УДК 614.8.084

# ОСОБЕННОСТИ ТЕРРОРИСТИЧЕСКИХ УГРОЗ ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ И МЕРЫ ПО СНИЖЕНИЮ ТЕРРОРИСТИЧЕСКИХ РИСКОВ

**Чл.-корр. РАН, д-р техн. наук *Н.А. Махутов, Е.Ф. Дубинин*,**
**канд. экон. наук *В.И. Куксова***
**Институт машиноведения им. А.А.Благонравова РАН (ИМАШ РАН)**

*Рассмотрены опасности и угрозы в природно-техногенно-социальной системе, особенности террористических угроз для КВО, типы и тенденции современного терроризма. Отмечено, что террористические воздействия могут являться инициирующими факторами аварий и катастроф. Для минимизации террористических рисков для КВО предложено мероприятия по снижению уязвимости КВО проводить в два этапа. Первый этап предполагает защиту критических элементов КВО от экстремальных воздействий с целью предупреждения локальных повреждений в системе. Второй этап предусматривает совершенствование структуры объекта – резервирование, построение защит для локализации отказов, предотвращения каскадных эффектов и наиболее катастрофических сценариев после нанесения объекту локальных повреждений.*

**Ключевые слова:** критически важные объекты, террористические угрозы, риск, инициирующие факторы, техногенные аварии и катастрофы, уязвимость, защищенность, критический элемент, системы защиты.

# PECULIARITIES OF TERRORIST THREATS TO CRITICAL FACILITIES AND MEASURES TO REDUCE TERRORIST RISKS

**Corresponding member of the RAS, Dr. (Tech.) *N.A. Makhutov*, *E.F. Dubinin*,**
**Ph.D. (Econ.) *V.I. Kuksova***
**The A.A. Blagonravov Institute of Machines Science**
**of the Russian Academy of Sciences**

*The article deals with the dangers and threats in the natural-technogenic-social system, the peculiarities of terrorist threats to critical facilities, the types and trends of modern terrorism. It is noted that terrorist attacks can be initiating factors of accidents and disasters. In order to minimize terrorist risks for critical facilities, it is proposed that measures to reduce the vulnerability of critical facilities be carried out in two stages. The first stage involves the protection of critical elements of critical facilities from extreme impacts in order to prevent local damage in the system. The second stage involves improving the structure of the facility – reservation, building protections to localize failures, to prevent cascading effects and the most catastrophic scenarios after causing local damage to the facility.*

**Keywords**: critical facilities, terrorist threats, risk, initiating factors, technogenic accidents and disasters, vulnerability, protection level, critical element, protection systems.

## Опасности и угрозы в природно-техногенно-социальной системе

К настоящему времени сформирована достаточно большая научная и научно-методическая база для проведения анализа угроз чрезвычайных ситуаций (ЧС) различного характера на критически важных объектах (КВО), исследования процессов их ини-

циирования и развития, снижения уязвимости объектов по отношению к техногенным авариям и катастрофам различной природы.

В общем случае угрозы для КВО носят вероятностный характер, определяемый возможностью воздействия на объект поражающих факторов конкретного вида вследствие реализации некоторого опасного события – внутреннего или внешнего [1,2].

Опасности, реализующиеся в виде недопустимых для элементов КВО воздействий потоков вещества, энергии и информации, могут существенно снизить эффективность их функционирования или привести к разрушению (рис. 1).


Рис. 1. Схема реализации опасных воздействий на КВО

Собственно процесс развития опасности можно описать следующей логической последовательностью:

- нарушение технологического процесса, допустимых пределов эксплуатации, условий содержания и т.п.;
- накопление дефектов, приводящих к аварии;
- разрушение конструкции;
- образование поражающих факторов;
- воздействие (взаимодействие) поражающих факторов на объект;
- реакция на поражающее воздействие.

Для реализации опасности необходимо выполнение минимум трех условий: опасность реально действует (присутствует); объект находится в зоне действия опасности; объект не имеет достаточных средств защиты [3,4].

В зависимости от основных источников опасностей угрозы для КВО могут подразделяться на техногенные, природные и социальные (рис. 2).


Рис. 2. Систематизация угроз для КВО

Угрозы в природно-техногенно-социальной сфере могут быть также классифицированы по объектам, величине нанесенного ущерба, вероятности возникновения, причинам воздействия, направлениям и целому ряду других показателей (рис. 3).

