

БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

DOI: 10.25629/SMW.2026.01.09

УДК: 504.064

Бережной Д.А., доктор технических наук, доцент, Академия Государственной противопожарной службы МЧС России

Бутузов С.Ю., доктор технических наук, доцент, Академия Государственной противопожарной службы МЧС России

Ивакина Н.И., Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России

Berezhnoy D.A., Doctor of Technical Sciences, Associate Professor, Academy of the State Fire Service of the Ministry of Emergency Situations of Russia

Butuzov S.Yu., Doctor of Technical Sciences, Associate Professor, Academy of the State Fire Service of the Ministry of Emergency Situations of Russia

Ivakina N.I., All-Russian Research Institute for Civil Defense and Emergencies of the Ministry of Emergency Situations of Russia

Алгоритм информационного обмена при ЧС на объектах Росатома с использованием технологии блокчейн

Аннотация

В статье рассматривается алгоритм информационного взаимодействия при чрезвычайных ситуациях на объектах Госкорпорации «Росатом». Учитывая специфику угроз, таких как природные катаклизмы, антропогенные воздействия и высокий уровень геополитической чувствительности, предложен поэтапный алгоритм передачи, обработки и подтверждения критической информации. В основу алгоритма положен механизм децентрализованной фиксации и маршрутизации данных с использованием технологии блокчейн, что обеспечивает прозрачность, устойчивость и отказоустойчивость системы в условиях разрушения инфраструктуры. Отдельное внимание уделено учёту вероятностных характеристик отказов и роли человеческого фактора в процессе взаимодействия. Предложенное решение может быть применено при разработке цифровых платформ кризисного реагирования для атомной отрасли, а также при построении комплексных систем безопасности на уровне стратегических объектов.

Ключевые слова

алгоритм взаимодействия, чрезвычайная ситуация, блокчейн, Росатом, надёжность, цифровое оповещение, отказоустойчивость

An algorithm for information exchange during emergencies at Rosatom facilities using blockchain technology

Abstract

This article examines an algorithm for information exchange during emergencies at Rosatom State Corporation facilities. Considering the specific nature of threats, such as natural disasters, anthropogenic impacts, and high geopolitical sensitivity, a step-by-step algorithm for transmitting, processing, and confirming critical information is proposed. The algorithm is based on a mechanism for decentralized data recording and routing using blockchain technology, ensuring transparency, stability, and fault-tolerance in the event of infrastructure disruption.

Special attention is paid to the probabilistic characteristics of failures and the role of the human factor in the interaction process. The proposed solution can be applied in the development of digital crisis response platforms for the nuclear industry, as well as in the construction of integrated security systems at strategic facilities.

Keywords

Interaction algorithm, emergency, blockchain, Rosatom, reliability, digital alerting, fault tolerance

Введение

В условиях повышенной техногенной и геополитической напряжённости особую актуальность приобретает вопрос обеспечения устойчивого функционирования критической инфраструктуры, к числу которой относятся объекты Госкорпорации «Росатом», расположенные в пограничных пространствах.

Эти объекты обладают стратегическим значением и находятся под воздействием множества факторов риска — от природных катастроф до внешних техногенных и антропогенных угроз.

Особенность функционирования объектов ядерной энергетики в таких условиях заключается в необходимости организации высоконадежного информационного взаимодействия между множеством органов исполнительной власти, государственными органами (МЧС России, Росгидромет, ФСБ России), службами предприятия, военными подразделениями и международными структурами (в случае возникновения трансграничного ЧС). При этом эффективность взаимодействия во многом определяется своевременностью обмена информацией, устойчивостью каналов связи, корректностью восприятия сигнальных сообщений в условиях стресса и высокой неопределённости.

Анализ последствий аварий на объектах атомной энергетики — Три-Майл-Айленд (1979), Чернобыльская АЭС (1986), Фукусима-1 (2011) — показывает, что одна из ключевых причин масштабных последствий заключалась не только в технических сбоях, но и в информационной несогласованности между службами, затруднённой оценке реального положения дел и опоздании с принятием решений. Таким образом, разработка алгоритмов информационного взаимодействия в условиях чрезвычайных ситуаций (ЧС) является неотъемлемой и актуальной частью современной системы безопасности.

