УДК 351.861 *nazarov@sibpsa.ru*

ПОДХОДЫ К ВЫБОРУ РАЦИОНАЛЬНЫХ ПАРАМЕТРОВ ЭЛЕМЕНТОВ СИСТЕМЫ МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ТЕХНОГЕННОГО ХАРАКТЕРА ПРИ ПОСТРОЕНИИ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ НАСЕЛЕНИЯ

APPROACHES TO THE SELECTION OF RATIONAL PARAMETERS OF ELEMENTS OF THE SYSTEM FOR MONITORING EMERGENCY SITUATIONS OF A ANTHROPOGENIC NATURE IN THE CONSTRUCTION OF A COMPREHENSIVE SYSTEM FOR THE SAFETY OF THE POPULATION

Назаров А. А.,
Сибирская пожарно-спасательная академия
ГПС МЧС России, Железногорск

Nazarov A.,
Siberian Fire and Rescue Academy
EMERCOM of Russia, Zheleznogorsk

В статье проведен анализ существующих методов и подходов построения системы защиты населения от ЧС техногенного характера, а также особенностей оценки и мониторинга техногенных источников риска концепции развития современной теории безопасности сложных систем Critical Infrastructure Resilience (CIR) (жизнеспособность критической инфраструктуры). Показано, что в основе традиционного подхода (Safety I) безопасность оценивается как отсутствие нежелательных последствий и отчетливых признаков опасности, представляя бимодальные сведения о режиме функционирования системы в критериях «опасно (неправильно)» и «безопасно (правильно)». Подход Safety II, действует с позиции мультимодальности функционирования системы, основываясь на принципе мониторинга как сбоя системы, так и нормальной ее работы, прогнозирования событий и направлений их развития. Отмечено, что реализуемая в настоящий момент в России концепция в целом соотносится с принципами Safety II, что проявляется в ориентации обоих подходов на принятие превентивных управленческих решений и сохранение работоспособности системы даже в кризисных ситуациях. На основе проведенного анализа и обобщения результатов исследований, выполненных другими авторами, сделан вывод о необходимости применения новых подходов учитывающих, как региональные особенности построения системы, так и рациональное использование ресурсов в зависимости от возникающих угроз на основе гибких мультимодальных показателей.

Ключевые слова: жизнеспособность критической инфраструктуры; мониторинг; комплексная безопасность; риск; параметрический подход; системный анализ.

The article analyzes the existing methods and approaches in the construction of a system for protecting the population from man-made emergencies, as well as the features of assessing and monitoring man-made sources of risk in the concept of the development of the modern theory of security of complex systems «Critical Infrastructure Resilience» (CIR). It is shown that in the basis of the traditional approach (Safety I), safety is evaluated as the absence of undesirable consequences and clear signs of danger, presenting bimodal information about

the mode of operation of the system in the criteria: «dangerous (incorrect)» and «safe (correct)». The Safety II approach is suitable from the point of view of the multi-modality of the system functioning, based on the principle of monitoring both the system failure and its normal operation, predicting events and directions of their development. It is noted that the concept currently being implemented in Russia generally correlates with the principles of Safety II, which is manifested in the orientation of both approaches to making preventive management decisions and maintaining the system's operability even in crisis situations. Based on the analysis and generalization of the results of research carried out by other authors, it is concluded that it is necessary to apply new approaches that take into account both the regional features of the system construction and the rational use of resources, depending on emerging threats, in conditions of limited resources on the basis of flexible multi-modal indicators.

Keywords: critical infrastructure resilience; monitoring; integrated security; risk; parametric approach; system analysis.

Безопасность любого государства заключается в защите его конституционного строя, суверенитета и территориальной целостности, установлении политической, экономической и социальной стабильности, безусловном исполнении законов и решительном противодействии возникающим внешним и внутренним угрозам. В «Стратегии национальной безопасности Российской Федерации» [1], утвержденной, подчеркиваются неразрывная взаимосвязь и взаимозависимость национальной безопасности и социально-экономического развития страны [2].

