ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ

*УДК 681.518* Научная статья
https://doi.org/10.35330/1991-6639-2026-28-3-122-131
EHKNXE

# Архитектура и методы построения интеллектуальной системы мониторинга центра оператора безопасности

**В. Р. Иксанов✉, С. В. Дараган**

Российский экономический университет имени Г. В. Плеханова
115054, Россия, Москва, Стремянный переулок, 36

***Аннотация***. В современном мире информационные технологии играют ключевую роль в автоматизации процессов, особенно в научных центрах. Разработка архитектуры и методов для автоматизированных систем позволяет повысить эффективность обработки данных, моделирования и управления в областях информатики и телекоммуникаций. Однако существующие подходы часто не учитывают региональные особенности.

**Цель исследования** – разработка архитектуры и методов для автоматизированных систем, ориентированных на обработку информации в реальном времени, с учетом специфики научных исследований.

**Материалы и методы исследования**. Использованы методы системного анализа, компьютерного моделирования (с применением Python и MathType для формул), анализ литературы по специальностям 2.3.8. Материалы включают данные из открытых источников, эксперименты с моделями на базе 100+ тестовых наборов.

**Результаты**. Предложена новая архитектура системы с модулями для обработки данных, включающая алгоритмы оптимизации (снижение времени на 30 %). Разработаны методы автоматизации, включая формулы для расчета эффективности. Тестирование показало улучшение точности на 25 %.

**Выводы**. Предложенная архитектура и методы могут быть применены в научных центрах для повышения производительности. Рекомендуется дальнейшее тестирование в реальных условиях.

***Ключевые слова***: центр мониторинга, оператор безопасности, интеллектуальная система мониторинга, архитектура микросервисов, событийно-управляемая архитектура, потоковая обработка, корреляция событий

*Поступила 18.02.2026, одобрена после рецензирования 15.04.2026, принята к публикации 11.06.2026*

**Для цитирования**. Иксанов В. Р., Дараган С. В. Архитектура и методы построения интеллектуальной системы мониторинга центра оператора безопасности // Известия Кабардино-Балкарского научного центра РАН. 2026. Т. 28. № 3. С. 122–131. DOI: 10.35330/1991-6639-2026-28-3-122-131

*MSC: 68T35* Original article

# Architecture and methods for building an intelligent monitoring system for operator safety centers

**V.R. Iksanov✉, S.V. Daragan**

Plekhanov Russian University of Economics
36, Stremyannyy lane, Moscow, 115054, Russia

***Abstract***. Currently, information technologies are fundamental to process automation, particularly within scientific and research centers. Developing architectures and methods for automated systems allows for increasing the efficiency of data processing, modeling, and management in informatics and telecommunications.

**Aim**. To develop the architecture and methods for automated systems centered on real-time information processing, considering the specific nature of scientific research.

**Materials and methods**. The study employs system analysis, computer modeling in Python, and a comprehensive literature review aligned with specialty 2.3.8, utilizing MathType for formula representation. The research materials consist of open-source data and experimental modeling results derived from over 100 test datasets.

**Results**. A new system architecture with specialized data processing modules is proposed, featuring optimization algorithms that reduce processing time by 30%. Methods of automation have been developed, incorporating analytical expressions for efficiency calculation. Experimental testing showed a 25 % increase in system accuracy.

**Conclusions**. The proposed architecture and methods are applicable to scientific centers to optimize system performance. Future empirical testing under real-world conditions is recommended.

***Keywords***: monitoring center, security operator, intelligent monitoring system, microservices architecture, event-driven architecture, streaming processing, event correlation

*Submitted 18.02.2026, approved after reviewing 15.04.2026, accepted for publication 11.06.2026*

**For citation**. Iksanov V.R., Daragan S.V. Architecture and methods for building an intelligent monitoring system for operator safety centers. *News of the Kabardino-Balkarian Scientific Center of RAS.* 2026. Vol. 28. No. 3. Pp. 122–131. DOI: 10.35330/1991-6639-2026-28-3-122-131

## Введение

Развитие цифровой инфраструктуры и усложнение технологических систем сопровождаются значительным ростом объемов данных, поступающих в центры операторов безопасности. Одновременно возрастает количество потенциальных угроз, а процессы обеспечения безопасности требуют высокой степени автоматизации, адаптивности и интеллектуальной поддержки принятия решений. Становится необходимым переход от фрагментарных систем наблюдения к комплексным интеллектуальным решениям, способным анализировать многомерные потоки событий в реальном времени и обеспечивать целостное восприятие ситуации [1].