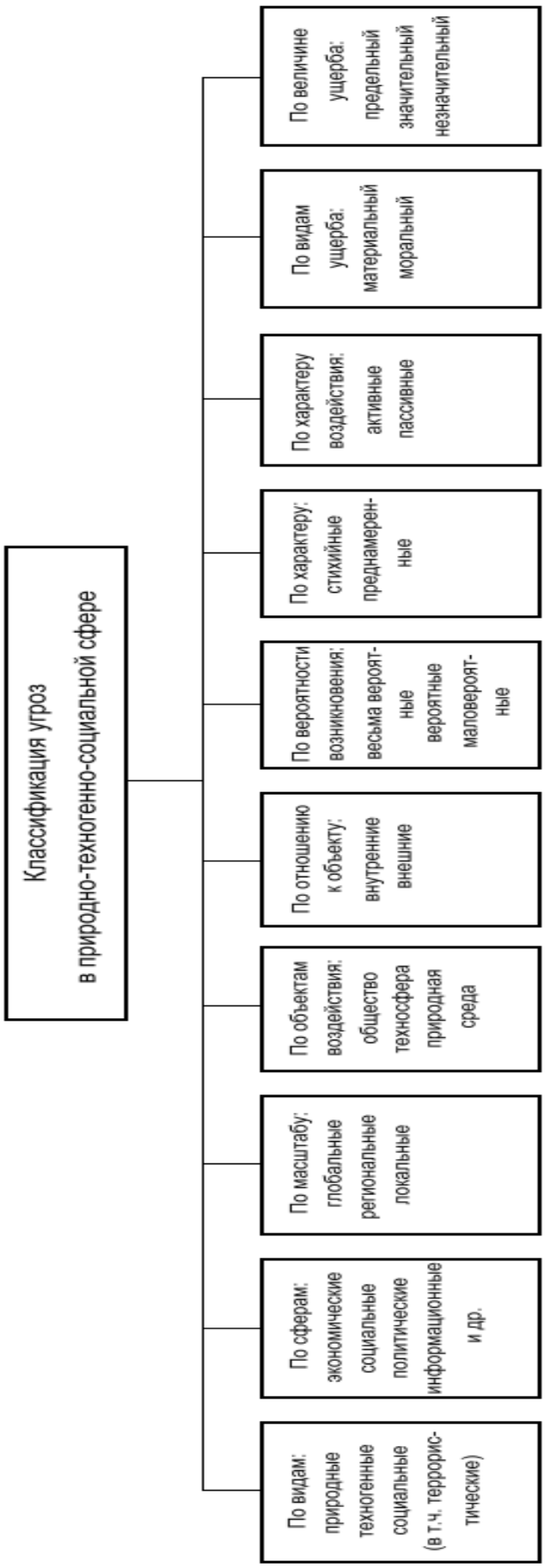


Рис. 3. Классификация природно-техногенно-социальных угроз

Анализ произошедших аварий и техногенных катастроф на опасных производственных объектах (ОПО) и КВО показывает, что их возникновение связано с различными причинами, такими как: отказы (неполадки) оборудования; ошибочные действия персонала; несовершенство технологий и проекта; внешние воздействия природного и техногенного характера [3-8], а также несанкционированные действия посторонних лиц, вандализм, террористические воздействия.

Основными *природными источниками угроз* для КВО при штатном функционировании являются опасные метеорологические и гидрологические явления, опасная сейсмическая активность, опасные уровни воды, раннее образование ледостава и появление льда, пожары, иные природные явления, могущие привести к нарушению (прекращению) функционирования таких объектов или их критических элементов.

К *техногенным источникам угроз* для КВО следует отнести аварии, отказы или повреждения критических элементов рассматриваемых объектов или технических устройств на иных объектах, обеспечивающих безопасное функционирование КВО, нарушения производственных процессов на КВО, которые могут вызвать инциденты безопасности, иные техногенные инциденты, могущие привести к нарушению (прекращению) функционирования таких объектов. Данные источники могут быть внутренними (некачественно изготовленные элементы подсистем; некачественные программные средства обработки информации; другие технические средства, применяемые на КВО) и внешними (повреждение линий связи, электроснабжения; сетей инженерных коммуникаций).

*Источники, связанные с поражающими факторами техногенных и природных аварий и катастроф* в результате пожаров, взрывов, радиационных и химических аварий, землетрясений, ураганов, наводнений (воздействие осколков; тепловые, радиационные и химические воздействия и др.). Возникновение этих источников трудно спрогнозировать. Они также могут быть внутренними и внешними по отношению к объекту.

В качестве *антропогенного источника угроз* для КВО можно рассматривать субъекта (личность), имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами объекта. Эти источники угроз могут быть как внешними так и внутренними, как случайными**,** так и преднамеренными. Особую опасность представляют несанкционированные действия физических лиц: террористов, преступников, экстремистов, которые могут привести к возникновению большинства прогнозируемых угроз.

## Особенности террористических угроз для КВО по сравнению с угрозами природно-техногенного характера

Чрезвычайные ситуации, инициируемые террористическими актами, развиваются по законам, аналогичным ЧС, вызванным природно-техногенными катастрофами, и могут анализироваться с помощью методов решения классических задач теории рисков. В то же время для ЧС, инициированных террористическими воздействиями, характерны отличительные особенности, которые необходимо учитывать в ходе анализа террористических угроз, рисков и террористических механизмов инициирования чрезвычайных ситуаций на КВО.

Некоторые важные сходства и различия воздействий на КВО террористических актов, природных и техногенных катастроф приведены в табл. 1.

Можно отметить следующие особенности террористических угроз для КВО.

*Преднамеренность террористического воздействия, определяющая более динамичный характер террористических рисков*. Изменение спектра и интенсивности угроз для террористических воздействий проходит значительно динамичнее, чем для угроз природно-техногенного характера. Это происходит, в том числе, за счет анализа террориста-

ми уровня защищенности объекта по отношению к различным видам угроз, идентификации поражающих факторов, по отношению к которым объект оказывается наименее защищенным, и сосредоточении усилий на осуществлении соответствующего типа атаки.

Террористы способны постоянно расширять свой арсенал механизмов инициации ЧС, используя современные материалы и технологии; реагировать на изменения систем защиты объекта и извлекать уроки из ошибок, совершенных при нападении на объекты в прошлом.

*Таблица 1*

**Сходства и различия воздействий на КВО террористических актов, природных и техногенных катастроф**

| № | Характеристики | Природные катастрофы | | | Техногенные катастрофы | | Террористические акты |
|---|---|---|---|---|---|---|---|
| | | Ураган | Землетрясение | Наводнение | Утечка радиоактивных веществ | Утечка химически опасных веществ | Террористическое воздействие на КВО |
| 1 | Преднамеренность действия | – | – | – | – | – | + |
| 2 | Неопределенность начала события | + | – | – | + | + | + |
| 3 | Поражение наиболее важных подсистем КВО | + – | + – | + – | + – | + – | + |
| 4 | Географические ограничения воздействия | + | + | + | + | + | – |
| 5 | Локальный характер угрозы | + | + | + | + | + | + |
| 6 | Национальный характер угрозы | – | – | – | – | – | + |

*Высокий уровень неопределенности (неизвестности), связанный с человеческим фактором, сложность оценки системы ценностей и логики поведения террористов.* Существенной особенностью террористических угроз и рисков является резкое возрастание роли человеческого фактора, который становится определяющим. Поэтому при проведении оценки террористической (диверсионной) уязвимости рассматриваемого объекта необходимо учитывать уровень технической оснащенности террористов, их навыки, возможные знания об объекте, а также способность использовать существующие (а иногда и создавать новые) уязвимости объекта для организации атак.

Реальное осуществление террористических угроз для КВО происходит по схеме, представленной на рис. 4.

В результате оценки диверсионной уязвимости рассматриваемого КВО должен быть существенно расширен перечень проектных воздействий и проектных сценариев аварий путем включения в исходный перечень совокупности запроектных сценариев, которые могут быть инициированы террористическими воздействиями. Подобное расширение осуществляется на основе оценки материальных и интеллектуальных ресурсов террористов.