В целях реализации полномочий государства в области защиты населения и территорий от чрезвычайных ситуаций в настоящее время в России создана и успешно функционирует единая государственная система предупреждения и ликвидации чрезвычайных ситуаций (РСЧС). Единая система РСЧС объединяет органы управления, силы и средства федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций, привлекаемых для предупреждения и ликвидации чрезвычайных ситуаций [3].

Согласно установленному правовыми актами порядку, единая система состоит из функциональных и территориальных подсистем, действующих на федеральном, межрегиональном, региональном, муниципальном и объектовом уровнях. Указанная квалификация уровней системы обусловлена принципом соответствующего реагирования, достаточными силами и средствами адекватно возникающих угроз (чрезвычайным ситуациям).

Классификации чрезвычайных ситуаций природного и техногенного характера (угроз) определена Постановлением Правительства [4] и предусматривает шесть типов чрезвычайных ситуаций в зависимости от тяжести последствий и вовлеченной в ситуацию территории

Каждый режим функционирования предусматривает проведение ряда мероприятий, осуществляемых органами управления системы. Одним из ключевых мероприятий является сбор, обработка и обмен в установленном порядке информацией в области защиты населения и территорий от ЧС и обеспечение пожарной безопасности, изучение состояния окружающей среды, мониторинг опасных природных явлений и техногенных процессов.

Сбор и обработка данных мониторинга является как основой для принятия превентивных мер предотвращения ЧС, так и условием своевременного реагирования на инциденты. В зависимости от полученных данных органы управления принимают соответствующее решение. Обобщённая схема

мероприятий по сбору данных и мониторингу обстановки в зависимости от режима функционирования представлена на рис. 1.

