https://doi.org/10.18322/PVB.2020.29.02.6-16
ОРИГИНАЛЬНАЯ СТАТЬЯ / ORIGINAL PAPER
УДК 614.8.084

Методология синтеза адаптивной системы комплексной безопасности на предприятии жизнеобеспечения населения региона

© **Е. В. Гвоздев**✉

Национальный исследовательский Московский государственный строительный университет (Россия, 129337, г. Москва, Ярославское шоссе, 26)

РЕЗЮМЕ

Введение. Решение задач, связанных с качественным оказанием услуг населению городов (водоснабжение, энергоснабжение, горячее водоснабжение, отопление, утилизация отходов), является неотъемлемой частью работы органов власти (региональных образований, регионов, субъектов, муниципалитетов, их округов). К организациям, оказывающим данные услуги, относятся предприятия жизнеобеспечения населения, в технологическом процессе которых, как правило, задействованы участки (площадки) опасных производственных объектов. На таких предприятиях предложено создавать систему комплексной безопасности, которая объединяет все отраслевые (ведомственные) подсистемы безопасности и является неотъемлемой частью их системы управления. Устойчивое функционирование рассматриваемых предприятий во многом зависит от ресурсной обеспеченности (финансовые и материальные средства, время, персонал и т. д.) созданной на предприятии системы комплексной безопасности, которая имеет ограничения по объему. До сих пор на практике распределение ресурса для поддержания комплексной безопасности осуществляется на основе интуитивных соображений руководителей направлений безопасности предприятия. При таком подходе созданная на предприятии система комплексной безопасности становится уязвимой.

Методы исследования. Проанализированы подходы с использованием существующих методов в комплексной безопасности предприятий, рассмотрены особенности их применения. Предложено совместное применение метода анализа иерархий и метода построения “дерева событий”, с помощью которых появляется возможность определить исходные инициирующие события, установить факт возникновения опасности, реализовать попытку спрогнозировать возможные сценарии воздействия опасностей на объекты защиты предприятий жизнеобеспечения населения.

Постановка задачи. Комплексная безопасность предприятий жизнеобеспечения населения характеризуется состояниями, рассматриваемыми в определенный момент времени, отклонение от параметров функционирования которых может привести к сбою в деятельности как отдельной отраслевой подсистемы безопасности, так и системы комплексной безопасности предприятия в целом. На основании информации об оценке риска в отраслевых подсистемах безопасности, их сопоставления между собой с точки зрения уровня воздействия требуется определить перечень мероприятий с учетом их физической реализуемости в условиях ограничений в обеспечении рассматриваемой системы ресурсами (финансовые и материальные средства, персонал).

Решение задачи. Предложен подход, позволяющий провести последовательную поэтапную оценку состояния системы комплексной безопасности предприятия, который основан на совместном применении методов анализа иерархий и построения “дерева событий” и характеризуется простотой применения, наглядностью, динамичностью, универсальностью и унифицированностью.

Выводы. Достоинством предлагаемого подхода является возможность наблюдать за изменением свойств состояния отраслевых подсистем безопасности, что позволит создать экспертную или интеллектуальную систему управления безопасностью предприятия. Использование представленного подхода даст возможность проводить дальнейшие исследования по совершенствованию методологии синтеза адаптивной системы комплексной безопасности предприятия, что имеет важное хозяйственное для России значение.

Ключевые слова: риск; устойчивость; надежность; качество; вероятность; ущерб; оценка.

Для цитирования: *Гвоздев Е. В.* Методология синтеза адаптивной системы комплексной безопасности на предприятии жизнеобеспечения населения региона // Пожаровзрывобезопасность/Fire and Explosion Safety. — 2020. — Т. 29, № 2. — С. 6–16. DOI: 10.18322/PVB.2020.29.02.6-16.

✉ *Гвоздев Евгений Владимирович*, e-mail: evgvozdev@mail.ru

Methodology for the synthesis of an adaptive integrated security system at a regional life support enterprise

© **Evgeniy V. Gvozdev**✉

National Research Moscow State University of Civil Engineering (Yaroslavskoe shosse, 26, Moscow, 129337, Russian Federation)

ABSTRACT

Introduction. Solving problems related to providing high-quality services to the population of cities (water supply, energy supply, hot water supply, heating, waste disposal) is an integral part of the work of government bodies (regional entities, regions, subjects, municipalities, and their districts). These include enterprises that provide life support to the population, in the technological process of which, as a rule, sections (sites) of hazardous production facilities are involved. At such enterprises, it is proposed to create a comprehensive security system that combines all industry (departmental) security subsystems and is an integral part of their management system. The sustainable functioning of the enterprises in question largely depends on the availability of resources (financial and material resources, time, personnel, etc.) of the integrated security system created at the enterprise, which has volume restrictions. Until now, in practice, the allocation of resources to maintain comprehensive security is based on the intuitive considerations of the company's security managers. When this approach is implemented, the integrated security system created at the enterprise becomes vulnerable.

Method of research. Approaches using existing methods in the complex security of enterprises are analyzed, and the features of their application are considered. A joint application of the hierarchy analysis method and the "tree of events" method is proposed, which makes it possible to determine the initial initiating events, establish the fact of hazard occurrence, and make an attempt to predict the possible effects of hazards on the objects of protection of life-support enterprises of the population.

Problem statement. Complex security of enterprises providing life support to the population is characterized by conditions considered at a certain time, deviation from the parameters of which can lead to a failure in the activities of a separate industry security subsystem, and in the activities of the complex technosphere security system of the enterprise as a whole. Based on information about the risk assessment in the industry security subsystems, their comparison with each other in terms of the level of impact, it is necessary to determine the list of measures taking into account their physical feasibility in the conditions of restrictions in providing the system with resources (financial and material resources, personnel).

Problem solution. The proposed approach to allow consistent, gradual assessment of the state of the complex system of technosphere safety of the company, which is based on the joint application of methods of analysis of hierarchies and the construction of "tree event" which is characterized by ease of use, clarity, dynamism, versatility and commonality.