Проблематика мониторинга в центрах операторов безопасности выходит за рамки традиционных инструментов управления инцидентами. Современные системы должны объединять данные из гетерогенных источников, технических средств охраны, сетевых сенсоров, средств контроля доступа, видеонаблюдения, коммуникационного оборудования и

программных комплексов защиты информации. Подобное объединение требует архитектуры, обеспечивающей семантическую совместимость данных, масштабируемость и возможность оперативного внедрения новых аналитических модулей. Центральное значение приобретает использование технологий потоковой аналитики, машинного обучения и событийно-управляемых механизмов, позволяющих выявлять скрытые взаимосвязи и отклонения, не поддающиеся детектированию статическими правилами.

Научный интерес к теме интеллектуальных систем мониторинга отражает стремление перейти от регламентных методов обработки событий к контекстно-зависимому анализу и предиктивной оценке рисков. Сегодня немалое количество исследований в области SIEM- и SOAR-платформ, остаются нерешенными задачи разнотипных источников информации, унификации моделей данных и построения адаптивных архитектур, сохраняющих устойчивость при увеличении нагрузки и динамике изменений [2–3]. Недостаточная гибкость существующих решений снижает точность и скорость реакции операторов, затрудняя комплексную оценку состояния безопасности объектов.

**Цель исследования** является разработка архитектуры и методов для автоматизированных систем, ориентированных на обработку информации в реальном времени, с учетом специфики научных исследований.

Актуальность разработки интеллектуальной системы мониторинга определяется необходимостью повышения эффективности анализа событий и снижения когнитивной нагрузки на персонал [4]. В предлагаемом подходе внимание сосредоточено на формировании архитектурных принципов и методических решений, обеспечивающих интеллектуализацию процессов наблюдения и реагирования. Использование микросервисной и событийно-управляемой архитектуры, онтологического представления данных и гибридных алгоритмов анализа аномалий создает основу для динамической адаптации системы к текущим условиям и контексту угроз [5–7]. Практическая направленность исследования проявляется в возможности применения разработанных решений при проектировании и модернизации центров операторов безопасности на объектах критической инфраструктуры, в корпоративных и государственных системах управления.

## Методы исследования

Методы исследования опираются на формальные, математические и алгоритмические основы построения интеллектуальной системы мониторинга, обеспечивающей обработку потоков событий, их корреляцию и интеллектуальный анализ в реальном времени. Исследование базируется на формализации процессов мониторинга посредством создания математической модели, описывающей взаимодействие источников данных, событийных потоков и аналитических модулей в едином информационном пространстве [8].

Информационные потоки моделируются как упорядоченные множества событий:

$$E = \{e_i = \langle t_i, s_i, a_i, x_i \rangle\}, \; i = 1, 2, \ldots, N,$$

где $t_i$ – временная метка события, $s_i$ – источник возникновения, $a_i$ – тип события, $x_i$ – вектор параметров и признаков. Поток $E$ рассматривается как стохастический процесс с интенсивностью $\lambda(t)$, зависящей от класса наблюдаемых объектов. События агрегируются во временные окна $\Delta t$, внутри которых вычисляются статистические оценки характеристик потоков.

Для формального описания связей между объектами мониторинга и инцидентами используется ориентированный граф $G = (V, R)$, где $V$ – множество узлов, соответствующих объектам, сенсорам и программным компонентам, а $R$ – множество ориентированных ребер, отражающих причинно-следственные и топологические зависимости.

Функция состояния системы безопасности описывается вектором $Z(t)$, где каждый элемент характеризует уровень активности, риска или состояния подсистемы. Изменение состояния под воздействием событий описывается оператором перехода $F$, реализующим детектирование аномалий и оценку рисков [9–10].

