

## ОСНОВЫ ФОРМИРОВАНИЯ МЕТОДОВ И СИСТЕМ АВАРИЙНОЙ ЗАЩИТЫ ОБЪЕКТОВ ТЕХНОСФЕРЫ ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

**Член-корреспондент РАН Н.А. Махутов,  
кандидат техн. наук М.М. Гаденин, О.Н. Юдина  
Институт машиноведения им. А.А. Благонравова РАН**

*Важнейшей частью процесса управления безопасностью, включающей проведение диагностических измерений, экспертизы, испытаний и оценки параметров объектов, среды и человека, являются разработка и развитие методов аварийной защиты потенциально опасных технических объектов и систем. Целью функционирования систем защиты является предотвращение отказов технических объектов, связанных с угрозой для здоровья и жизни людей, опасностью для окружающей среды, а также с серьезным экономическим и моральным ущербом, которые, по возможности, были бы либо исключены, либо обладали в течение всего установленного срока их службы весьма малой вероятностью проявления. Показано, что системы защиты технических систем, окружающей среды, а также операторов и персонала, в общем случае подразделяется на жесткие, функциональные, естественные, охранные и комбинированные. Построение систем защиты должно быть ориентировано на виды ситуаций при функционировании объектов - штатные ситуации, отклонения от штатных ситуаций, проектные, запроектные и гипотетические аварийные ситуации. Общая структура построения диагностических комплексов, являющихся основой для работы систем защиты, должна включать последовательную и систематизированную иерархию определяющих производственный процесс параметров и иметь возможность их сравнения с соответствующими данными для исходных состояний объектов и для типовых штатных и аварийных ситуаций. Наиболее полно и последовательно вопросы обеспечения безопасности сложных технических систем с использованием рассматриваемых систем защиты в настоящее время решаются в отраслях атомной энергетики, авиационной, ракетно-космической и глубоководной техники.*

**Ключевые слова:** техногенная безопасность, системы аварийной защиты, чрезвычайные ситуации, аварии, катастрофы, диагностика, мониторинг, объекты техносферы.

## ESSENTIAL PRINCIPLES OF FORMATION OF METHODS AND SYSTEMS OF EMERGENCY PROTECTION AGAINST EMERGENCY SITUATIONS FOR OBJECTS OF THE TECHNOSPHERE

**Corresponding Member of the RAS N.A. Makhutov,  
Ph.D. (Tech.) M.M. Gadenin, O.N. Yudina**

**The A.A. Blagonravov Institute for Machines Science of the Russian Academy of Sciences**

*The most important part of process of the safety management including carrying out of diagnostic measurements, examinations, tests and an estimation of installations parameters, environment and persons are working out and an evolution of emergency protection methods for potentially dangerous technical installations and systems. The purpose of functioning of protection systems is prevention of refusals of the technical objects connected with threat for health and life of people, danger to environment and also with serious economic and moral losses,*

which would be or are excluded, or would have very small probability of initiation during all established period of their service. It is shown what systems of protection of technical systems, environment, and also operators and personnel, is generally subdivided on hard, functional, natural, security and combined. Creation of protection systems has to be focused on kinds of situations at functioning objects - regular situations, the deviations from regular situations provided by the design, beyond design basis and hypothetical emergencies. The general structure of creation of the diagnostic complexes which are an essential principle for functioning of protection systems has to include the consecutive and systematized hierarchy of the parameters defining production and to have a possibility of their comparison with the relevant data for initial states of objects and for standard regular conditions and emergencies. Most fully and consistently problems of safety maintenance of technical systems with use of considered approaches for their protection are solved in branches of a nuclear energy, aircraft, space-rocket and deep-water equipment now.

**Keywords:** engineering safety, systems of emergency protection, emergency situations, accidents, disasters, diagnostics, monitoring, objects of the techno sphere.

### 1. Постановка проблемы

Одним из стратегических направлений развития во времени  $\tau$  техногенной сферы является безопасность  $S(\tau)$  в широком смысле ее понимания. Безопасность техносферы заключается в том, чтобы риски  $R(\tau)$  отказов  $R_o(\tau)$ , аварий  $R_a(\tau)$  и катастроф  $R_k(\tau)$  технических объектов, связанные с угрозой для здоровья и жизни людей, опасностью для окружающей среды, а также с серьезным социальным  $U_c(\tau)$  экономическим  $U_s(\tau)$ , моральным  $U_m(\tau)$  и интегральным  $U(\tau)$  ущербом, по возможности, были либо исключены, либо обладали в течение всего установленного срока их службы весьма малыми вероятностями их проявления  $P_c(\tau), P_s(\tau), P_m(\tau)$  и  $P(\tau)$  [1-5]. Важнейшей частью процесса управления безопасностью  $S(\tau)$ , включающей проведение диагностических измерений, экспертизы, мониторинга, натурных испытаний или оценки одной или нескольких указанных выше характеристик опасных состояний объектов, среды и человека, являются разработка и развитие методов оперативной и аварийной защиты заданного уровня  $Z(\tau)$  потенциально опасных технических объектов и систем [2, 3, 6, 7].



Рис. 1. Структура систем защиты объектов техносферы от чрезвычайных ситуаций

Обобщенный анализ систем защиты технических объектов, окружающей среды, а также операторов и персонала предложен в [1-8]. Они были подразделены на следующие основные группы 1 – 4 [3,8]: жесткие, функциональные, естественные, охранные и комбинированные (рис. 1). Системы, датчики мониторинга и защиты ориентированы на три вида *A, B, B* состояний – штатные, аварийные, катастрофические.

В первом случае *A* защита при всех состояниях обеспечивается созданием бункеров, скафандров, контайментов, резко снижающих прямое воздействие поражающих факторов на жизненно важные элементы объектов, операторов и персонал. Во втором случае *B* защита обеспечивается соответствующим построением систем управления - режимным ведением рабочих процессов, диагностикой штатных, аварийных и катастрофических ситуаций, срабатыванием систем автоматизированной защиты. В третьем случае *B* используются различные пассивные (самозащищенные) системы. Комбинированная защита используются одновременно в различных сочетаниях принципов жесткой (1), функциональной (2) и естественной (3) защиты для всех видов состояний *A, B, B*. В последнее время к названным выше добавляется специальная охранный защита (4), функционирующая совместно с ними для создания защитного барьера от разного рода несанкционированных воздействий на сложную техническую систему (СТС). При этом комплектование разных категорий технических систем (объектов технического регулирования – ОТР, опасных производственных объектов – ОПО, критически КВО и стратегически СВО важных объектов) названными типами и уровнями защиты осуществляется, как правило, в зависимости от их уникальности, опасности и значимости, а также от использования на них тех или иных видов диагностики и мониторинга.