Conclusion. The advantage of the proposed approach is the ability to observe changes in the properties of the state of industry security subsystems, which will allow you to create an expert or intelligent enterprise security management system. The use of this approach will allow us to conduct further research in improving the methodology for synthesizing the adaptive system of integrated enterprise security, which is of great economic importance for Russia.

Keyword: risk; stability; reliability; quality; probability; damage; assessment.

For citation: E. V. Gvozdev. Methodology for the synthesis of an adaptive integrated security system at a regional life support enterprise. *Pozharovzryvobezopasnost/Fire and Explosion Safety*, 2020, vol. 29, no. 2, pp. 6–16 (in Russian). DOI: 10.18322/PVB.2020.29.02.6-16.

✉ *Evgeniy Vladimirovich Gvozdev*, e-mail: evgvozdev@mail.ru

Введение

Показатель качества жизнеобеспечения населения (далее — ЖОН) России с точки зрения предоставления ему требуемого набора благ в виде услуг (водоснабжение, энергоснабжение, горячее водоснабжение, отопление, утилизация отходов) наглядно проявляется не только в период возникновения чрезвычайных ситуаций (ЧС) природного и техногенного характера, но и в период повседневной деятельности функционирования предприятий, участвующих в ЖОН, в технологическом процессе которых, как правило, задействованы участки (площадки) опасных производственных объектов (далее — предприятия ЖОН). Предприятия ЖОН относятся к объектам, входящим в систему жилищно-коммунального хозяйства (ЖКХ) регионов (муниципальных образований), т. е. они предоставляют населению России материальные средства и услуги по установленным нормам и нормативам в жизненно важных видах (ГОСТ Р 22.3.01–94. Безопасность в чрезвычайных ситуациях. Жизнеобеспечение населения в чрезвычайных ситуациях. Общие требования).

В структуру системы ЖКХ регионов (муниципальных образований) входят также предприятия ЖОН, участвующие в обеспечении населения России электрической энергией, теплом и горячим водоснабжением. В самом крупном в России Московском регионе бесперебойное качественное предоставление перечисленных жизненно важных услуг возложено на Публичное акционерное общество (ПАО) "Мосэнерго", самую крупную среди генерирующих компаний России, которая входит в структуру ПАО "Газпром" и обеспечивает Московский регион электрической энергией, теплом и горячим водоснабжением.

Поддержание устойчивого функционирования рассматриваемого предприятия ЖОН Московского региона будет обеспечено за счет выполнения мероприятий по защищенности и стойкости системы комплексной безопасности (далее — СКБ), объединяющей все отраслевые (ведомственные) подсистемы безопасности и являющейся неотъемлемой частью их системы управления. На рис. 1 представлена СКБ, которую предложено создавать на пред-

Рис. 1. Система комплексной безопасности, создаваемая на предприятии

Fig. 1. Integrated security system (ISS) created at the enterprise

приятиях ЖОН и которая предназначена для устойчивого преодоления опасностей, квалифицируемых как ЧС природного или техногенного характера [1–3].

Для каждого из направлений безопасности (см. рис. 1) разработаны собственные требования, изложенные в различных федеральных законах: например, по промышленной безопасности — в Федеральном законе № 116-ФЗ "О промышленной безопасности опасных производственных объектов" (от 21.07.1997 г.), а по пожарной безопасности — в Федеральном законе № 69-ФЗ "О пожарной безопасности" (от 21.12.1994 г.). Механизм реализации требований, разрабатываемых в форме подзаконных актов, поручен ведомству (куратору), за которым закреплено направление безопасности. Работа ведомства направлена на совершенствование и разработку мероприятий по минимизации (исключению) риска в закрепленном за ним отраслевом направлении безопасности.

В мировой практике оценка безопасности техногенных объектов, основанная на использовании понятия риска аварии, находит широкое применение в различных отраслях промышленности [4, 5]. Требование к минимизации риска сформировалось как развитие понятий "надежность" и "безотказность" и характеризуется в том числе частотой негативных событий.

Первые исследования по риск-ориентированному подходу в промышленности как развитию представлений о надежности и безотказности можно отнести к началу 80-х годов прошлого столетия [6]. В настоящее время установлено, что показатель риска аварии должен быть основным показателем техногенной безопасности [7–10].

Устойчивое функционирование рассматриваемого предприятия ЖОН Московского региона во многом зависит от *показателей ресурсной обеспеченности* (финансовые и материальные средства, время, персонал и т. д.) СКБ, созданной на предприятии, которые из-за отсутствия возможностей предприятия имеют ограничения, т. е. не способны покрыть в полном объеме запросы руководителей служб (отделов) — кураторов направлений комплексной безопасности.

Несмотря на то что сейчас для распределения ресурса в отраслевых направлениях безопасности (ведомствах) разработано и принято к исполнению множество различных методик (руководств), до сих пор каждым из них применяются различные, отличающиеся друг от друга подходы при использовании рисковых или "факторных" показателей, сопоставление которых вызывает серьезные затруднения даже у специалистов-экспертов. Сделан вывод о том, что на практике распределение ресурса предприятия, предназначенного для комплексной безопасности, в виде единого объема осуществляется на основе интуитивных соображений руководителей (ведомственных) направлений безопасности.

При реализации такого подхода СКБ предприятия становится уязвимой в тех местах, где направления деятельности недостаточно обеспечены ресурсной поддержкой для их безопасного функционирования (рис. 2). Представленная в виде схемы на рис. 2 информация наглядно подтверждает наличие проблем в рассматриваемой области, что свидетельствует об актуальности исследований.

Цель настоящей работы — создать подход, основанный на комплексной оценке рисков в СКБ предприятия, который в целях их минимизации (исключения) позволит обосновать требуемый для рассматриваемой системы объем ресурсов.

Объектом исследования является СКБ, созданная на предприятии (ПАО "Мосэнерго"), включающая в себя множество отдельных (отраслевых) направлений безопасности и функционирующая в условиях ограничений в ресурсном обеспечении предприятия.

