ISSN 3033-6554 (online)
https://epinb.ru

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Научная статья
УДК 338.22.021.2

Статья поступила в редакцию 06.01.2026;
одобрена после рецензирования 09.02.2026;
принята к публикации 20.02.2026.

Особенности использования сетецентрического управления ресурсами в производственном секторе уголовно-исполнительной системы

Алексей Владимирович Родионов, Александр Эдуардович Китайкин

Академия права и управления Федеральной службы исполнения наказаний,
Рязань, Россия

Аннотация:
Введение. В условиях глобальной индустрии технических преобразований и нарастания системных дисбалансов производственный комплекс уголовно-исполнительной системы сталкивается с необходимостью кардинальной технологической реконструкции. Классические иерархические управленческие структуры демонстрируют свою неэффективность, проявляющуюся в неспособности адекватно реагировать на актуальные проблемы современности. Данный комплекс взаимосвязанных проблем формирует потребность в принципиально новой архитектуре управления, ориентированной на достижение адаптивности, устойчивости и высокой степени интеллектуальной зрелости в жестко регламентированной среде. ***Цель.*** Исследование нацелено на выявление и анализ нарастающих рисков, осмысление глубинных противоречий, сдерживающих развитие производственного сектора уголовно-исполнительной системы и обоснование сетецентрической парадигмы как механизма структурной и функциональной трансформации. Оно иллюстрирует потенциал данной модели управления, ее способности к решению задач в контексте противодействия совокупности системных угроз. ***Методы.*** Основой исследования является комплексный анализ актуальных вызовов современности, стоящих перед производственным сектором уголовно-исполнительной системы. Методология включает обзор и последующий синтез научных разработок по проблемам кибербезопасности, кадрового дефицита, экологии, логистики, интеграции искусственного интеллекта (далее – ИИ). В исследовании используется метод логического моделирования. ***Результаты*** работы дают теоретическое обоснование способности сетецентрической модели стать основным драйвером структурных изменений. Ее эффективность обеспечивается за счет формирования единого информационно-коммуникационного контура, организующего горизонтальное взаимодействие. В рамках исследования продемонстрированы ключевые эффекты от внедрения модели. Принцип распределенной системы реализует скоординированное реагирование на киберугрозы, основанное на коллективном анализе и локализации происшествий. Кадровый дефицит смягчается за счет создания постоянно обновляемой базы знаний, где опыт каждого сотрудника становится общим достоянием всех участников сети. Формирование целостного информационного поля позволяет прогнозировать и минимизировать воздействие экологических и логистических рисков. Сложности внедрения ИИ преодолеваются через создание защищенной среды с локальной обработкой конфиденциальных данных и поступлением в контур лишь обезличенных аналитических выводов. Конечным итогом реализации парадигмы служит формирование качественно новой операционной среды.

Ключевые слова:
сетецентрическое управление ресурсами, уголовно-исполнительная система (УИС), производственный сектор УИС, кибербезопасность, дефицит кадров, экологические риски, разрыв цепочек поставок, искусственный интеллект (ИИ), системная трансформация

Для цитирования:
Родионов А. В., Китайкин А. Э. Особенности использования сетецентрического управления ресурсами в производственном секторе уголовно-исполнительной системы // *Экономическая политика и национальная безопасность*. 2026. № 1 (3). С. 94–103.

Информация об авторах:
Родионов А. В. – доктор экономических наук, доцент
Академия ФСИН России, Рязань, Россия
(Российская Федерация, 390000, г. Рязань, ул. Сенная, д. 1)
профессор кафедры экономики, менеджмента, организации производственной деятельности и трудовой адаптации осужденных
avrpost@bk.ru, https://orcid.org/0000-0002-9311-4896
Китайкин А. Э.
Академия ФСИН России, Рязань, Россия
(Российская Федерация, 390000, г. Рязань, ул. Сенная, д. 1)
адъюнкт факультета подготовки научно-педагогических кадров
kitaikin.aleksandr@yandex.ru

ISSN 3033-6554 (online)
https://epinb.ru

Original article

The article was submitted January 6, 2026;
approved after reviewing February 9, 2026;
accepted for publication February 20, 2026.

Features of using network-centric resource management in the manufacturing sector of the penal system

