Научная статья
УДК 004+519; DOI: 10.61260/2307-7476-2025-2-23-39

КОМПЛЕКСНАЯ МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ, ФУНКЦИОНАЛЬНОЙ И ПОЖАРНОЙ БЕЗОПАСНОСТИ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ В ТЕХНОСФЕРЕ

✉Тукмачева Марина Алексеевна;
Шестаков Александр Викторович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉mtukmacheva@mail.ru

Аннотация. Совокупность информационных, производственных рисков и их агрегирование в пожарной опасности имеют разрушительный характер для техносферы. Ограниченные несистемные исследования в области формального описания моделей информационной, функциональной и пожарной безопасности на опасных производственных объектах обусловливают необходимость развития комплексной математической модели применительно к техносфере. Рассмотрены математические модели на основе Марковских процессов, которые используются при решении различных задач для чрезвычайных ситуаций на опасных производственных объектах.

Ключевые слова: математическая модель, Марковская модель, информационная безопасность, функциональная безопасность, пожарная безопасность, опасный производственный объект, техносфера

Для цитирования: Тукмачева М.А., Шестаков А.В. Комплексная математическая модель информационной, функциональной и пожарной безопасности опасных производственных объектов в техносфере // Природные и техногенные риски (физико-математические и прикладные аспекты). 2025. № 2 (54). С. 23–39. DOI: 10.61260/2307-7476-2025-2-23-39.

Scientific article

A COMPLEX MATHEMATICAL MODEL OF INFORMATION, FUNCTIONAL, AND FIRE SAFETY OF DANGEROUS PRODUCTION FACILITIES IN THE TECHNOSPHERE

✉Tukmacheva Marina A.;
Shestakov Alexander V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉mtukmacheva@mail.ru

Abstract. The combination of information and production risks and their aggregation in fire hazards have a destructive effect on the technosphere. Limited and unsystematic research in the field of formal description of models of information, functional, and fire safety at hazardous production facilities necessitates the development of a comprehensive mathematical model for the technosphere. Mathematical models based on Markov processes are considered, which are used to solve various problems related to emergencies at hazardous production facilities.

Keywords: mathematical model, Markov model, information security, functional security, fire safety, hazardous production facility, technosphere

For citation: Tukmacheva M.A., Shestakov A.V. A complex mathematical model of information, functional, and fire safety of dangerous production facilities in the technosphere // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty) = Natural and man-made risks (physico-mathematical and applied aspects). 2025. № 2 (54). P. 23–39. DOI: 10.61260/2307-7476-2025-2-23-39

Введение

В техносфере значительную угрозу представляют собой опасные производственные объекты (ОПО). Сложные технологические процессы, наличие опасных материалов и уязвимости информационной безопасности высокоинтеллектуального производственного оборудования подвергают производственные объекты и их прилегающие территории серьезным потенциальным угрозам, связанным с технологическими процессами, такими как пожары, аварии, киберинциденты, негативные воздействия на людей и окружающую среду.

Анализ рисков – эффективный способ заблаговременной подготовки и организации превентивных мер и мероприятий, поскольку можно детализировать и уяснить, какой процесс и как выходит из-под контроля, и каким образом возможно предотвратить сбой.

Традиционные методы анализа рисков ориентированы, как правило, на обеспечение безопасности технологических процессов, при этом не в полной мере учитывают аспект технологических сбоев, обусловленных преднамеренными угрозами и воздействиями, известными как злонамеренные действия [1]. Внезапные злонамеренные действия в отношении технологических процессов целесообразно рассматривать в перечне процедур оценки рисков безопасности ОПО, особенно критических. Критически важные объекты, такие как производственные объекты или объекты информационной инфраструктуры, являются идеальной мишенью для преднамеренных разовых или нескольких атак одновременно [2].

Чрезвычайные ситуации и аварии, связанные с технологическими процессами, не являются единичными, включая пожары, взрывы и выбросы токсичных веществ [3].

К наиболее известным авариям и чрезвычайным ситуациям, связанным с промышленной безопасностью, относятся катастрофа на химическом предприятии по производству циклогексанона и капролактама во Фликсборо (Flixborough, Англия, 1974), химическом заводе во Севезо (Seveso, Италия, 1976), заводе по производству пестицидов Бхопале (Bhopal, Индия, 1984), взрыв на нефтеперерабатывающем заводе компании Бритиш Петролиум в Техас-Сити (США, 2005), катастрофа глубоководной нефтяной буровой платформы «Дипуотэ Хорайзон» в Мексиканском заливе (Deepwater Horizon, США, 2010), кибератака вируса Stuxnet на контроллеры системы управления технологическим производством SCADA по обогащению урана на предприятии атомной промышленности в Натанзе (Natanz, Иран, 2010).

Количество техногенных аварий с каждым годом не снижается, как показывают статистические данные МЧС России на рис. 1.

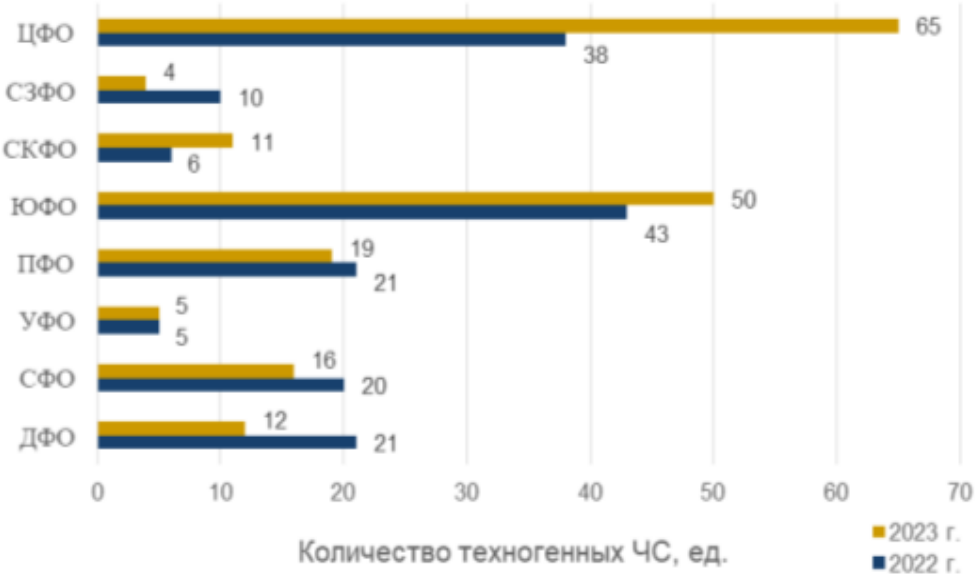

Рис. 1. **Динамика изменения числа техногенных чрезвычайных ситуаций в 2022–2023 гг. по федеральным округам (https://mchs.gov.ru)**

Количество чрезвычайных ситуаций техногенного характера в 2023 г. по сравнению с 2022 г. увеличилось на 11,6 % [4].

В связи с высокой динамикой развития городов и уплотнением застроек жилые кварталы вплотную приближаются к ОПО, что увеличивает риски масштаба аварии.

