МНОГОУРОВНЕВАЯ АРХИТЕКТУРА СИСТЕМЫ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ВОЗДЕЙСТВИЯ В ЭРГАТИЧЕСКИХ СИСТЕМАХ

Мещеряков Р. В.[1], Селиверстов Д. Е.[2], Русаков К. Д.[3]

DOI: 10.21681/2311-3456-2025-5-119-127

Цель исследования: *проектирование многоуровневой системы мониторинга и реагирования на воздействия, обеспечивающей устойчивость сложных эргатических систем за счет использования резервного контура управления и адаптивного распределения ресурсов.*

Методы исследования: *системный анализ, моделирование, синтез архитектуры, распределение ресурсов.*

Результаты исследования: *разработана многоуровневая архитектура системы мониторинга и реагирования на воздействия, направленная на повышение устойчивости сложных эргатических систем. Предложено структурное решение, включающее основной и резервный контуры управления, что обеспечивает непрерывность мониторинга и координацию реагирования даже при частичной деградации или отказе коммуникационной инфраструктуры. Спроектирован механизм адаптивного перераспределения ресурсов между компонентами архитектуры, обеспечивающий эффективное функционирование системы в условиях переменной нагрузки и ограниченных вычислительных и сетевых возможностей. Теоретическая значимость работы заключается в развитии научных представлений о построении многоуровневых архитектур защиты эргатических систем, обеспечивающих их функционирование в условиях сложных воздействий. Практическая значимость определяется возможностью применения спроектированных архитектурных решений при создании и модернизации распределенных автоматизированных комплексов различного назначения с целью повышения их устойчивости и эффективности мониторинга.*

Научная новизна: *впервые предложена многоуровневая архитектура системы мониторинга и реагирования на воздействия, в которой реализовано разделение на основной и резервный контуры управления, обеспечивающее устойчивость функционирования при деградации связи и отказах. Впервые разработан механизм адаптивного перераспределения ресурсов между уровнями системы, позволяющий поддерживать эффективность мониторинга и реагирования в условиях переменной нагрузки и ограниченных вычислительных и сетевых возможностей.*

Ключевые слова: *отказоустойчивость, киберустойчивость, федеративное взаимодействие, резервный контур управления, адаптивное распределение ресурсов, эргатические системы, автоматизированные комплексы, кибербезопасность.*

Введение

Современные эргатические системы управления представляют собой сложные интеграции технических средств, программного обеспечения и операторов, обеспечивающие выполнение критичных процессов в промышленности, транспорте и других социально-значимых сферах [1]. Их устойчивое функционирование напрямую зависит от способности противостоять разнообразным информационно-техническим воздействиям (ИТВ), включая преднамеренные кибератаки, случайные сбои оборудования, ошибки операторов и деградацию каналов связи. С ростом масштабов цифровизации и взаимосвязанности компонентов таких систем значительно возрастает риск каскадных отказов, когда локальные нарушения могут привести к разрушению всей функциональной цепочки [2]. Особенно критично это для систем, обеспечивающих безопасность государства и общества, где последствия отказов могут быть катастрофическими.

Традиционные централизованные системы мониторинга и реагирования, в том числе классические системы обнаружения и предотвращения вторжений (IDS/IPS), остаются уязвимыми к ряду фундаментальных проблем. Основной недостаток – наличие единой точки отказа, при выходе из строя которой вся система защиты становится неработоспособной. Централизованные решения плохо масштабируются и неэффективно обрабатывают большие объёмы данных при динамически изменяющейся нагрузке [3]. В современных исследованиях активно развиваются многоуровневые и распределённые архитектуры, которые позволяют повысить отказоустойчивость и гибкость реагирования. Примером являются гибридные системы, объединяющие периферийные и облачные

1 Мещеряков Роман Валерьевич, доктор технических наук, профессор РАН, ФГБУН «Институт проблем управления им. В. А. Трапезникова Российской академии наук», г. Москва, Россия. ORCID: 0000-0002-1129-8434. E-mail: mrv@ipu.ru

2 Селиверстов Дмитрий Евгеньевич, кандидат технических наук, ФГБУН «Институт проблем управления им. В. А. Трапезникова Российской академии наук», г. Москва, Россия. ORCID: 0009-0004-8412-7873. E-mail: Seliverstov_dmitriyy@rambler.ru

3 Русаков Константин Дмитриевич, «Институт проблем управления им. В. А. Трапезникова Российской академии наук», г. Москва, Россия. ORCID: 0009-0004-8412-7873. E-mail: rusakov@ipu.ru

вычислительные узлы, что позволяет распределять вычислительную нагрузку и обеспечивать баланс между быстротой реагирования и глубиной аналитики [4]. Важным направлением развития является также федеративный принцип взаимодействия (распределённое взаимодействие автономных уровней без передачи исходных данных), реализованный, например, в многоагентных системах на основе методов глубокого обучения, позволяющих обмениваться знаниями между узлами без передачи чувствительных данных [5]. Однако анализ отечественных и зарубежных решений показал, что существующие разработки недостаточно учитывают необходимость резервирования управления и адаптивного перераспределения ресурсов, что особенно важно в условиях деградации коммуникационной инфраструктуры и ограниченных вычислительных возможностей [6].

