост интенсивности автоматизированных атак, использование ботнетов, распределённых сканеров и подмены легитимных учётных данных повышают значимость методов, позволяющих выявлять отклонения поведения пользователей после аутентификации. Традиционные системы обнаружения вторжений преимущественно опираются на сигнатурные или статистические модели и недостаточно эффективны при анализе слабовыраженных и высокочастотных аномалий, маскируемых под легитимный трафик.

Одновременно биометрические методы аутентификации демонстрируют высокую устойчивость к компрометации учётных данных, однако они не обеспечивают контроль действий пользователя после успешного входа. Это создаёт необходимость применения комплексного подхода, объединяющего подтверждение личности и анализ её последующего сетевого поведения. В данной работе предлагается интегральная модель обеспечения безопасности распределённых систем, основанная на разложении сетевого трафика в ряды Фурье для выделения спектральных признаков поведения [1], а также на

применении современных алгоритмов биометрической идентификации (FaceNet [2], VGGFace [3], IrisCode [4]). Введён интегральный критерий риска, учитывающий биометрическую близость к шаблону пользователя и спектральное отклонение от эталонного поведения. Показано, что предложенный подход позволяет увеличить достоверность обнаружения аномалий и снизить вероятность ложных допусков.

**Математическое моделирование сетевых процессов.** Трафик распределённой системы можно формализовать как функцию *f(t),* описывающую интенсивность обмена пакетами, задержку или уровень загрузки сети. Поскольку сетевые процессы нередко обладают периодической компонентой (например, периодические heartbeat-сообщения, циклы синхронизации), такой временной ряд может быть представлен разложением в ряд Фурье:

$$f(t) = a_0 + \sum_{n=1}^{\infty}\left( a_n \cos\frac{2\pi nt}{T} + b_n \sin\frac{2\pi nt}{T} \right), \quad (1)$$

где: $T$ – характерный период наблюдаемой системы.

Коэффициент $a_n$:

$$a_n = \frac{2}{T}\int_0^T f(t)\cos\frac{2\pi nt}{T}dt\,.$$

Коэффициент $b_n$:

$$b_n = \frac{2}{T}\int_0^T f(t)\sin\frac{2\pi nt}{T}dt\,.$$

Высокие значения коэффициентов $a_n$ и $b_n$ на определённых частотах отражают устойчивую повторяющуюся активность. В нормальном режиме спектр распределённой системы характеризуется стабильными частотами, соответствующими:

- регулярным синхронизациям узлов;
- циклическому обновлению маршрутов;
- фоновым сетевым процедурам.

Пусть наблюдается изменение спектра на частоте $\omega_k$. Тогда, для выявления атак с помощью спектральных методов можно ввести метрику отклонения:

$$D(\omega_k) = \left| S_{текущее}(\omega_k) - S_{опорное}(\omega_k) \right|, \quad (2)$$

где *S(ω)* — амплитудный спектр:

$$S(\omega_n) = \sqrt{a_n^2 + b_n^2},\ \omega_n = \frac{2\pi n}{T}\,.$$

Если *D(ωk)* превышает порог $\delta_k$, фиксируется аномалия:

$$D(\omega_n) > \delta_n\,.$$

Возникновение новых частотных компонент или усиление гармоник может свидетельствовать об аномальной активности, такой как:

- скрытое сканирование сети, что проявляется в виде низкочастотных периодических всплесков;
- DDoS-атаки, демонстрирующие рост высокочастотной составляющей;
- внедрение вредоносного ПО, вызывающее появление новых регулярных шаблонов обмена.

Пользователь может пройти биометрию, но затем его поведение может отличаться спектрально и тем самым демонстрировать аномальные сетевые частоты, характерные для автоматизированных скриптов, ботов и скрытого сканирования сети. Дополнительный спектральный анализ показывает разницу спектров $\Delta S(\omega)$ по (2) [1], [2].