Для минимизации рисков возникновения техногенных аварий необходимо анализировать возможные угрозы возникновения неблагоприятных событий и применять заблаговременные профилактические мероприятия, которые в нормативно-технических документах по функциональной безопасности ОПО соотнесены с типовыми независимыми слоями защиты и методами снижения риска по ГОСТ Р МЭК 61511-3–2018 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности», которые должны снижать определенный риск по меньшей мере в 10 раз, как представлено на рис. 2.

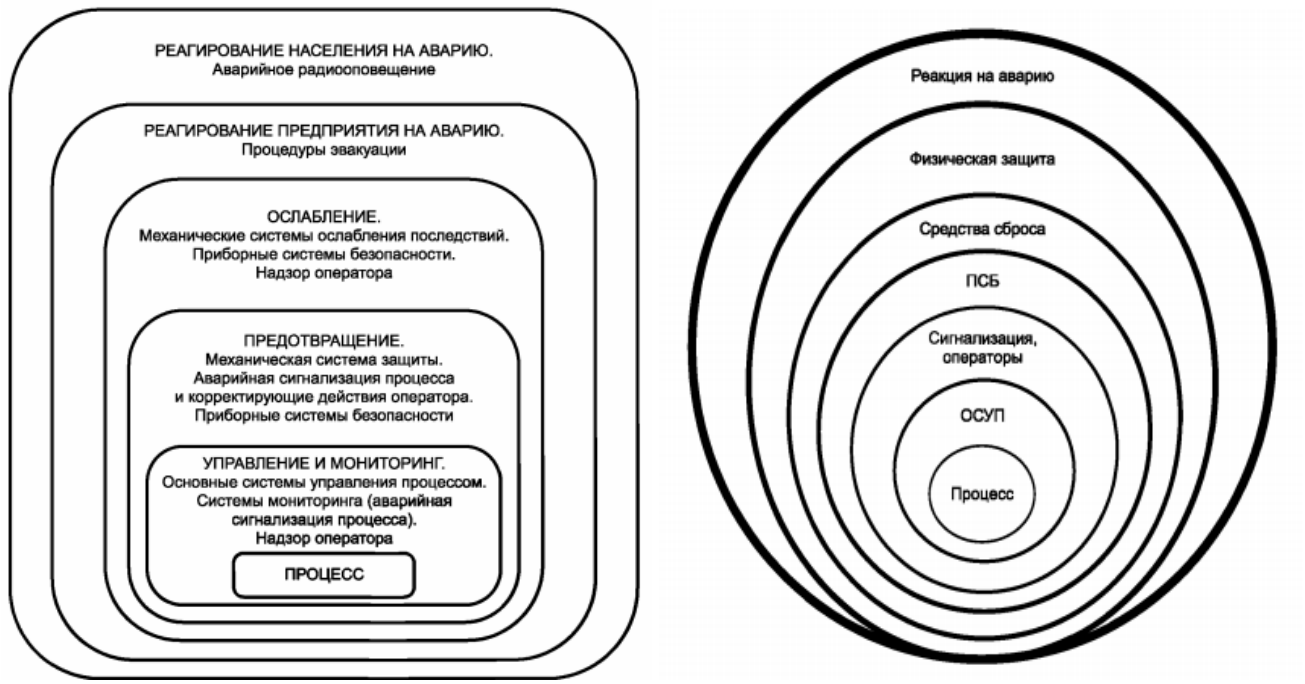

Рис. 2. **Типовые слои защиты ОПО (ГОСТ Р МЭК 61511-3–2018)**

Традиционные походы к системному описанию ОПО выражены в декомпозиции приборной системы (автоматизированная система управления технологическим процессом (АСУ ТП) на основную систему управления процессом (ОСУП или распределенную систему управления (РСУ) и приборную систему безопасности (ПСБ или систему противоаварийной автоматической защиты (ПАЗ), что отображено на рис. 3.

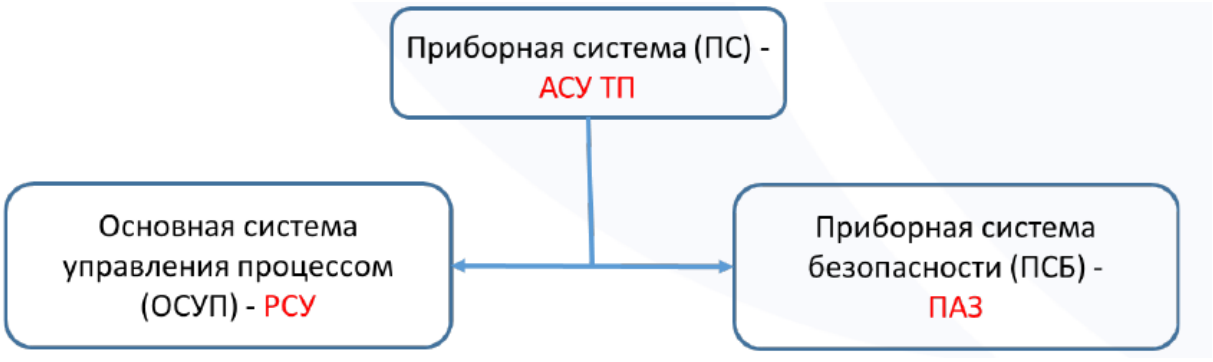

Рис. 3. **Декомпозиция приборной системы ОПО (СТО S.QS)**

Регламентированная нормативно-правовыми актами концепция снижения риска, например ГОСТ Р МЭК 61511-3–2018, применительно к реализации опасностей технологических процессов и послойному представлению системы защиты, отображена на рис. 4.