В аналитическом исследовании был проведён анализ патентов и научных публикаций, посвящённых системам мониторинга и реагирования на ИТВ. Результаты анализа показали, что несмотря на значительный прогресс, сохраняется проблема отсутствия комплексных архитектур, которые могли бы функционировать в условиях неопределённости и частичных отказов. Это определяет актуальность задач, связанных с проектированием многоуровневых систем нового поколения, в которых сочетаются принципы федеративного взаимодействия, резервирования и адаптивного управления ресурсами.

Цель настоящей работы заключается в проектировании многоуровневой архитектуры системы мониторинга и реагирования на ИТВ с резервным контуром управления и механизмом адаптивного распределения ресурсов, направленной на обеспечение устойчивости сложных эргатических систем в условиях динамических внешних и внутренних воздействий. В статье представлено структурное решение проектируемой архитектуры и механизм адаптивности, а также обсуждается теоретическая и практическая значимость предложенного подход.

Анализ архитектурных решений

В эргатических системах устойчивость функционирования напрямую зависит от архитектуры средств мониторинга и реагирования на информационно-технические воздействия (ИТВ). Архитектурное решение определяет, насколько эффективно система способна противостоять отказам отдельных элементов, деградации каналов связи и динамически изменяющимся нагрузкам [7]. Современные подходы к построению систем мониторинга и реагирования эволюционировали от централизованных решений к многоуровневым и распределённым системам. Однако, даже самые современные разработки имеют свои ограничения, что обуславливает необходимость поиска новых архитектурных принципов. В данном разделе проводится анализ существующих решений с выделением их преимуществ и недостатков для определения требований к проектируемой системе.

Централизованные архитектуры исторически стали первыми решениями для систем защиты информации и мониторинга. Они характеризуются наличием единого центра, который принимает все решения по обработке данных и реагированию. Такие системы просты в администрировании и понятны с точки зрения логики управления [8], однако их главный недостаток – наличие единой точки отказа. Сбой или атака на центральный узел приводит к полной потере контроля, что делает такие решения непригодными для высоконагруженных и критичных систем. Централизованные архитектуры плохо масштабируются при росте числа элементов и генерируемых событий [9].

Следующим этапом развития стали многоуровневые системы, где функции мониторинга и реагирования распределяются между локальным, промежуточным и глобальным уровнями. Пример такой системы представлен в [10], где локальные узлы выполняют первичный анализ, промежуточные – корреляцию данных и принятие решений в своих сегментах, а глобальный уровень обеспечивает стратегическую координацию. Многоуровневая структура позволяет повысить отказоустойчивость и снизить нагрузку на центральные компоненты, но остаётся зависимость от верхнего уровня: при его отказе координация сегментов нарушается.

Современные исследования активно развивают распределённые архитектуры, где все узлы равноправны и обмениваются информацией напрямую без выделенного центра управления. Такой подход позволяет минимизировать риски полного отказа системы и повысить её гибкость [11], однако он предъявляет повышенные требования к алгоритмам синхронизации и маршрутизации данных. В работе [12] показано, что распределённые решения обеспечивают высокую устойчивость к динамическим изменениям структуры сети, но сложность их внедрения и администрирования пока остаётся серьёзным ограничением.

Федеративные архитектуры сочетают принципы многоуровневых и распределённых систем. Узлы обрабатывают данные локально и передают на верхние уровни только агрегированные результаты. Такой подход позволяет снизить нагрузку на каналы связи, сохранить конфиденциальность данных и повысить масштабируемость [13]. Тем не менее, федеративные решения требуют сложных алгоритмов адаптивного управления ресурсами, чтобы обеспечить баланс между локальной автономностью и глобальной координацией [14].

Анализ существующих подходов показал, что ни одна из рассмотренных архитектур не обеспечивает комплексного решения по ключевым направлениям – устойчивости, адаптивности и резервированию управления. Для построения многоуровневой системы мониторинга и реагирования на информационно-технические воздействия необходимо выделить совокупность требований, которые станут основой для проектируемой архитектуры и механизма её функционирования. На основе проведённого системного анализа и современных научных исследований [15–20] сформулирован ряд ключевых требований. Рассмотрим их подробно. Первым требованием является отказоустойчивость и отсутствие единой точки отказа. Здесь каждый уровень и узел системы должны сохранять базовые функции мониторинга и реагирования при отказе центральных компонентов или деградации каналов связи. Второе требование касается непрерывности мониторинга за счёт резервного контура управления. Оно подразумевает существование отдельного резервного контура, способного автоматически перехватывать управление при сбое основного уровня и обеспечивать координацию действий в условиях критической ситуации. Третье требование относится к адаптивному распределению ресурсов, то есть, система должна динамически перераспределять вычислительные и сетевые ресурсы в зависимости от текущей нагрузки, доступности каналов и приоритетности задач, минимизируя задержки обработки событий. Четвертое требование предъявляется к масштабируемости и модульности архитектуры, которая должна поддерживать гибкое добавление новых узлов и сегментов без необходимости глобальной реконфигурации системы.