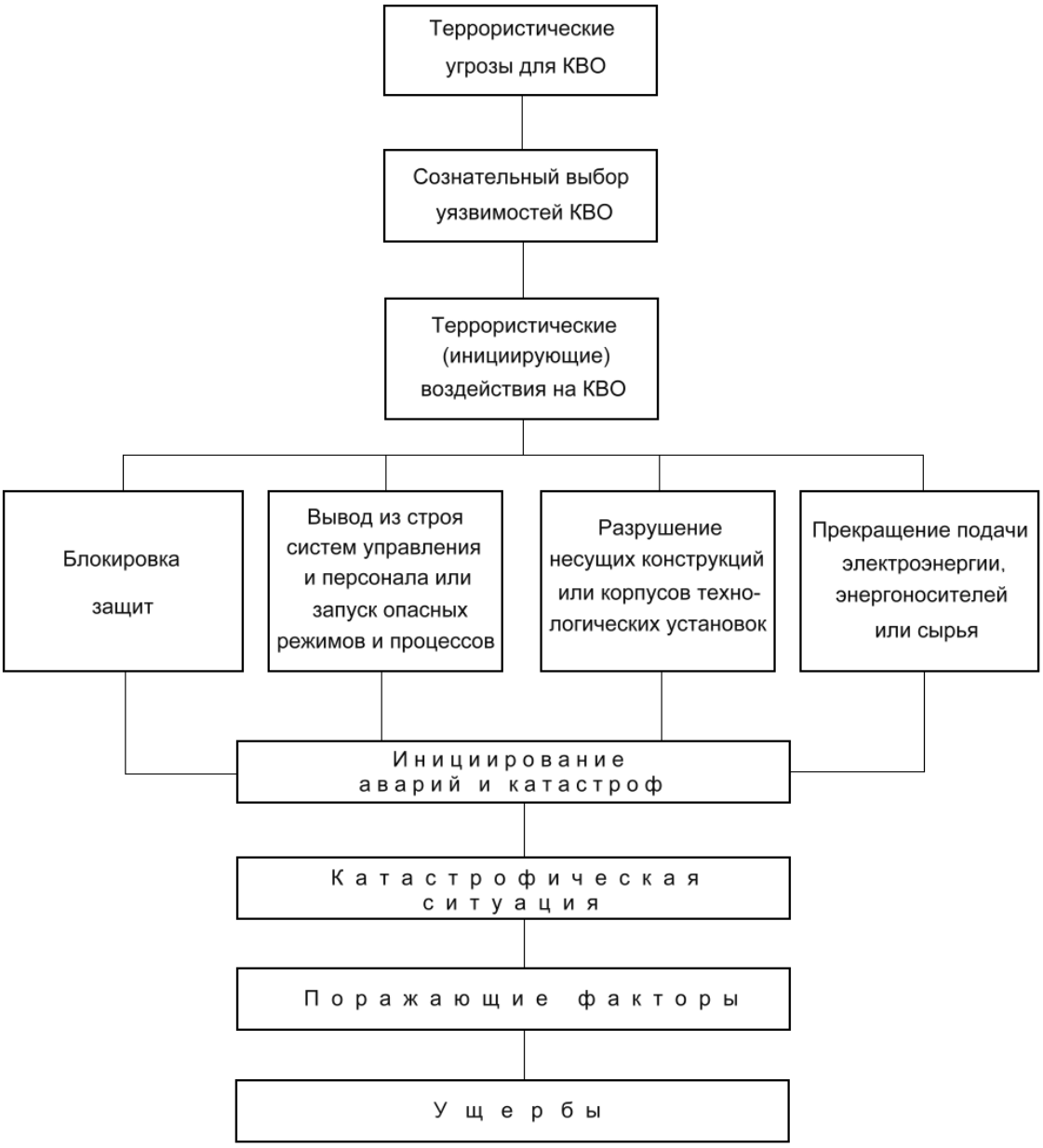


Рис. 4. Реализация террористических угроз для КВО

В данной связи могут быть выделены:

- материальные ресурсы: технические средства, оборудование, «человеческий материал», которые могут быть использованы для террористической атаки;
- нематериальные ресурсы: квалификация, опыт, знания;
- наличие доступа к внутренним модулям и процедурам объекта.

*Широкий диапазон масштабов и способов осуществления террористических угроз.* При решении задач обеспечения безопасности КВО от природно-техногенных катастроф могут быть выделены превалирующие виды поражающих факторов для рассматриваемой системы: сейсмический риск, риск наводнений, риск химического заражения и т.д. и разработаны необходимые мероприятия по обеспечению защищенности системы от пора-

жающих факторов природно-техногенных аварий и катастроф с целью их снижения. При обеспечении защищенности КВО от террористических проявлений спектр возможных угроз значительно шире. Так, *ряд видов террористических воздействий не имеет аналогов в структуре поражающих факторов природно-техногенных катастроф*. Это, например, кибертерроризм или электромагнитные воздействия, направленные на вывод из строя систем управления КВО. Важной отличительной *особенностью террористических механизмов инициирования катастроф является также более сложная связь между факторами, определяющими уровень риска, чем при природно-техногенных ЧС*.

С учетом изложенного анализ террористических угроз и оценка террористического риска в дополнение к оценкам риска штатного функционирования для КВО представляет собой комплексную междисциплинарную задачу с использованием результатов различных дисциплин: социальных – в части оценки террористических угроз, намерений и планов террористов; технических – в части оценки уязвимости объектов к террористическим воздействиям; экономических – в части калькуляции ущербов от аварий.

## Террористические воздействия как инициирующие факторы аварий и катастроф. Типы современного терроризма

К основным типам террористических воздействий относятся:

- нападение на объекты критической инфраструктуры, потенциально опасные для населения, с целью их разрушения или нарушения технологического режима;
- взрывы и иные террористические воздействия в местах массового нахождения людей;
- захват заложников и похищение людей;
- захват самолетов и других транспортных пассажирских средств;
- выведение из строя систем управления авиационным и железнодорожным транспортом, линий электроснабжения, средств связи, компьютерной и иной электронной техники;
- кибернетические атаки на наиболее важные компьютерные сети и системы с целью нарушения их работы;
- распространение через СМИ ложной информации, воздействующей на общественное мнение и вызывающей беспорядки в обществе;
- рассеивание химических и радиоактивных веществ в местах массового нахождения людей;
- отравление продовольствия и систем водоснабжения;
- распространение инфекций и патогенных микроорганизмов.