Alexey V. Rodionov, Alexandr E. Kitaykin

The Academy of the FPS of Russia, Ryazan, Russia

Abstract:
Introduction. In the context of global technological transformation and growing systemic imbalances, the manufacturing complex of the penal system is facing the need for radical technological reconstruction. Traditional hierarchical management structures are proven to be ineffective, as they are unable to respond adequately to the pressing issues of the present day. The combination of interrelated issues highlights the need for a fundamentally new management architecture focused on achieving adaptability, sustainability, and a high degree of intellectual maturity in a highly regulated environment. ***Purpose.*** The research aims at identifying and analysing growing risks, understanding the underlying contradictions that impede the development of the manufacturing sector in the penal system, and justifying the network-centric paradigm as a mechanism for structural and functional transformation. The study illustrates the potential of such a management model and its ability to address challenges in the context of countering systemic threats. ***Methods.*** The research is based on a comprehensive analysis of the current challenges facing the manufacturing sector of the penal system. The methodology involves reviewing and synthesising scientific research on cybersecurity, staff shortages, environmental issues, logistics and the integration of artificial intelligence (hereinafter – AI). The study uses the method of logical modelling. ***The results*** of the research provide a theoretical substantiation of the potential of the network-centric model to become the main driver of structural changes. Its effectiveness is ensured by the formation of a unified information and communication framework organising horizontal interaction. The study demonstrates the key effects of implementing the model. The distributed system principle implements a coordinated response to cyber threats based on collective analysis and incident localisation. The staff shortage is mitigated by creating a constantly updated knowledge base, where the experience of each employee becomes the common property of all network participants. The formation of a comprehensive information field makes it possible to predict and minimise the impact of environmental and logistical risks. The difficulties of implementing AI are overcome by creating a secure environment with local processing of confidential data and only anonymised analytical conclusions entering the system. The ultimate result of implementing this paradigm is the formation of a qualitatively new operating environment.

Keywords:
network-centric resource management,
penal system,
penal system manufacturing sector,
cybersecurity,
staff shortage,
environmental risks,
supply chain disruption,
artificial intelligence (AI),
systemic transformation

For citation:
Rodionov, Alexey V., and Alexandr E. Kitaykin. 2026. “Industrial'noe derevyannoe domostroenie kak drajver importozameshcheniya sprosa v lesopromyshlennom komplekse RF” [“Features of using network-centric resource management in the manufacturing sector of the penal system”] (In Russ.). *Ekonomicheskaya politika i natsional'naya bezopasnost' [Economic policy and national security]* 3, no. 1 (February):94–103.

Information about the authors:
Rodionov A. V. – Doc. Sci. (Econom.), Docent
The Academy of the FPS of Russia
(1, Sennaya str., Ryazan, 390000, Russian Federation)
Professor of the Department of Economics, Management, Organization of Production Activity and Labor Adaptation of Convicts
avrpost@bk.ru, https://orcid.org/0000-0002-9311-4896
Kitaykin A. E.
The Academy of the FPS of Russia
(1, Sennaya str., Ryazan, 390000, Russian Federation)
Postgraduate of the Faculty of Research and Teaching Staff Training
kitaikin.aleksandr@yandex.ru

ВВЕДЕНИЕ

В условиях стремительной цифровой трансформации и усложнения технологической среды производственный комплекс уголовно-исполнительной системы (далее – УИС) России испытывает воздействие множества структурных проблем. Их разрешение предполагает необходимость разработки и реализации инновационных управленческих решений. Традиционные иерархические модели управления, основанные на принципах

высокой централизации и ограниченной пропускной способности информации, демонстрируют свою слабость перед лицом современных угроз (Бродецкий и др. 2023). Интенсификация кибератак, приобретающих все более изощренные формы, создает непосредственную опасность нарушения цикла производственно-хозяйственной деятельности.

Параллельно наблюдается усугубление структурного дисбаланса на рынке труда в сфере обеспечения квалифицированных кадров (Зоидов и др. 2024). Данная тенденция провоцирует процессы деградации корпоративного знания и системные сбои в операционной деятельности. Актуален также комплекс экологических рисков, связанных с необходимостью соблюдения ужесточающегося нормативно-правового законодательства и минимизации антропогенной нагрузки в рамках производственной деятельности (Апевалова и Кутыева 2015).

Системная уязвимость дополнительно усугубляется глобальной тенденцией к дестабилизации логистических цепочек, создающей угрозу устойчивости ресурсного, компонентного и технологического обеспечения (Букринская и Липатова 2023). Кроме того, внедрение технологий искусственного интеллекта (далее – ИИ) порождает новые противоречия, затрагивающие сферы управленческого контроля, этико-правового регулирования и адаптации в жестко регламентированной среде (Дешура и Павлов 2024). Указанные многоуровневые вызовы носят взаимосвязанный характер, общей основой которых является несоответствие архаичных организационных структур требованиям динамичной и нестабильной внешней среды. В связи с этим возникает настоятельная потребность в конструировании новой управленческой парадигмы, способной обеспечить устойчивость, адаптивность и интеллектуальное развитие производственного комплекса в условиях нестабильности и структурных сдвигов.

Одним из перспективных направлений преодоления перечисленных вызовов может стать концепция сетецентрической архитектуры управления ресурсами. Настоящее исследование посвящено анализу ключевых системных противоречий производственного комплекса УИС и теоретико-методологическому обоснованию применения сетецентрической модели как инструмента для его структурной и функциональной трансформации. В рамках исследования анализируется влияние, оказываемое внедрением горизонтальных сетевых структур, объединенных в единый информационно-коммуникационный контур, на разрешение комплекса системных угроз.