Современная постановка проблем обеспечения безопасности и защищенности объектов СТС должна быть увязана с базовыми параметрами  $S(\tau)$ ,  $Z(\tau)$ ,  $R(\tau)$ ,  $P(\tau)$ ,  $U(\tau)$ , группами защит 1 – 4, видами состояний (*A, B, B*) и категориями опасности объектов (ОТР, ОПО, КВО, СВО).

Системы защиты объектов и операторов создаются с учетом возможных семи (1 – 7) классов аварий и катастроф, предложенных в [1–3, 6-10]: 7 – планетарных, 6 - глобальных, 5 - национальных, 4 - региональных, 3 - местных, 2 - объектовых, 1 - локальных. Защита операторов, персонала и населения при планетарных, глобальных, национальных и региональных катастрофах наиболее сложна.

## **2. Методы обеспечения защиты и безопасности при эксплуатации объектов**

Каждой разновидности отказов, аварий и катастроф соответствует свой спектр видов состояний (*A, B, B*), групп (1 – 4) систем защиты и категорий (ОТР, ОПО, КВО, СВО) объектов.

Указанной на рис. 1 структуре систем защиты соответствует общая характеристика ущербов  $U(\tau)$  и вероятностей  $P(\tau)$  возникновения отказов, аварий и катастроф в различных областях жизнедеятельности и жизнеобеспечения (рис. 2).

Наиболее тяжелыми могут быть ущербы от катастрофических проявлений оружия массового поражения (ОМП) в мирных, кризисных, террористических и военных ситуациях для состояний *A, B, B*.

Основной принцип построения функционирования защиты состоит в переносе центра тяжести всех мероприятий на предотвращение возможностей, вероятностей  $P(\tau)$  возникновения тяжелых аварий и катастроф или снижение рисков  $R(\tau)$  их возникновения.

В соответствии с рис. 1 и 2 для критически (КВО) и стратегически (СВО) важных объектов, создающих угрозы планетарных (7), глобальных (6) и национальных (5) катастроф необходимо [1-8]:

- создание и использование всех систем защиты (1-4);

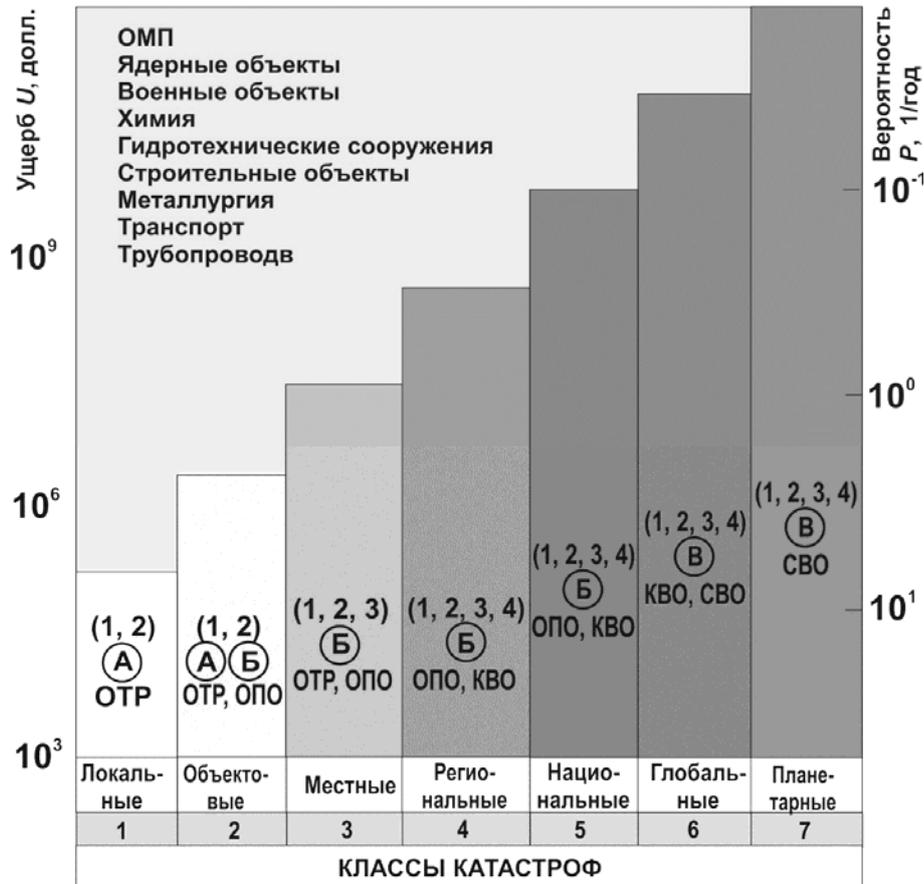


Рис. 2. Обобщенная схема ущербов  $U(\tau)$  и вероятностей  $P(\tau)$  возникновения отказов, аварий и катастроф различных классов

- проведение комплексного анализа рисков  $R(\tau)$  безопасности  $S(\tau)$  и защищенности  $Z(\tau)$ ;
- минимизация рисков  $R(\tau)$  до приемлемого уровня  $[R(\tau)]$ .