Фурье-анализ позволяет выявлять такие несоответствия. Для сравнения поведения воспользуемся выражением:

$$\Delta S(\omega) = \left| S_{mal}(\omega) - S_{norm}(\omega) \right|.$$

$\Delta S$ выделяет частоты, на которых злоумышленник отличается от нормального пользователя. Графики спектров сетевого временного ряда нормального пользователя, злоумышленника и $\Delta S(\omega)$, полученные с помощью преобразования Фурье, представлены на рисунках 1 – 3 [1].

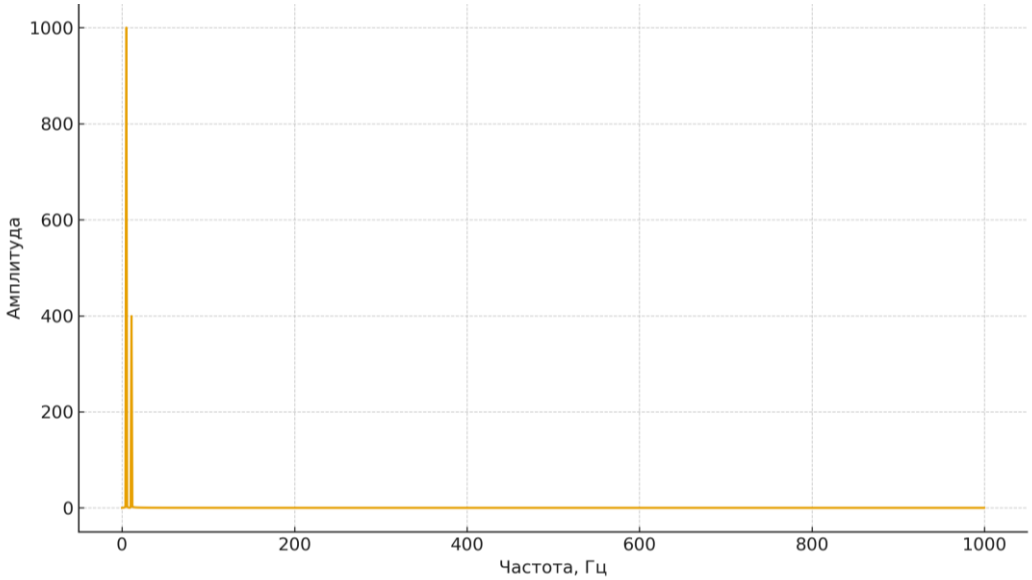


**Рисунок 1 – Спектр нормального пользователя / Figure 1 – The spectrum of a normal user**

На графике видны два доминирующих пика на низких частотах (около 5÷11 Гц). Это соответствует регулярной, «человеческой» активности: обычные запросы, навигация, стандартные операции в системе. Спектр относительно «чистый», без плотного высокочастотного «грязного» шума.