МАТЕРИАЛЫ И МЕТОДЫ

Рассматриваемая парадигма способствует созданию адаптивных механизмов киберзащиты, способных к эволюции в ответ на изменяющиеся угрозы. Одновременно она создает институциональные условия для трансформации неформального индивидуального профессионального опыта в кодифицированный организационный капитал, что обеспечивает устойчивое накопление и передачу критически важных компетенций. Кроме того, данная архитектура предоставляет методологическую и инструментальную основу для упреждающего воздействия на внешние раздражители, в частности, для минимизации потенциальных экологических и логистических угроз. Вместе с тем такая архитектура формирует контролируемую среду, необходимую для исследования и внедрения масштабируемых алгоритмов искусственного интеллекта (далее – ИИ) (с соблюдением безопасности и управляемости).

Анализ научных публикаций помог выявить несколько ключевых вызовов современности. К таким вызовам относятся киберугрозы (Пищик и Алексеев 2024), дефицит кадров (Морозова и Семенихина 2020), экологические риски (Лазарева 2012), разрыв цепочек поставок (Шемякина 2023) и интеграция ИИ (Заготовкин и Рыльский 2025).

Кибербезопасность направлена на выявление и отражение угроз объектов, которые связаны с IT-технологиями, компьютерными и телекоммуникационными сетями, а также хранением, переработкой и передачей информации (Решетникова и др. 2022). Это направление является предметом пристального изучения специалистов, занимающихся исследованием и анализом современных угроз и выявлением методов противодействия им. Следующий вызов – дефицит кадров, напрямую связанный с системным кадровым кризисом в России (Климова и Писаренко 2024). Фундаментальной причиной обострения проблемы выступает институциональный

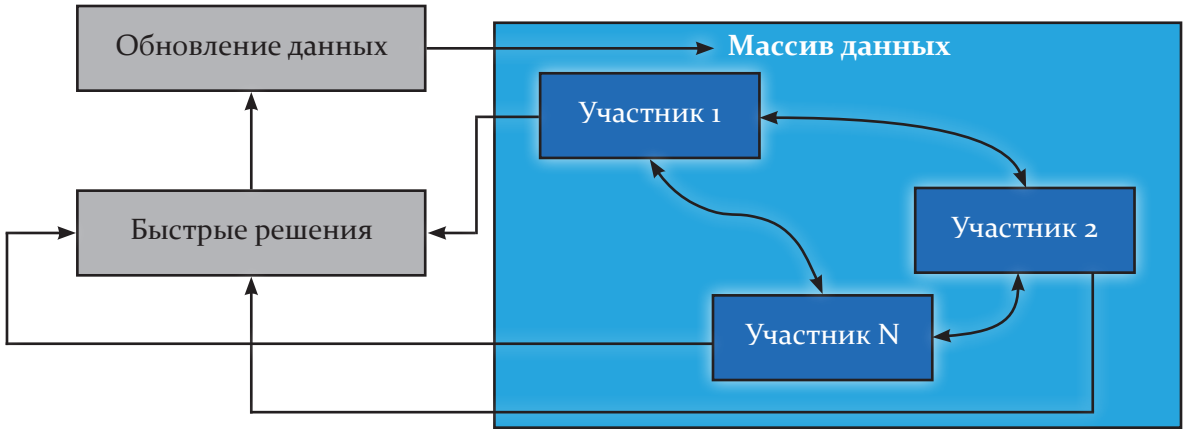
ISSN 3033-6554 (online)
https://epinb.ru

разрыв между динамично меняющимся спросом со стороны экономических агентов и инерционным предложением со стороны национальной системы образования. Кризис кадров в данном направлении лимитирует возможности для адекватного ответа на другие комплексные вызовы (Климова и Писаренко 2024). Еще одним системным вызовом являются экологические риски (Маккаева и др. 2022).

Повышение значимости данной проблемы в публичном пространстве приводит к увеличению спроса на научные труды аналитиков, направленных на осмысление и поиск решений экологических проблем. Следующая группа рисков связана с разрушением логистических связей. Нарушение целостности и функционирования глобальных логистических сетей, ставшее особенно заметным в последние годы, создает существенные риски для экономической безопасности. Их последствия выражаются в увеличении стоимости производства, товарном дефиците и росте инфляционных процессов. Эксперты в своих трудах уделяют особое внимание оценке логистических рисков, уязвимостям цепочек поставок и поиску методов оперативного восстановления их функциональности. Наряду с цифровыми угрозами, дефицитом кадров, экологическим кризисом и разрушением логистических связей серьезной проблемой становится интеграция ИИ (Полухтин 2023).

Исследователи отмечают его ограниченную применимость в текущих реалиях, недостаток специалистов требуемой квалификации, этические и правовые риски, баланс между автоматизацией и человеческим контролем (Пузанова и Ларина 2025). Все данные вызовы объединяет одна глубинная проблема – дисфункциональность и архаичность традиционных иерархических структур в контексте цифровой реальности, что остро проявляется в закрытых и регламентируемых системах, к которым относится УИС, где производственный сектор зачастую существует в условиях информационной изоляции и жесткой вертикали управления.

Таким образом, локальная реконструкция в рамках прежней парадигмы неспособна решить совокупность связанных между собой проблем. К организации и координации ресурсов необходим иной подход, который обеспечит достижение высокой скорости реагирования на угрозы, сохранение компетенций и построение управляемой среды. Как показал анализ, таким критериям преимущественно соответствует сетецентрическая архитектура управления, основанная на создании единого информационно-коммуникационного контура, который в режиме реального времени объединяет всех участников процесса (схематически представлено на рисунке).