С позиций теории безопасности  $S(\tau)$  и рисков  $R(\tau)$  научной основой количественного определения рисков  $R(\tau)$  является функциональная связь между основными его параметрами  $P(\tau)$  и  $U(\tau)$

$$R(\tau) = F_R \{P(\tau), U(\tau)\} \leq [R(\tau)] = \frac{R_k(\tau)}{n_R} \quad (1)$$

где  $R_k(\tau)$  – критические (неприемлемые) риски,  
 $n_R$  – запас по рискам, ( $n_R \geq 1$ )

При этом параметры  $P(\tau)$  и  $U(\tau)$  рисков  $R(\tau)$  в свою очередь являются зависящими от антропогенных, природных и техногенных опасных иницирующих, повреждающих и поражающих факторов [1-11]

$$R(\tau) = F_R \{R_A(\tau), R_{II}(\tau), R_T(\tau)\} \quad (2)$$

Интегральные ущербы  $U(\tau)$  и вероятности  $P(\tau)$  с учетом социальных, экономических и моральных аспектов будут

$$U(\tau) = F_U \{U_c(\tau), U_s(\tau), U_m(\tau)\} \quad (3)$$

$$P(\tau) = F_P \{P_c(\tau), P_s(\tau), P_m(\tau)\} \quad (4)$$

В общем случае (рис. 3) система выражений (1) – (4) составляет исходную научную базу [1, 3, 8-13] для создания систем защиты  $Z(\tau)$ , удовлетворяющих заданным уровням безопасности  $S(\tau)$  по критериям приемлемых рисков в (1).

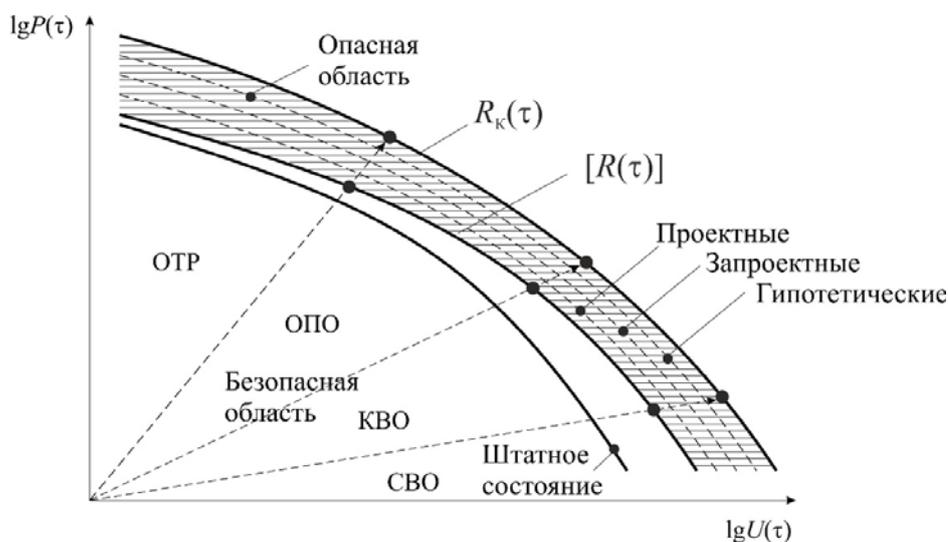


Рис. 3. Принципиальная схема взаимовязанного анализа параметров риска, состояний и опасности объектов

Безопасность  $S(\tau)$  в анализируемое время  $(\tau)$  может считаться обеспеченной, если сформировавшиеся риски  $R(\tau)$  меньше, чем  $[R(\tau)]$

$$S(\tau) = [R(\tau)] - R(\tau) \geq 0 \quad (5)$$

Уровень защищенности объектов, природы и человека от отказов, аварий и катастроф с учетом (5) количественно можно оценить по относительной величине рисков

$$Z(\tau) = 1 - R(\tau)/[R(\tau)] \geq 0 \quad (6)$$

Анализ интегральных экономических потерь при наиболее тяжелых катастрофах на атомных электростанциях (ТМА – США, ЧАЭС – СССР, Фокусима-1 – Япония), относящихся к стратегически важным объектам, показал [2, 3, 14], что прямые интегральные экономические ущербы  $U(\tau)$  достигали  $10^{10}$  долл. США, а интегральные прямые и косвенные ущербы при таких катастрофах могут быть выше в 10 и более раз. Постулированная в отечественных и зарубежных нормах безопасности АЭС приемлемая вероятность  $[P(\tau)]$  находится в пределах от  $10^{-6}$  до  $10^{-7}$  1/год. При общемировом числе функционировавших

АЭС в период 1970 – 2010 гг., начиная с первой катастрофы в США частота (вероятность)  $P(\tau)$  их возникновения постепенно снижалась от  $2 \cdot 10^{-3}$  1/год до  $2 \cdot 10^{-4}$  1/год. В атомной энергетике величина  $P(\tau)$  принимается эквивалентной техногенному риску  $R(\tau)$ . Приведенные данные показывают, что условия (5), (6) в атомной энергетике пока не достигнуты.

В настоящее время проблемы безопасности  $S(\tau)$ , рисков  $R(\tau)$  и защищенности достаточно остро стоят перед разработчиками объектов добычи, переработки и транспортировки углеводородов (нефти, газа) на континентальном шельфе [15]. Катастрофа на морской платформе США в Мексиканском заливе сопровождалась интегральным ущербом на уровне  $6 \cdot 10^{10}$  долл.

В число важных высокорисковых объектов техносферы, относящихся к категориям КВО и СВО, входят объекты ракетно-космической техники (космические аппараты гражданского и оборонного назначения, космодромы). Катастрофы на них с гибелью космонавтов и персонала (от  $10^0$  до  $10^2$  человек) приводили в ряде случаев к таким же прямым ущербам, как и на атомных электростанциях.

С учетом приведенных выше данных, Парламентская комиссия по анализу тяжелой аварии на Саяно-Шушенской ГЭС, сопровождавшейся гибелью технического персонала, разрушением машинного зала и общим экономическим ущербом  $U(\tau)$  до  $2 \cdot 10^{11}$  руб., предложила [17] считать необходимым обеспечение защищенности  $Z(\tau)$  КВО и СВО от катастроф по критериям рисков  $R(\tau)$  и  $[R(\tau)]$  на основе выражения (6).

Решение этой задачи сопряжено с расчетным определением требуемых затрат  $Z_R(\tau)$  на снижение рисков  $R(\tau)$  до приемлемого уровня  $[R(\tau)]$ .

$$Z_R(\tau) = \frac{1}{m_z} \{R(\tau) - [R(\tau)]\} \quad (7)$$

где  $m_z$  – коэффициент эффективности затрат ( $m_z \geq 1$ )

При выполнении научно обоснованных комплексных мероприятий расчетного, конструкторско-технологического, нормативного, надзорного характера величина  $m_z$  может быть доведена до  $2 \div 10$ .