Особую значимость эта проблема приобретает применительно к объектам Росатома, расположенным вблизи границ, где возможны как воздействия двойственной природы (природные и техногенные), так и затруднённый координационный обмен данными в силу юрисдикционных ограничений и необходимости синхронизации с международными протоколами.

Поэтому цель настоящей статьи — разработка и представление алгоритма информационного взаимодействия в условиях ЧС, в условиях функционирования объектов Росатома в

пограничных регионах с учётом современных требований к надёжности, устойчивости и многоуровневой координации. В рамках исследования рассматриваются:

- классификация возможных угроз и воздействий (внешние и внутренние);
- принципы построения алгоритма обмена информацией между субъектами;
- оценка надёжности каналов и компонентов системы связи в экстремальных условиях;
- практические предложения по совершенствованию существующих решений.

Теоретические основы информационного взаимодействия при ЧС

Информационное взаимодействие в условиях ЧС — это процесс обмена информацией в условиях чрезвычайной ситуации (ЧС), что представляет собой структурированный процесс передачи, обработки и интерпретации критически важной информации между субъектами системы реагирования.

Основной целью данного процесса является обеспечение своевременного принятия решений, организация защитных мероприятий (включая эвакуацию), минимизация последствий аварий и обеспечение радиационной и техногенной безопасности персонала, населения и окружающей среды.

Содержательно информационный обмен охватывает три ключевых направления:

- оперативное взаимодействие, включающее сбор и передачу телеметрических данных, сигналов тревоги, параметров внешней среды и состояния оборудования в реальном времени;
- регламентированную отчётность, которая осуществляется по установленным протоколам и каналам связи между уровнями управления;
- прогностическую аналитику, формируемую на основе оценки сценариев развития ЧС, с учётом вероятностных моделей и данных, формируемых экспертами.

Уровень эффективности информационного обмена в условиях ЧС определяется несколькими взаимосвязанными факторами:

- сложившейся иерархией взаимодействующих субъектов, включая локальные, ведомственные и федеральные структуры;
- характером и масштабом внешних и внутренних угроз (природных, техногенных, антропогенных);
- автоматизацией мониторинговых и управляющих процессов;
- надёжностью технических средств передачи данных, устойчивостью каналов связи к внешним воздействиям и их резервированием.

Система информационного взаимодействия формируется в соответствии с рядом нормативных и методологических документов, основными из которых представлены в таблице 1.

Таблица 1 – Нормативные и регламентные основания

№	Наименование нормативного акта	Примечание
1	Федеральный закон № 68-ФЗ «О защите населения и территорий от ЧС»	Базовый закон по гражданской защите
2	Федеральный закон № 170-ФЗ «Об использовании атомной энергии»	Определяет принципы безопасности ядерных объектов
3	ГОСТ Р 22.0.10–96; ГОСТ Р 22.1.01–95	Регламентируют мониторинг и средства связи
4	Методические указания и приказы Росатома, МЧС, Роспотребнадзора	Операциональные регламенты взаимодействия
5	IAEA Safety Standards Series; Конвенция о раннем оповещении (1986)	Международные документы, обязательные в пограничных зонах

Особую специфику информационное взаимодействие приобретает на объектах, расположенных вблизи государственной границы, где требуется соблюдение норм международного права и наличие межведомственных соглашений с соседними странами.

Это позволяет обеспечить синхронизацию действий при трансграничных авариях и эффективную интеграцию в международные системы раннего оповещения, такие как IRMIS и RANET (МАГАТЭ).

На объектах Росатома система информационного взаимодействия реализована в рамках иерархически организованной архитектуры, состоящей из следующих уровней (таблица 2).