Таким образом можно сделать вывод, что для эффективного противодействия информационно-техническим воздействиям архитектура должна быть спроектирована таким образом, чтобы обеспечивать устойчивость, адаптивность и резервирование управления. Эти три фактора являются взаимосвязанными и определяют целостность решения. Таким образом, архитектура должна объединять преимущества многоуровневых и распределённых решений, дополняясь механизмами адаптивности и резервирования, что позволяет создать основу для высокоэффективных систем мониторинга и реагирования.

Постановка задачи исследования

Исходя из результатов проведенного анализа, задача исследования формулируется следующим образом: необходимо разработать многоуровневую архитектуру системы мониторинга и реагирования на информационно-технические воздействия эргатических систем, в которой реализованы требования устойчивости, адаптивности и резервирования управления. Архитектура должна включать основной и резервный контуры управления, а также механизм адаптивного перераспределения вычислительных и сетевых ресурсов, обеспечивающий эффективное функционирование системы в условиях динамически изменяющихся нагрузок, частичных отказов и деградации коммуникационной инфраструктуры. Формально задача исследования примет следующий вид. Дано: множество исходных данных $D = \langle V,E,\Lambda,\Omega\rangle$, V – множество узлов (компонентов системы мониторинга и реагирования), E – множество каналов связи между узлами, Λ – характеристики потоков данных и динамически изменяющихся нагрузок, Ω – множество сценариев частичных отказов и деградации коммуникационной инфраструктуры. Требуется: разработать многоуровневую архитектуру $A = \langle L,C,M\rangle$ где L – структура уровней архитектуры (локальный, сегментный, глобальный), C – основной и резервный контуры управления, M – механизм адаптивного перераспределения ресурсов между уровнями и узлами. При этом, архитектура A определяется на основе исходных данных $A = F(D)$, и обеспечивает выполнение таких требований как: устойчивость ($\forall\omega \in \Omega$: $\Phi_{work}(A,\omega) \geq \Phi_{min}$, где Φ_{work} – функциональность архитектуры при сценарии ω, а Φ_{min} – минимально допустимый уровень функционирования системы); адаптивность (M:$(\Lambda) \longrightarrow \Lambda'$, где M обеспечивает динамическое перераспределение ресурсов и потоков данных при изменениях нагрузки и состояния системы; резервирование управления ($\forall v \in V$: $\exists\ p(v,C_{main}) \vee p(v,C_{res})$, где $p(v,C)$ – наличие связного пути от узла v к основному C_{main} или резервному C_{res} контуру управления.

Разработка архитектуры

В предыдущих разделах статьи были определены исходные данные $D = \langle V,E,\Lambda,\Omega\rangle$ и сформулированы ключевые требования к разрабатываемой архитектуре: устойчивость, адаптивность и резервирование управления. Эти требования отражают специфику функционирования эргатических систем и являются основой для дальнейших проектных решений. На данном этапе основная цель – разработка многоуровневой архитектуры $A = \langle L,C,M\rangle$, которая позволит системе мониторинга и реагирования эффективно функционировать в условиях: динамически изменяющихся нагрузок Λ, частичных отказов и деградации инфраструктуры Ω, повышенных требований к непрерывности и надежности процессов управления.

Проектирование архитектуры предполагает последовательное выполнение нескольких шагов:

- определение уровневой структуры системы L, обеспечивающей устойчивость и разделение функций между компонентами;

- разработка основного и резервного контуров управления C, которые обеспечивают непрерывность мониторинга и реагирования при штатном режиме и в условиях отказов;
- создание механизма адаптивного перераспределения ресурсов M, необходимого для эффективного функционирования системы при изменении нагрузки и состояния сети;
- интеграция всех элементов в единую архитектуру и проверка её соответствия поставленным требованиям.

Формирование уровневой структуры архитектуры является ключевым этапом проектирования, поскольку именно структура уровней определяет, каким образом система будет обеспечивать устойчивость, адаптивность и резервирование управления. Основой проектируемого решения является концепция многоуровневой организации, позволяющая гибко распределять функции между компонентами системы, минимизировать риски возникновения единой точки отказа и обеспечивать непрерывность работы в условиях деградации или частичных отказов инфраструктуры. Процесс проектирования уровней начинается с анализа особенностей информационно-технических воздействий и требований, вытекающих из постановки задачи. В частности, необходимо, чтобы каждый уровень выполнял собственный набор функций, а взаимодействие между уровнями обеспечивало согласованность процессов мониторинга и реагирования. Для достижения этих целей в рамках исследования предложено выделить три функциональных уровня: локальный, сегментный (промежуточный) и глобальный, которые формируют множество $L = \{L_1, L_2, L_3\}$.

Одноуровневые архитектуры, несмотря на простоту реализации, обладают существенными ограничениями. Централизация всех функций на одном уровне неизбежно создаёт единую точку отказа: сбой ключевого узла или канала связи приводит к полной потере работоспособности системы. Кроме того, такие решения не масштабируются при увеличении числа узлов и объёмов данных, что особенно критично для современных эргатических систем.

В противоположность этому, полностью распределённые решения обеспечивают высокий уровень отказоустойчивости за счёт равноправного взаимодействия всех узлов, однако требуют сложных алгоритмов синхронизации и маршрутизации данных. Это делает их уязвимыми к деградации связей и затрудняет централизованную координацию действий в условиях кризисных ситуаций.