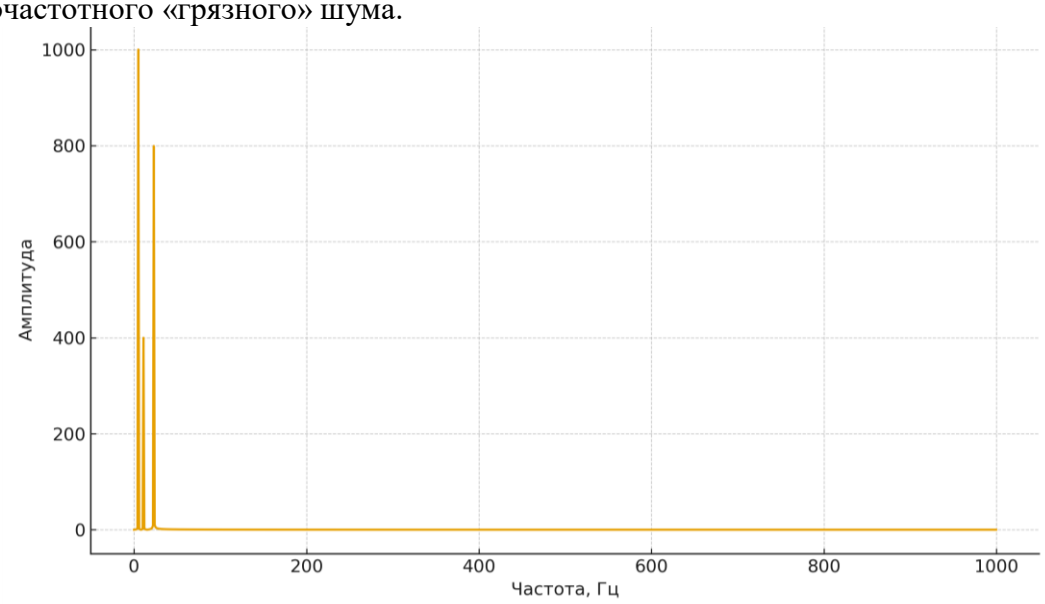


**Рисунок 2 – Спектр злоумышленника / Figure 2 – The attacker's spectrum**

Здесь, помимо нормальных компонент, появляется выраженный пик на более высокой частоте (около 23 Гц) и в целом усиливается частотная область. Такое поведение характерно для:

- частых однотипных запросов (скрипты, боты),
- сканирования портов/сервисов,
- автоматизированных атак с фиксированным временным шагом.

Для более глубокого анализа поведения пользователей введена метрика разницы спектров между нормальным и аномальным поведением. Метрика $\Delta S(\omega)$ позволяет выявить частоты, на которых наблюдаются существенно выраженные отклонения.