Таблица 2 – Нормативные и регламентные основания

Уровень	Основные субъекты и функции
Локальный	АСУ ТП, датчики, технологические контроллеры: первичный сбор и передача данных
Объектовый	Оперативно-диспетчерские службы, инженерный персонал: анализ, первичное принятие решений
Ведомственный	Росатом, ГУ МЧС России, Ростехнадзор: координация, передача команд, оценка радиационного фона
Федеральный	НЦУКС МЧС России, ФСБ России: стратегическое управление, международная координация
Международный	МАГАТЭ, профильные структуры сопредельных государств : стратегическое управление, международная координация

На практике функционирование этой структуры обеспечивается с помощью комплекса информационных и телекоммуникационных систем, включая:

- радиорелейные и спутниковые каналы связи, устойчивые к поражающим внешним воздействиям;
- защищённые цифровые каналы, функционирующие по закрытым протоколам;
- резервные линии, включая ПАКС, IP-телефонию, и ГАС «Выборы» (при межведомственном взаимодействии).

Анализ аварийных ситуаций, включая инциденты на АЭС «Три-Майл-Айленд» и «Фукусима-1», демонстрирует, что сбой любого звена в системе информационного обмена способен спровоцировать утрату или задержку критически важной информации, нарушение согласованности действий между уровнями реагирования и, как следствие, увеличение масштабов последствий аварии из-за несвоевременных, либо ошибочных решений.

В связи с этим обеспечение надёжности и отказоустойчивости информационной архитектуры приобретает принципиальное значение, особенно в условиях вероятностной природы отказов и высокой вероятности возникновения каскадных или комбинированных сценариев развития чрезвычайной ситуации.

Внешние и внутренние угрозы на объекты Росатома

Объекты Росатома, расположенные в пограничном пространстве, подвержены широкому спектру потенциально опасных воздействий. Условно их можно классифицировать по группам, представленным в таблице 3.

Классификация рисков позволяет не только систематизировать потенциальные источники угроз, но и выделить характерные сценарии развития ЧС, требующие адаптации архитектуры информационного обмена к мультифакторным условиям.

Таблица 3 — Типичные воздействия на ядерные объекты в пограничной зоне

Тип воздействия	Примеры	Потенциальные последствия
Природные	Землетрясения, наводнения, смерчи, молнии	Разрушение конструкций, отключение электроснабжения, выход из строя систем
Антропогенные (внешние)	Падение самолёта, взрывы на объектах инфраструктуры	Разгерметизация систем, пожар, отказ защитных систем
Антропогенные (внутренние)	Пожары, короткие замыкания, разрыв трубопроводов, взрыв газа	Массовый выход из строя оборудования, критическое повышение давления или температуры
Комбинированные	ЧС с участием человеческого фактора, аварии по общей причине	Потеря управляемости, каскадные отказы, затруднение информационного обмена

Расположение атомных объектов вблизи государственной границы усиливает воздействие ряда дестабилизирующих факторов. В таких регионах наблюдается ограниченность резервных логистических маршрутов, а также значительные трудности при координации с международными структурами гражданской обороны. Дополнительную сложность представляет собой возможность перекрёстного (трансграничного) влияния аварии, включая как природные, так и техногенные элементы.

Кроме того, при возникновении ЧС персонал может оказаться в условиях высокой неопределённости и стрессовой нагрузки, обусловленной нарушением управленческой вертикали, неясностью командных цепочек и разрывом каналов связи.

Например, землетрясение, превышающее уровень проектной сейсмичности, способно одновременно вывести из строя системы электроснабжения, локальные модули информационного обмена и насосные станции, что при отсутствии резервирования создаёт угрозу критического отказа.

Особенно уязвимыми оказываются каналы трансграничного оповещения и внешней координации, если инфраструктура на сопредельной территории также получает повреждение.

К числу наиболее деструктивных воздействий с малой вероятностью, но катастрофическими последствиями, относится падение летательного аппарата на территорию АЭС. При массе объекта порядка 20 тонн и скорости до 700 км/ч кинетическая энергия удара становится сопоставимой с уровнем прочностного ресурса защитной оболочки, особенно в случае устаревших или неукреплённых зданий.