Многоуровневый подход занимает промежуточное положение между этими крайностями. Он позволяет сохранить локальную автономность нижних уровней, при этом обеспечивая согласованность работы всей системы за счёт верхнего уровня, ответственного за стратегическое управление. Такая организация делает возможным как горизонтальное взаимодействие между сегментами, так и вертикальное управление потоками данных и ресурсов, что напрямую соответствует требованиям устойчивости, адаптивности и резервирования, определённым в постановке задачи.

В разработанной архитектуре выделяются три уровня, каждый из которых выполняет собственные функции и взаимодействует с другими уровнями по строго определённым правилам: локальный, сегментный и глобальный – см. рис. 1.

Рис. 1. Многоуровневая архитектура системы мониторинга и реагирования на информационно-технические воздействия

Локальный уровень (L_1) расположен на границе взаимодействия с физической или виртуальной средой. Его задача – первичная обработка данных, формируемых источниками информации. На этом уровне выполняются: фильтрация и нормализация поступающих событий; обнаружение простейших аномалий и известных сигнатур угроз; предварительное ранжирование событий по степени критичности; передача агрегированных данных на вышестоящие уровни для последующего анализа; выполнение локальных реакций, не требующих сложной координации (например, временная блокировка узла или ограничение сетевого трафика). Наличие автономных функций на локальном уровне позволяет системе реагировать на инциденты даже при частичной потере связи с верхними уровнями.

Сегментный уровень (L_2) выполняет роль промежуточного слоя, который объединяет несколько локальных узлов в рамках одного технологического сегмента. Основные задачи сегментного уровня включают: корреляцию событий, поступающих с локальных узлов; консолидацию контекстной информации о состоянии сегмента; принятие решений в границах сегмента при недоступности глобального уровня; управление распределением ресурсов между узлами данного сегмента; временное исполнение функций резервного контура управления в случае отказа глобального уровня. Благодаря этому сегментный уровень выступает в роли буфера, обеспечивая баланс между автономностью локальных узлов и стратегическим управлением всей системой.

Глобальный уровень предназначен для координации работы всей системы в целом. Его задачами являются: межсегментная корреляция данных и построение целостной картины состояния системы; формирование и распространение политик реагирования на информационно-технические воздействия; стратегическое распределение ресурсов между сегментами; активация или деактивация основного контура управления и передача функций резервному контуру в случае необходимости; анализ эффективности функционирования нижних уровней и адаптация их параметров. Таким образом, глобальный уровень обеспечивает высокий уровень согласованности действий всех компонентов и является ядром стратегического управления.

Взаимодействие между уровнями носит двунаправленный характер. Восходящие потоки данных ($L_1 \longrightarrow L_2 \longrightarrow L_3$) включают события, метрики и агрегированные результаты анализа, необходимые для формирования глобальной картины состояния системы. Нисходящие потоки управления ($L_3 \longrightarrow L_2 \longrightarrow L_1$) содержат политики реагирования, приоритеты и распределение ресурсов. Особая роль отводится резервному контуру управления: при отказе глобального уровня функции координации временно передаются сегментному уровню. Если же деградация затрагивает часть сегментных узлов, соседние сегменты берут на себя их управление, обеспечивая непрерывность работы всей системы.

Сформированная многоуровневая структура $L = \{L_1, L_2, L_3\}$ обеспечивает: устранение единой точки отказа за счёт распределения функций по уровням; адаптивность через возможность перераспределения ролей и ресурсов в ответ на изменения нагрузки и состояния сети; реализацию резервирования управления за счёт автоматического перераспределения функций между уровнями при отказах отдельных компонентов. Таким образом, предложенная уровневая структура создаёт фундамент для построения основной и резервной логики управления системой.

Проектирование контуров управления

Функционирование многоуровневой архитектуры невозможно без чётко организованных контуров управления, которые обеспечивают согласованность действий всех компонентов системы. В рамках разработанной структуры $L = \{L_1, L_2, L_3\}$ выделяются два взаимосвязанных контура управления – основной (C_{main}) и резервный (C_{res}). Их совместная работа направлена на обеспечение непрерывности процессов мониторинга и реагирования даже при частичных отказах инфраструктуры или деградации каналов связи. Основной контур обеспечивает работу системы в штатных условиях, тогда как резервный вступает в действие только при обнаружении сбоев или потере связи с ключевыми компонентами верхнего уровня. Такое разделение позволит не только снизить нагрузку на систему при нормальной работе, но и гарантировать устойчивость управления в кризисных ситуациях.

Основной контур управления предназначен для организации потоков данных и принятия решений в штатных условиях функционирования системы. Он базируется на принципах иерархической координации: нижние уровни (L_1, L_2) предоставляют агрегированные данные и локальные решения, а глобальный уровень (L_3) осуществляет анализ и формирование стратегических команд.