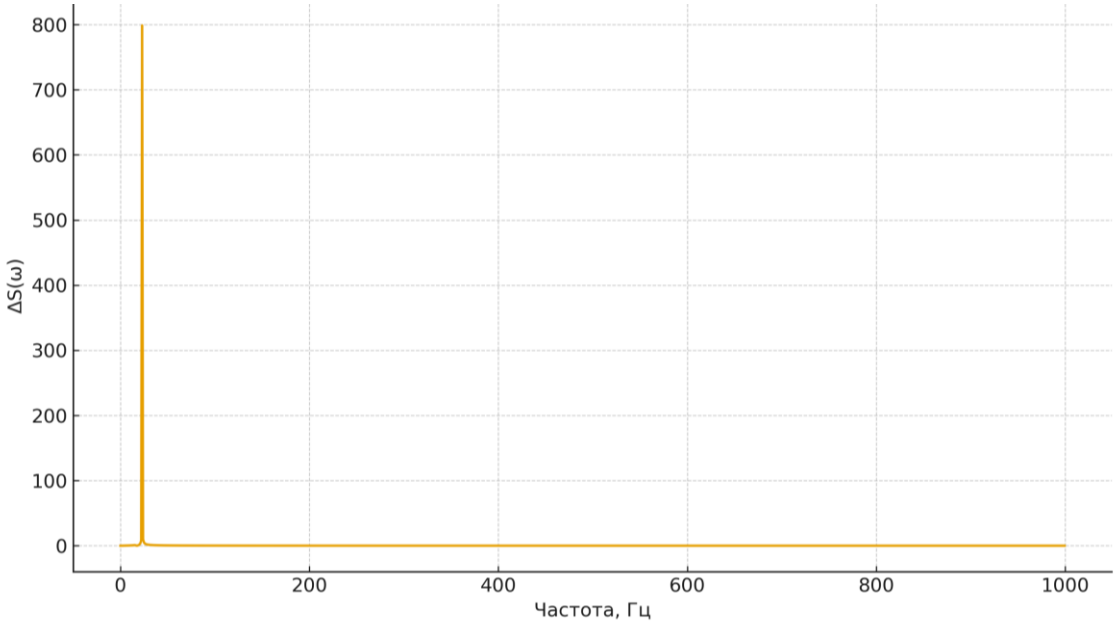


**Рисунок 3 – Разность спектров $\Delta S(\omega)$ / Figure 3 – Difference of spectra $\Delta S(\omega)$**

График $\Delta S(\omega)$ подчёркивает именно зоны отличий между нормальным и атакующим профилем. На низких частотах $\Delta S(\omega)$ обычно мала — злоумышленник имитирует нормальные действия. На частотах, соответствующих автоматизированной активности, наблюдаются ярко выраженные пики $\Delta S(\omega)$. Это создаёт удобный критерий для настройки порогов детектирования, вычисления интегрального показателя риска $K(u)$ и обучения моделей классификации «норма/атака».

Рост доли HTTPS и VPN приводит к невозможности применения методов анализа содержимого пакетов. В таких условиях актуальны подходы, основанные на спектральных и гибридных Fourier–Wavelet моделях, позволяющих классифицировать зашифрованный трафик по временным закономерностям без расшифрования. Такие подходы успешно применяются для выявления туннельных каналов, скрытых команд и аномальных периодических сигналов с автоматизацией [7].

Несмотря на классическое применение разложения в ряды Фурье [1], сетевой трафик обладает непостоянной частотной структурой, что требует применения вейвлет-преобразований. Вейвлет-анализ позволяет выделять локальные частотные особенности активности пользователя, что делает его эффективным дополнением к Fourier-моделям. Метод позволяет выявлять краткоживущие всплески активности, характерные для атак краткого периода (например, инъекций или сканирования) [8].

Современные распределённые системы требуют многослойной защиты, которая предотвращает как внешние сетевые атаки, так и внутренние злоупотребления. В данной работе предложена интеграция спектрального моделирования сетевых процессов (с использованием рядов Фурье) и биометрической идентификации пользователей, обеспечивающая согласованное повышение уровня защищённости. Эта связь формируется на трёх методологических уровнях: математическом, поведенческом и архитектурном [5].

Биометрические сигналы (в частности, IrisCode и FaceNet embeddings) также могут быть интерпретированы как периодические или квазипериодические. Последовательность данных IrisCode, описывающая фазовые характеристики радужки в полярной системе

координат, использует фильтры Габора — разновидность частотных фильтров, основанных на локализованных гармониках. При обработке лица (FaceNet, VGGFace) применяется декомпозиция изображений в пространственно-частотных признаках [5 – 7]. То есть биометрия уже «по природе» является частотным анализом, и ряды Фурье лежат в её основе.

Даже после успешной биометрической аутентификации поведение пользователя в системе должно контролироваться. И здесь спектральный анализ играет ключевую роль. Спектральный анализ подтверждает поведение пользователя (2), а биометрия подтверждает личность для пользователя $u$:

$$X_u = f(I_u)$$
$$d(X_u, R_u) \le \tau$$

где:

$R_u$ – шаблон пользователя;

$d$ — евклидово расстояние (FaceNet/VGGFace).

Интеграция спектральных методов и биометрической идентификации позволяет сопоставлять личность пользователя его цифровому поведенческому профилю. Биометрия подтверждает личность, тогда как спектральный анализ выявляет характерные частотные компоненты поведения, определяя отклонения, свойственные автоматизированным атакам [1]. Для объединения результатов биометрической аутентификации и спектрального анализа сетевого поведения вводится интегральный корреляционный критерий $K(u)$, определяемый для пользователя $u$. Пусть $X_u$ — биометрический вектор признаков пользователя, $R_u$ — его эталонный шаблон, $d(X_u, R_u)$ — метрика расстояния (евклидова), а $\Delta S(u)$ — нормированная метрика разницы спектров между текущим и опорным сетевым профилем данного пользователя. Тогда обобщённый критерий риска определяется выражением:

$$K(u) = \alpha \cdot d(X_u, R_u) + \beta \cdot \Delta S(u), \qquad (3)$$

где:

$\alpha$ — вес, позволяющий настроить модель по биометрии;

$\beta$ — вес, позволяющий настроить модель по анализу поведения;

$K(u)$ — безразмерный показатель риска.