Кроме того, подобное событие сопровождается вторичными факторами: взрывом авиатоплива, возникновением пожара, механическим разрушением систем безопасности и, как правило, потенциальным радиоактивным загрязнением территории. Несмотря на низкую оценочную вероятность (10^{-6} – 10^{-8} в год), данный сценарий рассматривается в проектных расчётах, особенно для объектов, находящихся вблизи аэропортов или маршрутов военной авиации.

Пожар является одним из наиболее вероятных источников внутренних отказов АЭС. Частота таких событий на ядерных объектах оценивается на уровне 10^{-1} реакторо-год.

Основные причины — короткие замыкания, возгорание кабельных трасс, перегрев оборудования, технологические ошибки при ремонте. В исторической перспективе значительный ущерб был нанесён в результате пожара на АЭС «Браунз-Ферри» (1975), когда огнём было повреждено более 2000 кабелей, включая цепи аварийного расхолаживания.

К числу малозаметных, но крайне опасных угроз относятся воздействия, характеризующиеся высокой скоростью и непредсказуемостью развития. Примером может служить образование летящих предметов вследствие разрыва трубопровода, разрушения вращающихся механизмов или взрыва газа. Такие объекты способны нарушить не только физическую целостность оборудования, но и непосредственно повредить сервера, узлы связи и каналы управления.

Кроме того, взрыв водорода или иных горючих газов, накопившихся в результате химических реакций, может инициировать цепную реакцию отказов с разрушением герметичных отсеков, коротким замыканием и дестабилизацией среды.

Дополнительную опасность представляет затопление — как результат разгерметизации трубопроводов или систем охлаждения. Оно способно вывести из строя ключевые компоненты информационной архитектуры, в том числе резервные блоки, расположенные в нижних ярусах зданий.

Особую сложность представляют собой сценарии, в которых одновременно реализуются несколько видов воздействий, усиливающих друг друга по эффекту домино. Примером может служить связка «землетрясение — пожар», где повреждение здания влечёт за собой возгорание кабельных трасс и обрыв каналов связи, или ситуация «технологический сбой — человеческая ошибка», в которой неправильная интерпретация сигналов тревоги ведёт к ухудшению ситуации.

Классическим примером является авария на АЭС «Три-Майл-Айленд» (1979), где совокупность технического отказа и неверных действий операторов привела к масштабному повреждению активной зоны реактора.

Такие события требуют особых архитектурных решений — дублирования каналов, автоматизации критических функций, а также регулярной подготовки персонала к действиям в условиях паники и разрушения стандартных алгоритмов управления.

Устойчивость информационного обмена при ЧС на объектах Росатома

В условиях чрезвычайной ситуации на ядерных объектах, особенно расположенных в приграничных регионах, критически важно обеспечить надёжный и непрерывный информационный обмен между всеми уровнями системы реагирования. Такая алгоритм должна сохранять работоспособность независимо от состояния внешней инфраструктуры, быть устойчива к физическим повреждениям и обеспечивать автоматическую маршрутизацию сигналов. Также принципиально значима синхронизация действий между участниками обмена, как на объекте, так и на ведомственном и федеральном уровнях.

Алгоритм опирается на иерархическую структуру, включающую как технические компоненты (датчики, каналы передачи, автоматизированные системы), так и человеческий фактор (операторы, диспетчеры, органы управления ЧС). Её целью является обеспечение устойчивой коммуникационной среды, способной функционировать в условиях разрушений, информационных перегрузок и временных ограничений.

Информационное взаимодействие в условиях ЧС организуется по принципу вертикальной передачи и согласования данных между управленческими уровнями.

Каналы информационного обмена и классификация передаваемой информации представлена в таблице 4.

Информационное взаимодействие между участниками системы реагирования при чрезвычайной ситуации может быть формализовано в виде направленного графа, где вершины соответствуют субъектам обмена, а рёбра — каналам передачи сообщений.

В рамках базового сценария информационный поток инициируется с уровня технологических датчиков и автоматизированных систем управления технологическими процессами (АСУ ТП), затем передаётся дежурному диспетчеру смены, переходит к оперативному штабу объекта, и далее — в ведомственные структуры, такие как Росатом и МЧС России. Оттуда информация поступает в Центр управления в кризисных ситуациях (ЦУКС), а при необходимости — в Федеральную службу безопасности или органы гражданской обороны, с последующим распространением среди населения средствами общественного оповещения.