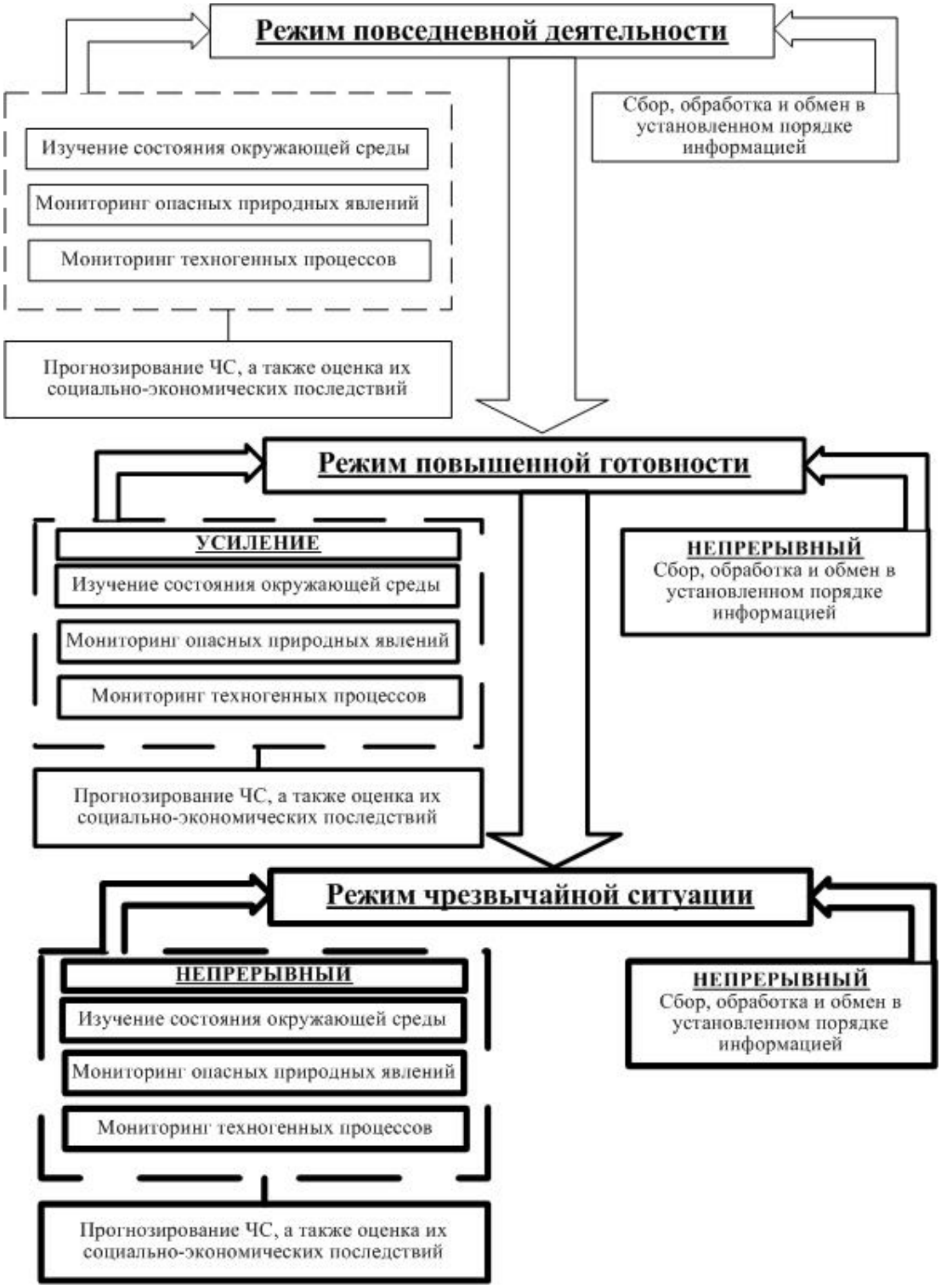

Рисунок 1. Схема организации мониторинга в зависимости от режима функционирования

В целях реализации задач в рамках функционирования системы РСЧС предусмотрено создание подсистемы мониторинга, лабораторного контроля и прогнозирования чрезвычайных ситуаций единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (СМП ЧС). Основные задачи, функции, организацию управления, состав сил и средств, а также деятельность СМП ЧС определены положением о функциональной подсистеме мониторинга, лабораторного контроля и прогнозирования чрезвычайных ситуаций единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций [5].

Исходя из установленных задач СМП ЧС, возможно выделить два основных направления: мониторинг и прогнозирование. Решение этих двух основных задач позволяет определить возможный характер ЧС и масштаба их развития, разработать рекомендации по управлению рисками ЧС, а также мероприятия по предупреждению, локализации, ликвидации и смягчению негативных последствий (рис. 2).

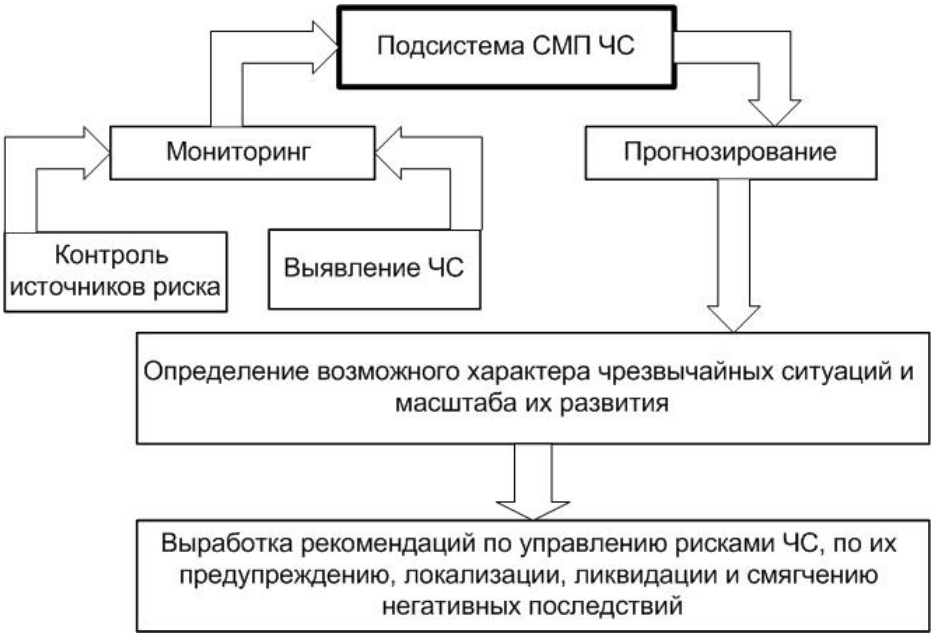

Рисунок 2. Задачи СМП ЧС (СМП – система мониторинга и прогнозирования; ЧС – чрезвычайная ситуация)