Большинство КВО, удары по которым могут иметь действительно масштабные разрушительные последствия, являются хорошо защищенными объектами. Это предприятия атомной промышленности, нефтеперерабатывающие заводы, терминалы по хранению и перекачке сжиженного газа и др. Факты серьезного нарушения работы таких объектов в результате терактов пока очень редки. Тем не менее, не следует недооценивать возможность террористических угроз перечисленным объектам, поскольку обеспечить полную физическую защиту ряда объектов невозможно. Это, например, системы большой протяженности (крупные нефтяные месторождения, многокилометровые трубопроводы, линии электропередач и др.). Так, на территории Российской Федерации эксплуатируется более 200 тыс. км магистральных трубопроводов, повышение защищенности которых от возможных террористических воздействий является актуальной задачей.

Основными предпосылками усиления террористической угрозы являются:

- сочетание организованных террористических групп с большим числом автономных ячеек и отдельных лиц;
- сращивание терроризма с преступностью, торговлей наркотиками и оружием;

- расширение источников финансирования терроризма;
- появление новых видов терроризма (информационного, технологического, кибернетического и др.);
- расширение средств проведения террористических актов (биологических, химических, радиологических);
- непредсказуемость так называемого «неразборчивого» терроризма, направленного на беспорядочное уничтожение случайных лиц;
- повышение интеллектуального уровня терроризма соответственно с темпами развития науки и техники.

КВО как потенциально опасные объекты и возможные цели террористов представляют значительную угрозу для природно-техногенно-социальной сферы. Заключенные в опасных объектах и технологиях потенциальные разрушительные силы создают объективную основу для целенаправленного использования их в качестве средств поражения с целью нанесения ущерба регионам, в которых они расположены. Это может быть достигнуто путем искусственного создания условий, необходимых для высвобождения и реализации их разрушительного потенциала. Например:
- создание зон катастрофического затопления при разрушении плотин;
- радиоактивное заражение местности при разрушении ядерных реакторов;
- химическое заражение атмосферы, почвы и воды при разрушении химических заводов, хранилищ, лабораторий;
- организация массовых пожаров путем поджога лесов, нефтяных и газовых скважин;
- распространение эпидемий и др.

В случае террористического воздействия на КВО весьма вероятно возникновение ЧС с образованием вторичных зон поражения. Ключевыми поражающими факторами, которые представляют опасность для населения, объектов экономики, жизнедеятельности в результате технологического теракта, являются ударные волны, токсические нагрузки, разлет осколков и обломков оборудования, тепловые излучения и вторичные поражающие факторы. Сравнение протекающих в этом случае процессов с природно-техногенными ЧС позволяет отнести террористические акты к катастрофическим рискам.

В табл. 2 приведен перечень некоторых критически важных объектов инфраструктуры, характеристика поражающих факторов и возможных зон поражения при различных инициирующих воздействиях природно-техногенного и террористического характера [9].

Многообразие террористических проявлений привело к возникновению различных классификаций терроризма, отличающихся признаками, положенными в основание. Так, проявление терроризма можно охарактеризовать по целям, масштабам, объектам воздействия и способам осуществления. В теории риска наиболее употребительной является классификация террористических воздействий в зависимости от видов применяемых средств, в соответствии с которой различают следующие основные типы терроризма: обычный, радиационный (ядерный), химический, биологический, электромагнитный, кибернетический, информационный.

При анализе террористических воздействий на КВО часто выделяют три типа терроризма: традиционный, технологический и интеллектуальный, различающиеся ресурсным обеспечением, сценариями организации атаки и структурами ущербов (табл. 3) [10].

Традиционный терроризм представляет собой организацию взрывов, пожаров, убийств физических лиц, на ограниченных зонах КВО с нанесением первичного ущерба.

Технологический терроризм подразумевает организацию мощных внешних несанкционированных воздействий на КВО, обеспечивающих прорыв их системы защиты, инициацию вторичных катастрофических процессов за счет хранящихся или перерабатываемых на этих объектах запасов опасных веществ ($W$), энергии € и информации ($I$) и эскалацию катастрофы за пределы КВО с существенным возрастанием вторичных и каскадных ущербов.

*Таблица 2*

**Перечень критически важных объектов**

| Отрасль народного хозяйства | Наименование объекта, производства (технологии) | Основные поражающие факторы | Возможные зоны поражения (отчуждения), км$^2$ |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| Электро-энергетика | Находящиеся в городской черте или непосредственной близости от мегаполиса:<br>- ядерные реакторы АЭС;<br>- хранилища отработанного ядерного топлива;<br>- плотины водохранилищ ГЭС | Взрывы, пожары, РЗМ.<br>Взрывы, пожары, РЗМ.<br>Волна прорыва | До нескольких сотен км$^2$.<br>От нескольких десятков до нескольких сотен км$^2$ |
| Атомная промышленность | Переработка отработанного ядерного топлива:<br>- радиохимические заводы;<br>- хранилища отработанного топлива | Взрывы, РЗМ | До нескольких тысяч км$^2$ |
| Нефтегазовая промышленность | Добыча и переработка нефти и газа:<br>- нефте- и газоперерабатывающие заводы, в т.ч. установки производства аммиака и других СДЯВ;<br>- резервуары хранения добытого сырья, нефтепродуктов | Взрывы, массовые пожары, ХЗ атмосферы | От нескольких десятков до нескольких сотен км$^2$ |
| Целлюлозно-бумажная промышленность | Бисульфатное производство целлюлозы с использованием технологических СДЯВ | Взрывы, массовые пожары, ХЗ атмосферы | От нескольких десятков до нескольких сотен км$^2$ |
| Пищевая промышленность | Хладокомбинаты | Взрывы, массовые пожары, ХЗ атмосферы | До нескольких км$^2$ |
| Коммунальное хозяйство | Станции водоочистки, очистные сооружения | Взрывы, массовые пожары, ХЗ атмосферы | До нескольких км$^2$ |
| Агропром | Склады безводного аммиака и аммиачной воды для удобрения почвы, дефолиации хлопчатника и др. культур. Базовые склады химических средств защиты растений | Взрывы, массовые пожары, ХЗ атмосферы | До нескольких км$^2$ |
| Микробиологическая промышленность | Научно-исследовательские центры и испытательные полигоны; производство биологических средств и рецептур; производство биодобавок к кормам, вредных для человека | Заражение атмосферы и местности биосферами | До нескольких км$^2$ |
| Транспортный комплекс | Наливные и контейнерные поезда. Автоцистерны. Танкеры и контейнеровозы | Взрывы, пожары. Радиоактивное или химическое заражение среды | До нескольких км$^2$ |
| Химическая промышленность | Основная химия:<br>- производство СДЯВ (хлор, аммиак, фосген, синильная кислота. Фосфорорганические соединения, сернистый ангидрид, фтористый водород, неорганические кислоты и др.);<br>- азотные и фосфатные удобрения;<br>- химические средства защиты растений;<br>- химические волокна и нити;<br>- синтетические красители, смолы и пластмассы | Взрывы, пожары.<br>ХЗ атмосферы и воды | От нескольких десятков до нескольких сотен км$^2$ |