Источник: *составлено авторами.*

Рисунок. Принципиальная схема сетецентрической системы управления ресурсами
Figure. Schematic diagram of a network-centric resource management system

На схеме отражены ключевые элементы модели: узлы сети (участники), связанные горизонтальными каналами связи, и общий массив актуальных данных, который может быть

реализован как технологически распределенное, но логически единое хранилище, что исключает наличие уязвимого центрального сервера. Модуль «Обновление данных» обеспечивает постоянную синхронизацию информации со всех точек сети, тем самым поддерживая ее целостность и актуальность. На основании анализа информации и выявления закономерностей, раздражителей, отклонений или оптимизации возможностей процесс «Быстрые решения» вырабатывает необходимые команды. Эти команды направляются обратно в узлы для исполнения. Так обеспечивается непрерывный процесс адаптивного управления. Схема наглядно показывает, как преодолевается главный недостаток традиционных иерархических структур – задержка и искажение информации. Все участники связаны между собой двусторонними каналами для коммуникации, образующими сеть горизонтального взаимодействия. При этом каждый из них синхронизирован с общим массивом данных. В производственном секторе УИС такими участниками (узлами) могут выступать производственные участки, цеха, отделы и службы. Подобная архитектура создает качественно новые возможности для управления сложными системами, включая преодоление актуальных вызовов, таких как киберугрозы, дефицит кадров и интеграция ИИ.

Для иллюстрации рассмотрим механизм решения первой из этих проблем. В рамках парадигмы сетецентрического управления сетевой узел играет двоякую функциональную роль. С одной стороны, каждый узел выступает потенциальной точкой уязвимости, а с другой – активным сенсором, генерирующим данные об угрозе. Сбор сведений от распределенных источников событий приводит к формированию единой аналитической картины. Координирующий контур системы на основании этих данных создает основу для ситуационной оценки, включающей степень ее критичности и типологии.

Такой механизм обеспечивает эволюцию от разрозненного локального реагирования к реализации скоординированных защитных действий, опирающихся на исчерпывающую ситуационную осведомленность. Результатом аналитической обработки является комплекс ответных мер, генерированный системой и нацеленный на парирование выявленной угрозы. В сетецентрической модели вырабатываемый ответ лишен универсальности. Вместо этого стратегия противодействия для каждого узла обусловливается спецификой его текущего статуса и ролью в общей сетевой архитектуре. В соответствии с диагностированным состоянием узла выбираются специфические ответные меры. Исправным элементам направляются обновления для готовности противостоять данной угрозе. Атакованные узлы подвергаются локальной изоляции. Поврежденные элементы подлежат восстановлению. Механизм передачи корректировок и оповещений является общим и функционирует в рамках единых каналов связи.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Ключевым преимуществом сетецентрического подхода в данном контексте выступает свойство системы осуществлять локализацию зараженных или скомпрометированных участков, сохраняя при этом общую операционную целостность и непрерывность работы системы. Ликвидация угрозы служит триггером для начала автоматизированного восстановительного процесса. В рамках сетецентрического управления это не только перезапустит систему с базовыми настройками, но и актуализирует политику безопасности на основе полученного опыта.

Описанный механизм адаптивного кибериммунитета раскрывает потенциал сетецентрической модели лишь для отдельной, хотя и критически важной области. Не менее актуально использование данного подхода для устранения глубинных системных дисбалансов, среди которых ключевым является кадровый дефицит. В контексте УИС эта проблема приобретает особую остроту ввиду дополнительных ограничений. Эти ограничения носят комплексный характер и включают три ключевых аспекта. Первичным негативным последствием является потеря уникальных знаний и опыта, что наносит ущерб интеллектуальному капиталу учреждения.

Для учреждений УИС, сталкивающихся с ограниченным кадровым резервом в силу своей специфики, уход опытного сотрудника представляет собой институциональный риск, ведущий к эрозии ключевых компетенций и утрате знаний, копившихся в течение

ISSN 3033-6554 (online)
https://epinb.ru

длительного времени. В иерархической системе эти знания, как правило, не документируются и не систематизируются. Следующей проблемой является отсутствие эффективной ротации и дублирования критически важных ролей. В практике УИС нередки случаи, когда критически важные функции сосредоточены в компетенции единственного сотрудника, что создает высокие операционные риски. Временное отсутствие такого сотрудника может привести к остановке процессов на вверенном ему участке. Третьим фактором выступает низкая скорость воспроизводства кадров. Замещение должностей связано с чрезмерно протяженными временными издержками, препятствующими быстрому восстановлению функциональности.

Применение сетецентрической модели принципиально меняет ситуацию. Знания уходящего специалиста не являются его персональным активом, т. к. они постоянно аккумулируются, структурируются и сохраняются в общей информационной среде. Это включает как формальные процедуры, так и критически важный контекст принятия решений (истории принятых решений с контекстом ошибок, оптимальные методики). В результате любой работник получает опосредованный доступ к коллективному интеллекту предприятия через централизованные базы знаний, документированный опыт направлений деятельности и интеллектуальных помощников, которые обучены на опыте учреждения и эмулируют экспертные функции.