### **3. Разработка и реализация систем защиты.**

С учетом рис. 1 и 2 и выражений (1) – (7) при местных, объектовых и локальных авариях, наряду с мероприятиями по их предотвращению, должны предусматриваться способы и системы защиты как для штатных условий функционирования потенциально опасных объектов, так для аварийных и послеаварийных ситуаций. Способы и системы защиты зависят от характера поражающих факторов.

В общем случае построение систем защиты объектов, операторов и персонала должно быть ориентировано на виды ситуаций при функционировании объектов: штатные ситуации, отклонения от штатных ситуаций, проектные, запроектные и гипотетические аварийные ситуации. Степень реальной защищенности  $Z(\tau)$  объектов, операторов и персонала снижается при переходе от штатных к проектным, запроектным и гипотетическим аварийным ситуациям для всех объектов техносферы (ОТР, ОПО, КВО, СВО). Это в значительной степени связано с тем, что для ОТР и ОПО имеется значительный отечественный и международный опыт обеспечения длительного безопасного функционирования объектов с проверенными и обоснованными условиями работы операторов и персонала. Для КВО и СВО сами гипотетические аварийные ситуации характеризуются существен-

ной неопределенностью условий их возникновения и сценариев развития [9]. Это, в свою очередь, определяет сложность анализа поражающих факторов и формирование соответствующих им требований к системам защиты.

С учетом сказанного, для штатных и аварийных ситуаций функционирования потенциально опасных технических систем, опасные  $Q(\tau)$  воздействия на их объекты, операторов, персонал и население можно классифицировать следующим образом.

Сверхслабые воздействия  $Q_{cc}(\tau)$  (электромагнитные, химические, радиационные, механические) находятся существенно ниже порогов чувствительности человека, и могут устанавливаться, и измеряться сверхчувствительными современными приборами.

Слабые воздействия  $Q_c(\tau)$  (тепловые, механические, акустические, электромагнитные, радиационные, химические) находятся на уровне частичных повреждений технических систем, восприятия органами чувств человека или незначительно превышают его.

Слабые воздействия на человека (операторов, персонал, население) сопутствуют обычно его профессиональной деятельности в штатных условиях и быту. Они порождаются техническими системами и обычными природными явлениями.

Умеренные воздействия  $Q_y(\tau)$  той же природы и происхождения, что и слабые, могут в десятки и сотни раз превосходить пороговые. Умеренные воздействия сопутствуют штатным и нештатным (предаварийным и аварийным) ситуациям на большинстве технических объектов (промышленных, строительных, горнодобывающих, транспортных, энергетических, химических).

Экстремально сильные воздействия  $Q_{эс}(\tau)$  техногенного и природного происхождения могут вызывать необратимые изменения в технических объектах и в организме или приводить к летальному исходу. Эти воздействия могут иметь место в штатных ситуациях при грубых нарушениях операторами и персоналом производственной дисциплины и техники безопасности, а также при авариях и катастрофах природно-техногенного характера, при террористических актах и в условиях военных конфликтов.

Экстремальные сверхсильные воздействия  $Q_{эсс}(\tau)$  (сверхзвуковые механические и ударные волны, отравления и удушья при сверхвысоких концентрациях отравляющих веществ, сверхмощные тепловые и радиационные потоки), как правило, приводят к повреждению объектов и к практически мгновенному летальному исходу. Такие воздействия возникают при тяжелых авариях и катастрофах на объектах с исключительно высокой потенциальной опасностью - объекты ядерного цикла, взрыво- пожароопасные объекты гражданского и оборонного комплекса, сверхзвуковая авиация и ракетно-космические системы. Эти воздействия возникают при террористических актах и в условиях военных конфликтов.

При увеличении интенсивности воздействий  $Q(\tau)$  от  $Q_{cc}(\tau)$  до  $Q_{эсс}(\tau)$  и по мере перехода объектов от ОТР к СВО (ОТР  $\rightarrow$  ОПО  $\rightarrow$  КВО  $\rightarrow$  СВО), происходит изменение состояний объектов от штатных к гипотетически катастрофическим с нарастанием  $U(\tau)$  и  $R(\tau)$  даже при снижении  $P(\tau)$ . С использованием данных рис. 1 и 2 эти обстоятельства отражаются обобщенной зависимостью (близкой к степенной), связывающей  $P(\tau)$  и  $U(\tau)$  в выражении (1), показанной на рис. 3.

$$\{R(\tau), P(\tau), U(\tau)\} = F_Q\{Q(\tau)\} \quad (8)$$

Учет поражающих факторов от всего спектра воздействий  $Q(\tau)$  по цепочке  $Q_{cc}(\tau) \rightarrow Q_c(\tau) \rightarrow Q_y(\tau) \rightarrow Q_{эс}(\tau) \rightarrow Q_{эсс}(\tau)$  при разработке методов, систем и средств защиты  $Z(\tau)$  операторов, персонала и населения при штатных и аварийных ситуациях требует формирования соответствующих технических требований и характеристик. Практика эксплуатации сложных и потенциально опасных технических систем, управляемых операторами

(атомные, гидравлические и тепловые электростанции, транспорт, авиация и т.п.) показывает, что значительный процент отказов подобных систем происходит по вине обслуживающего персонала  $R_a(\tau)$  в выражении (2).