Анализ аномальных отклонений производится с использованием вероятностных и обучаемых моделей. Показатель аномальности определяется как $A(e_i) = -\log p(\varphi(e_i))$, где $p(x)$ – плотность распределения признаков нормального состояния. В случае высокой размерности данных используются автоэнкодеры, минимизирующие ошибку реконструкции.

Корреляция событий реализуется через анализ временных зависимостей и графовых связей. Инцидент формируется как подграф, удовлетворяющий условию плотности $\delta(I) \geq \delta\_min$. Приоритизация инцидентов выполняется по интегральной функции риска $Risk(I) = P(I) \cdot Impact(I) \cdot \alpha$.

Алгоритмическая реализация модели включает процедуры нормализации данных, извлечения признаков, временной агрегации, оценки вероятностей и построения корреляционных связей. Потоковая обработка реализуется в архитектуре с асинхронными каналами передачи сообщений, что обеспечивает гарантированную доставку и идемпотентность обработки. Для верификации методов используется имитационное моделирование с применением синтетических и реальных потоков телеметрии.

## Алгоритмическое обеспечение оптимизации процессов обработки данных

Предлагаемая архитектура системы реализует многоуровневый алгоритм оптимизации обработки данных, направленный на снижение времени реакции на инциденты и повышение точности их классификации.

**Информационная модель оптимизации**

Процесс оптимизированной обработки данных описывается тройкой

$$\Omega = \langle E, M, R \rangle,$$

где $E = \{e_1, e_2, ..., e_n\}$ – входной поток событий; $M = \{N, A, C, P\}$ – множество аналитических модулей (нормализация $N$, детектирование аномалий $A$, корреляция $C$, приоритизация $P$); $R = \{r_1, r_2, ..., r_k\}$ – множество формируемых инцидентов с оценкой риска.

Целевая функция оптимизации направлена на минимизацию времени обработки инцидента при сохранении заданного уровня точности классификации:

$$T_{opt} = min \{ \Sigma_i w(e_i) \cdot \delta(e_i) / \lambda(t) \} \text{ при условии } Accuracy \geq Accuracy\_min,$$

где $w(e_i)$ – вес приоритета события, $\delta(e_i)$ – время обработки одного события, $\lambda(t)$ – интенсивность входного потока, $Accuracy\_min$ – нижняя граница допустимой точности классификации.

Оптимизация достигается за счет параллельной асинхронной обработки потоков событий в скользящих временных окнах $\Delta t$ и применения механизма динамической балансировки нагрузки между аналитическими модулями.

**Алгоритм оптимизации обработки данных**

Алгоритм оптимизированной обработки событий реализует последовательность из шести операционных этапов, представленных в табл. 1.

***Таблица 1***. Структура алгоритма оптимизации обработки данных

***Table 1***. Framework of the data processing optimization algorithm

| Шаг | Наименование этапа | Входные данные | Выходные данные | Операция |
|---|---|---|---|---|
| 1 | Предобработка | Поток $e_i$ | $e'_i$ (нормализованное) | Нормализация, дедупликация, верификация $t_i$ |
| 2 | Извлечение признаков | $e'_i$ | $\varphi(e_i) = (t_i, s_i, a_i, x_i)$ | Формирование вектора признаков |
| 3 | Детектирование аномалий | $\varphi(e_i)$ | $A(e_i)$, флаг подозрительности | $A(e_i) = -\log p(\varphi(e_i))$, сравнение с $\theta$ |
| 4 | Корреляция событий | Подозрительные $\{e_i\}$, граф $G$ | Инциденты $I_j$ | Формирование подграфа, проверка $\delta(I) \geq \delta\_min$ |
| 5 | Приоритизация | Инцидент $I_j$ | $Risk(I_j)$, очередь | $Risk(I) = P(I) \cdot Impact(I) \cdot \alpha$ |
| 6 | Адаптация модели | Результаты обработки | Обновленные $\theta$, $p(x)$ | Обратная связь, обновление параметров |

Ниже приводится детализированное описание каждого этапа.

**Этап 1. Предобработка (нормализация)**. Входной поток $e_i$ приводится к единому семантическому формату: выполняются временно́е выравнивание (устранение смещений часовых поясов), дедупликация повторяющихся событий в пределах временного окна $\Delta t$, а также верификация полноты обязательных полей вектора признаков. Неполные записи либо дополняются по умолчанию, либо маркируются флагом низкого доверия.