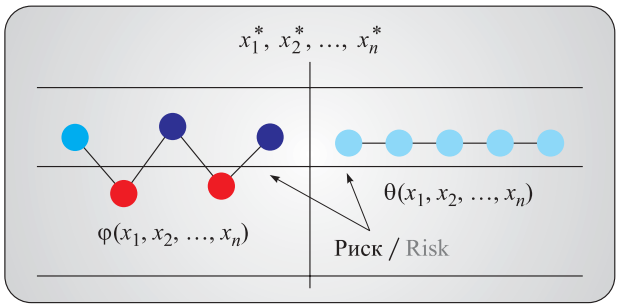

Рис. 2. Схема сравнения показателей обеспеченности подсистем безопасности

Fig. 2. Comparison scheme of security subsystem security indicators

Предметом исследования являются риски в подсистемах, входящих в СКБ предприятия, реализация которых может нанести вред двум и более отраслевым подсистемам безопасности.

Анализ исследований в обеспечении комплексной безопасности предприятий ЖОН

Проблеме комплексной безопасности предприятий ЖОН в настоящее время уделяется значительное внимание, так как она является составной частью национальной безопасности страны и требует совершенствования и достаточного ресурсного обеспечения для достижения главной цели — минимизации (исключения) риска возникновения опасностей, приводящих к ЧС.

При анализе безопасности и рисков, возникающих при эксплуатации предприятий ЖОН, установлено, что потенциальная опасность наступления на них ЧС, как и на других объектах техногенной инфраструктуры, обуславливается наличием следующих *инициирующих* факторов:

1) неконтролируемого выброса опасной энергии $E_i(\tau)$ (упругой, кинетической, тепловой, акустической, вибрационной);

2) неконтролируемого выброса опасных, в том числе горючих и отравляющих, веществ $W_i(\tau)$;

3) опасных нарушений и повреждений каналов передачи информационных потоков $I(\tau)$ в системах управления и регулирования технологическим процессом предприятий ЖОН (поражения блоков в АСУ ТП, в системах видеонаблюдения, связи и оповещения, в программных продуктах, в системах автоматизированной защиты) [11].

Последствия же, выраженные в виде ЧС, от воздействия указанных выше инициирующих факторов:

- *рассматриваются по отношению к объектам защиты* (персонал предприятия, здания, сооружения, оборудование, имущество);
- *рассчитываются в виде характеризуемой степени повреждений (ущербов)* (смерть или ущерб здоровью человека, значительные материальные потери);
- *выражаются регламентированным временным интервалом неоказания услуг в ЖОН*, превышение установленного значения которого рассматривается как ЧС, связанная с нарушением условий ЖОН.

Последняя формулировка имеет непосредственное отношение к предприятиям ЖОН, которые входят в систему ЖКХ региона (муниципального образования) и основу которых составляют предприятия электроэнергетики, водоснабжения и водоотведения, утилизации отходов и т. д.

В ходе анализа исследований, проводимых в комплексной безопасности организационных систем, рассматривались научные работы, выполненные российскими [7–10, 12–14] и зарубежными [15–17] исследователями.

В этих работах решались риск-ориентированные задачи (проблемы) с точки зрения комплексного подхода к анализу риска, его оценки и управления им, но детализированный вектор достижения цели был направлен в сторону одной из отраслевых подсистем безопасности (промышленной безопасности, пожарной безопасности, охраны труда, экологии и т. д.).

Отличие настоящей работы заключается в том, что комплексную безопасность предприятий ЖОН предлагается рассматривать, основываясь на взаимосвязи по риску между отраслевыми направлениями безопасности (промышленная и пожарная безопасность, защита от ЧС природного и техногенного характера, охрана труда и экологическая безопасность, антитеррористическая защищенность и т. д.), представляя ее в виде СКБ, создаваемой на предприятиях ЖОН.

Наряду с существующими критериями отнесения возникших опасностей к ЧС, показателями которых являются размеры ущербов, нанесенных населению, имуществу (оборудованию и т. д.), окружающей природной среде, в настоящем исследовании делается упор на последствиях, наступающих при превышении регламентированного временного интервала *неоказания услуг в ЖОН и рассматриваемых как ЧС*. Данный период времени имеет непосредственное отношение к предприятиям ЖОН, которые входят в систему ЖКХ региона (муниципального образования) и основу которых составляют предприятия электроэнергетики, водоснабжения и водоотведения, утилизации отходов и т. д.

При использовании математических моделей для решения проблемы комплексной безопасности на предприятиях ЖОН в основном предлагается использовать систему дифференциальных уравнений с нелинейными обратными связями вида:

$$\frac{\partial}{\partial t} X_i(t) = F_i(X_1, X_2, \ldots, X_n; t), \quad i = 1, 2, \ldots, n, \tag{1}$$

где X_i — фазовые переменные, с помощью которых определяется состояние рассматриваемого объекта в момент времени t.

В число фазовых переменных, характеризующих состояние безопасности объектов ЖОН Московского региона, например, для энергетической компании ПАО “Мосэнерго”, входит:

- перечень объектов (ТЭЦ, РТЭС, КТЭС) предоставляющих услуги по ЖОН в Московском регионе;

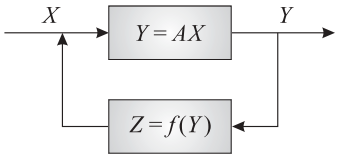

Рис. 3. Схема системы с обратной связью
Fig. 3. Diagram of feedback system

- перечень объектов (зданий, сооружений и т. д.), закрепленных за каждым из объектов ПАО "Мосэнерго" (ТЭЦ, РТЭС, КТЭС), предоставляющих услуги по ЖОН в Московском регионе;
- численность населения, проживающего (находящегося временно) на территориях, закрепленных за каждым из объектов ПАО "Мосэнерго" (ТЭЦ, РТЭС, КТЭС), предоставляющих услуги по ЖОН в Московском регионе;
- число и характеристики источников возникновения опасностей на объектах ПАО "Мосэнерго" (ТЭЦ, РТЭС, КТЭС), предоставляющих услуги по ЖОН в Московском регионе;
- состав, количественная и качественная характеристика сил и средств, предназначенных для предупреждения и ликвидации ЧС на объектах ПАО "Мосэнерго" (ТЭЦ, РТЭС, КТЭС), предоставляющих услуги по ЖОН в Московском регионе.

На основе применения системы уравнений (1) будет описано поведение объекта в условиях возникновения опасностей при условии известности данных в правой части уравнения (1) с нелинейной обратной связью (рис. 3).