Информационное обеспечение функциональной подсистемы СМП ЧС осуществляется путем информационного обмена с функциональными и территориальными подсистемами РСЧС сведениями о прогнозируемых и возникших чрезвычайных ситуациях и их последствиях, о радиационной, химической, медико-биологической, взрывной, пожарной и экологической безопасности на соответствующих территориях, а также сведениями о деятельности организаций независимо от форм собственности, органов местного самоуправления, государственных органов исполнительной власти.

Рисунок 3. Элементы СМП ЧС (СМП – система мониторинга и прогнозирования; ЧС – чрезвычайная ситуация; ГИС – геоинформационные системы; БД – база данных)

Утвержденная в настоящий момент концепция комплексной системы обеспечения безопасности жизнедеятельности населения (КСОБЖН), реализуемая межведомственной комиссией, предусматривает создание информационных систем, систем мониторинга на разных уровнях управления и, как следствие, создание рациональной и эффективной системы обеспечения безопасности населения путем снижения вероятности реализации угроз природного, техногенного характера. Достижение поставленных Концепцией задач планируется осуществить, в том числе, за счет:

– предотвращения кризисных ситуаций путем оснащения объектов защиты техническими средствами обеспечения безопасности и инструментальными средствами контроля функционирования средств (систем) жизнеобеспечения;

– эффективного мониторинга текущей обстановки и представления информации для действий территориальных органов федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и должностных лиц администраций объектов, обеспечивающей своевременность принятия управленческих решений. Общая схема построения КСОБЖН представлена на рис. 4.