Производственная деятельность УИС сопряжена со специфическими экологическими рисками, такими как утилизация отходов производства, неправильное обращение с отходами, загрязнение водных объектов, контроль за газообразными выбросами котельных, работающих на твердом топливе, и соблюдение природоохранного законодательства. Межгосударственный и мультидисциплинарный характер данной группы рисков требует трансформации разрозненного экологического мониторинга в единую систему профилактического управления. Механизм схож с описанным принципом сохранения и распределения знаний. Экологически релевантные данные, собираемые от разных источников в разных странах, перестают быть автономными активами. В единой информационной среде они структурируются в единый информационный поток, который становится объектом анализа. После экспертной оценки поток переходит в общее ситуативное экологическое знание. Он внедряется в информационную систему, обеспечивая равный доступ всем ключевым участникам сетевого взаимодействия, и уже в сетевом пространстве формирует основу для скоординированных результативных действий.

Подобный сетевой метод управления позволяет эффективно нейтрализовать основные источники экологических угроз. Первый характеризуется тем, что одни участники располагают данными об экологическом состоянии среды и факторов, воздействующих на нее, в то время как другие лишены доступа к ним, что ведет к несостоятельным решениям и, как следствие, к неблагоприятным последствиям. Вторая отличается отсутствием согласованного плана, что ведет к противоречиям или повторению действий, которые в свою очередь приводит к эскалации угроз. Благодаря системе постоянного сбора, непрерывной фиксации и дублирования информации в единой среде потеря критически важных данных сводится к минимуму. В основе этого лежит возможность перераспределять нагрузку между элементами сети. Низкая скорость реакции иерархических систем нивелируется за счет способности к самосинхронизации действий участников сети. Общие понимание ситуации помогает быстро перестраивать процессы, ограничивать потребление ресурсов на отдельных узлах и внедрять цикличные модели, тем самым увеличивая общую устойчивость всей системы.

Опыт применения сетевого подхода для зашиты предприятия от несанкционированного доступа к его ресурсам, базам знаний и управления экологическими рисками на основе единого информационно-коммуникационного контура также может показать свою эффективность в устранении разрывов логистических цепочек. Логистика в производственных подразделениях УИС выступает стратегической задачей ввиду нескольких ограничений. Таковыми являются географическая привязка к исправительным учреждениям (далее – ИУ) с жестко регламентированным пропускным режимом. Сбой в поставках влечет не только остановку производства и срыв сроков исполнения контрактов, но и ставит под угрозу соблюдение внутреннего распорядка ИУ.

Мощный удар по экономике наносят как геополитические конфликты, так и пандемии. Стоящие за ними централизованные модели преследуют жесткую архитектуру, которая превращает локальную проблему в катастрофу для всей цепи. Сетецентрический подход преобразовывает линейную структуру в динамичную саморегулирующую среду, где каждый элемент встроен в общее цифровое пространство для непрерывного обмена информацией. Суть происходящих изменений состоит в том, что если раньше важная информация оставалась в пределах одного отдела или учреждения, то теперь они переходят из личного ведения в общий доступ. Эти сведения собираются непрерывно и с минимальной задержкой открываются для обозрения для каждого вовлеченного участника.

В результате возникает единое и полное видение происходящего в логистической системе. Такой механизм служит надежной защитой, предотвращая ситуации, в которых локальное неведение вызывает общую дисфункцию. Дефицит информации постоянно ведет к ошибочным действиям, что лишь усугубляет ситуацию. Ярким примером является цепная реакция, при которой опасения потенциального дефицита побуждают участников рынка резко увеличивать запасы, тем самым и создавая реальный дефицит. Более того, сетецентрическая модель в управлении поставками выводит последние на новый уровень. Осуществляются не только наблюдение и фиксация, но и прогнозирование будущих разрывов в цепях. Объединение в одном пространстве многогранных потоков, данных формирует необходимую аналитическую базу, на основании которой система начинает распознавать потенциальные точки разрыва, моделировать кризисные сценарии до их наступления и предлагать упреждающие решения. В итоге вся логистическая структура обретает стабильность, то есть может не только выдерживать удары извне, но и гибко перестраиваться, быстро возвращаясь в состояние равновесия.

ЗАКЛЮЧЕНИЕ

Реализация описанных принципов формирует необходимые предпосылки для раскрытия фундаментальных преимуществ сетецентрической архитектуры, что непосредственно влияет на преодоление системных вызовов, стоящих перед организацией. Эта архитектура кардинально преобразует систему, создавая устойчивую экосистему равноценных точек взаимодействия вместо вертикальной системы подчинения.

Повышенная устойчивость и безопасность достигаются за счет ликвидации единого центра управления и хранения данных, благодаря чему система сохраняет функциональность даже в условиях целенаправленных атак или технических инцидентов на локальном уровне. Способность к локализации инцидентов и автономному функционированию сегментов сети обеспечивает общую операционную целостность системы, что является фундаментальным отличием от уязвимых централизованных моделей. Одновременно децентрализованная обработка информации на производственных участках трансформирует модель управления, повышая скорость и качество принимаемых решений.