В рамках C_{main} реализуются следующие процессы:

- сбор и агрегация данных на локальном и сегментном уровнях (локальные узлы (L_1) выполняют первичную обработку и передают результаты на сегментный уровень (L_2), где осуществляется корреляция и выделение критических событий);
- формирование стратегических решений на глобальном уровне (L_3) (данные анализируются в межсегментном контексте, что позволяет выявлять комплексные угрозы и определять приоритеты реагирования;

- нисходящая передача команд (глобальный уровень передаёт сегментам и локальным узлам инструкции, которые реализуют заданные сценарии реагирования и распределения ресурсов);
- обратная связь – на каждом цикле управления данные о выполнении команд возвращаются вверх, что позволяет корректировать стратегию и предотвращать каскадные сбои.

Таким образом, основной контур обеспечивает скоординированное взаимодействие всех уровней в нормальном режиме работы, поддерживая баланс между скоростью реакции и глубиной анализа.

Несмотря на эффективность основного контура, реальная эксплуатация сложных эргатических систем неизбежно связана с рисками отказов или временной недоступности ключевых компонентов. Для минимизации последствий подобных ситуаций необходим резервный контур управления, который обеспечивает непрерывность функционирования системы при нарушениях штатной структуры.

Резервный контур активируется в следующих случаях:

- потеря связи между сегментным (L_2) и глобальным (L_3) уровнями;
- отказ центрального управляющего узла или деградация критических каналов связи;
- резкий рост нагрузки, при котором основной контур не успевает обрабатывать входящие данные.

В режиме работы резервного контура часть функций глобального уровня временно передаётся сегментным узлам (L_2). Эти узлы берут на себя задачи по координации локальных узлов и принятию тактических решений на уровне сегмента. Взаимодействие между сегментами осуществляется по принципу горизонтальной федерации: соседние сегментные узлы могут обмениваться агрегированными данными и координировать свои действия без участия глобального уровня.

Ключевым элементом C_{res} является механизм синхронизации данных. При восстановлении основного контура резервный обеспечивает передачу накопленной информации о принятых решениях и текущем состоянии системы на глобальный уровень, что позволяет быстро вернуть архитектуру в штатный режим без потери данных и конфликтов между уровнями.

Разработанные основной и резервный контуры управления образуют единый комплекс $\{C_{main}, C_{res}\}$, обеспечивающий высокий уровень отказоустойчивости и непрерывности функционирования системы. Их взаимодействие позволяет: поддерживать нормальную работу системы в штатных условиях; сохранять способность к принятию решений при частичных отказах или деградации инфраструктуры; минимизировать последствия отказов за счёт быстрого автоматического переключения на резервный режим; гарантировать согласованность данных и процессов при возврате в стандартное состояние.

Таким образом, спроектированные контуры управления напрямую реализуют требование резервирования, сформулированное на этапе постановки задачи, и создают основу для дальнейшего синтеза механизма адаптивного распределения ресурсов.

Механизм адаптивного распределения ресурсов и интеграция архитектуры

Разработанная многоуровневая архитектура требует наличия управляющего механизма, который обеспечит её гибкость и способность реагировать на изменения внешних и внутренних условий функционирования. В этой роли выступает механизм адаптивного распределения ресурсов M, предназначенный для динамической настройки процессов мониторинга и реагирования в зависимости от текущей ситуации. Его ключевая задача – перераспределять ресурсы между уровнями и сегментами системы на основе анализа состояния сети и потоков данных Ω.

В основе работы M лежит использование параметров, описывающих текущее состояние системы:

- интенсивность событий $\lambda(t)$ – поток данных, поступающих на узлы в момент времени t, что отражает текущую активность сети и уровень информационно-технических воздействий;
- состояние каналов связи $\delta(t)$ – метрики качества каналов: пропускная способность, задержки, уровень ошибок, что позволяет оценивать доступность и надежность коммуникаций;
- загрузка узлов $\rho(t)$ – уровень использования вычислительных мощностей на каждом уровне архитектур;
- критичность потоков z – приоритеты обработки данных, зависящие от типа события и его значимости для защищаемой системы.

Данные параметры формируют динамическую карту состояния, которая служит входными данными для принятия решений о перераспределении ресурсов.

Механизм M работает циклично и включает три последовательных этапа. На первом этапе осуществляется оценка состояния системы. Здесь сегментный уровень (L_2) собирает телеметрию о нагрузке, доступности каналов и узлов. Данные агрегируются и передаются на глобальный уровень (L_3), где формируется целостная картина состояния системы. На втором этапе реализуется определение приоритетов, на основе критичности потоков z определяется порядок обработки событий. Критические инциденты

и процессы, влияющие на устойчивость системы, получают наивысший приоритет. Третий этап включает в себя перераспределение ресурсов, где часть задач узлов L_1 может быть передана на уровень L_2 для разгрузки периферии. Такой подход позволяет системе поддерживать стабильную работу даже при резких изменениях нагрузки или частичных отказах инфраструктуры.

Механизм M не функционирует изолированно, а тесно связан с уровнями архитектуры L и контурами управления C, формируя единую систему. Уровни L обеспечивают физическую и логическую основу системы, контуры C поддерживают непрерывность и резервирование функций, гарантируя, что даже при отказе отдельных компонентов система сохраняет способность к координации, а механизм M выступает связующим звеном, адаптивно настраивая взаимодействие уровней и обеспечивая эффективное использование доступных ресурсов. Интеграция всех элементов в единую структуру позволяет архитектуре удовлетворять требованиям устойчивости, адаптивности и резервирования, определённым в постановке задачи.

