DOI: 10.18137/RNU.V9187.26.01.P.79 УДК 004.056

**Запрягаев Фёдор Андреевич**
аспирант, НИИ АО «Концерн «Моринформсистема-АГАТ», Москва.
ORCID: 0009-0006-1366-0106
Электронный адрес: Fedor.bws16@yandex.ru
**Fyodor A. Zapryagaev**
Postgraduate, Research Institute of JSC "Concern "Morinformsystem-AGAT", Moscow.
ORCID: 0009-0006-1366-0106
E-mail address: Fedor.bws16@yandex.ru

**Николаев Андрей Анатольевич**
кандидат физико-математических наук, начальник отдела 01050-1 АО «Концерн «Моринформсистема-АГАТ», Москва.
Электронный адрес: 01050-1@concern-agat.ru
**Andrey A. Nikolaev**
Ph.D. of Physico-Mathematical Sciences, Head of Department 01050-1, JSC "Concern "Morinformsystem-AGAT", Moscow.
E-mail address: 01050-1@concern-agat.ru

# РАЗРАБОТКА КРИТЕРИЕВ ОЦЕНКИ ЭФФЕКТИВНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЙ ПРИ ПОМОЩИ СРЕДСТВ КОНТРОЛЯ И МОНИТОРИНГА

**Аннотация.** В статье рассматриваются актуальные подходы к разработке комплексной системы критериев оценки эффективности защиты критической информационной инфраструктуры промышленных предприятий. Особое внимание уделяется интеграции современных средств контроля и мониторинга как ключевого инструмента обеспечения устойчивости и безопасности. Авторами выделяются и анализируются четыре основные функциональные области для формирования критериев: 1) *зрелость системы мониторинга*, включая полноту сбора данных, интеллектуальность анализа на основе AI/ML (AIOps) и эффективность механизмов оповещения; 2) *эффективность риск-ориентированного управления устойчивостью*, охватывающая адаптивный анализ угроз (с применением цифровых двойников и симуляций), обоснованный выбор защитных мер и готовность к восстановлению; 3) *зрелость процессов аудита и контроля*, подразумевающая автоматизацию, непрерывность и контекстную релевантность проверок; 4) *эффективность специализированных средств защиты для АСУ ТП*, в частности качество индикаторов компрометации (IOC) и учет операционных ограничений. В работе обобщены современные практики в области риск-ориентированных методологий, построения систем мониторинга на базе решений с открытым исходным кодом (Prometheus, Grafana, Zabbix), аудита информационной безопасности и применения IOC в промышленных системах управления. Результатом исследования является структурированная система критериев, позволяющая перейти от оценки формального соответствия стандартам к измерению реальной способности критической информационной инфраструктуры противостоять сложным комбинированным угрозам и обеспечивать проактивное управление устойчивостью.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

***Ключевые слова:*** критическая информационная инфраструктура, оценка эффективности, кибербезопасность, мониторинг, управление устойчивостью, риск-ориентированный подход, индикаторы компрометации (IOC), AIOps, промышленные системы управления (АСУ ТП).

***Для цитирования:*** *Запрягаев Ф.А., Николаев А.А.* Разработка критериев оценки эффективности критической информационной инфраструктуры предприятий при помощи средств контроля и мониторинга // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2026. № 1. С. 79–88. DOI: 10.18137/RNU.V9187.26.01.P.79

# DEVELOPMENT OF CRITERIA FOR ASSESSING THE EFFECTIVENESS OF ENTERPRISE CRITICAL INFORMATION INFRASTRUCTURE USING CONTROL AND MONITORING TOOLS