РЗМ – радиоактивное заражение местности; ХЗ – химическое заражение; СДЯВ – сильно действующие ядовитые вещества.

*Таблица 3*

**Виды терроризма и структура ущербов для КВО**

| *Вид терроризма* | *Структура ущербов* |
|---|---|
| Традиционный терроризм | Первичные: 100% |
| Технологический терроризм | Первичные: 1-10%<br>Вторичные: 90-99% |
| Интеллектуальный терроризм | Первичные: < 0,1%<br>Вторичные: < 10%<br>Каскадные: > 90% |

Первичные ущербы, наносимые поражающими факторами террористического воздействия с применением особо опасных технологий и технических средств, составляют до 10% от совокупных ущербов, а вторичные ущербы, связанные с эскалацией аварии на объекте, составляют до 90% совокупных ущербов от террористической атаки [9,11]. Такие сценарии характерны при целенаправленном инициировании катастрофических техногенных процессов на опасных объектах ядерно-энергетического, гидротехнического, химико-технологического и биотехнологического комплексов.

Как правило, технологический терроризм предполагает:

- предварительный анализ структуры и уязвимостей КВО как сложной системы, потенциальных источников вторичных катастрофических процессов (запасов $W$, $E$, $I$), слабых мест в системах защиты и идентификацию наиболее эффективных сценариев атаки;
- идентификацию ключевых элементов и связей КВО, при выведении из строя которых система не сможет выполнять свои функции;
- использование уязвимостей и мощных инициирующих воздействий на КВО с целью прорыва систем защиты;
- оценку сценариев развития событий и определение таких конечных состояний КВО, которые способны инициировать мощные вторичные катастрофические процессы за пределами объекта.

Интеллектуальный терроризм предполагает организацию нарушений работы КВО за счет «слабых» несанкционированных воздействий, нацеленных на наиболее уязвимые элементы объекта на различных стадиях его жизненного цикла. На стадии проектирования и изготовления новых КВО в принимаемые конструкторские и технологические решения могут быть заложены опасные сценарии функционирования объекта при эксплуатации. Интеллектуальный терроризм на стадии эксплуатации предполагает внедрение члена террористической организации в штат организации, эксплуатирующей КВО, либо вербовку путем шантажа и/или подкупа оператора, уже работающего на объекте. При этом оператор-террорист обладает инсайдерской информацией об объекте, имеет доступ к процедурам контроля, системам зашиты, способен оказывать скрытые управляющие воздействия на систему, которые могут инициировать катастрофические сценарии развития событий. Террористическая атака осуществляется, главным образом, за счет не физических, а интеллектуальных ресурсов террористов, позволяющих использовать существующие и создавать новые уязвимости системы. Структура ущербов при атаке интеллектуального терроризма принципиально меняется. Первичные ущербы от поражающих факторов составляют до 1% общих ущербов, вторичные ущербы связанные с эскалацией аварии после разрушения атакованного компонента КВО могут достигать 10%, в то время как до 90% процентов совокупных ущербов будут относиться к катего-

рии каскадных, то есть связанных с каскадными отказами объектов критических инфраструктур, сопряженных с атакованным объектом при реализации сценариев внутри- и межинфраструктурных каскадов.

Поскольку технологический терроризм в сочетании с интеллектуальным может иметь место на стадии изготовления и испытания, по всей этой цепочке должны быть построены методы анализа террористических рисков и сформированы дополнительные разделы в соответствующих проектах нормативно-технической документации.

## Тенденции в области терроризма

Для выявления наиболее полного спектра террористических угроз для КВО в целях повышения их устойчивости и снижения уязвимости важное значение имеет учет существующих тенденций в области терроризма. По мнению ряда исследователей, основными тенденциями современного терроризма, учет которых имеет важное значение для противодействия террористической деятельности, являются следующие [12-15].

Сейчас наиболее значительная часть террористической активности в мире сосредоточена в зонах нескольких крупных вооруженных конфликтов в 1-2 регионах мира. Эта тенденция сохранится в долгосрочной перспективе. Вместе с тем террористическая активность (в меньших масштабах и низкой интенсивности) продолжит распространяться в странах, где ее уровень был минимальным.

В настоящее время 86% всех терактов осуществляется с помощью стандартных взрывчатых веществ, гранат, легкого и стрелкового оружия. Угрозы, связанные с возможным применением террористами ядерных, химических, биологических и радиологических материалов являются исключением. По мнению исследователей, эта тенденция сохранится в ближайшей и среднесрочной перспективе. При этом достаточно велика вероятность выбора террористами новых целей для ударов обычными средствами. Это, в первую очередь, системы и объекты критической инфраструктуры в энергетической, информационно-коммуникационной и банковско-финансовой сфере. Поэтому в указанных сегментах инфраструктуры особое внимание нужно уделять обеспечению общей устойчивости систем, их диверсификации, резервным мощностям и ресурсам.

Вероятность терактов с применением оружия массового поражения в настоящее время в целом достаточно мала. Вместе с тем по информации МАГАТЭ, за последнее десятилетие значительно увеличилось число фактов контрабанды радиоактивных материалов, пригодных для изготовления «грязной» бомбы. На IV Саммите по ядерной безопасности в качестве главной угрозы мировому сообществу названо попадание ядерного оружия в распоряжение экстремистов. В этой связи признано необходимым усилить меры безопасности для объектов, на которых находятся плутоний и обогащённый уран, и разработать мероприятия по противодействию ядерной контрабанде.