Каждое звено выполняет функции верификации достоверности информации, минимизации задержек передачи, автоматического резервного дублирования критически важных данных, а также регистрации всех действий в лог-файлах с целью последующего аудита.

Таблица 4 – Каналы информационного обмена и классификация передаваемой информации

Категория	Вид / Тип	Описание
Каналы обмена	Оптоволоконные линии связи	Основные высокоскоростные каналы, обеспечивающие защищённую передачу данных
	Спутниковая и радиосвязь	Альтернативные каналы, устойчивые к разрушению наземной инфраструктуры
	Протоколы автоматизированного обмена	АСУ ОИАС, ЕДДС, СЗИ — для интеграции с системами управления ЧС
	Резервные системы оповещения	Дублирующие каналы, автономные терминалы, аварийные модемы и IP-связь
Типы информации	Сигнальная	Аварийные сигналы тревоги, подтверждения событий
	Ситуационная	Данные мониторинга: давление, температура, координаты и характеристики среды
	Оценочная	Прогноз развития ситуации, анализ угроз, риск-оценки
	Командная	Управляющие сигналы: приказы, инструкции, протоколы реагирования

Особое внимание уделяется обеспечению устойчивости всей архитектуры к отказам по общей причине, что особенно актуально в условиях мультифакторного воздействия.

Предлагаемая алгоритм построена на трёхуровневой иерархии, обеспечивающей вертикальную и горизонтальную координацию. На первом, тактическом уровне, происходит обмен телеметрическими данными и управляющими сигналами внутри объекта — между оборудованием, операторами и системами технологического контроля. Второй, оперативный уровень охватывает штабные и координационные структуры, осуществляющие сбор, фильтрацию и анализ информации, генерацию управляющих команд и распределение ресурсов. Наконец, стратегический уровень включает ведомственные и федеральные органы, ответственные за нормативное регулирование, стратегическое прогнозирование и международное взаимодействие в случае трансграничных инцидентов.

Алгоритм информационного взаимодействия предъявляет высокие требования к устойчивости архитектуры. Она должна сохранять функциональность при воздействии вибраций, пожаров, перебоев питания и разрушений инфраструктуры. Конструкция системы учитывает вероятность отказов, выраженную через интенсивность отказов $\lambda(t)$ вероятность безотказной работы $R(t)$ и среднюю наработку до отказа $T_{ср}$.

Предусмотрена возможность автоматического перехвата управляющих функций при выходе из строя нижестоящих уровней, а также совместимость с международными протоколами оповещения (например, IRMIS или Common Alerting Protocol). Неотъемлемой частью алгоритма является обеспечение подготовки персонала, основанной на стандартизированных сценариях реагирования и алгоритмах взаимодействия.

Проверка жизнеспособности модели осуществляется путём проведения имитационного моделирования, отработки различных сценариев учений (включая такие, как падение воздушного судна, утечка радиоактивных веществ, сбой связи и др.), а также интеграции с цифровыми двойниками объектов. Эффективность модели дополнительно оценивается через применение количественных надёжностных параметров: вероятности безотказной работы $R(t)=e^{-\lambda t}$, интенсивности отказов λ , и средней наработки до отказа $T_{ср}=1/\lambda$. Эти показатели позволяют объективно определить устойчивость архитектуры и обосновать необходимость резервирования ключевых узлов системы.

Данной системе необходимо обеспечить устойчивое функционирование на постоянной основе. Для оценки надёжности систем связи и управления используется экспоненциальное распределение времени наработки до отказа, адекватное для фазы нормальной работы оборудования (в период отсутствия износа):

$$F(t)=1-e^{-\lambda t}, f(t)=\lambda e^{-\lambda t}, t \geq 0$$

где λ — интенсивность отказов,

$F(t)$ — вероятность отказа к моменту времени t ,

$R(t)=1-F(t)=e^{-\lambda t}$ — вероятность безотказной работы,

$T_{ср}=1/\lambda$ — средняя наработка до отказа.