**Abstract.** The article discusses the current approaches to developing a comprehensive system of criteria for assessing the effectiveness of protecting the critical information infrastructure (CII) of industrial enterprises. Particular attention is paid to the integration of modern control and monitoring tools as a key instrument for ensuring resilience and security. The authors identify and analyze four main functional areas for forming the criteria: 1) *monitoring system maturity*, including the completeness of data collection, the intelligence of analysis based on AI/ML (AIOps), and the effectiveness of alerting mechanisms; **2)** *effectiveness of risk-driven resilience management*, covering adaptive threat analysis (using digital twins and simulations), justified selection of protective measures, and recovery readiness; 3) *maturity of audit and control processes*, implying automation, continuity, and contextual relevance of checks; 4) *effectiveness of specialized protection tools for ICS*, in particular, the quality of Indicators of Compromise (IOC) and consideration of operational constraints. The paper summarizes modern practices in the field of risk-driven methodologies, building monitoring systems based on open-source solutions (Prometheus, Grafana, Zabbix), information security auditing, and the application of IOCs in industrial control systems. The result of the research is a structured system of criteria that allows for a shift from assessing formal compliance with standards to measuring the real ability of CII to withstand complex combined threats and ensure proactive resilience management.

***Keywords*: *critical*** information infrastructure (CII), effectiveness assessment, cybersecurity, monitoring, resilience management, risk-driven approach, indicators of compromise (IOC), AIOps, industrial control systems (ICS).

***For citation:*** Zapryagaev F.A., Nikolaev A.A. (2026) Development of criteria for assessing the effectiveness of enterprise critical information infrastructure using control and monitoring tools. *Vestnik of Russian New University. Series: Complex Systems: Models, analysis, management.* No. 1. Pp. 79–88. DOI: 10.18137/RNU.V9187.26.01.P.79 (In Russian).

## *Критерии оценки эффективности критической информационной инфраструктуры предприятий с использованием средств контроля и мониторинга: современные подходы*

Оценка эффективности критической информационной инфраструктуры (далее – КИИ) предприятий требует комплексных критериев, учитывающих как технические, так

и организационные аспекты. Современные исследования подчеркивают важность интеграции мониторинга, аудита, анализа уязвимостей и оценки устойчивости к угрозам.

*Основные критерии и индикаторы эффективности*

*Оценка функционала безопасности.* Анализ выполнения ключевых задач системы защиты КИИ с помощью таких показателей, как идентификация рисков (ID), киберзащита (PR), обнаружение инцидентов (DE), реагирование (RS) и восстановление (RC) [1].

*Анализ устойчивости и уязвимостей.* Проведение оценки устойчивости инфраструктуры к угрозам через систематический анализ активов, моделирование взаимосвязей между компонентами и применение методов вероятностного и симуляционного моделирования (включая метод Монте-Карло) [2; 3].

*Организация мониторинга и контроля.* Обеспечение непрерывного наблюдения за состоянием системы с помощью автоматизированных инструментов (таких как Prometheus и Grafana), проведение аудитов безопасности, регулярный анализ логов событий и контроль действий администраторов [4–6].

*Проведение аудита и обеспечение соответствия.* Регулярная проверка и оценка системы защиты на соответствие требованиям национальных и международных стандартов (например, ISO 27001) с использованием общепринятых моделей аудита [6; 7].

*Измерение эффективности защитных мер.* Комплексная оценка результативности мер безопасности путем анализа произошедших инцидентов, использования индикаторов компрометации (IOC) и интеграции данных из технических и нетехнических источников [8; 9].

Рассмотрим критерии и методы оценки эффективности критической информационной инфраструктуры предприятий при помощи средств контроля и мониторинга.

### *Адаптация риск-ориентированных методик для управления устойчивостью критической инфраструктуры*

Обеспечение устойчивости критической инфраструктуры приобретает всё более важное значение, поскольку данные системы сталкиваются со сложными угрозами – от стихийных бедствий до кибератак. Современные научные изыскания концентрируются на трансформации традиционных методов защиты, основанных на управлении рисками, в комплексные программные обеспечения управления устойчивостью. Данная трансформация подразумевает интеграцию оценки рисков, адаптивного контроля и передней аналитики для поддержания выполнения критически важных функций в неблагоприятных условиях [1].

Хронология научных разработок наглядно демонстрирует эволюцию от управления рисками к интегрированным заготовкам для программного обеспечения устойчивости в период с 2015 по 2025 год, где маркеры большего размера соответствуют работам с более высоким индексом цитирования [2].