С учетом изложенного (рис. 1-3 и выражений (1) – (7)), можно заключить, что при формировании общих принципов и требований к технике и технологиям предупреждения и предотвращения техногенных аварий и катастроф и систем защиты от них следует иметь в виду, что:

– при анализе безопасности высокорисковых объектов с переходами ОТР → ОПО → КВО → СВО целесообразно использовать одно- и многопараметрические системы моделирования, включающие интегральные параметры риска  $R(\tau)$  по (1) и (2) и учитывающие вероятности  $P(\tau)$  по (3) возникновения аварий и катастроф, а также ущербы  $U(\tau)$  по (3) от них; при этом статистические и детерминированные модели при анализе функционала  $F$  риска в (1) реализуются в зависимости от потенциальной опасности объекта и тяжести аварийных ситуаций, а при росте последних сокращаются объемы исходной статистической информации и повышается роль детерминированных методов;

– построение диагностических моделей и систем диагностики должно осуществляться для различных стадий развития аварийных ситуаций: при штатных ситуациях используются встроенные системы диагностики или унифицированные мобильные; в аварийных проектных ситуациях к указанным выше добавляются мобильные специальные системы, предназначенные для работы в условиях поражающих воздействий от этих аварийных ситуаций; при запроектных и гипотетических аварийных ситуациях возможности оперативной диагностики резко сокращаются, и основное значение приобретают дистанционные измерительные комплексы;

– для случаев ненулевых вероятностей возникновения аварий и катастроф на высокорисковых объектах должны создаваться системы жесткой, функциональной, естественной, охранной и комбинированной защиты; по мере повышения потенциальной опасности наиболее перспективными следует считать перекрестные системы автоматической защиты для объектов и операторов.

При разработке базовых концепций безопасности  $S(\tau)$  и защищенности  $Z(\tau)$  [6, 10] приоритетными являются мероприятия, предупреждающие аварии и катастрофы и снижающие  $P(\tau)$ , а также мероприятия, уменьшающие последствия  $U(\tau)$  подобных негативных событий.

Основное требование концепции обеспечения безопасности  $S(\tau)$  – снижение рисков аварий и катастроф  $R(\tau)$  – реализуется на базе следующих составляющих ее основу принципов:

- организации безопасного функционирования технической системы;
- недопущения наихудшего случая возникновения чрезвычайной ситуации;
- обеспечения качества исходных компонентов системы;
- непрерывных эксплуатационных наблюдений и документирования;
- непрерывной диагностики, мониторинга и оперативного анализа условий возникновения наиболее опасных предельных состояний.

Эти составляющие одновременно являются и направлениями в перспективных научных исследованиях, и каждая из них определяет свой круг задач, который необходимо решать всякий раз при разработке новых и совершенствовании уже существующих технических систем высокой потенциальной опасности и способов их защиты.

Рассматриваемые подходы к обеспечению безопасности  $S(\tau)$  функционирования технических систем и разработки соответствующих систем их защиты  $Z(\tau)$  являются составной частью общей теории безопасности. Под общими принципами обеспечения безопасности  $S(\tau)$  и защищенности  $Z(\tau)$  следует подразумевать концептуальные положения о возможных путях предотвращения, накопления и локализации последствий от

потенциально возможных угроз - катастроф, аварий природного и техногенного происхождения. Пути обеспечения безопасности могут быть условно разделены на три направления (принципа):

- предупреждение и предотвращение потенциальных аварий и катастроф – минимизация  $P(\tau)$ ;
- локализация аварий и минимизация последствий системами защиты в случае их возникновения – минимизация  $U(\tau)$ ;
- прекращение функционирования потенциально опасных объектов на ранних стадиях развития тяжелых аварий и катастроф.

Общие принципы обеспечения техногенной безопасности  $S(\tau)$  и повышения защищенности  $Z(\tau)$  должны учитываться на стадиях проектирования, строительства, эксплуатации и планового вывода из эксплуатации соответствующих сложных технических систем (ОПО, ОТР, КВО, СВО). Под обеспечением безопасности технической системы при этом в основном подразумевается реализация следующих основных принципов:

- создание безаварийных объектов с возможностью реализации только безопасных отказов;
- создание системы защиты, препятствующих развитию поражающих факторов;
- реализация мероприятий, способствующих ликвидации последствий аварий.

Одним из важных элементов в обеспечении безопасности функционирования сложной технической системы является наличие комплексной, обязательной к выполнению, программы, определяющей состав, последовательность, организацию, методические основы, содержание и этапы выполнения мероприятий, обеспечивающих заданный уровень безопасности  $S(\tau)$  по критериям  $R(\tau)$  и  $[R(\tau)]$  на основе (5). Программа обеспечения безопасности  $S(\tau)$  может быть индивидуальной (на составную часть объекта), групповой (на группу объектов, объединенных функциональной значимостью, технологическим процессом и т.д.).

В такой программе должны быть отражены:

- требуемые уровни рисков  $R(\tau)$  и безопасности  $S(\tau)$  функционирования сложной технической системы, в том числе в экстремальных ситуациях при всех воздействиях  $Q(\tau)$  по (8);
- пути достижения требуемого уровня безопасности  $S(\tau)$  по приемлемым рискам  $[R(\tau)]$  в выражении (5) (рациональные конструктивные и структурные решения; использование высоконадежного и качественного оборудования и его резервирование);
- системы защиты, обеспечивающие безошибочную работу обслуживающего персонала с малыми рисками  $R_a(\tau)$  в (2);
- способы поддержания необходимого уровня работоспособности технической системы в аварийных ситуациях по условию (5), в том числе с использованием систем защиты (управление аварией) по выражению (6);
- способы минимизации (смягчения) последствий  $U(\tau)$  возможной аварии;
- методы достижения необходимого уровня подготовки обслуживающего персонала (культура безопасности);
- система учета, сбора и анализа причин отказов в работе объектов при эксплуатации;
- ответственность эксплуатирующих организаций;
- структуры независимого контроля эксплуатации;
- опыт эксплуатации, испытаний и обосновывающих научных исследований.

#### 4. Основы построения систем защиты

Основными этапами построения и реализации систем защиты являются (рис. 4):

- декомпозиция процесса функционирования сложных технических систем, объектов и процессов с выделением, соответственно, элементарных операций и обобщенных элементов;



Рис. 4. Структурная схема объектов, опасных ситуаций, диагностики и защиты

- составление алгоритма функционирования во времени ( $\tau$ ) технических систем и объектов;
- формирование видов возможных аварийных состояний;
- определение вероятностей изменения состояния, оценка эффективности резервирования и информационного обеспечения;
- формирование перечня особых ситуаций и установление категории (степени) их опасности;
- выделение из всего множества опасных компонентов особоответственных, при единичном отказе которых становится невозможным безопасное функционирование технических систем и объектов;
- получение конечных результатов анализа для построения систем защиты.