Значительную актуальность приобретает проблема информационного терроризма и противодействия ему. Росту информационного терроризма способствует глобальность и неподконтрольность информационной сети Интернет, используемой террористами, преступниками и политическими экстремистами для пропаганды, сбора средств и вербовки кадров, а также для связи в реальном времени при проведении операций. Террористические организации все больше приобретают *сетевой, распределенный характер.* Большинство терактов организуются не террористами-одиночками, а организованными группировками, которые поддерживаются не только лицами, чьи интересы террористы отстаивают, но и целыми государствами. В будущий период времени для усиления информационно-политического эффекта терактов уровень организации и координации атак

(спланированные серии одновременных терактов и т.п.) будут играть не меньшую роль, чем системы вооружений, материалы и уровень технического обеспечения террористов.

Для успешного противодействия терроризму важно изучать, и учитывать тенденции в части особенностей поведения и мотивации его прямых или косвенных участников. Это предполагает рассмотрение терроризма как результата взаимодействия сложной комбинации различных факторов – исторических, политических, идеологических, культурных, религиозных, психологических и экономических. В настоящее время по большей части исходными мотивами террористов являются религиозно-националистические убеждения, часто базирующиеся на противопоставлении интересов богатых и бедных стран, Севера и Юга. В целом, исходя из мотивов террористической деятельности, можно выделить и типы терроризма: экономический, этнический, политический и социальный. В то же время анализ некоторых террористических актов последнего времени показывает, что все чаще выбор тех или иных действий террористами осуществляется в результате сопоставления возникающих при этом выгод и издержек. Для анализа процесса принятия решения потенциальным «рациональным» террористом с учетом материальных и моральных выгод и потерь может быть использована стандартная модель экономической теории преступности

$$R = W - pD, \tag{1}$$

где $R$ – возникающая у террориста чистая выгода при совершении преступления; $p$ – вероятность, что террорист будет пойман и наказан; $W$ – величина выгоды террориста от преступления; $D$ – величина потерь террориста в результате его наказания.

Однако концепция рационального поведения террориста не учитывает должным образом влияния значительной группы социально-политических и культурно-исторических факторов.

## Меры по снижению террористических рисков для КВО

Противодействие терроризму предполагает, с одной стороны, борьбу с террористами, как инициаторами и исполнителями террористических атак, а с другой – повышение защищенности объектов от террористических воздействий, то есть достижение состояния, при котором обеспечиваются условия для их безопасного функционирования, предотвращения или минимизации риска чрезвычайных ситуаций, инициированных террористами.

В государственной системе мер по борьбе с терроризмом главная роль принадлежит ФСБ, ФПС, МВД, СВР и ФСО РФ. Другие федеральные органы участвуют в предупреждении, выявлении и пресечении террористической деятельности в пределах своей компетенции.

Для обеспечения защищенности и безопасности КВО необходим специальный анализ методов и сценариев проведения террористических актов и реакций существующих и создаваемых КВО на террористические воздействия с определением уровня их уязвимости, то есть анализ степени несоответствия принятых мер защиты прогнозируемым угрозам или заданным требованиям безопасности.

При решении задач по обеспечению безопасности КВО ключевым понятием является понятие риска. Риск определяется через функционал $FR$ вероятности наступления катастрофы (природного или техногенного характера) и величины ущерба [16]:

$$R = F_R\{P,U\} = \sum R_i = \sum P_i \cdot U_i \ , \tag{2}$$

где $n$ – количество сценариев $S_i$ ($i$ = 1, 2,..., $n$) развития аварий на КВО; $P_i$ и $U_i$ ( $i$ = 1, 2,..., $n$ ) – соответственно вероятности реализации различных сценариев достижения предельных состояний, включая реализацию террористической угрозы, и ущербы, соответствующие этим сценариям; $R$ – риск, связанный с природно-техногенной катастрофой.

Специфические особенности рисков технологического терроризма определяются способностью террористов осуществлять сознательный выбор сценария атаки с целью максимизации причиняемого ущерба. Этот выбор может определяться на основе оценки уязвимостей КВО и ущербов, которые можно ожидать в случае успешной реализации атаки. В связи с этим возникает обратная связь между уязвимостью системы по отношению к террористической угрозе и самой террористической угрозой.

Поэтому анализ террористических рисков требует привлечения дополнительных методов и средств, и более существенного вклада со стороны социальных наук, чем это имеет место в случае оценки природно-техногенных рисков. Оценка рисков технологического терроризма должна проводиться с привлечением подходов теории игр, учитывающих наличие двух противодействующих сторон (террористов и антитеррористов), которые действуют рационально, в соответствии со своими целями и системами ценностей, и способны реагировать на действия противоположной стороны.

На практике всегда существует большое количество не поддающихся точной оценке возможных путей осуществления угроз безопасности КВО. В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является первым фактором, определяющим защищенность объекта. Вторым фактором является прочность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их преодоления. Третьим фактором является величина ущерба в случае успешного осуществления угроз безопасности [17].

Действие защиты КВО будет выражаться в снижении условных вероятностей локальных повреждений объекта вследствие воздействий на него различных поражающих факторов, либо условных вероятностей реализации различных промежуточных событий, способствующих приведению объекта в различные поврежденные состояния, в случае локальных повреждений. Системы защиты снижают уязвимость КВО и призваны скорректировать структуру сценарного дерева: они позволяют заблокировать или существенно снизить вероятность реализации наиболее неблагоприятных сценариев и вводят дополнительные сценарии, обеспечивающие малые степени повреждения. Введение системы защиты приводит к смещению влево кривой распределения ущербов для рассматриваемого объекта [11,18].

При построении систем защиты критериями по выбору вида защит должны быть допустимые уровни воздействия опасных веществ (*W)*, энергии (*E*), информации (*I*) на объекты защиты.

Анализ террористических угроз для КВО показывает, что они, как правило, ориентированы на реализацию комбинированных сценариев воздействий, предполагающих достаточно мощные физические воздействия на ключевые элементы КВО и точечные воздействия на системы управления. Физические воздействия на элементы КВО могут осуществляться на основе использования химических, радиационных, термических, гидродинамических и т.д. поражающих факторов. Весьма опасными для систем управления являются проявления электромагнитного и кибернетического терроризма.