Адаптация риск-ориентированных методологий включает в себя комбинацию аудита рисков информационной безопасности и адаптивного управления устойчивостью, что позволяет проводить многоуровневый анализ угроз, уязвимостей и контрмер. Такой подход обеспечивает проведение агрегированных оценок устойчивости и обоснованный выбор стратегий восстановления, повышая уровень ситуационной осведомленности операторов. Новые программные обеспечения, такие как метод CERA, дают возможность кри-

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

тически важным объектам проводить самооценку устойчивости, выявлять уязвимости и определять целевые технические, организационные и security-меры. Всё более широкое применение находит интеграция цифровых технологий, включая цифровые двойники и искусственный интеллект (далее – ИИ), для мониторинга в реальном времени, прогнозной аналитики и сценарного стресс-тестирования, что поддерживает проактивное и основанное на данных управление устойчивостью.

Сложность и высокая степень взаимозависимости компонентов критической инфраструктуры требуют применения интегрированных подходов к моделированию новых аналитических методов для учета динамических уязвимостей и каскадных рисков. Сценарии множественных и комбинированных угроз подчеркивают необходимость разработки программного обеспечения, которое учитывает последовательность и природу опасных событий, стратегии восстановления и количественно измеримые индексы устойчивости. Практическая реализация управления устойчивостью требует координации возможностей по реагированию, мониторингу, прогнозированию и обучению, что часто поддерживается цифровыми инструментами и имитационными моделями [2].

Практическое применение включает стратегии восстановления энергосистем на основе оценки рисков, инструменты оценки устойчивости для маломасштабных катастроф и управление активами на основе показателей эффективности для адаптации дорожного хозяйства к изменениям климата. Финансируемые ЕС проекты, такие как PRECINCT, демонстрируют ценность совместного управления киберфизической безопасностью и использования цифровых двойников и симуляторов для оценки уязвимостей [2].

Для структурирования полученных результатов составлена сводная таблица, которая связывает ключевые подтемы с репрезентативными публикациями. В Таблице систематизированы четыре основных направления:

1) адаптация риск-ориентированной устойчивости (интеграция аудита рисков с адаптивным управлением);

2) цифровые инструменты и инструменты на основе ИИ для повышения устойчивости (использование цифровых двойников, ИИ и моделирования для поддержки мониторинга и принятия решений);

3) моделирование множественных угроз и процессов восстановления (фреймворк для комбинированных угроз и стратегий восстановления);

4) инструменты самооценки и оперативного управления (методы и инструменты для оценки и управления устойчивостью на уровне объекта).

Современные исследования свидетельствуют о переходе от традиционного управления рисками к интегрированному адаптивному управлению устойчивостью критической инфраструктуры. Эта эволюция использует риск-ориентированные методологии, цифровые технологии и основы для работы с множественными угрозами, позволяя противостоять сложным динамическим рискам и обеспечивая поддержку обоснованного и проактивного принятия решений операторами инфраструктуры.

### *Ключевые элементы построения эффективной системы мониторинга серверной инфраструктуры предприятия*

Эффективный мониторинг серверной инфраструктуры предприятия является критически важным для обеспечения надежности, производительности и безопасности. Совре-

менные системы интегрируют сбор данных в реальном времени, автоматизированное оповещение и переднюю аналитику для проактивного управления и оптимизации серверных сред [2].

### *Основные компоненты и передовые практики*

*Выбор платформы и автоматизация.* Успешные системы мониторинга часто базируются на платформах с открытым исходным кодом, таких как Prometheus и Grafana, которые выбираются благодаря своей гибкости, масштабируемости и возможностям визуализации. Автоматизация процессов развертывания и конфигурации позволяет упростить установку и техническое обслуживание, минимизируя ошибки ручного ввода и обеспечивая согласованность конфигураций.

*Комплексный сбор данных.* Интеграция множества источников данных, таких как метрики серверов, состояние сети и журналы приложений, обеспечивает целостную наблюдаемость среды. Инструменты, подобные Zabbix, а также специализированные решения с использованием Python, Telegraf и InfluxDB, способствуют эффективному сбору, хранению и анализу метрик.

*Оповещение в реальном времени и кастомизация.* Интеллектуальные системы оповещения осуществляют категоризацию и приоритизацию инцидентов на основе критичности и заданных пользователем пороговых значений, что гарантирует своевременное реагирование на критические события. Настраиваемые информационные панели и системы уведомлений повышают уровень оперативной осведомленности персонала.