При построении систем защиты могут быть применены следующие подходы [1-5, 8, 11-19]:

- использование существующих аналогов и последних научно-технических достижений в компьютерных, робототехнических, материаловедческих, управленческих технологиях;

- аналитический расчет ресурса и живучести систем защиты на основе определения нижнего допустимого уровня аварийной устойчивости с учетом возможных чрезвычайных ситуаций в процессе длительной эксплуатации;

- использования расчетных и физических моделей объектов и систем защиты на различных стадиях развития аварийных ситуаций.

Расчетные и физические модели объектов с развитыми системами диагностики, мониторинга и защиты должны представлять собой (рис. 5) системы, функционирующие в реальном масштабе времени по сценарию, задаваемому как в направлении утяжеления чрезвычайной ситуации, так и в обратном направлении.



Рис. 5. Взаимодействие системы диагностики и защиты объектов в штатных и нештатных ситуациях

Такие системы в общем случае должны обеспечивать вывод заранее подготовленных наборов данных о способах защиты в указанные моменты времени, регистрацию реакции объекта на внутренние и внешние воздействия, поступающих из датчиков и систем мониторинга и диагностики, и фиксацию времени  $\tau$  их поступления для последующего перехода от одного типа защиты к другому [18].

Математические модели объекта и систем защиты должны моделировать во времени  $\tau$  все заданные для анализа состояния  $(A, B, V)$ . Такие модели должны отражать реальные состояния объектов, и тем самым обеспечивать работоспособность систем защиты и их программного обеспечения в наиболее тяжелых условиях, не позволяющих использовать физическое моделирование.

Стратегия обеспечения безопасности и построения систем защиты должны строиться по трем направлениям:

- стратегия управления безопасностью и рисками сложных технических систем, объектов и процессов;

- стратегия обеспечения глубоко эшелонированной защиты (защиты в глубину) по всем характеристикам и группам;

- стратегия генеральных технических и организационных решений.

Первое направление строится на следующих принципах:

- использование теории безопасности и рисков;
- ответственность проектной и эксплуатирующей организации;
- государственный, региональный и объектовый надзор и контроль за безопасностью сложных технических систем, объектов и процессов на всех стадиях их жизненного цикла.

Второе направление строится на следующих принципах:

- глубокая многобарьерная, комбинированная и эшелонированная защита (защита в глубину);

- прогнозирование, предупреждение, предотвращение развития аварий по наиболее опасным сценариям;

- ослабление последствий аварий за счет эффектов естественной защиты.

Третье направление включает:

- научно обоснованная апробированная инженерно-техническая практика создания систем защиты с учетом передовых разработок по созданию унифицированных и специальных методов и средств защиты.

- обеспечение качества, надежности, ресурса и живучести систем защиты;

- учет и использование человеческого фактора во всех сценариях развития чрезвычайной ситуации;

- оценка, тестирование и комплексная проверка систем защиты и безопасности;

- учет возрастающей роли несанкционированных и террористических воздействий.

При эксплуатации потенциально опасного объекта с помощью технического диагностирования и мониторинга должно быть определено состояние его функционирования (штатное, предаварийное, аварийное) и осуществлен поиск источников и причин возникновения состояний вида *Б* и *В*.

При построении систем защиты следует использовать следующие принципы их функционирования:

- автоматическое прерывание технологических процессов при возникновении аварийных ситуаций;

- ограничение последствий чрезвычайных ситуаций (локализация выходов радиации, отравляющих веществ, пожаров, взрывов, обеспечение своевременной эвакуации людей);

- создание исполнительных механизмов автоматизированного закрытия определяющих распространение опасных последствий чрезвычайной ситуации систем и структур (клапанов, проемов, дверей, проходов и т.п.);

- разделение помещений и компонентов объекта противоаварийными перегородками и перекрытиями.

Критериями выбора у групп и принципов защиты должны быть допустимые уровни воздействий:

- для персонала - защита от неконтролируемого выброса опасных веществ (токсины, отравляющие, радиоактивные и биологически опасные вещества), снижение интенсивности облучения, теплового воздействия, давления воздушной ударной волны и акустического воздействия, защита от первичных и вторичных поражающих факторов, в т.ч. осколков;

- для оборудования - защита от радиации, температур, давления и колебаний;

- для опасных веществ - защита от детонации, возгорания, осколков и ударной волны;

- для систем управления, контроля и мониторинга – защита от прерывания или неконтролируемого искажения информационных потоков.

Наиболее представительными являются группы и средства систем защиты, основанные на принципе прерывания (подавления) аварийного процесса или опасного сопутст-

вующего фактора, а также отключающие из функциональной схемы объекта аварийные блоки. Это различного рода предохранительные устройства, системы пожаротушения, системы аварийной остановки ядерных реакторов и многие другие.

По принципу действия эти системы защиты можно подразделить на:

- предохраняющие элементы объектов или окружающую среду от опасных для них входных параметров от аварийного воздействия (это, как правило, системы жесткой защиты);

- отключающие аварийные блоки: принцип их действия может быть различным в зависимости от характера входного сигнала (механический, электрический, тепловой, радиационный и т.д.) и требований к такой системе защиты (по быстрдействию, восстанавливаемости, прочности, надежности и т.п.);

- прерывающие аварийные процессы (прекращение подачи рабочего вещества или энергии, подключение резервного оборудования, активное подавление поражающих факторов на аварийном участке) или отключающие аварийные блоки (это, как правило, системы функциональной защиты);

- локализирующие развитие и последствия аварии (посредством жесткой защиты, дополнительно возможно использование элементов функциональной защиты) - ограничивают масштаб аварии и их применение признано наиболее эффективным и существенно повышающим безопасность таких сложных технических систем.

Группа систем функциональной защиты включает в себя следующие элементы:

- подгруппу регистрации технологических параметров процессов и преобразования данных;

- подгруппу анализа данных;

- подгруппу исполнительных механизмов для управления объектом и ликвидации (локализации, ослабления) последствий аварии или аварийного состояния.

Такие системы могут быть реализованы в виде систем диагностирования и контроля, а также в виде систем противоаварийной защиты.