В общем случае сложную техническую систему, в том числе КВО, следует рассматривать как совокупность структурно связанных между собой элементов.

Для снижения уязвимости КВО можно использовать три взаимодополняющих метода.

1. Общее «усиление» КВО, повышение запасов для всех его элементов и связей, без предварительной оценки их уязвимости, предусматривающее наделение объекта доста-

точным внутренним ресурсом, позволяющим противостоять любым внешним дестабилизирующим воздействиям. Данный метод является наиболее затратным и часто приводит к избыточной защите объекта от отдельных видов угроз.

2. Локальное «усиление», под которым понимается снижение локальной уязвимости предварительно идентифицированных элементов и связей КВО, которые являются наиболее уязвимыми. При реализации этого метода ставится задача предупредить локальные отказы элементов, являющиеся инициирующими событиями для дальнейшего развития аварии на объекте. Данный метод предусматривает детальную оценку угроз и повышения защищенности элементов КВО к выявленным угрозам. Он предполагает комплекс мер, направленных на защиту ключевых, критических элементов КВО от экстремальных воздействий с целью предупреждения локальных повреждений в системе.

*Критические элементы КВО* (конструктивные или технологические) являются наиболее значимыми. Выход их из строя приводит к прекращению нормального функционирования объекта в целом или чрезвычайным ситуациям. *Если критические элементы (КЭ) недостаточно устойчивы или слабо защищены, они становятся наиболее уязвимыми местами объекта.* Вопросы защиты критических элементов рассмотрены в работе [10].

При заранее спланированных террористических воздействиях атакам будут подвергаться в первую очередь КЭ объектов, как наиболее важные для безопасного функционирования всего объекта. В свете появления новых технических средств и совершенствования сценариев террористических атак существующих защит может оказаться недостаточно, и КВО станет уязвимым, если не предпринять дополнительных защитных мер.

3. Снижение структурной уязвимости путем изменения структуры КВО, позволяющего снизить уязвимость объекта в целом путем исключения из его структуры наиболее опасных и уязвимых взаимосвязей или введения системы резервирования и защиты. Цель этого подхода – исключение каскадных процессов в случае отказа отдельных элементов КВО.

С учетом вышеизложенного, мероприятия по снижению уязвимости КВО представляется целесообразным проводить в два этапа.

Первый этап работ предполагает разработку комплекса мер, направленных на защиту ключевых (критических) элементов КВО от экстремальных воздействий с целью предупреждения локальных повреждений в системе.

Реализация действий второго этапа предусматривает совершенствование структуры объекта, введение резервирования, построение активных и пассивных средств зашиты, направленных на локализацию отказов, предотвращение каскадных эффектов и снижение вероятности наиболее катастрофических сценариев после нанесения объекту локальных повреждений [19,20].

Повышение защищенности КВО от террористических воздействий предполагает разработку объектовой антитеррористической концепции – комплекса научно-обоснованных положений о сущности и содержании террористических угроз объекту и об основах антитеррористической защиты на объекте. КВО должен быть размещен, спроектирован, сооружен, эксплуатироваться, и выводиться из эксплуатации с учетом возможных террористических воздействий. Ранее уже отмечалось, что ЧС, инициируемые террористическими атаками, развиваются по законам, аналогичным ЧС, вызванным природно-техногенными катастрофами. Поэтому системы и элементы КВО, важные для безопасности, должны обладать стойкостью к внешним воздействиям природного и техногенного происхождения, то есть к воздействию поражающих факторов источников ЧС. В этом случае объем и характер потерь и разрушений на них будет зависеть не только от характера воздействия поражающих факторов, но и от своевременности и масштаба превентивно осуществленных мер по подготовке к функционированию в условиях чрезвычайных ситуаций.

Повышение защищенности КВО во время ЧС достигается проведением превентивного комплекса организационных, инженерно-технических и технологических мероприятий, направленных на максимальное снижение воздействия поражающих факторов при ЧС. Организационные мероприятия предусматривают планирование действий руководства и всех служб КВО. Инженерно-технические мероприятия предусматривают комплекс работ, обеспечивающих повышение стойкости производственных зданий и сооружений, оборудования, коммунально-энергетических систем. Технологические мероприятия обеспечивают повышение устойчивости работы КВО путем изменения технологического процесса, исключающего возможность образования вторичных поражающих факторов [21]. Сюда относятся:

1. Рациональное размещение КВО, зданий и сооружений.
2. Рациональное размещение и защита основного оборудования.
3. Обеспечение надежной защиты персонала.
4. Повышение надежности инженерно-технического комплекса КВО.
5. Исключение или ограничение поражения от вторичных факторов.
6. Обеспечение надежности и оперативности управления производством.
7. Повышение надежности системы энергоснабжения.
8. Подготовка КВО к переводу на аварийный режим работы.
9. Подготовка к восстановлению нарушенного производства.

Для решения поставленной задачи должны быть построены системы защиты критически важных объектов и их подсистем от террористических угроз и выбраны типы этих защит. При функционировании КВО в штатном режиме, как правило, предусматривается использование жесткой, функциональной, естественной и комбинированной защиты объекта. Для повышения антитеррористической защищенности объекта необходимо также разработать план комплексных мероприятий, предусматривающий проектирование и построение системы физической (охранной) защиты объекта; создание подсистемы обнаружения возможного нарушителя, пытающегося проникнуть на объект; задержку его передвижения; действия сил безопасности.

На объектах должна быть разработана распорядительная документация, регламентирующая действия охраны и взаимодействующих органов при угрозах проникновения и проникновении диверсионно-террористических групп на объект [20].

Приоритетным требованием к мероприятиям антитеррористической защиты должна стать их дифференцированность, учет категорий потенциальной опасности объектов, оценка реальности террористических угроз, масштабов возможных последствий. Иными словами, объем мероприятий антитеррористической защиты должен соответствовать уровню террористических угроз.