В результате интеграции сформирована архитектура $A = \langle L,C,M \rangle$, в которой уровни, контуры управления и механизм адаптивности функционируют как единое целое. Такая организация позволяет системе не только противостоять текущим информационно-техническим воздействиям, но и активно адаптироваться к изменяющимся условиям эксплуатации, обеспечивая высокий уровень надёжности и непрерывности работы.

Заключение

В ходе проведенного исследования предложена многоуровневая архитектура системы мониторинга и реагирования на информационно-технические воздействия в сложных эргатических системах. Разработанная архитектура включает три взаимосвязанных компонента:

- уровневую структуру L, обеспечивающую распределение функций между локальными, сегментными и глобальными узлами;
- два контура управления C_{main} и C_{res} реализующих резервирование и непрерывность процессов мониторинга и реагирования;
- механизм адаптивного распределения ресурсов M, позволяющий динамически настраивать работу системы в условиях изменяющихся нагрузок и частичных отказов.

Впервые предложено объединение этих элементов в единую архитектуру $A = \langle L,C,M \rangle$ которая удовлетворяет требованиям устойчивости, адаптивности, резервирования управления. Проведённая аналитическая проверка и сценарное моделирование показали, что данное решение позволяет исключить наличие единой точки отказа и поддерживать функционирование системы даже при деградации каналов связи, резком росте нагрузки или отказе глобального уровня.

Теоретическая значимость работы заключается в развитии научных представлений о проектировании многоуровневых архитектур для защиты эргатических систем и формализации принципов их построения на основе системного анализа. Практическая значимость определяется возможностью применения полученных результатов при создании или модернизации распределённых автоматизированных комплексов различного назначения – в промышленности, транспорте, энергетике, связи – для повышения их устойчивости и эффективности процессов мониторинга и реагирования.

Таким образом, предложенная архитектура формирует основу для построения новых поколений интеллектуальных систем обеспечения безопасности, способных адаптироваться к изменяющимся условиям эксплуатации и противостоять современным информационно-техническим воздействиям.

Литература

1. Железнов Э. Г., Комиссаров П. В., Цымай Ю. В. Исследование эргатических систем управления // Современные наукоёмкие технологии. – 2021. – № 4. – С. 45–53.
2. Al-Khaysat H., et al. Risk Assessment for Cyber Resilience of Critical Infrastructures // Applied Sciences. – 2024. – Vol. 14, № 24. – Article 11807. – DOI: 10.3390/app142411807.
3. Diana L., Dini P., Paolini D. Overview on Intrusion Detection Systems for Computers Networking Security // Computers. – 2025. – Vol. 14, no. 3. – P. 87. – DOI: 10.3390/computers14030087.
4. Lezzi M., Corallo A., Lazoi M., Nimis A. Measuring Cyber Resilience in Industrial IoT: A Systematic Literature Review // Management Review Quarterly. – 2025. – Vol. 75, № 4. – С. 1213–1235. – DOI: 10.1007/s11301-025-00495-8.
5. Soltani M., Khajavi K., Jafari Siavoshani M., Jahangir A. H. A multi-agent adaptive deep learning framework for online intrusion detection // Cybersecurity. 2023. Vol. 6, Iss. 2. P. 45–59. DOI 10.1186/s42400-023-00199-0.
6. Калашников А. О., Бугайский К. А., Аникина Е. В., Перескоков И. С., Петров Ан. О., Петров Ал. О., Храмченкова Е. С., Молотов А. А. Применение логико-вероятностного метода в информационной безопасности (Часть 2) // Вопросы кибербезопасности. 2023. № 5(57). С. 113–127. DOI 10.21681/2311-3456-2023-5-113-127.
7. Власов Д. С. Мультикритериальная модель систематизации способов обнаружения инсайдера // Вопросы кибербезопасности. 2024. № 2(60). С. 66–73. DOI 10.21681/2311-3456-2024-2-66-73.