Делегирование полномочий и устранение вертикальных задержек смещает фокус управления с простого реагирования на инциденты к их упреждающему планированию. Ключевым проявлением гибкости и масштабируемости является облегченный процесс интеграции. Новые производственные активы добавляются в систему как независимые узлы, интегрируемые в общую среду обмена данными, что исключает необходимость дорогостоящей реконфигурации централизованной инфраструктуры. Данный подход обеспечивает естественное поэтапное наращивание мощности системы. Параллельно достигается усиление конфиденциальности и суверенитета данных. Важная информация обрабатывается локально в узлах, в то время как в общий сетевой контур передаются результаты аналитической обработки. Это значительно снижает риски утечки данных. Серьезным аргументом является то, что данная архитектура устанавливает этически приемлемые рамки для применения ИИ. При этом работа с конфиденциальными данными ведется на местах обособленно. В общую сеть поступают лишь итоговые анонимные показатели, что снижает количество юридических и этических споров, касающихся приватности и защиты информации.

Несмотря на значительный потенциал сетецентрической модели, ее реализация в УИС сталкивается с системными ограничениями, которые необходимо учитывать на этапе проектирования. Жесткие нормативные рамки порождают препятствия попыткам осуществить

ISSN 3033-6554 (online)
https://epinb.ru

переход к горизонтальным моделям кооперации. Ситуацию осложняет отсутствие у кадрового состава необходимой цифровой грамотности. Серьезным сдерживающим фактором служит и вопрос значительного финансирования на начальном этапе. Оно требуется для построения надежной защиты от угроз и цифровой инфраструктуры, которые подразумевают затраты на приобретение аппаратной части. Отдельную проблему создает потребность в стабильной коммуникации и согласованности информации между ИУ.

Решение этой задачи превращается в сложный инженерно-технический проект. К сложностям также приводит объективная потребность в обновлении законодательства. Нормативная база деятельности УИС в настоящее время не учитывает специфику сетевого управления. Таким образом, внедрение сетецентрической парадигмы в производственные подразделения УИС представляет собой не частичную модернизацию, а масштабную организационно-управленческую трансформацию, комплексный механизм, способный одновременно решать несколько задач. К ним относятся усиление защиты для противодействия цифровым угрозам, восполнение кадрового потенциала и эффективное управление факторами экологической и логистической нестабильности.

Создание единого информационно-коммуникационного контура для горизонтального взаимодействия и обмена данными преобразует производственные объекты в адаптивную, жизнестойкую и интеллектуально насыщенную операционную среду. Ключевое системообразующее качество предполагаемой модели заключается в поддержании стабильности и безопасности системы через отказ от единого центра и распределенности управления и данных. Децентрализация ликвидирует точки риска и сохраняет общую работоспособность системы при локальных инцидентах. Когда принятие алгоритмических решений происходит независимо в различных узлах системы, это исключает концентрацию власти в одном источнике, одновременно обеспечивая открытость процессов и возможность верификации. Использование такого подхода способствует формированию приемлемых контролируемых рамок для интеграции ИИ. В них можно точно регулировать степень автоматизации под конкретные цели, не отказываясь от контроля со стороны человека.

Одновременно такая модель способствует решению проблем накопления и приумножения интеллектуального потенциала предприятия. Она преобразует индивидуальные компетенции и личный опыт в актив, доступный каждому элементу сети. Целевым результатом преобразований является построение качественно новой среды с иными характеристиками для производственной деятельности. Ключевыми чертами этой экосистемы являются способность к упреждающему реагированию, оперативная реорганизация под влиянием различных факторов внешней и внутренней среды и непрерывное обучение, повышающее эффективность процессов. Сетецентрическая модель лишена уязвимостей иерархических систем – таких как ограниченность информации и ее медленное получение. Она подразумевает принципиально новый подход к управлению, соответствующий текущим реалиям. Инновационность заключается в переносе принципов работы распределенных сетей и их адаптации к специфическим условиям закрытой и контролируемой системы. Внедрение описанного подхода в производственный сектор УИС послужит отправной точкой для тиражирования в других высокорегламентированных и социально ответственных отраслях.

СПИСОК ИСТОЧНИКОВ / REFERENCES

Апевалова З. В., Кутыева Э. Р. Экологические аспекты деятельности современного гостиничного предприятия: анализ экологических рисков // *Science Time*. 2015. № 9 (21). С. 28–35.

Apevalova, Zoya V., and Elmira R. Kutyeva. 2015. “Ekologicheskie aspekty deyatelnosti sovremennogo gostinichnogo predpriyatiya: analiz ekologicheskih riskov” [“Environmental aspects of a modern hotel enterprise: analysis of environmental risks”] (In Russ.). *Science Time*, 21 no. 9 (September):28–35. URL: https://elibrary.ru/item.asp?id=24254784.