СКБ, созданная и функционирующая на предприятии, имеет обратную связь, учет значений которой играет принципиальную роль в управлении рисками [18].

При анализе устойчивости систем комплексной безопасности часто используется приближение суммы одинаково распределенных независимых случайных величин с конечными средними и дисперсией. В этом случае применяются доказательства, прописанные в законе нормального распределения плотности вероятности:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \qquad (2)$$

где μ — математическое ожидание (среднее значение);

σ — среднеквадратическое отклонение;

σ^2 — дисперсия распределения.

В упрощенном виде формула для данного закона может быть записана в виде

$$f(x) \approx \exp\left(-\frac{(x-\mu)^2}{\sigma^2}\right). \qquad (3)$$

При обработке результатов статистики реализованных рисков в отраслевых направлениях безопасности, входящих в СКБ предприятия, чаще используется предлагаемый к рассмотрению закон:

$$f(x) \approx x^{-\alpha}, \quad x >> 1, \quad \alpha \approx 1. \qquad (4)$$

Именно этот закон характеризует распределение числа пострадавших при некачественном оказании услуг, статистических данных по количеству аварий на объектах ПАО "Мосэнерго" (ТЭЦ, РТЭС, КТЭС), предоставляющих услуги по ЖОН в Московском регионе.

Перспективным же направлением, связанным с оценкой риска, является применение вейвлет-анализа как метода экспресс-диагностики и оперативного прогноза кризисного состояния. Методы вейвлет-анализа можно применять к данным различной природы, например к одномерным функциям или двумерным изображениям. Грубую классификацию вейвлет-алгоритмов можно осуществить путем выделения непрерывного (CWT — *Continuous Wavelet Transform*) и дискретного (DWT — *Discrete Wavelet Transform*) вейвлет-преобразований. В то же время набор вейвлет-коэффициентов гораздо быстрее можно получить в случае дискретного преобразования, причем он даст достаточно точное представление о сигнале при меньшем объеме получаемых в результате данных [19].

Так как в состав СКБ входит множество отраслевых подсистем безопасности (см. рис. 1), оптимальное функционирование рассматриваемой системы будет напрямую зависеть от показателей эффективности входящих в нее подсистем.

Постановку задачи для оценки рисков в комплексной безопасности предприятий ЖОН можно представить следующим образом.

Постановка задачи для оценки рисков в комплексной безопасности предприятий ЖОН

Комплексная безопасность предприятий ЖОН в каждый момент времени i характеризуется некоторыми состояниями x_i, управление которыми осуществляется с помощью мероприятий u_i (рис. 4).

Общий вид структуры оценки состояния СКБ приведен на рис. 5.

Требуется рассмотреть и обосновать последовательную реализацию задач по оценке СКБ с учетом временных показателей i:

1. На основании информации о состоянии комплексной безопасности x_i по фиксированным статистическим результатам происшедших за временной

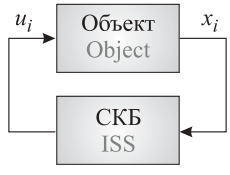

Рис. 4. Взаимодействие управляющего объекта с СКБ
Fig. 4. Interaction of the control object with ISS

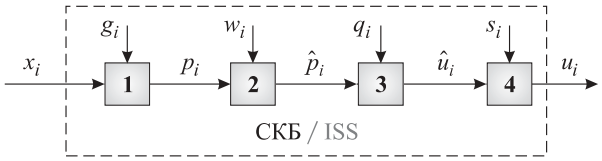

Рис. 5. Общий вид структуры оценки состояния СКБ
Fig. 5. General view of the structure for assessing the state of ISS

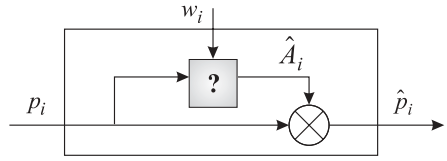

Рис. 6. Алгоритм ранжирования показателей в общем виде
Fig. 6. Algorithm for ranking indicators in general

интервал событий (рассматриваемых как ЧС), когда было задействовано две и более отраслевых подсистем безопасности g_i, требуется определить *локальные показатели риска* для тех отраслевых подсистем, которыми была инициирована опасность p_i.

2. На основании информации о показателях риска p_i и характеризующей их информации w_i, рассматриваемой с точки зрения причинно-следственных связей, требуется определить критерии для *оценки глобального показателя рисков* СКБ $\hat{p}_i$.

3. На основании информации об оценке глобального показателя рисков СКБ $\hat{p}_i$ и результатов выявленных отклонений q_i от требований, утвержденных отраслевым направлением безопасности (чеклисты), требуется провести сопоставление мероприятий по устранению выявленных отклонений $\hat{u}_i$, которым присвоен собственный уровень (ранг), с точки зрения степени воздействия опасности на объекты защиты предприятия.

4. На основании информации об оценке рисков $\hat{p}_i$ в отраслевых подсистемах безопасности, проранжированных в виде мероприятий $\hat{u}_i$, и сопоставлении их между собой, а также о существующих на предприятии ограничениях в ресурсном (финансовые и материальные средства, персонал) обеспечении СКБ s_i требуется определить перечень мероприятий $\hat{u}_i$, которые будут реализованы в запланированный предприятием период с учетом их физической реализуемости.

Обоснование выбора методов исследования

Процессы управления комплексной безопасностью на различных предприятиях во многом аналогичны. Кроме того, во многом схожи и сопутствующие им проблемы, связанные с воздействием опасностей на объекты защиты. Выбор метода должен предполагать обоснованный и понятный способ рейтингования рисков возникновения опасностей. Выбор метода должен учитывать и количественную, и качественную информацию о предпочтениях лица, принимающего решения (юридического лица). Для совершенствования и развития комплексной безопасности необходим метод, позволяющий по универсальным правилам решать задачи (проблемы) с учетом их реальной сложности и существующих на предприятиях ЖОН ограничений в ресурсном обеспечении [20].