Весовые коэффициенты $\alpha$ и $\beta$ выбираются в зависимости от приоритета точности биометрической аутентификации и чувствительности к аномалиям поведения. Чем выше значение $K(u)$, тем выше уровень подозрительности активности пользователя. При превышении порога $K_{пор}$ система инициирует дополнительные проверочные процедуры или блокировку сессии. Нормировка метрик $d(X_u, R_u)$ и $\Delta S(u)$ на интервал [0; 1] позволяет интерпретировать $K(u)$ как безразмерный риск-показатель, пригодный для сравнения между различными пользователями и сценариями атак.

Схема архитектурной интеграции спектрального моделирования сетевых процессов с биометрическим модулем представлена на рис. 4.

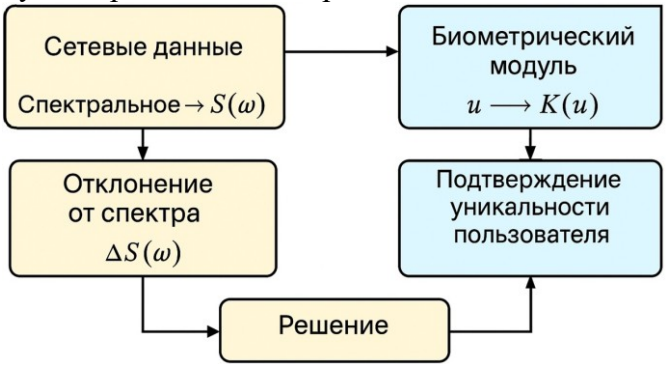


**Рисунок 4 – Схема архитектурной интеграции спектрального моделирования сетевых процессов с биометрическим модулем / Figure 4 – Architectural Integration of Spectral Network Process Modeling with a Biometric Module**

Помимо базовых сверточных архитектур FaceNet [2], современные системы применяют улучшенные векторные пространства, такие как FaceNet++ [9], использующие более плотные эмбеддинги и усиленную регуляризацию. Использование глубоких эмбеддингов повышает качество биометрической идентификации при низком качестве изображения, угловых искажениях и слабой освещенности. Подобные алгоритмы обеспечивают более точные оценки расстояния $d(X_u, R_u)$, что снижает вероятность ложных совпадений и усиливает роль биометрических факторов в расчёте интегрального критерия риска $K(u)$ [9].

Стандартизация биометрических данных является ключевым условием масштабируемости и интероперабельности систем аутентификации в распределённых вычислительных архитектурах. Стандарт ISO/IEC 19794-5:2011 определяет требования к структуре геометрических представлений лица, включая разметку ключевых точек, формат хранения и параметры совместимости между устройствами и сервисами биометрической обработки. Использование стандартизированных форматов позволяет корректно передавать биометрические шаблоны между облачными сервисами, edge-узлами и локальными компонентами системы, минимизируя потери точности и повышая устойчивость аутентификации к атакам повторного предъявления [10].

**Результаты исследований и их обсуждение.** Рассмотрим вычисление обобщённого критерия риска $K(u)$ для весов $\alpha = 0.6$ и $\beta = 0.4$ при нормированных метриках $d(X_u, R_u)$ и $\Delta S(u)$ в интервале [0; 1]. Били рассмотрены три пользователя со следующими показателями:

1) нормальный пользователь: $d = 0.15$, $\Delta S = 0.10$;
2) пограничный случай: $d = 0.30$, $\Delta S = 0.35$;
3) злоумышленник: $d = 0.55$, $\Delta S = 0.70$.

По формуле (3) были получены значения K(u):

K(нормальный) = 0.6·0.15 + 0.4·0.10 = 0.13;

K(пограничный) = 0.6·0.30 + 0.4·0.35 ≈ 0.32;

K(злоумышленник) = 0.6·0.55 + 0.4·0.70 = 0.61.