При $\lambda t \ll 1$ используется приближённое выражение:

$$F(t) \approx \lambda t \text{ (при условии высокой надёжности)}$$

Интенсивность отказов во времени имеет характерную U-образную форму:

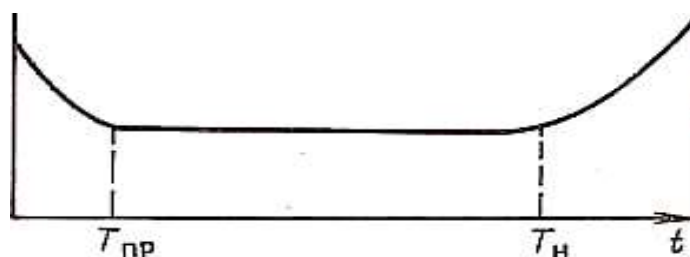


Рисунок 1 – Зависимость интенсивности отказов элемента от наработки

Таблица 5 – Зависимость интенсивности отказов элемента от наработки

Этап	Диапазон времени	Характер отказов
1. Приработка	$0 \leq t < T_{пр}$	Повышенная интенсивность (скрытые дефекты)
2. Нормальная эксплуатация	$T_{пр} \leq t \leq T_{н}$	Постоянная λ
3. Износ	$t > T_{н}$	Резкий рост отказов (старение)

Для расчётов второго периода (наиболее надёжного) целесообразно применять экспоненциальную алгоритм, особенно при анализе резервированных каналов передачи данных, маршрутизаторов и АСУ.

Для повышения надёжности ИТ-компонентов на объектах Росатома при ЧС:

- использовать физическое и логическое резервирование;
- обеспечивать географическое распределение узлов;
- внедрять автоматическое переключение на резерв при потере связи;
- регулярно тестировать оборудование на отказоустойчивость;
- применять алгоритмы самодиагностики и самовосстановления.

Устойчивость алгоритма информационного взаимодействия в условиях чрезвычайных ситуаций определяется её способностью сохранять функциональность и обеспечивать выполнение ключевых функций даже при воздействии разрушительных факторов.

К таковым относят отказ оборудования, природные катаклизмы, пожары, перебои в электроснабжении, влияние человеческого фактора и целенаправленные атаки на информационные ресурсы. В контексте обеспечения устойчивости особое внимание уделяется рискам отказов по общей причине (Common Cause Failure, CCF), скорости реакции на тревожные сигналы, наличию и готовности резервных каналов связи, а также способности модели адаптироваться к меняющимся условиям, сохраняя при этом приоритетный режим информационного обмена между уровнями управления.

Алгоритм информационного взаимодействия при чрезвычайных ситуациях на объектах Росатома с использованием технологии блокчейн

В современных условиях функционирования атомных объектов, для обеспечения выдвигаемых требований устойчивости системы, особенно тех объектов, что расположены вблизи государственной границы, особую актуальность приобретает построение защищённых, прозрачных и децентрализованных систем информационного взаимодействия. Одним из перспективных решений является интеграция технологии блокчейн в архитектуру оповещения и реагирования на чрезвычайные ситуации.

Предлагаемый алгоритм включает следующие ключевые компоненты:

1. Генератор сигнала - операторский интерфейс системного диспетчера или автоматизированного комплекса управления (АСУ ТП), обеспечивающий первичный ввод информации о возникшей ЧС.

2. Смарт-контракт - специализированный программный модуль, который регистрирует событие в распределённой базе, формируя уникальный блок с данными инцидента.

3. Участники системы - ведомственные и федеральные органы (Росатом, Ростехнадзор, МЧС России, ФСБ России), а также международные организации (например, МАГАТЭ), подключённые к системе оповещения.

4. Механизм подтверждения доставки - логика, реализующая отслеживание статуса получения сигнала каждым субъектом.

5. Интерфейс визуализации - аналитическая панель с географической картой, статусами реагирования и журналом блоков.