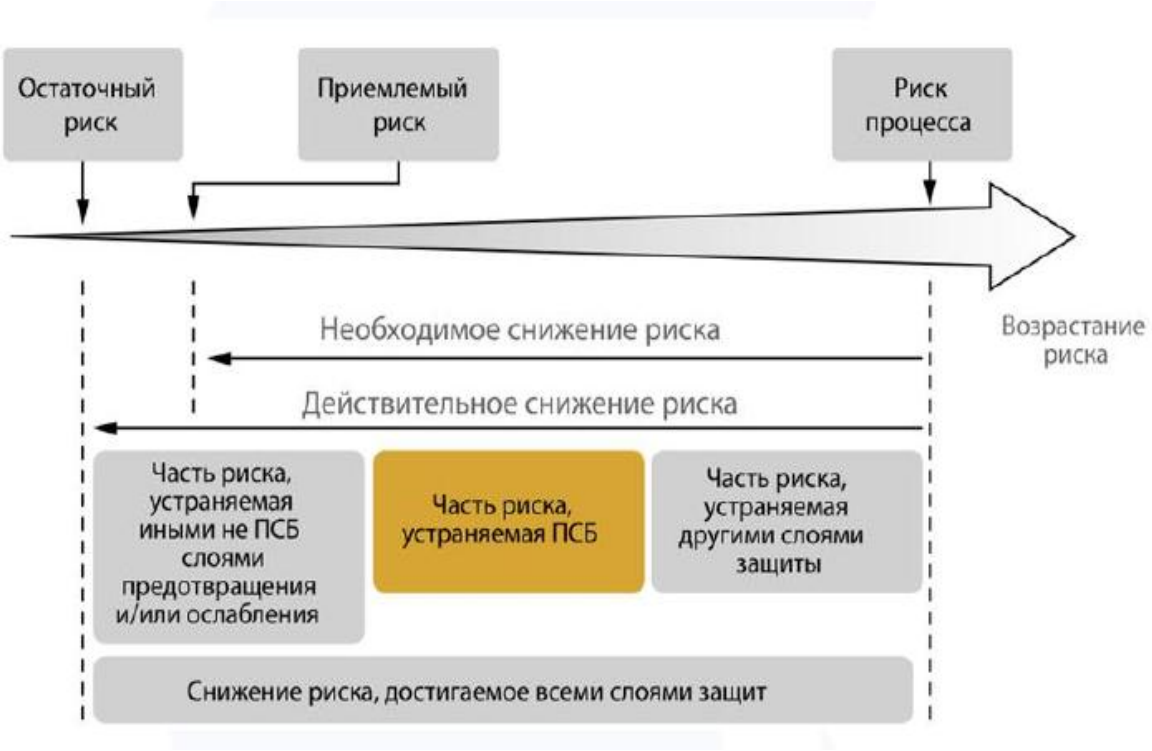

Рис. 4. **Организация снижения рисков (СТО S.QS)**

Подтвержденные факты воздействующих факторов и условий, которые обусловили возникновение чрезвычайных ситуаций и аварий, привели к пересмотру важности вновь разработанных, апробированных и доверенных методологий оценки рисков безопасности процессов [5], таких как:

– анализ опасностей и работоспособности HAZOP (HAZARD and OPERABILITY), гармонизированный в национальных стандартах, например, ГОСТ Р 51901.11–2005 «Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство», ГОСТ Р 27.012–2019 «Надежность в технике. Анализ опасности и работоспособности (HAZOP)», ГОСТ Р МЭК 61508–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования», ГОСТ Р МЭК 61511–2018 и стандартах организаций, например, СТО S.QS.6 (нефтегазовых предприятий, 2024);

– анализ уровней защиты LOPA (Layer of Protection Analysis) как метод оценки опасностей, рисков и уровней защиты, гармонизированный в национальных стандартах, например, ГОСТ Р 58771–2019 «Менеджмент риска. Технологии оценки риска», ГОСТ Р МЭК 62502–2014 «Менеджмент риска. Анализ дерева событий», ГОСТ Р МЭК 31010–2021 «Надежность в технике. Методы оценки риска»;

– количественная оценка рисков, представленная в ГОСТ Р 58970–2020 «Менеджмент риска. Количественная оценка влияния рисков на стоимость и сроки инвестиционных проектов», ГОСТ Р 51897–2021 «Менеджмент риска. Термины и определения».

Сформирован гармонизированный тезаурус рисков в различных предметных областях, основные сведения о которых сведены в табл. 1.

Таблица 1

Гармонизированный тезаурус рисков

№№ п/п	Перечень терминов	Семантические объекты определения термина	Нормативно-правовой акт
1	2	3	4
1	Авария	Разрушение. Неконтролируемый взрыв (выброс)	Федеральный закон от 21 июля 1997 г. № 116-ФЗ; СТО S.QS
2	Анализ опасности технологических процессов	Методология. Идентификация опасностей. Анализ опасности (работоспособности)	Приказ Ростехнадзора от 3 ноября 2022 г. № 387; СТО S.QS
3	Безопасность	Риск (отсутствие)	Приказ Ростехнадзора от 3 ноября 2022 г. № 387; СТО S.QS
4	Опасность	Источник. Вред (потенциальный)	ГОСТ Р 27.012–2019; ГОСТ Р 51897–2021; ГОСТ Р МЭК 61511–1; СТО S.QS
5	Опасное событие	Событие. Вред	ГОСТ Р МЭК 61511–1; СТО S.QS
6	Риск	1) Следствие влияния неопределенности. 2) Сочетание события и тяжести вреда	ГОСТ Р 27.012–2019; ГОСТ Р МЭК 61511–1; СТО S.QS
7	Риск процесса	Риск. Состояние процесса	ГОСТ Р МЭК 61511–1; СТО S.QS
8	Технологический процесс	Совокупность превращений или изменений параметров	ГОСТ Р 27.102–2021; СТО S.QS
9	Уровень риска	Мера. Комбинация нескольких видов рисков	ГОСТ Р 27.012–2019; СТО S.QS
10	Функциональная безопасность	Часть общей безопасности процесса. Зависимость от функционирования системы и слоев защиты	ГОСТ Р МЭК 61511–1; СТО S.QS

Существующее разнообразие качественных и количественных методов оценки рисков, как, например, подтверждается в приложении А ГОСТ Р ИСО/МЭК 31010 «Менеджмент риска. Методы оценки риска», основано на математических, статистических или графических моделях. Универсальный метод оценки рисков, применяемый для любого опасного производственного объекта, а также технологического процесса, отсутствует [6].

Одним из наиболее применяемых методов количественной оценки рисков (с возможностью получения количественных выходных данных), согласно ГОСТ Р ИСО 31010–2021, является математический аппарат Марковских процессов, который используется при анализе сложных восстанавливаемых систем.

Характерная ОПО связность информационной, функциональной и пожарной безопасности представляет собой взаимосвязь моделей, математически описывающая функционирование сложной системы [7]. Совокупность взаимосвязанных математических моделей представляет собой комплексную математическую модель и позволяет исследовать такие свойства, как надежность, прочность, долговечность и ряд других.

Для построения комплексной модели используется системный подход, методы имитационного моделирования и методы моделирования на основе Марковских процессов.

Рассмотрим более подробно особенности применения моделей Марковского процесса как случайного процесса, в котором вероятность нового состояния зависит только от состояния в настоящий момент времени и не зависит от предыдущих состояний.

Основная часть

Целью исследования является выявление ключевых аспектов, используемых для оценки рисков информационной, функциональной и пожарной безопасности технологических процессов и достоверности применяемых методов и моделей в промышленности.

В существующей практике нефтегазовой промышленности федеральными нормами и правилами (ФНиП) и ведомственными нормативными актами, регулирующими проведение анализа опасностей и оценку рисков аварий на ОПО, рекомендованы такие методы анализа риска, как «Проверочного листа» (структурированые или частично структурированные интервью); структурированный анализ сценариев методом «Что будет, если..» (SWIFT); идентификации опасностей (HAZID); анализ опасности и работоспособности объекта в целом (HAZOP); анализ видов и последствий отказов (FMEA); анализ видов, последствий и критичность отказов (FMECA); анализ дерева неисправностей/отказов (FTA); анализ дерева событий (ETA); анализ мер безопасности, слоев защиты (LOPA); анализ «Галстук-бабочка» (Bow-Tie); количественная оценка риска аварий (Quantitative Risk Assessment, QRA).

Результаты анализа доступных источников показывают, что, несмотря на обширные исследования методов оценки рисков безопасности технологических процессов в промышленности, взаимодействие рисков информационной, функциональной и пожарной безопасности технологических процессов на опасных производственных объектах и их совместная оценка с использованием подхода, основанного на устойчивости, надежности и достоверности, не были подробно изучены.

При проведении комплексной оценки рисков в промышленности, как указано в обзорном исследовании, выполненном в 2024 г. группой ученых Делфтского технологического университета (Delft University of Technology, Нидерланды) [5] крайне важно учитывать три аспекта: риск для безопасности технологического процесса, риск для безопасности производства и устойчивость технологического процесса.