*Интеграция аспектов безопасности и IoT.* Внедрение IoT-сенсоров и специализированных security-модулей усиливает возможности мониторинга, обеспечивая обнаружение физических и киберугроз в режиме реального времени, а также контроль действий сторонних сервисов.

*Искусственный интеллект и предиктивная аналитика.* Передовые системы задействуют методы ИИ в рамках концепции искусственного интеллекта для ИТ-операций (AIOps) для обнаружения аномалий, прогнозного технического обслуживания и автоматизированного анализа первопричин инцидентов, что дополнительно повышает доступность системы и сокращает необходимость ручного вмешательства.

Сравнительный анализ инструментов мониторинга и их ключевых характеристик демонстрирует, что связка Prometheus + Grafana обеспечивает работу с метриками в реальном времени и их визуализацию с высоким уровнем автоматизации. Zabbix предлагает комплексный мониторинг производительности и доступности с развитой системой оповещений. IoT-ориентированные системы отличаются высоким уровнем интеграции функций безопасности и мониторинга физических параметров. Решения на базе AI/AIOps предоставляют наиболее совершенные возможности, такие как предиктивная аналитика и автоматическое обнаружение аномалий [3].

Эффективная система мониторинга серверной инфраструктуры предприятия представляет собой комбинацию автоматизированного сбора данных в реальном времени, настраиваемой системы оповещений и передовых аналитических функций. Интеграция инструментов с открытым исходным кодом, технологий интернета вещей и методов ИИ обеспечивает создание крепкого, масштабируемого и безопасного управления инфраструктурой, соответствующего операционным потребностям организации.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

***Современные практики внедрения систем аудита информационной безопасности для критической инфраструктуры***

Современные практики внедрения систем аудита информационной безопасности для критической инфраструктуры эволюционируют в ответ на усложнение угроз, нормативные требования и необходимость непрерывного совершенствования. Актуальные подходы смещаются в сторону риск-ориентированных, стандартизированных и технологически продвинутых решений, выходящих за рамки традиционных проверок соответствия.

Ключевые практики и методологии характеризуются следующими аспектами. Внедрение систем руководствуется международными (серия ISO 27001/270xx, стандарты NIST) и национальными стандартами, что обеспечивает соответствие глобальным и локальным регуляторным требованиям. Сам процесс аудита становится все более риск-ориентированным, фокусируясь на идентификации, анализе и управлении информационными рисками на протяжении всего жизненного цикла систем критической инфраструктуры. Современные системы используют интегрированные платформы, объединяющие функции аудита соответствия, оценки уязвимостей и обеспечения готовности к проведению расследований. Автоматизация процессов с использованием специализированного программного обеспечения и облачных архитектур оптимизирует сбор данных, анализ и формирование отчетности, снижая долю ручного труда и повышая точность результатов [9].

Новые методологии внедряют математические модели и техники визуализации данных, позволяя выходить за рамки бинарных результатов (соответствует/не соответствует). Это обеспечивает получение детализированной информации о security-пробелах и позволяет приоритизировать мероприятия по устранению недостатков на основе оценки рисков и потенциального воздействия. Непрерывный мониторинг и двухрежимные системы аудита (национального и комбинированного типа) обеспечивают оценку в реальном времени и быстрое реагирование на возникающие угрозы, поддерживая полный цикл обеспечения безопасности. Гибкие, ориентированные на клиента структуры проектируются с учетом возможности адаптации как для крупных корпораций, так и для субъектов МСП, позволяя кастомизировать контрольные меры и задачи по минимизации рисков в соответствии с потребностями организации [6].

Сравнительный анализ современных практик аудита демонстрирует, что стандартизированный риск-ориентированный подход обеспечивает соответствие требованиям ISO/NIST и фокусируется на управлении рисками. Автоматизация и интеграция процессов значительно сокращают объем ручных операций и повышают точность. Применение продвинутой аналитики и визуализации позволяет проводить детальный анализ пробелов и осуществлять эффективное устранение причин выявленных несоответствий. Непрерывный и двухрежимный аудит поддерживает адаптивное обеспечение безопасности в режиме реального времени, а клиентоориентированные программные шаблоны обеспечивают масштабируемость решений для организаций любого размера [7].