Функционирование системы начинается с поступления первичной информации о ЧС от датчиков или оперативного персонала. С помощью генератора сигнала осуществляется структуризация данных — выбор типа ЧС, геолокации и описание инцидента. Эти данные формируют JSON-объект, который автоматически передаётся в смарт-контракт.

Смарт-контракт записывает сигнал в блокчейн-цепочку, фиксируя:

- временную метку,
- идентификатор события,
- тип аварии,
- координаты объекта,
- хеш-ссылку на предыдущий блок,
- цифровую подпись оператора.

После этого система автоматически инициирует рассылку уведомлений всем зарегистрированным участникам взаимодействия. Каждый субъект подтверждает получение сигнала, при этом данные о доставке записываются в лог и визуализируются на аналитической карте.

Разработана блок-схема алгоритма информационного взаимодействия на основе блокчейна представлена на рисунке 2.

Алгоритм функционирования разработанной системы включает несколько последовательно реализуемых этапов, обеспечивающих оперативность, достоверность и прозрачность информационного обмена при реагировании на чрезвычайные ситуации.

Интерфейс управления предоставляет в режиме реального времени визуализацию статуса рассылки уведомлений, включая информацию о получателях, подтвердивших или не подтвердивших получение, а также о тех, кому сигнал доставлен не был. Данные отображаются в аналитическом модуле системы, что позволяет оперативно оценить полноту охвата оповещения.

Сохранение блока в неизменяемом журнале событий, который выполняет функцию аудита действий по каждому сигналу ЧС, обеспечивает возможность последующего анализа, формализации управленческих решений и формирования доказательной базы при необходимости.