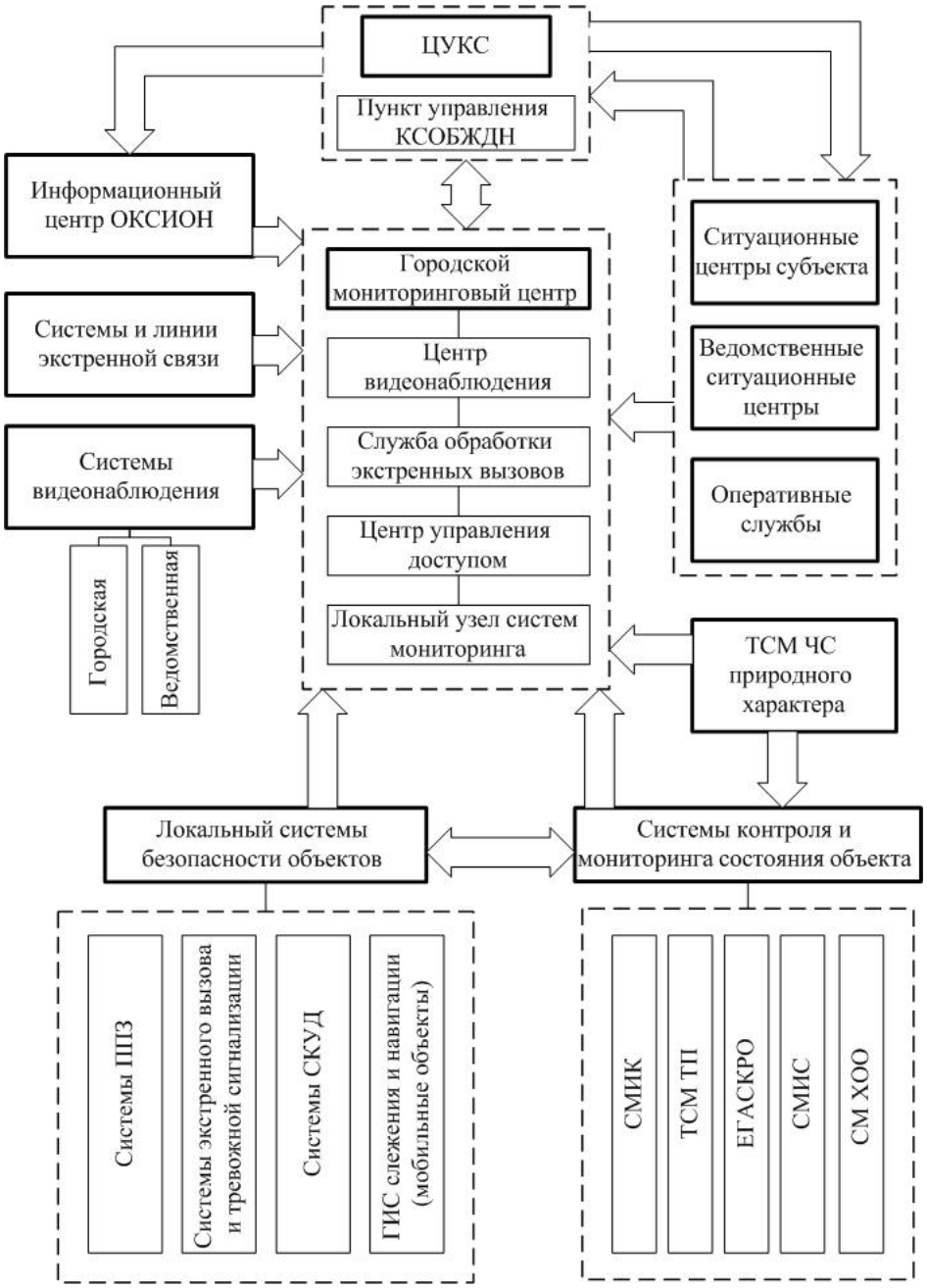

Рисунок 4. Общая структура системы мониторинга КСОБЖН (ЦУКС – Центр управления в кризисных ситуациях; ТСМ – технические средства мониторинга; СМИК – система мониторинга инженерных конструкций; СМИС – система мониторинга инженерных систем; ЕГАСКРО – система контроля радиационной опасности; СМ ХОО – система мониторинга химически опасных объектов; ППЗ – противопожарная защита; СКУД – система контроля и управления доступом; ГИС – геоинформационная система)

Несмотря на большой объем накопленных знаний в данной области, остаются проблемные вопросы при решении задачи обоснования рациональных параметров системы защиты населения от чрезвычайных ситуаций техногенного характера. Кроме того, существующие методики не ориентированы на проектирования систем комплексной безопасности на территориях, отличающихся специфическими рисками.

Обзор работ в данной области на современном этапе развития показывает, что в последние годы одной из тенденций в области изучения сложных систем является использование термина «критическая инфраструктура», являющаяся совокупным определением различных сфер деятельности человека, в рамках которых сохраняются жизненно важные функции общества и личности. Данный термин закреплен в Директиве Совета Европейского Союза 2008/114/ЕС от 8 декабря 2008 г. «О европейских критических инфраструктурах и мерах по их защите» [6]. В большинстве рассмотренных зарубежных работ обеспечение комплексной безопасность жизнедеятельности человека и общества рассматривается в парадигме данного термина. Комплексное научное направления в данной области за рубежом получило название Critical Infrastructure Resilience (CIR) (жизнеспособность критической инфраструктуры); оно затрагивает широкий спектр вопросов оценки устойчивости функционирования систем различной природы, управления безопасности в широком смысле.

Исследованиям в этой области в рамках концепции CIR за рубежом посвящены работы: L. Labaka; J. Hernantes; J. M Sarriegi; S. Cassotta; R. Sidortsov; C. Pursiainen; M. E. Goodsite и др. [7–11]. В большинстве исследований решаются задачи по разработке систем индикаторов, отражающих состояние как системы, так и основных влияющих на системы факторов. Эти индикаторные системы, как правило, представлены иерархической структурой. При оценке индикаторов в основном применяются методы экспертной оценки различных показателей компонентов системы.