В обзоре [5] обобщены существующие методы оценки рисков для безопасности технологического процесса и оценки рисков для безопасности производства, показаны возможности для внедрения концепции устойчивости, достоверности, подхода к моделированию для рассмотрения взаимодействия между рисками для безопасности технологического процесса и рисками для безопасности производства и их комплексного рассмотрения. Приведена оценка достоверности существующих методов и моделей в рамках опасных промышленных объектов.

Процессы в реальном времени могут быть как дискретными, так и непрерывными. Основная задача формальных моделей в вопросах безопасности состоит в том, чтобы охарактеризовать наблюдения как параметрический случайный процесс, параметры которого оцениваются с применением четкого и определенного подхода. Это позволит построить теоретическую модель основного процесса с возможностью прогноза выходных данных и определить статистические свойства наблюдений.

Результаты анализа преимуществ и недостатков основных методов оценки безопасности, защищенности и отказоустойчивости технологических процессов, представленные в государственном докладе [5], сведены в табл. 2.

Таблица 2

Анализ методов оценки рисков функциональной безопасности

Метод	Сильные стороны	Ограничения
1	2	3
Байесовский анализ. Байесовская сеть (Bayesian network, BN)	Формирует знания даже при разрежении данных. Применим для анализа сложных систем. Обновление в PMB	Чувствительность к выбору предшествующих состояний. Значительный вычислительный ресурс
Анализ «Галстук-бабочка» (Bow Tie Analysis)	Визуальное представление взаимосвязей между опасностями и угрозами. Комплексный подход как к преднамеренным, так и к непреднамеренным угрозам	Может упускать из виду определенные сценарии. Полагается на экспертные суждения и оценки. Может отсутствовать взаимозависимость между различными галстуками-бабочками

Метод	Сильные стороны	Ограничения
1	2	3
Анализ дерева событий (Risk management. Event tree analysis. ETA)	Систематическая визуализация последовательности событий. Определяет количественно вероятность различных исходов	Требуется четкое инициирующее событие. Он может не охватывать все возможные последовательности событий. Полагается на точные данные о вероятности каждого события
Анализ рисков, анализ аварий (Functional Resonance Analysis Method, FRAM)	Фокусируется на изменчивости и производительности систем. Подчеркивается влияние изменчивости на безопасность. Согласовывается с устойчивостью за счет ориентации на адаптивность	Требуется глубокое понимание функциональности системы. Его качественная природа может быть сложной для включения в традиционные методы. Ограниченные примеры практической реализации
Анализ дерева отказов (Fault Tree Analysis, FTA)	Графическое представление комбинаций отказов, приводящих к нежелательному событию. Количественный метод, позволяет рассчитать вероятность главного события. Помогает в выявлении первопричин сбоев	Сложный для больших систем. Требуются точные и исчерпывающие данные об отказах. Может не отражать динамические взаимодействия в системе
Анализ опасности и работоспособности HAZOP	Всестороннее выявление и анализ потенциальных опасностей. Способствует междисциплинарному сотрудничеству для проведения тщательной оценки. Высокая систематичность, обеспечивающая всесторонний охват режимов отказа	Менее точен для процессов со сложными взаимосвязями. Фокусируется на отдельных событиях, а не на комбинациях
Анализ мер безопасности (Layers of Protection Analysis, LOPA)	Для упрощения, количественной оценки и определения приоритетности рисков. Облегчает информирование о рисках между различными заинтересованными сторонами	Менее пригоден для работы с непредсказуемыми и качественными угрозами безопасности
Методика анализа рисков безопасности (Process Resilience Analysis Framework, PRAF)	Учитывает технические и социальные факторы. Обеспечивает количественную оценку с использованием данных о производительности установки	Отсутствует всестороннее сравнение с другими методами. Для больших систем может быть дорогостоящим с точки зрения вычислений. Предположительные ограничения, такие как нормальное распределение неопределенных параметров
Методика анализа рисков безопасности с учетом технических и социальных факторов (Resilience-based Integrated Process Systems Hazard Analysis, RIPSHA)	Интегративный метод, учитывает технические, человеческие и организационные факторы. Основан на инженерии устойчивости. Возможность адаптации в зависимости от жизненного цикла установки	Это может быть ресурсоемким и требовательным. Количественное сравнение с другими методами анализа опасности отсутствует. Требует обширного сбора данных из различных источников
Матрица рисков	Определение приоритетов рисков безопасности технологических процессов. Способствует четкому информированию о рисках. Для первоначальной проверки рисков безопасности	Потенциальное чрезмерное упрощение угроз безопасности. Полагается на качественные и субъективные оценки
Анализ безопасности сложных систем (Systems-Theoretic Accident Model and Processes, STAMP)	Аварии как системные сбои. Учет человеческих, организационных и технических факторов	Отсутствует формальная математическая основа. Отсутствуют конкретные уязвимости в крупномасштабных системах
Анализ рисков безопасности (Security and Vulnerability Assessment, SVA)	Комплексная оценка потенциальных угроз безопасности. Выявляет уязвимые места и предлагает контрмеры. Учет технических и человеческих факторов	Субъективизм оценок эксперта. Обновления при изменении ландшафта угроз. Не полный охват потенциальных уязвимостей
Марковский анализ	Применен к сложным системам, используя более высокий порядок процессов Маркова	Ограничен только моделью, математическими вычислениями и предположениями

Согласно представленному выше анализу, пять методологий – BN, FRAM, PRAF, RIPSHA и STAMP – являются особенно перспективными для комплексного подхода к технологической безопасности, защите и отказоустойчивости в промышленности.

В работе [8] предлагается прогнозная аналитика, основанная на усвоении данных для динамического моделирования рисков и сценариев надежности промышленных цифровых систем управления технологическими процессами с помощью последовательного метода Монте-Карло и метода фильтрации частиц на основе сопряженных функций (Markov/CCMT).

Результаты [9] показывают, что в рамках прогнозной аналитики на основе Марковских цепей/CCMT можно получать сверхточные прогнозы в режиме реального времени. Многоэтапное прогнозирование временных рядов для выявления состояний деградации на системном уровне и значимых с точки зрения рисков сценариев развития также может быть реализовано при использовании стратегии смешанного объединения и сокращения состояний в глубоком поиске моделей. Прогнозная аналитика на основе Марковских цепей/CCMT способна предоставлять интеллектуальным системам комплексных критически важных инженерных систем проактивную информацию.

Анализ рисков с использованием цифровых методов является важнейшим инструментом для разработки стратегий по предотвращению несчастных случаев и принятию мер по их смягчению. Использование цифрового анализа рисков в технологических процессах крайне актуально из-за проблем с мерами безопасности, возникающих в неблагоприятных условиях эксплуатации [10].

Метод оценки, разработанный в работе [11], позволяет научно рассчитать значение пожарного риска путем количественной оценки пожарного риска в зданиях. В сочетании с технологией BIM (информационное моделирование зданий) этот метод позволяет быстро и достоверно оценить пожароопасность целевой модели здания. На основе метода анализа пожароопасности для проектирования (FRAME) в работе [11] предлагается система оценочных индексов для зданий в периоды эксплуатации и технического обслуживания с точки зрения потенциального уровня риска, приемлемого уровня риска и уровня защиты.

Марковские процессы с дискретным и непрерывным временем

Рассмотрим применимость Марковских процессов с дискретным и непрерывным временем в зависимости от изменений состояний системы во времени.