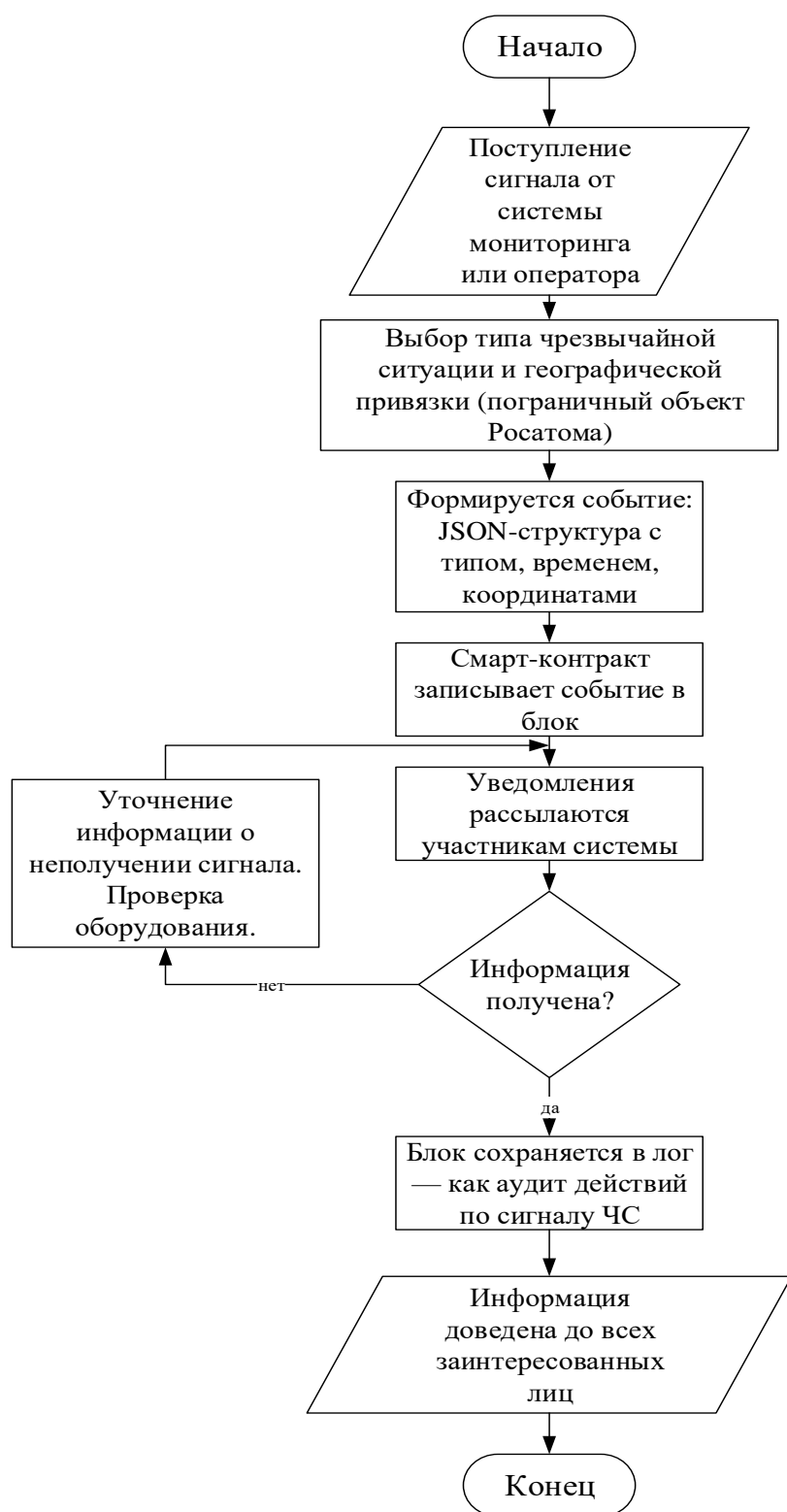


Рисунок 2 – Алгоритм информационного взаимодействия при чрезвычайных ситуациях на объектах Росатома с использованием технологии блокчейн

Заключение

Разработка алгоритма информационного взаимодействия в условиях чрезвычайных ситуаций на объектах Росатома, расположенных в пограничной зоне, позволила сформулировать

универсальный и технологически адаптируемый подход к управлению критическими сообщениями. В отличие от традиционных централизованных систем оповещения, предложенный алгоритм реализует децентрализованную фиксацию и отслеживание сигналов посредством блокчейн-технологии, что исключает возможность потери, искажения или несанкционированного удаления информации.

Рассмотренная структура алгоритма охватывает весь цикл информационного реагирования: от инициации сигнала до подтверждения доставки и визуализации статуса реагирования. Такой подход обеспечивает не только оперативность и прозрачность обмена, но и возможность последующего аудита и анализа эффективности действий всех задействованных субъектов. Интеграция алгоритма с системой цифровых двойников объектов и с международными протоколами (например, IRMIS и CAP) создаёт основу для построения комплексной цифровой платформы управления ЧС на ядерных объектах.

Интеграция методов количественной оценки надёжности технических элементов в алгоритм информационного взаимодействия позволяет создать гибкий и адаптируемый алгоритм обмена, устойчивый к отказам по общей причине и внешним дестабилизирующим факторам.

Таким образом, предложенный алгоритм может служить основой для внедрения современных решений в области информационной безопасности атомной отрасли и стать частью цифровой трансформации системы реагирования Росатома в условиях повышенной угрозы и геополитической нестабильности.

Литература

1. Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».
2. Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии».
3. ГОСТ Р 22.0.10–96. Безопасность в чрезвычайных ситуациях. Организация и ведение мониторинга.
4. ГОСТ Р 22.1.01–95. Безопасность в чрезвычайных ситуациях. Системы оповещения.
5. Международное агентство по атомной энергии (МАГАТЭ). IAEA Safety Standards Series No. GS-R-2.
6. Руководство по анализу надёжности элементов систем безопасности. М.: Росатом, 2021.
7. Мельников С.В. Надёжность технических систем и управление рисками. — М.: Академия, 2019.
8. Rasmussen N.C. Reactor Safety Study. WASH-1400. U.S. NRC, 1975.
9. Отчёт по результатам расследования аварии на АЭС Три-Майл-Айленд. U.S. NRC, 1980.
10. Чернобыльская АЭС: причины, последствия, уроки. Доклад МАГАТЭ, 1996.

Поступила в редакцию: 03.02.26

Принята к публикации: 20.03.26