Наличие широкого спектра работ в данной области российских и зарубежных исследователей подтверждает актуальность темы и характеризует определенную степень ее разработанности. Тем не менее, несмотря на обширную базу знаний, описывающую алгоритм построения и функционирования системы как в рамках отечественной концепции КСОБЖ, так и зарубежной CIR, вопросы выбора и обоснования рациональных параметров системы мониторинга при построении системы не затронуты. Кроме того, рассмотренные подходы не учитывают поэтапное построение системы в условиях органичных ресурсов, а также региональных особенностей и специфических рисков территории с особым режимом функционирования.

Один из перспективных подходов обеспечения безопасности (Safety II) предлагается шведским ученым Эриком Холлнагелем (Erik Hollnagel) [12]. В основе традиционного подхода (Safety I) безопасность оценивается как отсутствие нежелательных последствий и отчетливых признаков опасности, представляются бимодальные сведения о режиме функционировании системы в критериях: «опасно (неправильно)» и «безопасно (правильно)». Это приводит к тому, что управленческое решение по реагированию происходит когда что-то случается или определяется как неприемлемый риск. Подход Safety II изначально действует с позиции мультимодальности функционирования системы, основываясь на принципе мониторинга как сбоя системы, так и нормальной ее работы, прогнозирования событий и направлений их развития. Основной упор при контроле делается на выявление точек процесса с высокой вариативностью и сложностью. Отмечено, что реализуемая концепция КСОБЖН в целом соотносится с принципами Safety II, что проявляется в ориентации обоих подходов на принятие превентивных управленческих решений и сохранение работоспособности системы даже в кризисных ситуациях. В настоящее время в России реализация этого подхода отчасти получила свое отражения в риск-ориентированном подходе при оценке и организации реагирования на риски.

В результате анализа, проведенного в данной работе, а также исследования различных концепций обеспечения безопасности выделены два основных направления в области исследования техногенных источников риска на современном этапе: оценка,

анализ риска и управление риском. Отмечено, что в настоящий момент в проводимых исследованиях наблюдается переход от концепции минимизации возможного ущерба к концепции превентивной стратегии управления риском, концентрации внимания на нормальном функционировании системы и ее элементов, повышение роли систем контроля и мониторинга при управлении. В рамках вышеуказанной парадигмы приоритетная роль отводится системам контроля и мониторинга состояний системы в соответствии со сложностью и опасностью контролируемой системы.

На основе полученных данных возможно сформулировать концептуальную математическую модель системы, описывающую общее состояние системы мониторинга чрезвычайных ситуаций техногенного характера в зависимости от уровня опасности объектов мониторинга.

$$Pm \cup \{A_t \subseteq (A_n \cup B_m), B_m\},$$

где P_m – множество состояний системы мониторинга чрезвычайных ситуаций техногенного характера; A_t – множество состояний уровня опасности источника техногенного риска; A_n – множество состояний уровня опасности внешних воздействий, обусловленных природно-климатическими условиями; B_m – множество оценок элементов системы мониторинга в зависимости от характеристик контролируемого объекта.

В рамках реализации риск-ориентированного подхода, принятой в Российской Федерации оценки состояний уровня опасности источника техногенного риска и уровня опасности внешних воздействий, обусловленных природно-климатическими условиями, предлагается использовать 6-бальную оценочную шкалу. Оценку элементов системы мониторинга в зависимости от характеристик контролируемого объекта предлагается проводить по разрабатываемому алгоритму с использованием разновидностей кривой Харрингтона [13–16].

На основе проведенного анализа и результатов исследований, выполненных другими авторами, возможно сформулировать общую задачу, а именно обосновать выбор элементов системы мониторинга с определёнными значениями B_m, при которых значение P_m не превышает значения $P_{кр}$, и стремится максимуму, где $P_{кр}$ критическое состояние системы мониторинга. Для решения данной задачи предлагается использовать общий подход, представленный на рис. 5.