Таким образом, при выборе порогового значения $K_{пор}$ в диапазоне 0.4–0.5 нормальный пользователь и пограничный случай будут допущены, тогда как активность злоумышленника будет классифицирована как подозрительная и потребует дополнительных проверок.

На рисунке 5 представлены контурные линии значений $K(u)$ в зависимости от расстояния $d(X_u, R_u)$ и разницы спектров $\Delta S(u)$. Линейная структура изолиний отражает аддитивный характер модели.

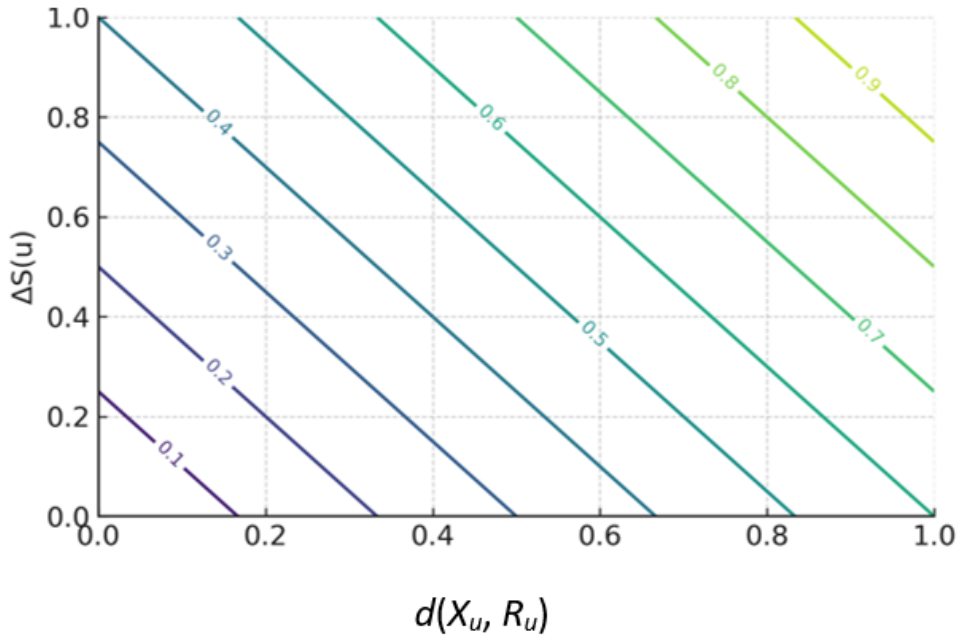


**Рисунок 5 – Контуры уровня $K(u)$ при α = 0.6, β = 0.4 / Figure 5 – Contour Levels of $K(u)$ at α = 0.6, β = 0.4**

Для фиксированного значения $\Delta S(u)$ функция $K(u)$ линейно возрастает с ростом $d(X_u, R_u)$, что позволяет интерпретировать вклад биометрической компоненты отдельно (рис. 6).