Системы диагностирования технического оборудования и управления должны включать в себя тестовые виды диагностики на базе компьютерной техники. Системы контроля параметров должны быть отградуированы на включение при достижении заданного уровня их предельных значений. При этом система диагностирования должна определять состояние функционирования объекта (допустимое, предаварийное, аварийное), а также осуществлять поиск неисправностей.

Система противоаварийной защиты должна являться подсистемой общей автоматизированной системы управления объектом и ее действия должны быть приоритетными и иметь равные с общей автоматизированной системой управления показатели надежности функционирования.

С учетом изложенного, общие принципы построения систем защиты заключаются в следующем:

- резервирование (для обеспечения требуемых показателей надежности применяется дублирование элементов системы защиты);

- независимость элементов;

- разделение элементов (элементы должны быть размещены и функционально связаны таким образом, чтобы в результате аварии не вышли одновременно все элементы защиты, выполняющую одинаковую функцию);

- различие (разнотипность) - защита систем и элементов, выполняющих одну задачу от однотипного отказа путем выполнения их различными по конструкции, принципу действия и другим параметрам.

Из изложенного выше следует, что реализация в настоящее время и в перспективе комплексных научных, конструкторско-технологических и эксплуатационных решений по эффективному созданию и функционированию техносферы для жизнедеятельности

человека, общества и государства возможна для условий приемлемых рисков по выражению (1). Для этого в соответствии с принципиальной схемой по рис. 6 необходимо выполнение ряда определяющих мероприятий.

Для любого объекта техносферы (ОТР, ОПО, КВО, СВО) в технических заданиях и технико-экономических обоснованиях проекта следует представить все спектры воздействий  $Q(\tau)$  на объекты с установлением реакций объекта на эти воздействия. На этой основе должны быть выделены и обоснованы поражающие и повреждающие факторы антропогенного, техногенного и природного характера со своими вероятностями  $P(\tau)$  по выражению (4) и сопутствующими ущербами  $U(\tau)$  по выражению (3). Это дает возможность количественного определения рисков  $R(\tau)$  по выражениям (1) и (2). Риски  $R(\tau)$  и  $[R(\tau)]$  являются исходными для расчетного определения безопасности  $S(\tau)$  по выражению (5) и защищенности  $Z(\tau)$  по выражению (6). Если условия (5) и (6) не выполняются, осуществляется разработка комплексных многоуровневых и многоцелевых мероприятий с обязательными затратами  $Z_R(\tau)$  на снижение рисков  $R(\tau)$  до приемлемых  $[R(\tau)]$ . При этом, решающую роль играют мероприятия по построению и развитию систем защиты, в том числе автоматизированной, включаемой в работу при выходе рисков  $R(\tau)$  в опасную зону. Затраты  $Z_R(\tau)$  и экологические риски  $R(\tau)$  снижают эффективность создания и развития объектов техносферы. Учет этого обстоятельства позволяет принимать обоснованные решения как о возможности, так и о невозможности реализации предлагаемых проектов для всех потенциально опасных объектов техносферы, в первую очередь - критически и стратегически важных.

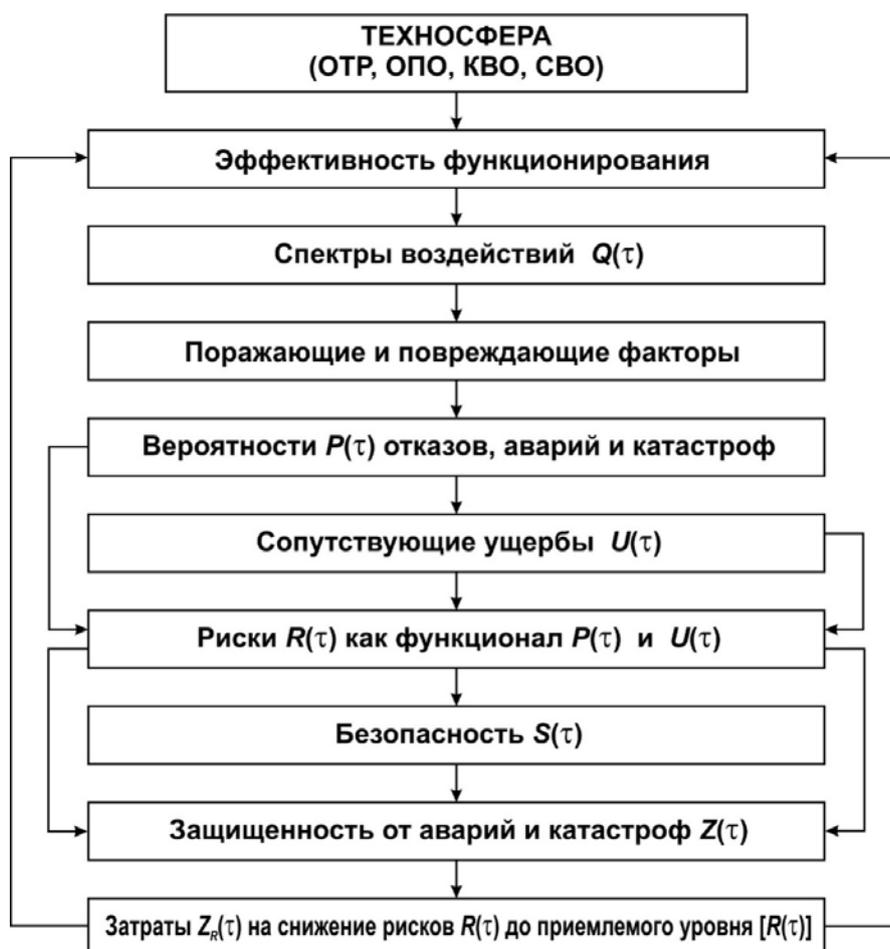


Рис. 6. Принципиальная схема анализа и обеспечения безопасности и защищенности по критериям риска для достижения эффективного создания и функционирования техносферы