В предыдущем разделе при описании последовательности реализации задач управления СКБ наиболее сложное решение отнесено ко 2-му и 3-му блокам рассматриваемой задачи, которые должны представляться в виде зависимостей (нарушения — требования; опасность — значимость для безопасности), расчета параметров (весовых коэффициентов), показателей безопасности и ранжирования их по значимости воздействия на безопасность. Решение представленных задач можно описать следующим выражением:

$$\hat{p}_i = p_i + \hat{A}_i p_i = (I + \hat{A}_i) p_i, \qquad (5)$$

где $p_i = 0$ (нет i-го нарушения) или $p_i = 1$ (есть i-е нарушение);

$\hat{A}_i = \mathrm{diag}(\hat{a}_i^j)$ — диагональная матрица искомых весовых коэффициентов (рис. 6).

Парные сравнения ($p_i = 0$, $p_i = 1$) приводят к записи характеристик сравнений в виде квадратной таблицы чисел, которая называется матрицей.

Сравнивая набор показателей с точки зрения важности, получим следующую матрицу:

$$\hat{A}_i = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}. \qquad (6)$$

Эта матрица обратно симметричная, т. е. имеет место свойство

$$a_{ij} = 1/a_{ji}. \qquad (7)$$

Представленному выше описанию во многом отвечает метод анализа иерархий (далее — МАИ). МАИ — методологическая основа для решения задач выбора альтернатив посредством их многокритериального рейтингования. МАИ создан американским ученым Томасом Саати и вырос в настоящее время в обширный междисциплинарный раздел науки, имеющий строгие математические многовариантные обоснования [15].

На основе МАИ предлагается составить список *всех возможных рисков возникновения ЧС* (задействовано две и более отраслевых подсистем безопасности) p, далее с привлечением экспертов оценить значимость каждого показателя $\hat{A}_i = \mathrm{diag}(\hat{a}_i^j)$ с учетом некоторой обобщенной для всех возможных случаев информации (опыта экспертов) w (рис. 7).

Рис. 7. Схема предварительной оценки параметров экспертами
Fig. 7. Scheme for preliminary assessment of parameters by experts

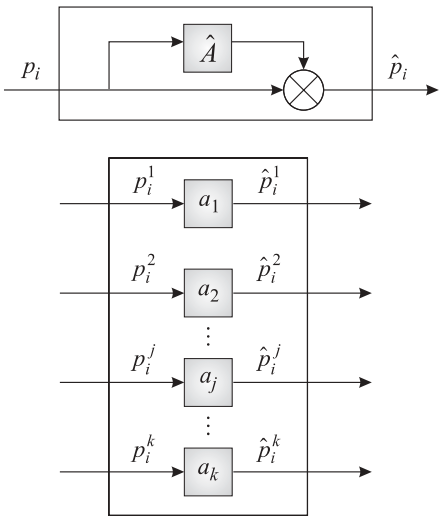

Рис. 8. Статический алгоритм ранжирования показателей
Fig. 8. Static ranking algorithm for indicators

Далее предлагается оценивать текущее состояние СКБ предприятия ЖОН путем суммирования параметров, соответствующих k выявленным отклонениям от установленных в отраслевом направлении безопасности требований, в виде выражения

$$K = \sum a_k. \quad (8)$$

В результате решение задачи, связанной с ранжированием показателей опасности, будет иметь вид, представленный на рис. 8.

Достоинством применения МАИ является возможность произвести параметризацию всех рисков вследствие обеспечения статичности блоков 2 и 3 (ранжирования рисков), инициирование которых приведет к возникновению ЧС [21].

Однако предлагаемый метод позволяет решить задачу в блоках 2 и 3, но не способен охватить остальные блоки (1 и 4) (см. рис. 4).

Для решения задачи в полном объеме (во всех четырех блоках) требуется обеспечить статичность всех рассматриваемых блоков, сделать так, чтобы их "внутренняя часть" зависела от состояния отраслевых подсистем, входящих в СКБ, а на выходе каждого из блоков формировалась общая информация о состоянии СКБ предприятия. Для решения задачи в такой постановке применимы два возможных подхода. *Первый* основан на математическом моделировании процессов управления в системе. В практической деятельности предприятий из-за определенной сложности математических моделей он мало применяется. *Второй* подход основан на логико-вероятностных моделях системы — построения дерева (причинно-следственных связей) всех возможных событий в системе (рис. 9).

Такой подход широко применяется на практике, особенно при решении задач, связанных с анализом управления безопасностью технических систем, которые успешно решаются с помощью метода построения "дерева событий" [22].

Однако метод построения "дерева событий" должен быть сопряжен с представленным выше МАИ, т. е. при их совместном применении обеспечивать комплексность для получения требуемых показателей в такой сложной системе, как СКБ.

Совместное применение методов МАИ и построения "дерева событий" позволит определить исходное инициирующее событие, установить факт возникновения опасности, реализовать попытку проникнуть в будущее, ответив на следующие вопросы:

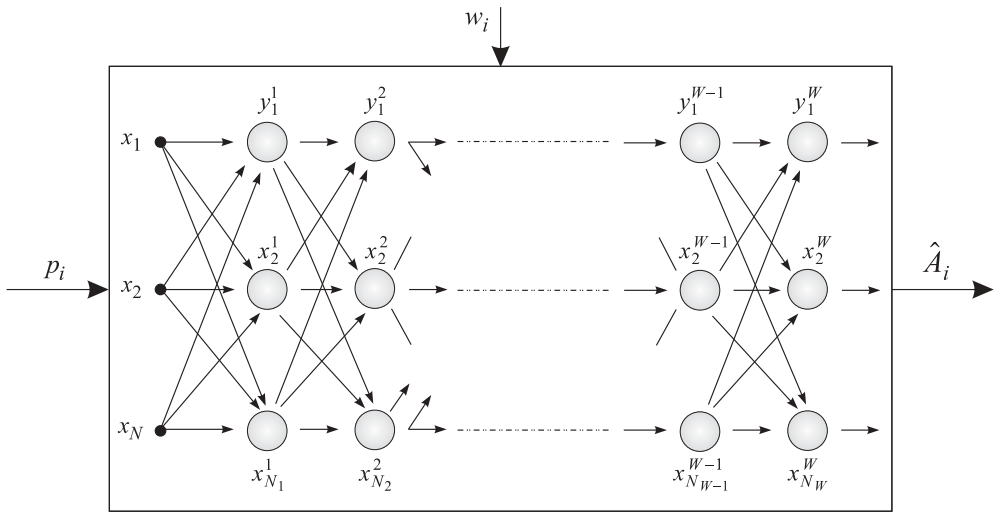

Рис. 9. Схема расчета показателей опасности с помощью метода построения "дерева событий"
Fig. 9. The scheme of calculation of risk indicators using the method of constructing the "tree of events"