Марковские процессы применимы в областях, где моделируются процессы случайной смены состояний в системе. Марковские процессы используются в таких сферах, как моделирование систем массового обслуживания, исследование технических систем (исправен – не исправен), моделирование принятия решений в ситуациях, когда результаты частично случайны, а частично находятся под контролем лица, принимающего решения. Применение Марковских методов регламентировано ГОСТ Р МЭК 61165–2019 для решения задач надежности в технике, а ГОСТ Р 51901.15–2005 – для оценки и анализа вероятностных характеристик технических систем на этапе оценки и анализа рисков.

Математическое описание Марковских процессов представляется в виде систем дифференциальных или алгебраических уравнений, решение которых, в общем случае, получить в явном виде не удается. Это требует применения численных методов решения систем дифференциальных или алгебраических уравнений.

Не все случайные процессы можно моделировать Марковскими процессами, поскольку некоторые процессы могут иметь более сложную структуру зависимостей между событиями. Также результаты моделирования могут быть неустойчивыми, если вероятности переходов между состояниями отличаются для разных начальных состояний.

Марковские процессы применимы в области информационной безопасности для решения широкого спектра задач, таких как: обнаружение вторжений в компьютерные системы; моделирование процессов распространения компьютерных вирусов; управление рисками информационной безопасности; моделирование процессов возникновения киберугроз

и эксплуатации уязвимостей в информационных и киберфизических системах; оптимизация и повышение надежности защищенных информационных систем.

В области функциональной безопасности Марковские процессы применимы для анализа работы систем, функционирование которых может быть представлено совокупностью состояний и переходов между ними. Подходит для разных условий, например, исследование систем с резервированием, отказ которых зависит от последовательности событий; анализ систем со сложной стратегией технического обслуживания и ремонта.

В области пожарной безопасности Марковские цепи используют для моделирования функционирования систем противопожарной защиты объектов, например автоматических установок пожаротушения. Можно определить вероятности состояний системы в процессе эксплуатации: режим готовности, временного отключения, срабатывания, восстановления готовности и тестирования. Позволяют оценить эффективность системы и выработать рекомендации по повышению ее эффективности.

Марковские процессы, переходящие из одного состояния в другое в определенные фиксированные моменты времени, являются дискретными Марковскими процессами. Такие процессы целесообразны для моделирования поведения сложных систем, находящихся в различных состояниях. Процессы применимы в прогнозировании надежности технических систем [6], оптимизации производительности телекоммуникационных сетей, при расчете среднего времени пребывания в каком-либо состоянии [12, 13] и др.

В ситуации моделируемого процесса с дискретным временем система S имеет n возможных дискретных состояний: S_1, S_2, ..., S_n. Изменение состояний происходит незамедлительно и четко фиксированные моменты времени t_i, i = 1, 2, …. Состояния выражают обычно с помощью графа состояний и переходов (рис. 5), где также изображены значения вероятностей переходов.

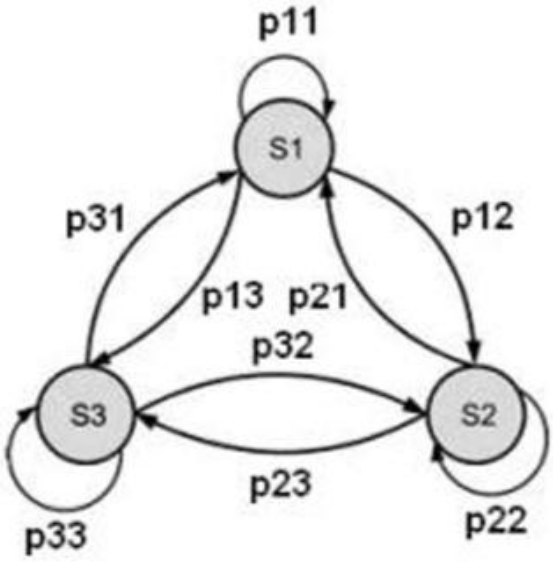

Рис. 5. **Граф состояний и переходов с дискретным временем ([6])**

Граф состояний, содержащего n вершин, можно представить в виде матрицы вероятностей переходов размером $n \times n$, элементами которой будут вероятности переходов p_{ij} между вершинами графа:

$$||P_{ij}|| = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix},\ 0 \le p_{ij} \le 1,\ \sum_{j=1}^{n} p_{ij} = 1.$$

На ОПО переход из одного состояния технологических процессов системы в другое может происходить как в результате отказа или восстановления элемента системы, так и при воздействии внешних событий, такие как угрозы информационной безопасности на программное обеспечение технологического процесса или человеческие ошибки.

Исследуемая система может находиться в одном из состояний: S_1, S_2, ..., S_n. После любого шага *k* может осуществиться какое-либо несовместимое событие: $S_1^{(k)}$, $S_2^{(k)}$, …, $S_n^{(k)}$. Вероятность событий для *k*-го шага можно выразить:

$$p_1(k) = p(S_1^{(k)}),\ p_2(k) = p(S_2^{(k)}),\ \ldots,\ p_j(k) = p(S_j^{(k)}),\ \ldots,\ p_n(k) = p(S_n^{(k)}).$$

Таким образом, для каждого шага *k* соответствует равенство:

$$p_1(k) + p_2(k) + \cdots + p_j(k) + \cdots + p_n(k) = 1.$$

Вероятности $p_j(k)$, $j = \overline{1,n}$ являются вероятностями состояний.

При оценке риска аварии на ОПО или поломки технологического процесса некоторой технической системы с состояниями S_1, S_2, ..., S_n необходимо определить вероятности состояний системы после *k*-го шага.

Математической моделью нахождения вероятностей состояний однородной Марковской цепи является рекуррентная зависимость:

$$p_j(k) = \sum_{i=1}^{n} p_i(k-1)p_{ij},$$

где $p_j(k)$ – вероятность *j*-го состояния системы после *k*-го шага, $j = \overline{1,n}$; $p_i(k-1)$ – вероятность *i*-го состояния системы после $(k-1)$-го шага, $i = \overline{1,n}$; p_{ij} – вероятности переходов системы из состояния S_i к состоянию S_j; *n* – количество состояний системы.

Оценка рисков некоторой системы технологического процесса на ОПО возможна с применением Марковского анализа. Система может находиться в работоспособном состоянии и неработоспособном состоянии, при отказе в обслуживании система способна восстанавливаться. Система начинает полноценно функционировать при *t*=0 и может перейти к неработоспособному состоянию через другие функциональные состояния, имеющие меньшее количество функционирующих элементов.

По схеме дискретных Марковских процессов в работе [6] предложена методика оценки рисков в пять этапов: определить состояния системы S_1, S_2, ..., S_n; определить конечное число возможных состояний системы; составить и разметить граф состояний; определить исходное состояние; по рекуррентной зависимости определить вероятности $p_j(k)$, $j = \overline{1,n}$.

Реализация Марковского процесса также возможна в представлении последовательности переходов из одного состояния в другое в виде цепи. Чтобы определить, в какое новое состояние может перейти процесс из текущего *i*-го состояния, необходимо разбить интервал [0; 1] на подынтервалы с соответствующей вероятностью и с помощью генератора случайных чисел получить случайное число и определить, в какой из интервалов оно попадает. Таким способом, результатом работы модели является Марковская цепь.