Таким образом, современные системы аудита информационной безопасности для критической инфраструктуры акцентируют управление рисками, автоматизацию процессов, применение передней аналитики и адаптивность. Интеграция международных стандартов, использование современных технологий и ориентация на принципы непрерывного совершенствования позволяют таким системам обеспечивать робастные, масштабируемые и практико-ориентированные механизмы защиты критически важных активов.

### *Индикаторы компрометации в системах промышленного управления: аналитический обзор и практические аспекты*

Современные системы промышленного управления становятся все более частой мишенью для сложных кибератак, что делает идентификацию и использование индикаторов компрометации важнейшим элементом своевременного обнаружения и реагирования на инциденты. Под индикаторами компрометации понимаются специфические артефакты или паттерны, такие как аномальный сетевой трафик, хэши файлов или записи в системных журналах, которые сигнализируют о потенциально вредоносной активности в средах промышленной автоматизации.

К распространенным индикаторам относятся аномальные сетевые подключения, несанкционированные изменения управляющей логики, подозрительные хэши файлов и неожиданное поведение систем. Данные индикаторы могут быть соотнесены с известными сценариями атак, такими как Stuxnet и Industroyer, что способствует раннему обнаружению и реагированию на угрозы. Однако не все индикаторы, эффективные в традиционных ИТ-средах, демонстрируют аналогичную результативность в системах операционных технологий. Исследования подтверждают, что некоторые индикаторы обладают большей распознаваемостью и практической ценностью именно в условиях промышленных систем, что подчеркивает необходимость разработки специализированных индикаторов для СПУ.

Существуют различные стандарты представления индикаторов компрометации, однако их внедрение в СПУ ограничивается специфическими операционными требованиями и наличием унаследованных систем. Для идентификации и сопоставления индикаторов с тактиками и техниками атак всё активнее применяются такие инструменты, как фреймворк-безопасности MITRE ATT&CK для ICS, системы обнаружения аномалий на основе машинного обучения и фреймворк-проактивного поиска угроз. Библиотеки индикаторов риска и системы обнаружения вторжений, основанные на телеметрии, обеспечивают непрерывную оценку рисков и оперативную идентификацию индикаторов компрометации [9].

К ключевым препятствиям для эффективного развертывания индикаторов в СПУ относятся: наличие унаследованных систем, отсутствие стандартизированных форматов индикаторов и операционные ограничения. В научной сфере отмечается потребность в более комплексных исследованиях и практических инструментах, адаптированных конкретно для сред промышленной автоматизации, а также в усовершенствованных методах сопоставления индикаторов с эволюционирующими техниками атак [7; 9].

Эффективное использование индикаторов компрометации в системах промышленного управления требует специализированных подходов, готовых решений в области программирования, структур и постоянной адаптации к новым угрозам. Развитие стандартов, инструментов обнаружения и методов контекстного анализа является ключевым фактором усиления киберзащиты и устойчивости промышленных систем.

### *Выводы*

На основе анализа представленных материалов разработана система критериев оценки эффективности защиты КИИ предприятий через призму применения средств контроля и мониторинга. Критерии сгруппированы по ключевым функциональным областям.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

***Критерии зрелости системы мониторинга***

*Полнота и интегрированность сбора данных.* Охват всех ключевых компонентов (серверы, сеть, приложения, IoT-устройства) и интеграция данных из разнородных источников (метрики, логи, данные о безопасности) в единую платформу (на примере решений Prometheus/Zabbix + Grafana).

*Интеллектуальность анализа и реагирования.* Уровень использования AI/ML для прогнозной аналитики, автоматического обнаружения аномалий (AIOps) и проведения автоматизированного анализа первопричин инцидентов, что сокращает время реагирования и снижает нагрузку на персонал.

*Эффективность механизмов оповещения.* Наличие настраиваемой системы оповещений, обеспечивающей приоритизацию инцидентов на основе оценки критичности и бизнес-воздействия, а также интеграцию с каналами коммуникации (email, тикет-системы).