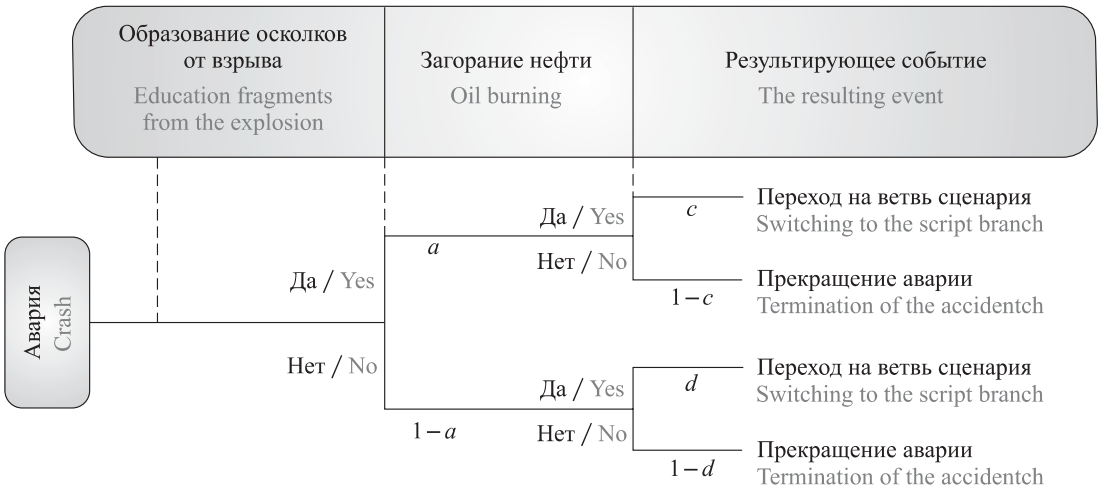

Рис. 10. "Дерево событий" для случая взрыва (пожара) емкости для хранения нефтепродуктов
Fig. 10. "Event tree" for the event of an explosion (fire) of a tank for storing petroleum products

- Что произойдет после возникновения опасности?
- Какие сценарии развития ситуации могут быть реализованы при возникновении вторичных факторов опасности, при ее воздействии на две и более отраслевых подсистем безопасности?
- Какой предполагаемый масштаб ущерба может быть нанесен СКБ и с какой вероятностью?

Пример построения дерева событий представлен на рис. 10.

При совместном рассмотрении двух рассмотренных методов (МАИ + метод построения "дерева событий") будет обеспечена статичность блоков 1–4 (см. рис. 4), правильно построенное дерево не будет коренным образом меняться в процессе работы системы, а на выходе в динамике будут сформированы различные значения для разных сочетаний возникновения опасностей и показателей ущерба от их воздействий.

Достоинством представленного комплексного подхода являются следующие качественные характеристики:

1. *Простота*. Для управления СКБ потребуется только выявлять отклонения от установленных требований и заносить их в базу данных. Все остальное будет преобразовано в требуемую форму запрограммированной технической системой в режиме реального времени.

2. *Наглядность*. Использование технической системы позволит рассмотреть всю цепочку "причина – событие – следствие", тогда неочевидные опасности станут наглядными.

3. *Динамичность.* Представленный подход в явном виде с высоким быстродействием позволит при управлении СКБ решать динамические задачи, описание которых было представлено ранее.

4. *Комплексность*. Это прямой путь к полной автоматизации управления СКБ, в перспективе с органи-зацией и заменой людей запрограммированными техническими системами (роботами).

5. *Трудоемкость.* Привлечение экспертов (ученых, статистиков, практиков и т. д.) будет носить разовый характер. Они не будут постоянно оценивать выявленные отклонения, а значит, включать их в штат организации не потребуется.

6. *Универсальность.* Поскольку вопросы комплексной безопасности актуальны не только для предприятий ЖОН, но и для организаций любых отраслей промышленности всех форм собственности и масштабов производства, появится возможность в использовании всеми предприятиями запрограммированной технической системы. Особенности будут обусловлены требованиями отраслевых (узкоспециальных) правил безопасности, объем которых невелик.

7. *Унифицированность.* Представляется возможность применять данный подход для разработки программного комплекса, используемого надзорными (контрольными) органами. Если для всех отраслевых направлений безопасности будет действовать единая система оценки, то в режиме реального времени органы надзора (контроля) смогут получать информацию о состоянии комплексной безопасности во всех поднадзорных (подконтрольных) организациях. Отсюда появляется возможность регулировать периодичность проводимых проверок, реализовывать требования по риск-ориентированному подходу к проведению надзора (контроля), связанного с комплексной безопасностью предприятий.

Выводы

Представлен концептуальный подход к решению проблемы комплексной безопасности на предприятиях ЖОН. Реализация подхода в предлагаемой постановке на основе рисков позволит проводить на-

блюдение за изменением свойств отраслевых подсистем безопасности, входящих в СКБ предприятий.

Научную основу дальнейшей работы будет представлять подробное исследование и теоретическое описание блоков (см. рис. 5), которое будет включено в содержание методики оценки состояния СКБ предприятия, с помощью которой будет решена поставленная в статье задача. Именно отсутствие в данный момент предлагаемой для использования методики является тормозом развития и совершенствования СКБ.

В перспективе при реализации представленного подхода может быть создана экспертная или интеллектуальная система управления безопасностью предприятия.

Реализация предлагаемого подхода позволит повысить устойчивость функционирования СКБ на объектах ЖОН регионов (муниципальных образований), а при использовании на других предприятиях — перевести их СКБ на более высокий качественный уровень.