Бродецкий Г. Л., Герами В. Д., Гусев Д. А., Колик А. В. Трансформация цепей поставок в ситуации глобального кризиса. Анализ и прогноз // *Анализ и прогноз. Журнал ИМЭМО РАН*. 2023. № 2, С. 14–23. https://doi.org/10.20542/afij-2023-2-14-23

Brodetsky, Gennady L. [et al.]. 2023. “Transformatsiya tsepey postavok v situatsii global'nogo krizisa. Analiz i prognoz” [“Transformation of Supply Chains in a Global Crisis Situation. Analysis and Forecast”] (In Russ.). Analiz i prognoz. *Zhurnal IMEMO RAN [Analysis and Forecast. IMEMO RAS Journal]*, no. 2 (June):14–23. https://doi.org/10.20542/afij-2023-2-14-23

Букринская Э. М., Липатова О. Н. Проблемы формирования замкнутых цепей поставок в циклической экономике // *Вестник Астраханского государственного технического университета. Серия: Экономика.* 2023. № 4. С. 96–100. https://doi.org/10.24143/2073-5537-2023-4-96-100

Bukrinskaya, Elvira M., and Olga N. Lipatova. 2023. "Problemy formirovanija zamknutyh cepej postavok v ciklicheskoj jekonomike" ["Problems of Forming Closed Supply Chains in a Circular Economy"] (In Russ.). *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Ekonomika [Bulletin of the Astrakhan State Technical University. Series: Economics]*, no. 4 (December):96–100. https://doi.org/10.24143/2073-5537-2023-4-96-100

Дешура Ю. В., Павлов А. П. Основные проблемы внедрения искусственного интеллекта в деятельность государственных служащих // *Universum: экономика и юриспруденция* : [электронное издание]. 2024. № 10 (120). URL: https://7universum.com/ru/economy/archive/item/18248 (дата обращения: 18.12.2025).

Deshura, Y. V., and A. P. Pavlov. 2024. "Osnovnye problemy vnedrenija iskusstvennogo intellekta v dejatel'nost' gosudarstvennyh sluzhashhih" ["The Main Problems of Introducing Artificial Intelligence into the Activities of Civil Servants"] (In Russ.). *Universum: ekonomika i jurisprudencija [Universum: Economics and Jurisprudence]*, 120 no. 10 (October). URL: https://7universum.com/ru/economy/archive/item/18248 (дата обращения: 18.12.2025).

Заготовкин Д. Ф., Рыльский К. Проблемы интеграции искусственного интеллекта в судебную систему Российской Федерации // *Российские исследования. Право и политика.* 2025. Т. 9, № 1. С. 4–28. https://doi.org/10.12731/2576-9634-2025-9-1-215

Zagotovkin, Dmitry F., and Kirill Rylskij. 2025. "Problemy integracii iskusstvennogo intellekta v sudebnuju sistemu Rossijskoj Federacii" ["Problems of Integrating Artificial Intelligence into the Judicial System of the Russian Federation"] (In Russ.). *Rossijskie issledovanija. Pravo i politika [Russian Studies. Law and Politics]* 9, no. 1 (March):4–28. https://doi.org/10.12731/2576-9634-2025-9-1-215

Зоидов К. Х., Урунов А. А., Богатырев С. И., Остапенко В. А. Дефицит кадров: сравнительный анализ в России и зарубежных странах // *Региональные проблемы преобразования экономики.* 2024. № 6 (164). С. 164–172. https://doi.org/10.26726/1812-7096-2024-6-164-172

Zoidov, Kobiljon Kh. [et al.]. 2024. "Defitsit kadrov: sravnitel'nyj analiz v Rossii i zarubezhnyh stranah" ["Staff Shortage: A Comparative Analysis in Russia and Foreign Countries"] (In Russ.). *Regional'nyye problemy preobrazovaniya ekonomiki [Regional problems of economic transformation]* 164, no. 6 (June):164–72. https://doi.org/10.26726/1812-7096-2024-6-164-172

Климова П. А., Писаренко О. В. Проблема дефицита кадров в промышленном секторе: причины и пути решения // *Дискуссия.* 2024. № 12 (133). С. 258–265. https://doi.org/10.46320/2077-7639-2024-12-133-258-265

Klimova, P. A., and O. V. Pisarenko. 2024. "Problema defitsita kadrov v promyshlennom sektore: prichiny i puti reshenija" ["The Problem of Staff Shortage in the Industrial Sector: Causes and Solutions"] (In Russ.). *Diskussija [Discussion]*, 133 no. 12 (December):258–65. https://doi.org/10.46320/2077-7639-2024-12-133-258-265

Лазарева Е. И. Экологический риск-менеджмент в экономике инноваций: технологии управления экологическими рисками реализации стратегии инновационного развития экономики России // *Terra Economicus*. 2012. Т. 10, № 1-2. С. 113–116.

Lazareva, Elena I. 2012. "Jekologicheskij risk-menedzhment v jekonomike innovacij: tehnologii upravlenija jekologicheskimi riskami realizacii strategii innovacionnogo razvitija jekonomiki Rossii" ["Environmental Risk Management in the Innovation Economy: Technologies for Managing Environmental Risks of Implementing the Strategy for Innovative Development of the Russian Economy"] (In Russ.). *Terra Economicus* 10, no. 1-2 (February):113–116.