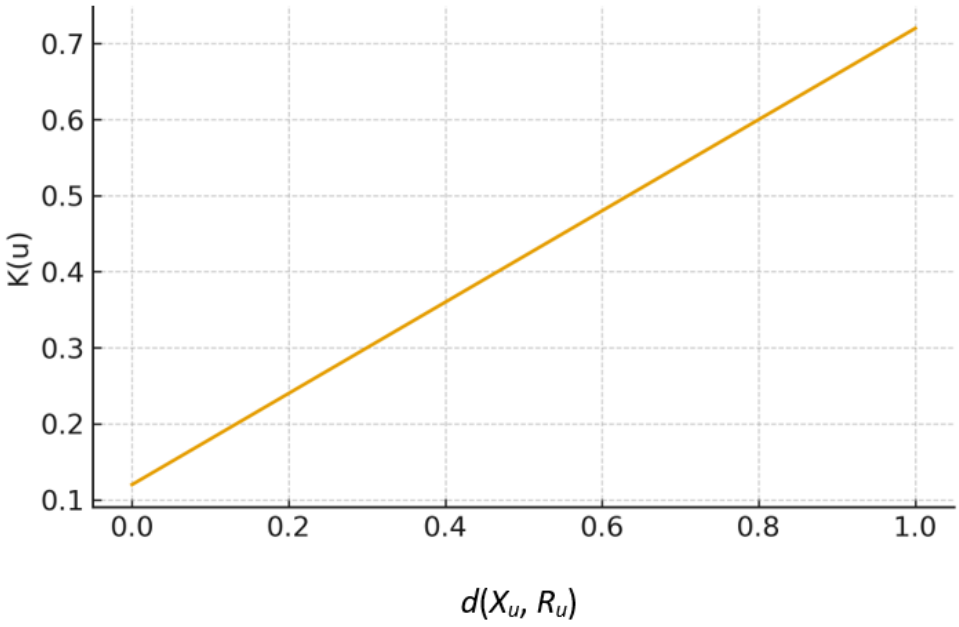


**Рисунок 6 – Зависимость $K(u)$ от $d(X_u, R_u)$ при $\Delta S(u) = 0.3$ / Figure 6 – Dependence of $K(u)$ on $d(X_u, R_u)$ at $\Delta S(u) = 0.3$**

Критерий $K(u)$ может быть использован для построения ROC-кривых, где по оси абсцисс откладывается уровень ложных допусков (FAR), а по оси ординат — уровень истинных срабатываний (TPR). Изменяя порог $K_{пор}$, можно получать различные пары значений (FAR, TPR) и тем самым выбирать оптимальный режим работы системы. Весовые коэффициенты α и β подбираются по экспериментальным данным с использованием методов оптимизации: минимизация EER, максимизация площади под

ROC-кривой (AUC) или многокритериальная настройка, учитывающая приоритеты оператора системы [11].

Таким образом, Фурье-анализ служит вторым уровнем защиты, контролируя поведение после биометрической проверки. Разложение в ряд Фурье позволяет выделить частотную структуру сетевой активности, выявить характерные гармоники и определить отклонения, связанные с аномальными воздействиями [4].

Этот подход позволяет:

- обнаруживать медленные атаки (slow-rate attacks);
- выявлять вредоносные периодические процессы;
- мониторить изменения в поведении протоколов консенсуса.

**Заключение.** В статье предложен комплексный подход к обеспечению безопасности распределённых вычислительных систем, основанный на совместном использовании биометрической идентификации и спектрального анализа сетевого трафика. Применение разложения в ряды Фурье позволяет формализовать поведенческий профиль пользователя в частотной области и выявлять высокочастотные компоненты, характерные для автоматизированных атак. Использование алгоритмов FaceNet, VGGFace и IrisCode обеспечивает надёжное подтверждение личности и снижает вероятность компрометации учётных данных.

Разработан интегральный критерий риска $K(u)$, объединяющий биометрическое расстояние и спектральное отклонение. Проведён численный анализ, демонстрирующий возможность разделения нормальных пользователей и злоумышленников по спектральным характеристикам поведения. Графические результаты подтверждают эффективность предлагаемой модели.

Перспективы дальнейших исследований включают использование вейвлет-преобразований для анализа нестационарных трафиков, адаптацию порогов обнаружения в зависимости от контекста пользователя и применение методов машинного обучения для классификации спектральных признаков [12].