***Критерии эффективности риск-ориентированного управления устойчивостью***

*Способность к адаптивному анализу угроз.* Использование методов моделирования (цифровые двойники, симуляции) для прогнозирования каскадных эффектов и оценки устойчивости к многочисленным и комбинированным угрозам.

*Обоснованность выбора защитных мер.* Наличие формализованного процесса выбора контрмер на основе агрегированной оценки рисков, а не только на основе соответствия стандартам. Включает использование математических моделей для приоритизации мероприятий.

*Готовность к восстановлению.* Наличие протестированных стратегий восстановления для различных сценариев инцидентов, основанных на оценке рисков (риск-ориентированное восстановление), и возможность их оперативной адаптации.

***Критерии зрелости процессов аудита и контроля***

*Степень автоматизации аудита.* Уровень интеграции и автоматизации процессов сбора доказательств, анализа соответствия и генерации отчетов с использованием специализированных платформ, что минимизирует ручной труд и повышает точность.

*Непрерывность контроля безопасности.* Реализация режима непрерывного аудита и мониторинга в реальном времени, выходящего за рамки периодических проверок, что обеспечивает оперативное выявление отклонений и адаптацию к новым угрозам.

*Контекстная релевантность контроля.* **С**оответствие применяемых контрольных мер (включая индикаторы компрометации) специфике технологических процессов и операционным требованиям КИИ, а не просто перенесение практик из корпоративных ИТ-сетей.

***Критерии эффективности специализированных средств защиты*** *(в частности,* ***для АСУ ТП)***

*Качество и релевантность используемых IOC (Indicators of Compromise).* Наличие и актуальность библиотек индикаторов, специфичных для промышленных систем (ICS), и их сопоставление с актуальными тактиками злоумышленников (например, через MITRE ATT&CK for ICS).

*Учет операционных ограничений.* Способность системы мониторинга и контроля функционировать в условиях унаследованных систем (legacy) и строгих операционных требований АСУ ТП без нарушения технологического процесса.

***Обобщающий показатель***

*Интегральная способность к проактивному управлению устойчивостью.* Синтез всех вышеперечисленных критериев, отражающий способность организации не только реаги-

ровать на инциденты, но и предвидеть их, адаптироваться к изменяющимся условиям и поддерживать выполнение критических функций при реализации угроз. Это проявляется в сокращении времени восстановления, снижении количества успешных инцидентов и повышении осведомленности персонала о текущем состоянии защищенности.

Данная система критериев позволяет перейти от оценки формального соответствия стандартам к измерению реальной способности КИИ предприятия противостоять современным сложным угрозам с использованием передовых средств контроля и мониторинга.

## Литература

1. *Краснов А.Е., Мосолов А.С., Феоктистова Н.А.* Оценка устойчивости критической информационной инфраструктуры к угрозам информационной безопасности // Безопасность информационных технологий. 2021. Т. 28. № 1. С. 106–120. DOI: 10.26583/bit.2021.1.09. EDN JMVYBG.

2. *Маслобоев А.В., Цыгичко В.Н.* Адаптация и расширение риск-ориентированной методологии защиты критически важных объектов для управления устойчивостью критической инфраструктуры // Надежность и качество сложных систем. 2024. № 4. С. 140–159. DOI: 10.21685/2307-4205-2024-4-16. EDN CGFXIY.

3. *Kure H., Islam S., Mouratidis H.* An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection. Neural Computing and Applications. 2022. Vol. 34. P. 15241–15271. DOI: https://doi.org/10.1007/s00521-022-06959-2

4. *Пулова Д.Д, Варфоломеев В.А.* Построение эффективной системы мониторинга серверной инфраструктуры предприятия // Интеллектуальные транспортные системы : Материалы III Международной научно-практической конференции, Москва, 30 мая 2024 г. Москва : Российский университет транспорта (МИИТ), 2024. С. 332–335. DOI: 10.30932/9785002446094-2024-332-335. EDN KODEWQ.

5. *Баранькова И.И., Петрова Д.А., Андронков А.Д.* Модернизация системы защиты информации объектов критической инфраструктуры металлургической промышленности // Бюллетень науки и практики. 2025. Т. 11. № 6. С. 122–128. DOI: 10.33619/2414-2948/115/17. EDN ZPINRJ.