Непрерывные Марковские процессы целесообразны для моделирования задач, связанных со случайной динамикой систем. В случае перехода из одного состояния в другое в заранее неизвестный, случайный момент времени Марковский процесс является с непрерывным временем. Процесс применим в оценке надежности технических систем, моделировании процессов, исследовании систем массового обслуживания.

В случайном процессе при $0 \le t_1 \le t_2 \le \ldots \le t_{n+1}$ выполняется следующее условие:

$$P(S(t_{n+1}) = S_{n+1} | S(t_1) = S_1, \ldots, S(t_n) = S_n) = P(S(t_{n+1}) = S_{n+1} | S(t_n) = S_n).$$

В системе с непрерывным временем также рассмотрены дискретные состояния S_1, S_2, ..., S_n, переход в которых может происходить в любой, случайный момент времени, а сумма вероятностей состояний равна единице для любого момента времени *t*:

$$\sum_{i=1}^{n} p_i(t) = 1.$$

В Марковском процессе с непрерывным временем задаются интенсивности переходов:

$$\lambda_{ij} = lim_{\Delta t \to 0} \frac{p_{ij}(\Delta t)}{\Delta t},$$

где $p_{ij}(\Delta t)$ – вероятность перехода системы из состояния S_i в состояние S_j за время Δt.

Диаграмму состояния переходов с непрерывным временем можно представить в виде графа с интенсивностью отказа каждого элемента λ и интенсивностью обновлений μ (рис. 6).

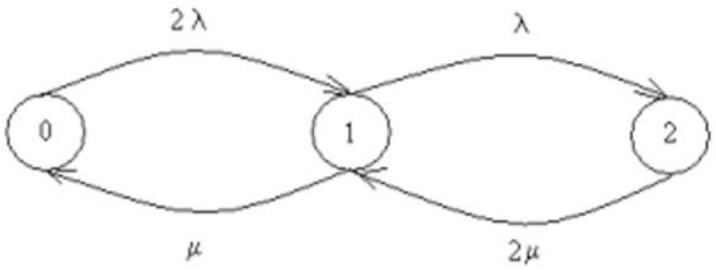

Рис. 6. **Граф состояний и переходов с непрерывным временем [6]**

Предположим, что некоторый технологический процесс на ОПО состоит из двух последовательных событий, для надежной работоспособности системы оба эти элемента должны работать. На рис. 6 рассмотрены состояния элементов: состояние 0 (оба элемента в работоспособном состоянии); состояние 1 (один элемент отказал, другой в работоспособном состоянии); состояние 2 (оба элемента отказали). Переходы состояний являются статистически независимыми событиями и интенсивность отказов λ и интенсивность обновлений μ постоянны.

Для данной системы матрица переходов принимает вид:

$$\|p_{ij}\| = \begin{vmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{vmatrix}.$$

Система уравнений будет иметь вид:

$$\begin{cases} -2\lambda p_0 + \mu p_1 = 0 \\ 2\lambda p_0 - (\lambda+\mu)p_1 + 2\mu p_2 = 0 \\ \lambda p_1 - 2\mu p_2 = 0 \\ p_0 + p_1 + p_2 = 1 \end{cases}.$$

Решение системы уравнений будет следующее:

$$p_0 = \frac{\mu^2}{\mu^2+2\mu\lambda+\lambda^2}, p_1 = \frac{2\lambda\mu}{\mu^2+2\mu\lambda+\lambda^2}, p_2 = \frac{\lambda^2}{\mu^2+2\mu\lambda+\lambda^2}.$$

Необходимую работоспособность системы можно выразить как:

$$A(t) = p_0 + p_1 = \frac{\mu^2+2\lambda\mu}{(\mu+\lambda)^2} .$$

Применимость подхода возможна для оценки рисков технических систем, состоящих из нескольких элементов, включенных параллельно или последовательно, имеющие причины для отказов и восстановлений.

В работе [6] сформулирована методика оценки рисков технических систем по схеме непрерывных Марковских процессов, состоящая из четырех этапов: определить состояния системы и интенсивности переходов (отказа и восстановления); составить и разметить граф состояний; составить систему дифференциальных уравнений Колмогорова; определить начальные условия и решить систему дифференциальных уравнений.

Скрытая Марковская модель

Одной из статистических моделей является скрытая Марковская модель. Данная модель анализирует последовательность наблюдаемых символов и интерпретирует процесс, который может остаться вне наблюдений. Состояния такой модели являются скрытыми или определяются только по наблюдаемым символам.

Простым примером дискретного Марковского процесса является случайный переход в одном измерении. Применительно к рассматриваемому исследованию нарушение информационной безопасности приведет к нарушению функциональной, а нарушение функциональной безопасности – к нарушению пожарной и аналогично в обратном порядке. В этом случае угрозы возникновения инцидентов функциональной безопасности могут перемещаться с определенной вероятностью в обе стороны.

Формально можно определить независимые случайные величины q_1, q_2, ... q_t, где каждая переменная принимает значение +1 (движение вперед) или −1 (движение назад) с вероятностью 50 % для каждого значения.

Статистически случайные события можно определить последовательностью q_t случайных величин, которые увеличиваются с помощью независимых и одинаково распределенных случайных величин S, таких что:

$$Q_n = \sum_{t=1}^{n} q_t$$

при $Q_0=0$, где математическое ожидание $E(Q_n) = 0$, а дисперсия $E(Q_n^2) = n$. Если $S_1, S_2, \ldots S_N$ – последовательность целых чисел, то:

$$P\ (q_{t+1}=S_j \mid q_t=S_i,\ q_{t-2}=S_k,) = P(q_{t+1}=S_j \mid q_t=S_i). \quad (1)$$

Уравнение (1) показывает, что вероятность того, что случайное событие окажется в точке S_j в момент времени $t + 1$, зависит только от его значения в настоящий момент времени, а не от того, как это событие образовалось и откуда оно появилось. Формально дискретный Марковский процесс допускает три определения, описанные в работе [14].

Стохастический процесс, характеризующийся моделью Маркова, может быть слишком ограниченным. Для повышения гибкости модели необходимо расширить модель, в которой наблюдаемый результат является вероятностной функцией состояния. Каждое состояние может давать несколько результатов в соответствии с уникальным распределением вероятностей, и каждый отдельный результат потенциально может быть получен в любом состоянии (рис. 7).