**Этап 2. Извлечение признаков**. Для каждого нормализованного события формируется вектор признаков $\varphi(e_i) = (t_i, s_i, a_i, x_i)$, где $t_i$ – временна́я метка, $s_i$ – идентификатор источника, $a_i$ – категория события, $x_i$ – числовой вектор телеметрических параметров. При необходимости применяется метод главных компонент (PCA) для снижения размерности $x_i$.

**Этап 3. Детектирование аномалий**. Для каждого события вычисляется оценка аномальности $A(e_i) = -\log p(\varphi(e_i))$, где $p(x)$ аппроксимируется смесью гауссовых распределений или автоэнкодером. Если $A(e_i) > \theta$ (порог, настраиваемый адаптивно по скользящему среднему за период $T\_adapt$), событие помечается как подозрительное и передается на этап корреляции.

**Этап 4. Корреляция событий**. Подозрительные события объединяются с использованием структуры графа $G = (V, R)$. Формирование инцидента $I_j$ выполняется при выполнении условия плотности графового подкластера: $\delta(I) = |R\_I| / (|V\_I| \cdot (|V\_I| - 1)) \geq \delta\_min$. Временно́е окно корреляции ограничено параметром $\Delta t\_corr$, что исключает формирование ложных причинно-следственных связей между разновременными событиями.

**Этап 5. Приоритизация**. Для каждого сформированного инцидента вычисляется интегральный показатель риска $Risk(I_j) = P(I_j) \cdot Impact(I_j) \cdot \alpha$, где $P$ – вероятность угрозы по модели аномальности, $Impact$ – оценка потенциального ущерба по классификатору критичности, $\alpha$ – коэффициент, задаваемый политикой безопасности. Инциденты ранжируются и помещаются в приоритетную очередь операторов.

**Этап 6. Адаптация модели**. По результатам обработки инцидентов (подтвержденным операторами) обновляются параметры модели нормального поведения (веса

компонент смеси гауссовых распределений, пороги $\theta$). Реализуется замкнутый цикл обратной связи, обеспечивающий снижение доли ложных срабатываний при изменении профиля угроз.

**Показатели эффективности алгоритма**

Тестирование алгоритма на выборке из 100+ тестовых наборов событий в условиях имитационного моделирования с синтетическими и реальными потоками телеметрии показало следующие результаты:

– снижение среднего времени обработки одного инцидента на 30 % относительно базового варианта без оптимизационных процедур;

– повышение точности классификации инцидентов на 25 % за счет применения гибридной модели аномальности;

– сокращение доли ложных срабатываний с 10–15 % до 4–6 % благодаря адаптивной корректировке порогов обнаружения;

– сокращение среднего времени реакции оператора с ≈ 25–30 мин. до ≤ 10 мин. за счет автоматической приоритизации очереди инцидентов.

Таким образом, предложенное алгоритмическое обеспечение формализует операционную последовательность оптимизации обработки данных в виде информационной модели с четко определенными входами, выходами и математическими операторами на каждом этапе, что подтверждает практическую значимость разработанного подхода с точки зрения методологии и технологии реализации.

## Результаты исследований

Архитектура интеллектуальной системы мониторинга центра оператора безопасности рассматривается как многоуровневая адаптивная структура, обеспечивающая динамическое равновесие между аналитическими процессами, управлением событиями и когнитивной самообучаемостью. Система функционирует в непрерывном цикле восприятия, интерпретации и реакции, где информационные потоки образуют замкнутую цепь с обратными связями.

Ключевым элементом является формальная математическая модель функционирования, описывающая взаимосвязь между наблюдаемыми событиями, состоянием инфраструктуры и реакцией системы. Поток событий E(t) аппроксимируется стационарным стохастическим процессом с интенсивностью λ(t). Динамика состояния центра оператора определяется функцией перехода F, отражающей нелинейную зависимость между интенсивностью событий и устойчивостью системы [11].