Рисунок 5 – Общий алгоритм решения задачи исследования

Одной из основных задач межведомственной комиссии является работа по внедрению и развитию систем КСОБЖН, с учетом особенностей субъектов Российской Федерации, а также проработка вопросов финансирования наиболее важных направлений комплекса. Поэтапное финансирование и реализация указанной концепции обусловливает необходимость обоснованного выбора оптимальных параметров системы, обеспечивающих наибольший эффект от внедрения на каждом этапе. Наблюдается противоречие между потребностью в повышении уровня безопасности жизнедеятельности населения за счет развития системы мониторинга и прогнозирования чрезвычайных ситуаций и сложившимися формальными процедурами, не обеспечивающими на практике возможность выбора оптимальных параметров при поэтапном построении системы, с учетом территориальных рисков.

Нивелирование данных противоречий может быть достигнуто применением новых подходов, учитывающих как региональные особенности построения системы, так и рациональное использование ресурсов в зависимости от возникающих угроз, в условиях ограниченных ресурсов.

Литература

1. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 декабря 2015 г. № 683). URL: http://kremlin.ru/acts/bank/40391.

2. Качанов С. А., Попов А. П. О месте аппаратно-программного комплекса «Безопасный город» в концепции «Умный город» // Технологии гражданской безопасности. 2019. Т. 16, № 3 (61). С. 4–9.

3. Постановление Правительства РФ от 30.12.2003 № 794 (ред. от 12.10.2020) «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций». URL: http://www.consultant.ru/document/cons_doc_LAW_45914/.

4. Постановление Правительства РФ от 21 мая 2007 г. № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера». URL: https://base.garant.ru/12153609/.

5. Приказ МЧС России от 4 марта 2011 года № 94 «Об утверждении Положения о функциональной подсистеме мониторинга, лабораторного контроля и прогнозирования чрезвычайных ситуаций единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (с изменениями на 26 декабря 2019 года)». URL: https://base.garant.ru/55171083/.

6. Директива №2008/114/ЕС Совета Европейского Союза «О европейских критических инфраструктурах и мерах по их защите». URL: https://base.garant.ru/70333008/

7. ANSI/ASIS 2009. Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use. ANSI/ASIS.SPC.1:2009. URL: https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf.

8. Labaka L., Hernantes J., Sarriegi J. M. Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant. Reliability Engineering and System Safety, 141: 92–105. 2015.

9. Cassotta S. et al. Cyber Threats, Harsh Environment and the European High North (EHN) in a Human Security and Multi-Level Regulatory Global Dimension: Which Framework Applicable to Critical Infrastructures under «Exceptionally Critical Infrastructure Conditions» (ECIC)?. Beijing Law Review, 10: 317–360. 2019.

10. Pursiainen C. H. et al. Critical Infrastructure Resilience Index: in book «Risk, Reliability and Safety: Innovating Theory and Practice». CRC Press, 2183–2189. 2017.

11. Holling C. S. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4 (1): 1–23. 1973.

12. Hollnagel E. Safety-I and Safety-II. The Past and Future of Safety Management. Ashgate, England, 187. 2014

13. Еремина Т. Ю., Назаров А. А. Идентификация и снижение рисков в рамках разработки комплекса «Безопасный субъект Российской Федерации» // Пожарная безопасность 2016. № 3. С. 121–129.

14. Рыбаков А. В. и др. О разработке модели мониторинга состояния системы комплексной безопасности закрытого административно-территориального образования // Сибирский пожарно-спасательный вестник. 2019. № 4. С. 65–69.

15. Рыбаков А. В., Назаров А. А., Мартинович Н. В. Параметрический метод определения комплексного показателя защищенности от техногенной чрезвычайной ситуации на территории ЗАТО // Сибирский пожарно-спасательный вестник. 2020. № 2. С. 72–79.

16. Назаров А. А., Мартинович Н. В. Мельник А. А. Определение комплексного показателя защищенности на основе исследования системы защиты населения и территории от техногенных рисков // Проблемы управления рисками в техносфере. 2020. № 2 (54). С. 94–103.