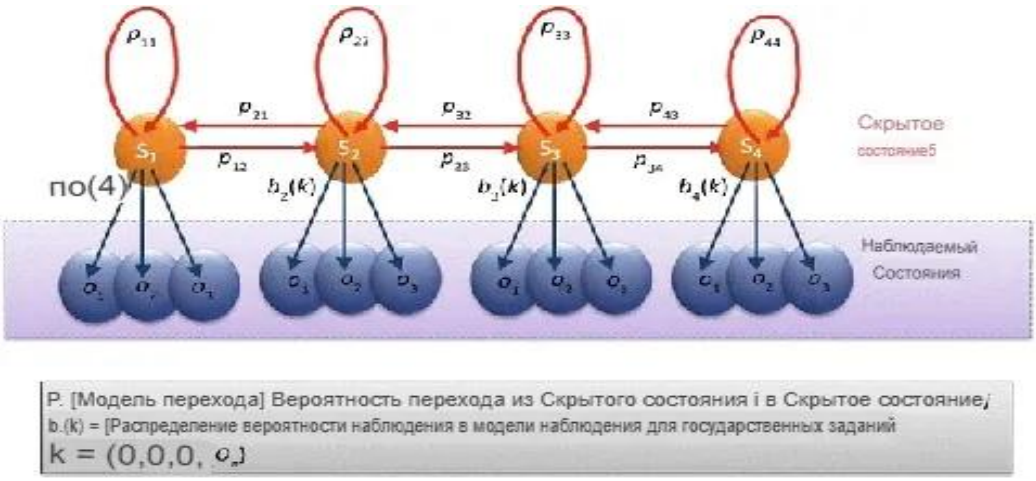

Рис. 7. **Скрытая Марковская модель с четырьмя скрытыми состояниями и тремя наблюдаемыми состояниями [14]**

На основе исследований в работе [14] модель можно применить к безопасности на ОПО. Модель представляет собой двойную вложенную стохастическую модель, что является скрытой Марковской моделью. Базовый стохастический процесс в модели создает последовательность состояний, которая не поддается непосредственному наблюдению и может быть только приблизительно описана с помощью другого набора стохастических процессов, создающих последовательность наблюдений (рис. 8).

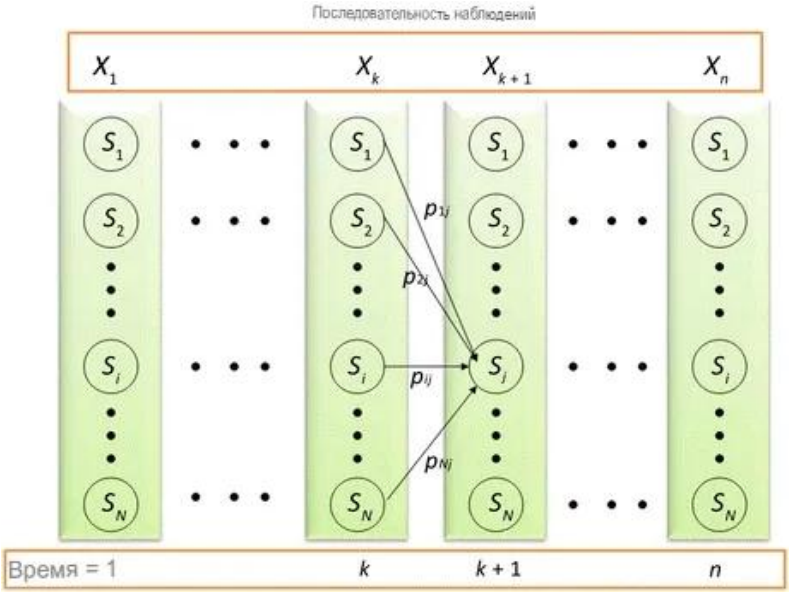

Рис. 8. **Скрытая Марковская модель: представление матрицы состояний [14]**

Ключевое отличие скрытой Марковской модели от обычной цепи Маркова заключается в анализе последовательности наблюдаемых состояний и возможности расчета вероятности возникновения определенной последовательности состояний. Это указывает на то, что последовательность состояний скрыта и может быть обнаружена только через последовательность наблюдаемых состояний или символов.

Специфика скрытой Марковской модели требует формального определения таких элементов, как количество скрытых состояний (N), распределение вероятностей перехода из состояния в состояние, вероятностей символов наблюдения и самих символов наблюдения.

В модели отдельные скрытые состояния представлены как $S=\{S_1, S_2, \ldots S_N\}$, а состояние в момент времени t представлено как q_t.

Для представления перехода из состояния i в состояние j распределение вероятностей представлено как $P=\{P_{ij}\}$, где:

$$p_{ij} = P(q_{t+1}=S_j \mid q_t=S_i)$$

при $1 \le i, j \le N$, $p_{ij} \ge 0$.

Распределение вероятностей символов наблюдения для состояния j представлено в виде $B=\{b_j(k)\}$, где:

$$b_j(k) = P(x_t=o_k \mid q_t=S_i)$$

при $1 \le j \le N$, $1 \le k \le M$.

Распределение начального состояния представлено в виде $\pi=\{\pi_i\}$, где:

$$\pi_i = P(q_1=S_i)$$

при $1 \le i \le N$.

Для физического процесса при определении параметров скрытой Марковской модели соответствующими значениями N, M, P, B, π можно будет проанализировать последовательность наблюдений (выходов) $x_1, x_2, x_3, \ldots$, в которой каждый x_t является одним из символов матрицы наблюдений O в момент времени t.

Формально скрытую Марковскую модель можно определить, указав параметры модели N и M, символы наблюдений O и три матрицы вероятностей P, B и π. Для упрощения выражения можно использовать формулу:

$$\lambda = (P, B, \pi).$$

Описанная скрытая Марковская модель имеет два допущения:

– Марковское предположение, что текущее состояние зависит только от предыдущего состояния – это представляет собой память модели;

– предположение о независимости, что выходной сигнал O_t в момент времени t зависит только от текущего состояния, то есть он не зависит от предыдущих наблюдений и состояний.

Заключение

Заблаговременное обнаружение рисков, их оценка и контроль имеют решающее значение для обеспечения безопасности в цифровизированных отраслях промышленности.

Анализ методов оценки рисков безопасности показал, что зарубежные научные работы и авторы вносят значительный вклад в развитие методов и моделей оценки рисков информационной, функциональной и пожарной безопасности технологических процессов. При этом следует учитывать необходимость адаптации некоторых из них к условиям российской промышленности и законодательным требованиям.

Для успешного применения математического аппарата Марковских процессов с дискретными состояниями для оценки надежности любой технической системы необходимо проработать полный список всех состояний системы (например, полное функционирование, частичное функционирование (ухудшение состояния), отказ, восстановление). Также необходимо понимать возможные переходы из состояния в состояние системы и знать вероятность переходов (p_{ij}) для систем с дискретным временем или интенсивность отказа (λ) и интенсивность восстановления (μ) для систем с непрерывным временем.

Главным преимуществом применения методов Марковского анализа с учетом всех ограничений является то, что стратегии технического обслуживания, например, приоритеты восстановления, можно легко смоделировать [15]. Кроме того, в модели можно отразить порядок, в котором происходят многократные отказы. Вместе с тем данный подход к оценке

рисков технических систем имеет ряд недостатков. Например, количество состояний системы и возможных переходов возрастает с увеличением количества элементов системы. В случае большого количества состояний технической системы наблюдается значительная вероятность ошибок и неточностей. При этом прогнозирование надежности технических систем с помощью математического аппарата Марковских процессов обеспечивает повышение эффективность их работы, профессиональной безопасности работников, а, следовательно, снижение экономических рисков предприятия.

Скрытую Марковскую модель можно использовать на опасных производственных объектах в представлении стохастической модели дискретных событий и разновидности цепи Маркова как цепочки связанных состояний или событий в области информационной, функциональной и пожарной безопасности, в которой следующее состояние зависит только от текущего состояния системы.

Учитывая рост рисков в области информационной, функциональной и пожарной безопасности на ОПО, а также различные угрозы безопасности в техносфере, появляется потребность в целостных методах, которые объединяют безопасность процессов, их защищенность, надежность и устойчивость.