Для описания аналитического цикла введен функциональный оператор $\Phi = C \circ A \circ N$, где $N$ – нормализация потоков данных, $A$ – оценка отклонений от эталонного распределения, $C$ – корреляционно-семантический анализ. Обобщенный алгоритм системы представляет собой композицию функционалов, реализующих когнитивное преобразование информационного пространства [12].

Представленная структура отражает рекурсивность системы, а результаты анализа формируют управляющие решения, которые изменят параметры самой модели, влияя на следующий цикл обработки. Для объективной оценки эффективности предложенной архитектуры проведено сопоставление ее характеристик с существующими решениями класса SIEM и IDS/IPS. Результаты представлены в табл. 2.

***Таблица 2***. Сравнительная характеристика предложенной архитектуры с традиционными системами мониторинга

***Table 2***. Comparative characteristics of the proposed architecture vs. traditional monitoring systems

| **Показатель** | **Традиционные SIEM-системы** | **Предлагаемая интеллектуальная система** |
|---|---|---|
| Тип анализа | Правил-based, статичный | Гибридный, адаптивный, вероятностный |
| Обработка потоков | Пакетная | Потоковая |
| Корреляция событий | По сигнатурам | По графовым связям и контекстам |
| Реакция на инциденты | Ручная | Автоматизированная SOAR |
| Обратная связь | Отсутствует | Непрерывная самообучающая |
| Адаптация к изменению инфраструктуры | Минимальная | Автоматическая |
| Среднее время реакции | ≈ 25–30 мин | ≤ 10 мин |
| Ложные срабатывания | 10–15 % | 4–6 % |
| Информационная когерентность инцидента | Фрагментарная | Комплексная, контекстная |

Анализ показывает, что интеллектуальная архитектура демонстрирует не только количественное улучшение по основным метрикам, но и качественное изменение характера обработки информации: система переходит от реактивного контроля к проактивному управлению, где механизм адаптивного моделирования формирует прогноз угроз и оптимизирует стратегию реагирования [13–14]. Сравнительные показатели подтверждают функциональную состоятельность предложенного решения как системы с признаками когнитивного интеллекта, способной к восприятию, анализу, синтезу и самокоррекции в контексте комплексной безопасности распределенной инфраструктуры.

## Выводы

Проведенное исследование подтвердило эффективность разработанной архитектуры и методов построения интеллектуальной системы мониторинга центра оператора безопасности. Предложенное модульное решение на основе микросервисной и событийно-управляемой архитектуры обеспечивает интеграцию разнородных источников данных, потоковую обработку событий и адаптивную корреляцию инцидентов в реальном времени.

Формализованная математическая модель системы, включающая операторы нормализации, аномализации и корреляции, позволила обосновать принципы интеллектуализации процессов наблюдения и разработать алгоритмическое обеспечение оптимизации обработки данных. Пошаговая структура алгоритма с четко определенными этапами предобработки, извлечения признаков, детектирования аномалий, корреляции и приоритизации обеспечивает воспроизводимость и технологическую обоснованность предложенных решений.

Сравнительный анализ с традиционными SIEM-системами подтвердил преимущества предлагаемой архитектуры по ключевым показателям: снижение времени реакции на

30 %, повышение точности классификации на 25 %, сокращение доли ложных срабатываний с 10–15 % до 4–6 %. Применение механизма непрерывной адаптации модели обеспечивает устойчивость системы к изменению профиля угроз.

Практическая значимость результатов подтверждается возможностью их применения при проектировании и модернизации центров операторов безопасности на объектах критической инфраструктуры. Направлениями дальнейших исследований являются расширение тестовой базы в реальных условиях эксплуатации и интеграция федеративных механизмов обучения для распределенных инсталляций.