В итоге реализация представленного к рассмотрению подхода в перспективе даст возможность разработать методологию синтеза адаптивной СКБ для решения научной проблемы динамического управления комплексной безопасностью предприятия, что имеет важное хозяйственное значение для России.

СПИСОК ЛИТЕРАТУРЫ

1. *Гвоздев Е. В.*, *Матвиенко Ю. Г.* Комплексная оценка риска на предприятиях жизнеобеспечения, имеющих опасные производственные объекты // Безопасность труда в промышленности. — 2019. — № 10. — С. 69–78. DOI: 10.24000/0409-2961-2019-10-69-78.
2. *Гвоздев Е. В.*, *Бутузов С. Ю.*, *Сулима Т. Г.*, *Арифджанов С. Б.* Формализованная модель оценки надежности тепловых электрических станций // Пожаровзрывобезопасность/Fire and Explosion Safety. — 2019. — Т. 28, № 2. — С. 47–56. DOI: 10.18322/PVB/2019.28.02.47-56.
3. *Gvozdev E. V.*, *Cherkina V. M.* The modern strategy to the process of managing complex security of the enterprise on the basis of rational centralization // International Journal of Innovative Technology and Exploring Engineering (IJITEE). — 2019. — Vol. 9, Issue 1. — P. 4614–4620. DOI: 10.35940/ijitee.A4944.119119.
4. Risk-based inspection. API Recommended Practice 580. — 2nd ed. — November 2009. — 84 p. URL: https://www.irantpm.ir/wp-content/uploads/2013/08/API-RP-580-Risk-Based-Inspection-2009.pdf (дата обращения: 02.03.2020).
5. Risk-Based Inspection Technology. API Recommended Practice 581. — 2nd ed. — September 2008. — 654 p. URL: https://www.irantpm.ir/wp-content/uploads/2011/08/API-581-2008.pdf (дата обращения: 02.03.2020).
6. *Хенли Э. Дж.*, *Кумамото Х.* Надежность технических систем и оценка риска / Пер. с англ. — М. : Машиностроение, 1984. — 582 с.
7. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности / Под ред. Н. А. Махутова. — М. : Знание, 2015. — 935 с.
8. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность / Под ред. Н. А. Махутова. — М. : Знание, 2018. — 1016 с.
9. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Фундаментальные и прикладные проблемы комплексной безопасности / Под ред. Н. А. Махутова. — М. : Знание, 2017. — 992 с.
10. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Анализ риска и проблем безопасности / Под ред. Н. А. Махутова. — В 4 ч. — М. : Знание, 2007. — Ч. 4. — 864 с.
11. *Махутов Н. А.*, *Матвиенко Ю. Г.*, *Романов А. Н.* Проблемы прочности, техногенной безопасности и конструкционного материаловедения. — М. : URSS, 2018. — 720 с.
12. *Гордиенко Д. М.* Пожарная безопасность особо опасных и технически сложных производственных объектов нефтегазового комплекса : дис. … д-ра техн. наук. — М., 2018. — 480 с.
13. *Новиков В. В.* Разработка теории и методов создания систем управления безопасностью труда на предприятиях машиностроения : дис. … д-ра техн. наук. — М., 2013. — 429 с.
14. *Мельникова Д. А.* Теоретические и практические аспекты построения системы управления промышленной безопасностью на опасных производственных объектах (на примере ООО “Газпром трансгаз Самара”) : дис. … канд. техн. наук. — Самара, 2016. — 120 с.
15. NFPA 14–2019. Standard for the Installation of Standpipe and Hose Systems. — Quincy, MA : NFPA, 2019. — 67 p.

16. *Aneiba A.*, *Melad M.* Performance evaluation of AODV, DSR, OLSR, and GRP MANET routing protocols using OPNET // International Journal of Future Computer and Communication. — 2016. — Vol. 5, No. 1. — P. 57–60. DOI: 10.18178/ijfcc.2016.5.1.444.
17. *Billinton R.*, *Li W.* Reliability assessment of electric power systems using Monte Carlo methods. — Boston, MA : Springer, 1994. — 351 p. DOI: 10.1007/978-1-4899-1346-3.
18. *Gandossi L.*, *Simola K.*, *Shepherd B.* The link between risk-informed in-service inspection and inspection qualification // Insight — Non-Destructive Testing and Condition Monitoring. — 2009. — Vol. 51, Issue 1. — P. 16–20. DOI: 10.1784/insi.2009.51.1.16.
19. *Шитов А. Б.* Разработка численных методов и программ, связанных с применением вейвлет-анализа для моделирования и обработки экспериментальных данных : дис. … канд. физ.-мат. наук. — М., 2001. — 125 с.
20. IAEA-TECDOC-1400. Improvement of in-service inspection in nuclear power plants. — Vienna, Austria : IAEA, 2004. — 35 p.
21. *Саати Т.* Принятие решений. Метод анализа иерархий / Пер. с англ. — М. : Радио и связь, 1993. — 278 с. URL: https://pqm-online.com/assets/files/lib/books/saaty.pdf (дата обращения: 05.01.2020).
22. *Горев В. А.* Надежность технических систем и техногенный риск. — М. : Изд-во МИСИ– МГСУ, 2018. — 120 с.