6. *Бакшеев А.С., Лившиц И.И.* Разработка методики мониторинга уровня информационной безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2023. № 2 (54). С. 85–98. DOI: 10.21681/2311-3456-2023-2-85-98. EDN KQLCWV.

7. *Рытов М.Ю., Мусиенко Н.О., Губсков Ю.А., Минин Ю.В.* Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры // Приборы и системы. Управление, контроль, диагностика. 2022. № 10. С. 10–18. DOI: 10.25791/pribor.10.2022.1364. EDN LZZWNT.

8. *Asiri M., Saxena N., Gjomemo R., Burnap P.* Understanding indicators of compromise against cyber-attacks in industrial control systems: A security perspective // ACM Transactions on Cyber-Physical Systems. 2023. Vol. 7. Pp. 1–33. DOI: https://doi.org/10.1145/3587255

9. *Asiri M., Arunasalam A., Saxena N., Celik Z.B.* Frontline responders: Rethinking indicators of compromise for industrial control system security. *Computers & Security*. 2025. Vol. 154. Article no. 104421. DOI: 10.1016/j.cose.2025.104421

## References

1. Krasnov A.E., Mosolov A.S., Feoktistova N.A. (2021). Assessing the resilience of critical information infrastructures to information security threats. *IT Security (Russia)*. (In Russian).

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

2. Masloboev A.V., Tsygichko V.N. (2024). Adapting and expanding the risk-driven methodology of critical entities protection to critical infrastructure resilience management. *Reliability and Quality of Complex Systems*. No. 4. Pp. 140–159. DOI: 10.21685/2307-4205-2024-4-16 (In Russian).
3. Kure H., Islam S., Mouratidis H. (2022). An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection. *Neural Computing and Applications*. Vol. 34. Pp. 15241–15271. DOI: https://doi.org/10.1007/s00521-022-06959-2
4. Pulova D.D., Varfolomeev V.A. (2024). Building an effective system for monitoring the enterprise server infrastructure. In: Ikonnikov S.E. (Ed) *Intellektual'nye transportnye sistemy* [Intelligent Transport Systems] : Proceedings of the III International Scientific and Practical Conference, Moscow, May 30, 2024. Moscow : Russian University of Transport (MIIT). Pp. 332–335. DOI: 10.30932/9785002446094-2024-332-335 (In Russian).
5. Barankova I.I., Petrova D.A., Andronkov A.D. (2025). Modernization of the information protection system of critical infrastructure facilities in the metallurgical industry. *Bulletin of Science and Practice*. Vol. 11. No. 6. Pp. 122–128. DOI: 10.33619/2414-2948/115/17 (In Russian).
6. Baksheev A., Livshitz I. (2023). Development of a methodology for monitoring the level of information security of critical information infrastructure objects. *Voprosy kiberbezopasnosti* [Cybersecurity Issues]. № 2 (54). С. 85–98. DOI: 10.21681/2311-3456-2023-2-85-98 (In Russian).
7. Rytov M.Yu., Musienko N.O., Gubskov Yu.A., Minin Yu.V. (2022) Audit and monitoring of the state of informatization objects in the process of designing complex information protection systems for significant objects of critical information infrastructure. *Instruments and Systems: Monitoring, Control, and Diagnostics*. No. 10. Pp. 10–18. DOI: 10.25791/pribor.10.2022.1364 (In Russian).
8. Asiri M., Saxena N., Gjomemo R., Burnap P. (2023). Understanding indicators of compromise against cyber-attacks in industrial control systems: A security perspective. *ACM Transactions on Cyber-Physical Systems*. Vol. 7. Pp. 1–33. DOI: https://doi.org/10.1145/3587255
9. Asiri M., Arunasalam A., Saxena N., Celik Z.B. (2025). Frontline responders: Rethinking indicators of compromise for industrial control system security. *Computers & Security*. Vol. 154. Article no. 104421. DOI: 10.1016/j.cose.2025.104421.

Поступила в редакцию: 26.12.2025
Поступила после рецензирования: 26.01.2026
Принята к публикации: 15.02.2026

Received: 26.12.2025
Revised: 26.01.2026
Accepted: 15.02.2026