Результаты выполненного анализа подтверждают необходимость дальнейших исследований в данном направлении с целью повышения уровня безопасности ОПО и минимизации рисков возникновения аварийных и опасных ситуаций.

Список источников

1. Baybutt P. Issues for security risk assessment in the process industries // J. Loss Prev. Process. Ind. 2017. № 49. P. 509–518.

2. A holistic framework for process safety and security analysis / Md T. Amin [et al.] // Comput. Chem. Eng. 2022. 2022. № 165.

3. Meyer T., Reniers G. Engineering risk management. Walter de Gruyter GmbH & Co KG, 2022.

4. Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review / M.Sh. Ab Rahim [et al.] // Journal of Loss Prevention in the Process Industries. 2024. Vol. 88. P. 105274. DOI: 10.1016/j.jlp.2024.105274. EDN IMLZLS.

5. О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2023 году: гос. доклад. М., 2024.

6. Ивахненко Н.Н. Особенности оценки надежности технических систем // Наука и перспективы. 2020. № 1. С. 56–67. EDN UOMLAV.

7. Тукмачева М.А., Шестаков А.В. Модель связности информационной, функциональной и пожарной безопасности опасных производственных объектов // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 98–126. DOI: 10.61260/2218-130X-2024-3-98-126. EDN ANQYHG.

8. Coupling of adjoint-based Markov/CCMT predictive analytics with data assimilation for real-time risk scenario forecasting of industrial digital process control systems / J. Chenyua [et al.] // Process Safety and Environmental Protection. 2023. Vol. 171. P. 951–974.

9. Bryan DFH, Ceng FIEE. Operation and Maintenance: Telecommunications Engineer's Reference. 1993.

10. Safety and risk analysis in digitalized process operations warning of possible deviating conditions in the process environment / C. Benson [et al.] // Process Safety and Environmental Protection. 2021 Vol. 149. P. 750–757.

11. Fire risk assessment for building operation and maintenance based on BIM technology / L. Wang [et al.] // Building and Environment. 2021. Vol. 205. P. 108188.

12. Андросенко О.С., Девятченко Л.Д., Маяченко Е.П. Постановка и решение задач Марковских процессов на ЭВМ: метод. указания и варианты контрольных заданий для студентов всех специальностей. Магнитогорск: ГОУ ВПО «МГТУ», 2007. 51 с.

13. Матвеев А.В. Методы моделирования и прогнозирования. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2022. 230 с. EDN IMLKWS.

14. Awad M., Khanna R. Hidden Markov Model. In: Efficient Learning Machines. Apress, Berkeley, CA, 2015.

15. Воднев С.А., Максимов А.В., Матвеев А.В. Модель комплексной оценки процесса технического обеспечения аварийно-спасательных средств подразделений МЧС России // Проблемы управления рисками в техносфере. 2018. № 2 (46). С. 73–80. EDN YLLCZN.

References

1. Baybutt P. Issues for security risk assessment in the process industries // J. Loss Prev. Process. Ind. 2017. № 49. P. 509–518.

2. A holistic framework for process safety and security analysis / Md T. Amin [et al.] // Comput. Chem. Eng. 2022. 2022. № 165.

3. Meyer T., Reniers G. Engineering risk management. Walter de Gruyter GmbH & Co KG, 2022.

4. Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review / M.Sh. Ab Rahim [et al.] // Journal of Loss Prevention in the Process Industries. 2024. Vol. 88. P. 105274. DOI: 10.1016/j.jlp.2024.105274. EDN IMLZLS.

5. O sostoyanii zashchity naseleniya i territorij Rossijskoj Federacii ot chrezvychajnyh situacij prirodnogo i tekhnogennogo haraktera v 2023 godu: gos. doklad. M., 2024.

6. Ivahnenko N.N. Osobennosti ocenki nadezhnosti tekhnicheskih sistem // Nauka i perspektivy. 2020. № 1. S. 56–67. EDN UOMLAV.

7. Tukmacheva M.A., Shestakov A.V. Model' svyaznosti informacionnoj, funkcional'noj i pozharnoj bezopasnosti opasnyh proizvodstvennyh ob"ektov // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2024. № 3. S. 98–126. DOI: 10.61260/2218-130X-2024-3-98-126. EDN ANQYHG.

8. Coupling of adjoint-based Markov/CCMT predictive analytics with data assimilation for real-time risk scenario forecasting of industrial digital process control systems / J. Chenyua [et al.] // Process Safety and Environmental Protection. 2023. Vol. 171. P. 951–974.

9. Bryan DFH, Ceng FIEE. Operation and Maintenance: Telecommunications Engineer's Reference. 1993.

10. Safety and risk analysis in digitalized process operations warning of possible deviating conditions in the process environment / C. Benson [et al.] // Process Safety and Environmental Protection. 2021 Vol. 149. P. 750–757.

11. Fire risk assessment for building operation and maintenance based on BIM technology / L. Wang [et al.] // Building and Environment. 2021. Vol. 205. P. 108188.

12. Androsenko O.S., Devyatchenko L.D., Mayachenko E.P. Postanovka i reshenie zadach Markovskih processov na EVM: metod. ukazaniya i varianty kontrol'nyh zadanij dlya studentov vsekh special'nostej. Magnitogorsk: GOU VPO «MGTU», 2007. 51 s.

13. Matveev A.V. Metody modelirovaniya i prognozirovaniya. SPb.: S.-Peterb. un-t GPS MCHS Rossii, 2022. 230 s. EDN IMLKWS.

14. Awad M., Khanna R. Hidden Markov Model. In: Efficient Learning Machines. Apress, Berkeley, CA, 2015.

16. Vodnev S.A., Maksimov A.V., Matveev A.V. Model' kompleksnoj ocenki processa tekhnicheskogo obespecheniya avarijno-spasatel'nyh sredstv podrazdelenij MCHS Rossii // Problemy upravleniya riskami v tekhnosfere. 2018. № 2 (46). S. 73–80. EDN YLLCZN.

Информация о статье:
Статья поступила в редакцию: 28.04.2025; одобрена после рецензирования: 20.05.2025;
принята к публикации: 01.06.2025

The information about article:
The article was submitted to the editorial office: 28.04.2025; approved after review: 20.05.2025;
accepted for publication: 01.06.2025

Сведения об авторах:
Тукмачева Марина Алексеевна, адъюнкт Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), e-mail: mtukmacheva@mail.ru, https://orcid.org/0009-0004-2496-7117
Шестаков Александр Викторович, заместитель начальника университета (по работе с личным составом), ведущий научный сотрудник отдела информационного обеспечения населения и технологий информационной поддержки РСЧС и пожарной безопасности Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, e-mail: alexandr.shestakov01@yandex.ru, https://orcid.org/0000-0002-8462-6515, SPIN-код: 5831-5451

Information about the authors:
Tukmacheva Marina A., adjunct of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), e-mail: mtukmacheva@mail.ru, https://orcid.org/0009-0004-2496-7117
Shestakov Alexander V., deputy head of the university (personnel affairs), leading researcher at the department of information support for the population and information support technologies for the Unified state system for emergency prevention and elimination of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of engineering sciences, e-mail: alexandr.shestakov01@yandex.ru, https://orcid.org/0000-0002-0778-32180000-0002-8462-6515, SPIN: 5831-5451