8. Lagraa S., Husak M., Seba H., Vuppala S., State R., & Ouedraogo M. A review on graph-based approaches for network security monitoring and botnet detection // International Journal of Information Security. 2024. Vol. 23. P. 119–140. DOI 10.1007/s10207-023-00742-7.
9. Hu Q., Yu S. -Y., Asghar M. R. Analysing performance issues of open-source intrusion detection systems in high-speed networks // Journal of Information Security and Applications. 2020. Vol. 51. Article 102426. DOI 10.1016/j.jisa.2019.102426.
10. Furrer F. J. Safe and secure system architectures for cyber-physical systems // Informatik Spektrum. – 2023. – Vol. 46. – № 2. – С. 96-103. – DOI: 10.1007/s00287-023-01533-z.
11. Sharma S., Sahay S. K. Evolution and impact of distributed intrusion detection systems in network security and management // Computer Networks. 2022. Vol. 206. Article 108784. DOI 10.1016/j.comnet.2021.108784.
12. Sharma A., Rani S., Boulila W. Blockchain-based zero trust networks with federated transfer learning for IoT security in industry 5.0 // PLOS ONE. 2025. Vol. 20, Iss. 6. Article e0323241. DOI 10.1371/journal.pone.0323241.
13. Lim W.Y.B., Xiong Z., Niyato D., et al. Federated Learning in Mobile Edge Networks: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. 2020. Vol. 22. Iss. 3. PP. 2031–2063. DOI: 10.1109/COMST.2020.2986024.
14. Xu R., Hang L., Jin W., Kim D. Distributed Secure Edge Computing Architecture Based on Blockchain for Real-Time Data Integrity in IoT Environments // Actuators. 2021. Vol. 10, Iss. 8. Article 197. DOI 10.3390/act10080197.
15. Ji R., Padha D., Singh Y. Survey and analysis of intrusion detection frameworks for cyber-physical systems: A comprehensive study // Recent Innovations in Computing. Lecture Notes in Electrical Engineering, vol. 1194. 2024. P. 307–317. DOI 10.1007/978-981-97-2839-8_21.
16. Singh S., Ahmed J., Raghuvanshi K. K., Agarwal P. Adaptive Resource Management Framework for Secure and Resilient IoT Communication Using Federated Learning and Quantum Encryption // Journal of Information Systems Engineering and Management. 2025. Vol. 10, No. 21s. DOI 10.52783/jisem.v10i21s.3405.
17. Rostami M., Goli-Bidgoli S. An overview of QoS-aware load balancing techniques in SDN-based IoT networks // Journal of Cloud Computing. 2024. Vol. 13. Article 89. DOI 10.1186/s13677-024-00651-7.
18. Belenguer A., Navaridas J., Pascual J. A. A review of federated learning in intrusion detection systems for IoT // arXiv. 2022. DOI 10.48550/arXiv.2024.12443.
19. Язов Ю. К., Авсентьев А. О. Пути построения многоагентной системы защиты информации от утечки по техническим каналам // Вопросы кибербезопасности. 2022. № 5(51). С. 2–13. DOI 10.21681/2311-3456-2022-5-2-13.
20. Zareian Jahromi M., Yaghoubi E., Yaghoubi E., Yusupov Z., Maghami M. R. An Innovative Real-Time Recursive Framework for Techno-Economical Self-Healing in Large Power Microgrids Against Cyber-Physical Attacks Using Large Change Sensitivity Analysis // Energies. 2025. Vol. 18, Iss. 1. Article 190. DOI 10.3390/en18010190.

MULTI-LEVEL ARCHITECTURE OF A MONITORING AND RESPONSE SYSTEM TO IMPACTS WITH BACKUP CONTROL AND ADAPTIVE RESOURCE ALLOCATION IN ERGATIC SYSTEMS

Meshcheryakov R. V.[4], Seliverstov D. E.[5], Rusakov K. D.[6]

Keywords: *fault tolerance, cyber resilience, federated interaction, backup control loop, adaptive resource allocation, ergatic systems, automated complexes, cybersecurity.*

Purpose of the article: *the design of a multi-level monitoring and response system for impacts, ensuring the resilience of complex ergatic systems through the use of a backup control loop and adaptive resource allocation.*

Research methods: *system analysis, modeling, architecture synthesis, resource allocation.*

Research results: *a multi-level architecture of a monitoring and response system for impacts has been developed, aimed at improving the resilience of complex ergatic systems. A structural solution is proposed, including primary and backup control loops, which ensures continuous monitoring and coordinated response even in cases of partial degradation or failure of the communication infrastructure. A mechanism for adaptive resource reallocation between architecture components has been designed, ensuring efficient system operation under variable loads and limited computing and network capabilities. The theoretical significance of the work lies in advancing scientific knowledge on the design of multi-level architectures for the protection of ergatic systems, ensuring their functionality under complex impacts. The practical significance is determined by the possibility of applying the designed architectural solutions in the creation and modernization of distributed automated complexes of various purposes to increase their resilience and the efficiency of monitoring processes.*

4 Roman V. Meshcheryakov, D.Sc., Professor of the Russian Academy of Sciences, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. ORCID: 0000-0002-1129-8434. E-mail: mrv@ipu.ru
5 Dmitry E. Seliverstov, Ph.D., V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. ru ORCID: 0009-0004-8412-7873. E-mail: Seliverstov_dmitriyy@rambler
6 Konstantin D. Rusakov, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. ORCID: 0009-0004-8412-7873. E-mail: rusakov@ipu.ru

Scientific novelty: *for the first time, a multi-level architecture of a monitoring and response system for impacts is proposed, implementing a separation into primary and backup control loops to ensure operational resilience under communication degradation and failures. For the first time, a mechanism for adaptive resource reallocation between system levels has been developed, allowing the maintenance of monitoring and response efficiency under variable loads and limited computing and network capabilities.*