**Список источников**

1. Оппенгейм А. Цифровая обработка сигналов. Prentice Hall, 2010.
2. Schroff F., Kalenichenko D., Philbin J. FaceNet: Unified Embedding for Face Recognition and Clustering // Proc. IEEE CVPR. 2015. pp. 815–823.
3. Parkhi O., Vedaldi A., Zisserman A. Deep Face Recognition // Proc. BMVC. Oxford Univ., 2015.
4. Daugman J. How IrisCode Works // IEEE Trans. Circuits and Systems Video Technology. 2003. Vol. 14. pp. 21–30.
5. Таненбаум Э., Ван Стин М. Распределённые системы: принципы и парадигмы. Pearson, 2020.
6. Столлингс В. Основы сетевой безопасности. Pearson, 2018.
7. Chen L., Sun M., Zhao Q. Hybrid Fourier-Wavelet Models for Encrypted Traffic Analysis // Computers & Security. 2023.
8. Mallat S. A Wavelet Tour of Signal Processing. — Academic Press, 2008.
9. Nguyen T., Vo M., Huynh D. FaceNet++: Enhanced Embedding Representations // Pattern Recognition Letters. 2024.
10. ISO/IEC 19794-5:2011. Информационные технологии. Биометрические форматы обмена данными. Часть 5: Геометрические данные лица.
11. Zhang Y., Liu H., Wang P. Fourier-Based Profiling of Network Behavior // IEEE Access. — 2021.
12. Kumar S., Patel R. Deep Biometric Fusion for Anomaly Detection // Journal of Network and Computer Applications. 2022.

**References**

1. Oppengeim A. Tsifrovaya obrabotka signalov. Prentice Hall, 2010.
2. Schroff F., Kalenichenko D., Philbin J. FaceNet: Unified Embedding for Face Recognition and Clustering. Proc. IEEE CVPR. 2015. pp. 815–823.

3. Parkhi O., Vedaldi A., Zisserman A. Deep Face Recognition. Proc. BMVC. Oxford Univ., 2015.
4. Daugman J. How IrisCode Works. IEEE Trans. Circuits and Systems Video Technology. 2003. Vol. 14. pp. 21–30.
5. Tanenbaum EH., Van Stin M. Raspredelennye sistemy: printsipy i paradigmy. Pearson, 2020.
6. Stollings V. Osnovy setevoi bezopasnosti. Pearson, 2018.
7. Chen L., Sun M., Zhao Q. Hybrid Fourier-Wavelet Models for Encrypted Traffic Analysis. Computers & Security. 2023.
8. Mallat S. A Wavelet Tour of Signal Processing. Academic Press, 2008.
9. Nguyen T., Vo M., Huynh D. FaceNet++: Enhanced Embedding Representations. Pattern Recognition Letters. 2024.
10. ISO/IEC 19794-5:2011. Informatsionnye tekhnologii. Biometricheskie formaty obmena dannymi. Chast' 5: Geometricheskie dannye litsa.
11. Zhang Y., Liu H., Wang P. Fourier-Based Profiling of Network Behavior. IEEE Access. 2021.
12. Kumar S., Patel R. Deep Biometric Fusion for Anomaly Detection. Journal of Network and Computer Applications. 2022.

## Информация об авторах

**Калиберда Игорь Владимирович –** старший преподаватель, Пятигорский институт (филиал) Северо-Кавказского федерального университета, ул. Ермолова, 46, г. Пятигорск, Ставропольский край, 357500, РФ. e-mail: kaliberda-igor@yandex.ru

**Вклад автора:**

**Калиберда Игорь Владимирович -** Проведение исследования – сбор, интерпретация и анализ полученных данных. Утверждение окончательного варианта – принятие ответственности за все аспекты работы, целостность всех частей статьи и ее окончательный вариант.

## Information about the authors

**Igor V. Kaliberda** – Senior Lecturer, Pyatigorsk Institute of the North Caucasus Federal University, 46 Yermolova Street, Pyatigorsk, Stavropol Territory, 357500, Russian Federation

**Contribution of the authors:**

**Igor V. Kaliberda** - Conducting research – data collection, analysis and interpretation.
Approval of the final manuscript – acceptance of responsibility for all types of the work, integrity of all parts of the paper and its final version.