## Заключение

Таким образом, номенклатура параметров, методов и средств комплексной оперативной диагностики элементов технических систем имеет широкий спектр и достаточно трудоемка при реализации в методическом и аппаратурном плане. Общая структура построения диагностических комплексов, являющихся основой для работы систем защиты, должна включать последовательную и систематизированную иерархию определяющих производственный процесс параметров. При этом должно реализовываться выявление изменений этих параметров при возникновении аварии и их сравнение с соответствующими данными для исходных состояний объектов и для типовых штатных и аварийных ситуаций. На основе этого системой защиты объекта осуществляется прогнозирование развития дефектов конструкции в процессе течения аварии с определением условий достижения предельных состояний, приводящих как к локальным, так и общим разрушениям, и прогнозированию и предотвращению их последствий. С усложнением и развитием объектов технических систем, и с повышением требований к их надежности и недопустимости создания чрезвычайных ситуаций, которые могут привести к тяжелым авариям и катастрофам, увеличивается число контролируемых структурных параметров технических систем и расширяется номенклатура привлекаемых для защиты таких объектов систем предотвращения их возникновения и недопущения или минимизации негативных последствий в случаях их развития. Наиболее полно и последовательно вопросы обеспечения безопасности сложных технических систем с использованием рассматриваемых систем защиты в настоящее время решаются в отраслях атомной энергетики, авиационной, ракетно-космической и глубоководной техники.

## Литература

1. Безопасность России Правовые, социально-экономические и научно технические аспекты. Техногенная, технологическая и техносферная безопасность. М.: МГОФ «Знание». - 2018. - 1016 с.
2. Безопасность России Правовые, социально-экономические и научно технические аспекты. Фундаментальные и прикладные проблемы комплексной безопасности. Сводный том. Научный руководитель чл.-корр. РАН Н.А. Махутов. М.: МГОФ «Знание». - 2017. 992 с.
3. Махутов Н.А. Безопасность и риски: системные исследования и разработки. Новосибирск: Наука. - 2017. - 724 с.
4. Terrorism: Reducing Vulnerabilities and Improving Responses: U.S.-Russian Workshop Proceedings. Washington, DC: The National Academies Press: 2004, p. 239.
5. Воробьев Ю.Л., Акимов В.А., Соколов Ю.И. Комплексная безопасность человека. М.: ВНИИ ГОЧС. - 2011. - 360 с.
6. Гаденин М.М. Структура многоуровневого мониторинга параметров безопасности техносферы и окружающей среды. Проблемы безопасности и чрезвычайных ситуаций. - 2012, № 1. С. 93-102.
7. Махутов Н.А., Гаденин М.М., Ахметханов Р.С., Юдина О.Н. Комплексный мониторинг состояния и безопасности окружающей среды и объектов техносферы // Партнерство цивилизаций. 2020. № 1-2. С. 157-172. DOI: 10.33917/ps.1-2.26-27.2020.157-172
8. Probabilistic Modeling in System Engineering. Ed. by A. Kostogryzov. – London: IntechOpen. - 2018 - 278 p.
9. Махутов Н.А., Гаденин М.М. Анализ предельных состояний и типов аварийных ситуаций в связи с оценкой ресурса безопасной эксплуатации // Проблемы машиностроения и автоматизации. - 2019, №2. С. 4-16.
10. Махутов Н.А., Гаденин М.М. Анализ и мониторинг опасных состояний объектов техносферы. Материалы XIX Международной научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций «Опыт ликвидации крупномасштабных

чрезвычайных ситуаций в России и за рубежом». 20 – 23 мая 2014 г. М.: ФГБУ ВНИИ ГОЧС (ФЦ). - 2014. С. 329-345

11. Махутов Н.А., Гаденин М.М., Юдина О.Н. Научный анализ рисков в жизнеобеспечении человека, общества и государства // Проблемы анализа риска. - 2019, том 16, № 2. С. 70-86. DOI: 10.32686/1812-5220-2019-16-2-70-86

12. Махутов Н.А., Гаденин М.М., Печеркин А.С., Красных Б.А. Расчетно-экспериментальные подходы к анализу и обеспечению ресурса и срока безопасной эксплуатации промышленных объектов // Безопасность труда в промышленности. - 2020. № 1. С. 7-15. DOI: 10.24000/0409-2961-2020-1-7-15

13. Махутов Н.А., Гаденин М.М., Печёркин А.С., Красных Б.А. Научные проблемы определения и управления ресурсом и сроком безопасной эксплуатации промышленных объектов // Безопасность труда в промышленности. - 2019. № 4. С. 7-15. DOI: 10.24000/0409-2961-2019-4-7-15

14. Анализ рисков и повышение безопасности водо-водяных энергетических реакторов. Под ред. Н.А. Махутова, М.М. Гаденина. М.: Наука. - 2009 – 499 с.

15. Безопасность России Правовые, социально-экономические и научно технические аспекты. Обоснование прочности и безопасности объектов континентального шельфа. М.: МГОФ «Знание». - 2015. - 664 с.

16. Makhutov N., Gadenin M., Razumovskiy I., Maslov S., Reznikov D.. Probability Modeling Taking into Account Nonlinear Processes of a Deformation and Fracture for the Equipment of Nuclear Power Plants. In Probability, Combinatorics and control (A. Kostogryzov and V. Koroleveds.) IntechOpen. London. - 2019

17. Разрушение гидроагрегата № 2 Саяно-Шушенской ГЭС: причины и уроки. //Сборник материалов в 3-х томах. - М.: НП «Гидроэнергетика России». - 2013.

18. Махутов Н.А. Конструкционная прочность, ресурс и техногенная безопасность. Часть 2. Обоснование ресурса и безопасности. — Новосибирск: Наука. - 2005. — 610 с

19. Махутов Н.А., Гаденин М.М., Юдина О.Н. Научная и информационная поддержка обеспечения безопасности в связи с чрезвычайными ситуациями. Проблемы безопасности и чрезвычайных ситуаций. - 2018. № 5. С. 3-26.

### **Сведения об авторах**

**Махутов Николай Андреевич**, чл.-корр. РАН, главный научный сотрудник, Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН). E-mail: safety@imash.ru. Тел. +7(495)930-80-78

**Гаденин Михаил Матвеевич**, ведущий научный сотрудник, Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН). E-mail: safety@imash.ru. Тел. +7(499)135-55-09

**Юдина Ольга Николаевна**, научный сотрудник, Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН). E-mail: mibsts@mail.ru. Тел. +7(495)624-25-88