References

1. Zheleznov, E. G., Komissarov, P. V., & Tsymai, Y. V. (2021). Issledovanie ergaticheskikh sistem upravleniya [Research of ergatic control systems]. Sovremennye Naukoemkie Tekhnologii [Modern High Technologies], (4), 45–53.
2. Al-Khaysat, H., et al. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures. Applied Sciences, 14(24), Article 11807. https://doi.org/10.3390/app142411807.
3. Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. Computers, 14(3), Article 87. https://doi.org/10.3390/computers14030087.
4. Lezzi, M., Corallo, A., Lazoi, M., & Nimis, A. (2025). Measuring Cyber Resilience in Industrial IoT: A Systematic Literature Review. Management Review Quarterly, 75(4), 1213–1235. https://doi.org/10.1007/s11301-025-00495-8.
5. Soltani, M., Khajavi, K., Jafari Siavoshani, M., & Jahangir, A. H. (2023). A multi-agent adaptive deep learning framework for online intrusion detection. Cybersecurity, 6(2), 45–59. https://doi.org/10.1186/s42400-023-00199-0.
6. Kalashnikov, A. O., Bugayskiy, K. A., Anikina, E. V., Pereskokov, I. S., Petrov, An. O., Petrov, Al. O., Khramchenkova, E. S., & Molotov, A. A. (2023). Primenenie logiko-veroyatnostnogo metoda v informatsionnoy bezopasnosti (Chast' 2) [Application of the logic-probabilistic method in information security (Part 2)]. Voprosy Kiberbezopasnosti [Cybersecurity Issues], 5(57), 113–127. https://doi.org/10.21681/2311-3456-2023-5-113-127.
7. Vlasov, D. S. (2024). Mul'tikriterial'naya model' sistematizatsii sposobov obnaruzheniya insaydera [multi-criteria model of systematization of insider detection methods]. Voprosy Kiberbezopasnosti [Cybersecurity Issues], 2(60), 66–73. https://doi.org/10.21681/2311-3456-2024-2-66-73.
8. Lagraa, S., Husak, M., Seba, H., Vuppala, S., State, R., & Ouedraogo, M. (2024). A review on graph-based approaches for network security monitoring and botnet detection. International Journal of Information Security, 23, 119–140. https://doi.org/10.1007/s10207-023-00742-7.
9. Hu, Q., Yu, S.-Y., & Asghar, M. R. (2020). Analysing performance issues of open-source intrusion detection systems in high-speed networks. Journal of Information Security and Applications, 51, 102426. https://doi.org/10.1016/j.jisa.2019.102426.
10. Zhu, Q., Rieger, C., & Basar, T. (2011). A hierarchical security architecture for cyber-physical systems. In Proceedings of the 4th International Symposium on Resilient Control Systems (ISRCS 2011) (pp. 15–20). https://doi.org/10.1109/ISRCS.2011.6016081.
11. Sharma, S., & Sahay, S. K. (2022). Evolution and impact of distributed intrusion detection systems in network security and management. Computer Networks, 206, 108784. https://doi.org/10.1016/j.comnet.2021.108784.
12. Sharma, A., Rani, S., & Boulila, W. (2025). Blockchain-based zero trust networks with federated transfer learning for IoT security in industry 5.0. PLOS ONE, 20(6), e0323241. https://doi.org/10.1371/journal.pone.0323241.
13. Lim, W. Y. B., Xiong, Z., Niyato, D., Miao, C., Yang, Q., & Poor, H. V. (2020). Federated learning in mobile edge networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 2031–2063. https://doi.org/10.1109/COMST.2020.2986024.
14. Xu, R., Hang, L., Jin, W., & Kim, D. (2021). Distributed secure edge computing architecture based on blockchain for real-time data integrity in IoT environments. Actuators, 10(8), Article 197. https://doi.org/10.3390/act10080197.
15. Ji, R., Padha, D., & Singh, Y. (2024). Survey and analysis of intrusion detection frameworks for cyber-physical systems: A comprehensive study. In Recent Innovations in Computing (Vol. 1194, pp. 307–317). Springer. https://doi.org/10.1007/978-981-97-2839-8_21.
16. Singh, S., Ahmed, J., Raghuvanshi, K. K., & Agarwal, P. (2025). Adaptive resource management framework for secure and resilient IoT communication using federated learning and quantum encryption. Journal of Information Systems Engineering and Management, 10(21s). https://doi.org/10.52783/jisem.v10i21s.3405.
17. Rostami, M., & Goli-Bidgoli, S. (2024). An overview of QoS-aware load balancing techniques in SDN-based IoT networks. Journal of Cloud Computing, 13, Article 89. https://doi.org/10.1186/s13677-024-00651-7.
18. Belenguer, A., Navaridas, J., & Pascual, J. A. (2022). A review of federated learning in intrusion detection systems for IoT. arXiv. https://doi.org/10.48550/arXiv.2024.12443.
19. Yazov, Y. K., & Avsentyev, A. O. (2022). Puti postroeniya mnogoagentnoi sistemy zashchity informatsii ot utechki po tekhnicheskim kanalam [Ways to build a multi-agent information security system against leakage through technical channels]. Voprosy Kiberbezopasnosti [Cybersecurity Issues], (5)(51), 2–13. https://doi.org/10.21681/2311-3456-2022-5-2-13.
20. Lin D., He Y., Zhang Q. Real-time optimization of network response under cyber-physical attacks // IEEE Transactions on Industrial Informatics. 2025. Vol. 21. Iss. 2. PP. 1501–1513. DOI: 10.1109/TII.2024.3391750.