Для развития систем физической (охранной) защиты наиболее важными являются следующие общие требования:

- определение категорий потенциальной опасности и способов антитеррористической защиты конкретных объектов должно осуществляться специально уполномоченными органами государственного управления;
- правила построения систем антитеррористической защиты должны быть едиными для всех потенциально опасных и критически важных объектов, независимо от форм собственности;
- реализация этих правил должна осуществляться федеральными органами исполнительной власти посредством разработки и внедрения в практику соответствующих правовых норм.

***Работа выполнена при финансовой поддержке РФФИ, грант №16-29-09575.***

## Литература

1. Безопасность России. Анализ риска и проблемы безопасности. Часть 1. Основы анализа риска и регулирования безопасности. Часть 2. Безопасность гражданского и оборонного комплексов и управление рисками. Часть 3. Прикладные вопросы анализа рисков критически важных объектов. Часть 4. Научно-методическая база анализа риска и безопасности. М.: МГФ «Знание». - 2006-2007.

2. Безопасность России. Анализ рисков и управление безопасностью (Методические рекомендации). М.: МГФ «Знание». - 2008. 672 с.

3. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Тематический блок «Национальная безопасность». Том 2. Безопасность и защищенность критически важных объектов. Часть 1. Научные основы безопасности и защищенности критически важных для национальной безопасности объектов / Под общ. ред. Махутова Н.А. М.: МГОФ «Знание». - 2012. 896 с.

4. Акимов В.А., Новиков В.Д, Радаев Н.Н. Природные и техногенные чрезвычайные ситуации: опасности, угрозы, риски. М.: ЗАО ФИО «Деловой мир». - 2002. 343с.

5. Махутов Н.А., Пермяков В.Н., Ахметханов Р.С., Резников Д.О., Дубинин Е.Ф. Анализ рисков и обеспечение защищенности критически важных объектов нефтегазохимического комплекса: учебное пособие. Тюмень: ТюмГНГУ. - 2013. 560 с.

6. Безопасность России. Регулирование ядерной и радиационной безопасности / Колл. авт. М.:МГОФ «Знание», НТЦ ЯРБ. - 2003. 400 с.

7. Безопасность России. Высокотехнологичный комплекс и безопасность России. Часть 2. Проблемы обеспечения безопасности оборонно-промышленного комплекса России. Раздел второй. М.: МГФ «Знание». - 2003. 624 с.

8. Махутов Н.А. Конструкционная прочность, ресурс и техногенная безопасность: В 2-х ч. / Новосибирск: Наука. - 2005. Ч 1: Критерии прочности и ресурса. 494 с., Ч.2: Обоснование ресурса и безопасности. 610 с.

9. Технологический терроризм и методы предупреждения террористических угроз // Сборник докладов научно-практической конференции. МЧС России, РАН. М.: Комбител, - 2004. 320 с.

10. Махутов Н.А., Ахметханов Р.С., Дубинин Е.Ф., Куксова В.И.. Снижение уязвимости КВО к террористическим воздействиям на основе повышения защищенности их критических элементов // Проблемы безопасности и чрезвычайных ситуаций. - 2018. №4. С.28-43.

11. Петров В.П., Резников Д.О., Куксова В.И, Дубинин Е.Ф. Оценка террористического риска и принятие решений о целесообразности построения систем защиты от террористических воздействий // Проблемы безопасности и чрезвычайных ситуаций. - 2007. №1. С. 89-105.

12. Степанова Е.А. Долгосрочный прогноз тенденций в области терроризма // Пути к миру и безопасности. - 2016. № 1 (50). С. 41-45.

13. Гридчин А.А., Пашкевич А.В. Управление международным антитеррористическим сотрудничеством / под редакцией доктора социологических наук, профессора Н.С. Данакина, генерал-полковника полиции, кандидата юридических наук А.П. Новикова. Монография. М.: Международный издательский центр «Этносоциум». - 2016. 268 с.

14. Метелев С.Е. Современный терроризм и методы антитеррористической деятельности: Монография. Омск. - 2008. 332 с.

15. Куклина И.Н. Мировой терроризм и международные структуры обеспечения безопасности // Мировые экономические и международные отношения. - 2005. №1.

16. Махутов Н.А., Резников Д.О. Научные основы оценки террористических рисков и парирования террористических угроз для сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. - 2015. № 2. С. 53-73

17. Махутов Н.А., Петров В.П., Ахметханов Р.С., Дубинин Е.Ф., Куксова В.И. Особенности поражающих факторов ЧС и их воздействие на системы диагностики КВО // Проблемы безопасности и чрезвычайных ситуаций. - 2011. №5. С. 24-45.

18. Махутов Н.А., Петров В.П., Резников Д.О., Куксова В.И. Идентификация определяющих параметров угроз, уязвимости и защищенности критически важных объектов по отношению к

превалирующим угрозам природного, техногенного и террористического характера // Проблемы безопасности и чрезвычайных ситуаций. - 2008. №2. С. 70-77.

19. Махутов Н.А., Резников Д.О. Сопоставительная оценка нормативного и основанного на управлении риском подходов к оценке защищенности сложных технических систем // Проблемы машиностроения и надежности машин. - 2011. №6. С.92-98.

20. Махутов Н.А., Петров В.П., Резников Д.О., Куксова В.И. Обеспечение защищенности критически важных объектов на основе снижения их уязвимости // Проблемы безопасности и чрезвычайных ситуаций. - 2009. №2. С.50-69.

21. Управление рисками техногенных катастроф и стихийных бедствий (пособие для руководителей организаций). Монография. Под общей редакцией Фалеева М.И./ РНОАР. М.: ФГБУ ВНИИ ГОЧС (ФЦ). - 2016. 270 с.

## Сведения об авторах

***Махутов Николай Андреевич***, главный научный сотрудник Федерального государственного бюджетного учреждения науки Институт машиноведения им. А.А. Благонравова (ИМАШ РАН). E-mail: safety@imash.ru, тел. +7 (495)930-80-78.

***Дубинин Евгений Федорович,*** научный сотрудник Федерального государственного бюджетного учреждения науки Институт машиноведения им. А.А. Благонравова (ИМАШ РАН). E-mail: mibsts@mail.ru, тел. +7 (495) 623-57-55.

***Куксова Варвара Игоревна,*** старший научный сотрудник Федерального государственного бюджетного учреждения науки Институт машиноведения им. А.А. Благонравова (ИМАШ РАН). E-mail: mibsts@mail.ru , тел. +7 (495) 624-91-54.