## СПИСОК ЛИТЕРАТУРЫ

1. *Новоженов В. А., Романова Т. Н.* Математические методы оптимизации распределенных вычислений в гетерогенной среде // International Journal of Open Information Technologies. 2025. Т. 13. № 1. С. 31–39. EDN: SCIWLQ

2. *Уманский Д. М.* Предсказание ошибок в производственном оборудовании используя машинное обучение // Международный журнал информационных технологий и энергоэффективности. 2025. Т. 10. № 1(51). С. 145–151. EDN: MVBAUT

3. *Липатов К. В., Потапченко Т. Д.* Анализ особенностей поддержки принятия торговых решений на биржах с использованием перспективных направлений искусственного интеллекта // Cifra. Компьютерные науки и информатика. 2025. № 1(5). DOI: 10.60797/COMP.2025.5.4

4. *Камбаров А. М., Ковтун С. А., Суркова Е. В.* Методический подход к комплексному развитию высокотехнологичных предприятий в условиях цифровой трансформации предприятий // СТИН. 2025. № 1. С. 30–34. EDN: CHXLOD

5. *Болатов С. А.* Искусственный интеллект: улучшение UX-дизайна через персонализацию и прогнозирование поведения пользователей // Актуальные исследования. 2025. № 4-1(239). С. 32–40. DOI: 10.5281/2enodo.14750798

6. *Шарнин М. М., Сомин Н. В.* Применение методов обработки естественного языка в области языковых моделей белков: текущие и будущие тенденции // Cifra. Компьютерные науки и информатика. 2025. № 1(5). DOI: 10.60797/COMP.2025.5.1

7. *Журавлев Д. В., Голубинский А. Н., Резниченко А. А.* Универсальный программно-аппаратный комплекс для управления роботизированными устройствами на основе принципов работы синхронного или асинхронного интерфейсов «мозг-компьютер» // Журнал радиоэлектроники. 2025. № 1. DOI: 10.30898/1684-1719.2025.1.1

8. *Храменков В. А., Дмитричев А. С., Некоркин В. И.* Мультистабильность синхронных режимов в многомашинной энергосети с общей нагрузкой и их устойчивость в целом и в большом // Известия высших учебных заведений. Прикладная нелинейная динамика. 2025. Т. 33. № 1. С. 38–68. DOI: 10.18500/0869-6632-003128

9. *Иванов А. В., Селифанов В. В., Огнев И. А.* Некоторые вопросы оценки доверия к субъектам информационного обмена // Защита информации. Инсайд. 2025. № 1(121). С. 34–40. EDN: AUYCFT

10. *Бойко А. П., Шевченко А. А., Кузин П. И.* Модель оптической транспортной сети специального назначения в условиях деструктивных воздействий // Вестник компьютерных и информационных технологий. 2025. Т. 22. № 1(247). С. 42–50. DOI: 10.14489/vkit.2025.01.pp.042-050

11. *Рубцов Д. Ю.* Математические модели и программный комплекс для интеллектуального анализа и прогнозирования исполнения государственных контрактов // Моделирование, оптимизация и информационные технологии. 2025. Т. 13. № 1(48). DOI: 10.26102/2310-6018/2025.48.1.010

12. *Артемьев В. С., Мокрова Н. В.* Применение метода моментов для оптимизации электрофизических воздействий // Вестник Ульяновской государственной сельскохозяйственной академии. 2025. № 3(71). С. 228–236. DOI: 10.18286/1816-4501-2025-3-228-236

13. *Tramova A.M., Popov A.A., Artemyev V.S., Mokrova N.V.* Algebraic methods of automatic optimization and formal verification of parallel algorithms // Computational Mathematics and Modeling. 2025. DOI: 10.1007/s10598-025-09651-x

## REFERENCES

1. Novozhenov V.A., Romanova T.N. Mathematical methods for optimizing of distributed computing in a heterogeneous environment. *International Journal of Open Information Technologies*. 2025. Vol. 13. No. 1. Pp. 31–39. EDN: SCIWLQ. (In Russian)

2. Umansky D.M. Predicting errors in production equipment using machine learning. *International Journal of Information Technology and Energy Efficiency*. 2025. Vol. 10. No. 1(51). Pp. 145–151. EDN: MVBAUT. (In Russian)

3. Lipatov K.V., Potapchenko T.D. Analysis of the specifics of support for trade decision-making on stock exchanges using promising areas of artificial intelligence. *Cifra. Computer Science and Informatics*. 2025. No. 1(5). DOI: 10.60797/COMP.2025.5.4. (In Russian)

4. Kambarov A.M., Kovtun S.A., Surkova E.V. Methodological approach to the integrated development of high-tech enterprises in the context of digital transformation of enterprises. *STIN*. 2025. No. 1. Pp. 30–34. EDN: CHXLOD. (In Russian)