References

1. O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii (Ukaz Prezidenta RF ot 31 dekabrya 2015 g. № 683).URL: http://kremlin.ru/acts/bank/40391

2. Kachanov S. A., Popov A. P. O meste apparatno-programmnogo kompleksa «Bezopasnyi gorod» v kontseptsii «Umnyi gorod» // Tekhnologii grazhdanskoi bezopasnosti. 2019. T. 16, № 3 (61). C. 4–9.

3. Postanovlenie Pravitel'stva RF ot 30.12.2003 № 794 (red. ot 12.10.2020) «O edinoi gosudarstvennoi sisteme preduprezhdeniya i likvidatsii chrezvychainykh situatsii». URL:
http://www.consultant.ru/document/cons_doc_LAW_45914/.

4. Postanovlenie Pravitel'stva RF ot 21 maya 2007 g. № 304 «O klassifikatsii chrezvychainykh situatsii prirodnogo i tekhnogennogo kharaktera». URL: https://base.garant.ru/12153609/.

5. Prikaz MChS Rossii ot 4 marta 2011 g. № 94 Ob utverzhdenii Polozheniya o funktsional'noi podsisteme monitoringa, laboratornogo kontrolya i prognozirovaniya chrezvychainykh situatsii edinoi gosudarstvennoi sistemy preduprezhdeniya i likvidatsii chrezvychainykh situatsii (s izmeneniyami na 26 dekabrya 2019 goda). URL: https://base.garant.ru/55171083/.

6. Direktiva №2008/114/ES Soveta Evropeiskogo Soyuza «O evropeiskikh kriticheskikh infrastrukturakh i merakh po ikh zashchite». URL: https://base.garant.ru/70333008/.

7. ANSI/ASIS 2009. Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use. ANSI/ASIS.SPC.1:2009. URL:
https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf.

8. Labaka L., Hernantes, J., Sarriegi J. M. 2015. Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant. Reliability Engineering and System Safety, 141: 92–105

9. Cassotta S. et al. 2019. Cyber Threats, Harsh Environment and the European High North (EHN) in a Human Security and Multi-Level Regulatory Global Dimension: Which Framework Applicable to Critical Infrastructures under «Exceptionally Critical Infrastructure Conditions» (ECIC)?. Beijing Law Review, 10: 317–360.

10. Pursiainen C.H. et al. 2017. Critical Infrastructure Resilience Index: in book «Risk, Reliability and Safety: Innovating Theory and Practice». CRC Press, 2183–2189.

11. Holling C. S. 1973. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4 (1): 1–23.

12. Hollnagel E. 2014. Safety-I and Safety-II. The Past and Future of Safety Management. Ashgate, England, 187.

13. Eremina T. Yu., Nazarov A. A. Identifikatsiya i snizhenie riskov v ramkakh razrabotki kompleksa «Bezopasnyi sub"ekt Rossiiskoi Federatsii» // Pozharnaya bezopasnost'. 2016. № 3. P. 121–129.

14. Rybakov A. V. et al. O razrabotke modeli monitoringa sostoyaniya sistemy kompleksnoi bezopasnosti zakrytogo administrativno-territorial'nogo obrazovaniya // Nauchno-analiticheskii zhurnal «Sibirskii pozharno-spasatel'nyi vestnik». 2019. № 4. P. 65–69.

15. Rybakov A. V., Nazarov A. A., Martinovich N. V. Parametricheskii metod opredeleniya kompleksnogo pokazatelya zashchishchennosti ot tekhnogennoi chrezvychainoi situatsii na territorii ZATO // Sibirskii pozharno-spasatel'nyi vestnik. 2020. № 2. C. 72–79.

16. Nazarov A. A., Martinovich N. V., Mel'nik A. A. Opredelenie kompleksnogo pokazatelya zashchishchennosti na osnove issledovaniya sistemy zashchity naseleniya i territorii ot tekhnogennykh riskov // Problemy upravleniya riskami v tekhnosfere. 2020. № 2 (54). P. 94–103.