REFERENCES

1. E. V. Gvozdev, Yu. G. Matvienko. Comprehensive risk assessment at the life support enterprises with hazardous production facilities. *Bezopasnost truda v promyshlennosti / Occupational Safety in Industry*, 2019, no. 10, pp. 69–78 (in Russian). DOI: 10.24000/0409-2961-2019-10-69-78.
2. E. V. Gvozdev, S. Yu. Butuzov, T. G. Sulima, S. B. Arifjanov. Formal model of evaluating the reliability of thermal power plants. *Pozharovzryvobezopasnost/Fire and Explosion Safety*, 2019, vol. 28, no. 2, pp. 47–56 (in Russian). DOI: 10.18322/PVB/2019.28.02.47-56.
3. E. V. Gvozdev, V. M. Cherkina. The modern strategy to the process of managing complex security of the enterprise on the basis of rational centralization. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 2019, vol. 9, issue 1, pp. 4614–4620. DOI: 10.35940/ijitee.A4944.119119.
4. *Risk-based inspection. API Recommended Practice 580.* 2nd ed. November 2009. 84 p. Available at: https://www.irantpm.ir/wp-content/uploads/2013/08/API-RP-580-Risk-Based-Inspection-2009.pdf (Accessed March 2, 2020).
5. *Risk-Based Inspection Technology. API Recommended Practice 581*. 2nd ed. September 2008. 654 p. Available at: https://www.irantpm.ir/wp-content/uploads/2011/08/API-581-2008.pdf (Accessed March 2, 2020).
6. E. J. Henley, H. Kumamoto. *Reliability of engineering and risk assessment*. Englewood Cliffs, Prentice-Hall, Inc., 1981 (Russ. ed.: E. J. Henley, H. Kumamoto. Bezopasnost truda v promyshlennosti. Moscow, Mashinrostroyeniye Publ., 1984. 582 p.).
7. N. A. Makhutov (ed.). *Bezopasnost Rossii. Pravovyye*, *sotsialno-ekonomicheskiye i nauchno-tekhnicheskiye aspekty. Nauchnyye osnovy tekhnogennoy bezopasnosti* [Security of Russia. Legal, socio-economic, and scientific and technical aspects. Scientific bases of technogenic safety]. Moscow, Znaniye Publ., 2015. 935 p. (in Russian).
8. N. A. Makhutov (ed.). *Bezopasnost Rossii. Pravovyye*, *sotsialno-ekonomicheskiye i nauchno-tekhnicheskiye aspekty. Tekhnogennaya*, *tekhnologicheskaya i tekhnosfernaya bezopasnost* [Security of Russia. Legal, socio-economic, and scientific and technical aspects. Man-made, technological and technosphere safety]. Moscow, Znaniye Publ., 2018. 1016 p. (in Russian).
9. N. A. Makhutov (ed.). *Bezopasnost Rossii. Pravovyye*, *sotsialno-ekonomicheskiye i nauchno-tekhnicheskiye aspekty. Fundamentalnyye i prikladnyye problemy kompleksnoy bezopasnosti* [Security of Russia. Legal, socio-economic, and scientific and technical aspects. Fundamental and applied problems of complex security]. Moscow, Znaniye Publ., 2017. 992 p. (in Russian).
10. N. A. Makhutov (ed.). *Bezopasnost Rossii. Pravovyye*, *sotsialno-ekonomicheskiye i nauchno-tekhnicheskiye aspekty. Analiz riska i problem bezopasnosti* [Security of Russia. Legal, socio-economic, and scientific and technical aspects. Analysis of risk and security problems]. In 4 parts. Moscow, Znaniye Publ., 2007. Part 4, 864 p. (in Russian).
11 N. A. Makhutov, Yu. G. Matvienko, A. N. Romanov. *Problemy prochnosti*, *tekhnogennoy bezopasnosti i konstruktsionnogo materialovedeniya* [Problems of strength, technogenic safety and structural materials science]. Moscow, URSS Publ., 2018. 720 p. (in Russian).

12. D. M. Gordienko. *Fire safety of particularly dangerous and technically complex production facilities of the oil and gas complex.* Dr. Sci. (Eng.) Diss. Moscow, 2018. 480 p. (in Russian).
13. V. V. Novikov. *Development of theory and methods for creating occupational safety management systems at machine-building enterprises*. Dr. Sci. (Eng.) Diss. Moscow, 2013. 429 p. (in Russian).
14. D. A. Melnikova. *Theoretical and practical aspects of building an industrial safety management system at hazardous production facilities (for example*, *Gazprom transgaz Samara LLC)*. Cand. Sci. (Eng.) Diss. Samara, 2016. 120 p. (in Russian).
15. *NFPA 14–2019. Standard for the Installation of Standpipe and Hose Systems*. Quincy, MA, NFPA, 2019. 67 p.
16. A. Aneiba, M. Melad. Performance evaluation of AODV, DSR, OLSR, and GRP MANET routing protocols using OPNET. *International Journal of Future Computer and Communication*, 2016, vol. 5, no. 1, pp. 57–60. DOI: 10.18178/ijfcc.2016.5.1.444.
17. R. Billinton, W. Li. *Reliability assessment of electric power systems using Monte Carlo methods*. Boston, MA, Springer, 1994. 351 p. DOI: 10.1007/978-1-4899-1346-3.
18. L. Gandossi, K. Simola, B. Shepherd. The link between risk-informed in-service inspection and inspection qualification. *Insight — Non-Destructive Testing and Condition Monitoring*, 2009, vol. 51, issue 1, pp. 16–20. DOI: 10.1784/insi.2009.51.1.16.
19. A. B. Shitov. *Development of numerical methods and programs related to the use of wavelet analysis for modeling and processing experimental data*. Cand. Sci. (Phys.-Math.) Diss. Moscow, 2001. 125 p. (in Russian).
20. *IAEA-TECDOC-1400. Improvement of in-service inspection in nuclear power plants*. Vienna, Austria, IAEA, 2004. 35 p.
21. *Saati T.* Decision Making. Method for analyzing hierarchies. URL: https://pqm-online.com/assets/files/lib/books/saaty.pdf (Accessed 05.01.2020).
22. V. A. Gorev. *Nadezhnost tekhnicheskikh sistem i tekhnogennyy risk* [Reliability of technical systems and technogenic risk]. Moscow, MISI–MGSU Publishing House, 2018. 120 p. (in Russian).

Поступила 03.03.2020, после доработки 27.03.2020;
принята к публикации 02.04.2020
Received March 3, 2020; Received in revised form March 27, 2020;
Accepted April 2, 2020

Информация об авторе

ГВОЗДЕВ Евгений Владимирович, канд. техн. наук, доцент кафедры комплексной безопасности в строительстве, Национальный исследовательский Московский государственный строительный университет, г. Москва, Российская Федерация; ORCID: 0000-0002-3679-1065; e-mail: evgvozdev@mail.ru

Information about the author

Evgeniy V. GVOZDEV, Cand. Sci. (Eng.), Associate Professor of Department of Integrated Safety in Civil Engineering, National Research Moscow State University of Civil Engineering, Moscow, Russian Federation; ORCID: 0000-0002-3679-1065; e-mail: evgvozdev@mail.ru