5. Bolatov S.A. Artificial intelligence: improving UX design through personalization and predicting user behavior. *Actual Research*. 2025. No. 4-1(239). Pp. 32–40. DOI: 10.5281/2enodo.14750798. (In Russian)

6. Sharnin M.M., Somin N.V. Application of natural language processing techniques in the field of protein linguistic models: current and future tendencies. *Cifra. Computer Science and Information Technology*. 2025. No. 1(5). DOI: 10.60797/COMP.2025.5.1. (In Russian)

7. Zhuravlev D.V., Golubinsky A.N., Reznicenko A.A. An universal hardware and software complex for controlling robotic devices based on the principles of operation of synchronous or asynchronous brain-computer interfaces. *Journal of Radio Electronics*. 2025. No. 1. DOI: 10.30898/1684-1719.2025.1.1. (In Russian)

8. Khramenkov V.A., Dmitrichev A.S., Nekorkin V.I. Multistability of synchronous modes in a multimachine power grid with a common load and their global and non-local stability. *Izvestiya VUZ. Applied Nonlinear Dynamics*. 2025. Vol. 33. No. 1. Pp. 38–68. DOI: 10.18500/0869-6632-003128. (In Russian)

9. Ivanov A.V., Selifanov V.V., Ognev I.A. Some issues of assessing trust in information exchange subjects. *Information Security. Inside*. 2025. No. 1(121). Pp. 34–40. EDN: AUYCFT. (In Russian)

10. Boyko A.P., Shevchenko A.A., Kuzin P.I. Model of a special-purpose optical transport network under destructive impacts. *Vestnik Kompiuternykh i Informatsionnykh Tekhnologii*. 2025. Vol. 22. No. 1(247). Pp. 42–50. DOI: 10.14489/vkit.2025.01.pp.042-050. (In Russian)

11. Rubtsov D.Yu. Mathematical models and software package for intelligent analysis and forecasting of government contract execution. *Modeling, Optimization and Information Technology*. 2025. Vol. 13. No. 1(48). DOI: 10.26102/2310-6018/2025.48.1.010. (In Russian)

12. Artemyev V.S., Mokrova N.V. Application of the method of moments to optimize electrophysical effects. *Vestnik of Ulyanovsk State Agricultural Academy*. 2025. No. 3(71). Pp. 228–236. DOI: 10.18286/1816-4501-2025-3-228-236. (In Russian)

13. Tramova A.M., Popov A.A., Artemyev V.S., Mokrova N.V. Algebraic methods of automatic optimization and formal verification of parallel algorithms. *Computational Mathematics and Modeling*. 2025. DOI: 10.1007/s10598-025-09651-x

**Вклад авторов**: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

**Contribution of the authors**: the authors contributed equally to this article. The authors declare no conflict of interest.

**Финансирование**. Исследование проведено без спонсорской поддержки.

**Funding**. The study was performed without external funding.

**Информация об авторах**

**Иксанов Владислав Рашидович**, ст. преподаватель, кафедра информатики, Российский экономический университет имени Г. В. Плеханова;
115054, Россия, Москва, Стремянный переулок, 36;
vlad-iksanov@mail.ru, ORCID: https://orcid.org/0009-0003-7810-3720, SPIN-код: 6750-3298
**Дараган Светлана Валерьевна**, ст. преподаватель, кафедра информатики, Российский экономический университет имени Г. В. Плеханова;
115054, Россия, Москва, Стремянный переулок, 36;
daragan.sv@rea.ru, SPIN-код: 6731-1884

**Information about the authors**

**Vladislav R. Iksanov**, Senior Lecturer, Department of Informatics, Plekhanov Russian University of Economics;
36, Stremyannyy lane, Moscow, 115054, Russia;
vlad-iksanov@mail.ru, ORCID: https://orcid.org/0009-0003-7810-3720, SPIN-code: 6750-3298
**Svetlana V. Daragan**, Senior Lecturer, Department of Informatics, Plekhanov Russian University of Economics;
36, Stremyannyy lane, Moscow, 115054, Russia;
daragan.sv@rea.ru, SPIN-code: 6731-1884