Маккаева Р. С. Э., Пайтаева К. Т., Айсханов С. К. Понятие экологического риска / *Поколение будущего: Взгляд молодых ученых – 2022* : сборник научных статей 11-й Международной молодежной научной конференции, г. Курск, 10–11 ноября 2022 г. / отв. ред. А. А. Горохов. Курск : Юго-Западный государственный университет, 2022. Т. 4, С. 76–78.

Makkaeva, Разет S. E., and Комета T. Pajtaeva, Sultan K. Ajschanov. 2022. "Ponjatie jekologicheskogo riska" ["The Concept of Environmental Risk"] (In Russ.) 76–8. In: Gorokhov A. A. (ed.) *Pokolenie budushhego: Vzgljad molodyh uchenyh – 2022 [Generation of the Future: The View of Young Scientists – 2022]* 4. Kursk : Yugo-Zapadnyy gosudarstvennyy universitet.

Морозова О. И., Семенихина А. В. Проблемы кадрового дефицита в условиях цифровой экономики // *Международный научно-исследовательский журнал*. 2020. № 6-4 (96). С. 93–97. https://doi.org/10.23670/IRJ.2020.96.6.130

Morozova, Olga I., and Anna V. Semenikhina. 2020. "Problemy kadrovogo defitsita v uslovijah cifrovoj jekonomiki" ["Problems of Staff Shortage in the Digital Economy"] (In Russ.). *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal [International research journal]* 96, no. 6-4 (Июнь):93–7. https://doi.org/10.23670/IRJ.2020.96.6.130

Пищик В. Я., Алексеев П. В. Актуальные проблемы кибербезопасности России: глобальный и национальный аспекты // *Теория и практика общественного развития.* 2024. № 10 (198). С. 112–121. https://doi.org/10.24158/tipor.2024.10.15

Pishchik, Victor Ya., and Petr V. Alekseev. 2024. "Aktualnye problemy kiberbezopasnosti Rossii: globalnyj i nacional'nyj aspekty" ["Topical Problems of Russia's Cybersecurity: Global and National Aspects"] (In Russ.). *Teorija i praktika obshhestvennogo razvitija [Theory and Practice of Social Development]* 198, no. 10 (October):112–21. https://doi.org/10.24158/tipor.2024.10.15

Полухтин И. М. Актуальные проблемы кибербезопасности в современном мире // *Вестник науки.* 2023. Т. 4, № 6 (63). С. 608–612

ISSN 3033-6554 (online)
https://epinb.ru

Polukhtin, I. M. 2023. “Aktual'nye problemy kiberbezopasnosti v sovremennom mire” [“Topical Problems of Cybersecurity in the Modern World”] (In Russ.). *Vestnik nauki [Science Bulletin]* 4, is. 63, no. 6 (June):608–12.

Пузанова Ж. В., Ларина Т. И. Интеграция прикладного искусственного интеллекта в магистерские программы непрофильных направлений: вызовы, тренды и перспективы // *Высшее образование в России.* 2025. Т. 34, № 8-9. С. 33–53. https://doi.org/10.31992/0869-3617-2025-34-8-9-33-53

Puzanova, Zhanna V., and Tatiana I. Larina. 2025. “Integracija prikladnogo iskusstvennogo intellekta v magisterskie programmy neprofil'nyh napravlenij: vyzovy, trendy i perspektivy” [“Integration of Applied Artificial Intelligence into Master's Programs of Non-Core Fields: Challenges, Trends, and Prospects”] (In Russ.). *Vysshee obrazovanie v Rossii [Higher Education in Russia]* 34, no. 8-9 (September):33–53. https://doi.org/10.31992/0869-3617-2025-34-8-9-33-53

Решетникова М. С., Пугачева И. А., Попов В. В. Киберугрозы: фактор неопределенности цифровой экономики // *Креативная экономика*. 2022. Т, 16, № 11. С. 4113–4130. https://doi.org/10.18334/ce.16.11.116551

Reshetnikova, Marina S., and Irina A. Pugacheva, Vladislav V. Popov. 2022. “Kiberugrozy: faktor neopredelennosti cifrovoj jekonomiki” [“Cyber Threats: A Factor of Uncertainty in the Digital Economy”] (In Russ.). *Kreativnaya ekonomika [Creative economy]* 16, no. 11 (November):4113–30. https://doi.org/10.18334/ce.16.11.116551

Шемякина Т. Ю. Проблемы управления рисками цепочки поставок // *Проблемы анализа риска.* 2023. Т. 20, № 4. С. 78–86. https://doi.org/10.32686/1812-5220-2023-20-4-78-86

Shemyakina, Tatyana Yu. 2023. “Problemy upravlenija riskami cepochki postavok” [“Problems of Supply Chain Risk Management”] (In Russ.). *Problemy analiza riska [Risk Analysis Problems]* 20, no. 4 (August):78–86. https://doi.org/10.32686/1812-5220-2023-20-4-78-86

Авторами внесен равный вклад в написание статьи.
Авторы заявляют об отсутствии конфликта интересов.

The authors have made an equal contribution to the writing of the article.
The authors declare no conflicts of interests.