Электронное научное издание «Устойчивое инновационное развитие: проектирование и управление»
www.rypravlenie.ru **том 14 № 3 (40), 2018, ст. 1**

УДК 351.75

ПАРАДИГМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ ГОСУДАРСТВЕННО ЗНАЧИМЫХ ОБЪЕКТОВ (СИСТЕМНЫЙ ПРОЕКТ «БЕЗОПАСНЫЙ ГОСУДАРСТВЕННО ЗНАЧИМЫЙ ОБЪЕКТ»)

Махутов Николай Андреевич, руководитель рабочей группы при Президенте РАН по анализу риска и проблем безопасности РГ РАН «РИСК И БЕЗОПАСНОСТЬ», руководитель рабочей группы секции по безопасности и правоохранительной деятельности Экспертного совета при Комитете Совета Федерации по обороне и безопасности, член-корреспондент РАН, доктор технических наук, профессор

Балановский Владимир Леонидович, ответственный секретарь рабочей группы секции по безопасности и правоохранительной деятельности Экспертного совета при Комитете Совета Федерации по обороне и безопасности, заместитель председателя комитета МТПП по комплексной безопасности, профессор Академии военных наук, действительный член Академии проблем качества и Всероссийской академии наук комплексной безопасности

Габур Сергей Павлович, член-корреспондент Академии проблем качества и Российской инженерной академии, кандидат экономических наук, Ph.D., заместитель председателя комитета МТПП по комплексной безопасности, заместитель руководителя секретариата РГ «Скрытые резервы безопасности» экспертного совета председателя коллегии военно-промышленной комиссии РФ

Аннотация

В настоящее время в России существует острая необходимость обеспечения гарантированной безопасности государственно значимых объектов (ГЗО). Решение данной проблемы имеет определенные (объективные и субъективные) сложности. Необходимо осуществление взаимосвязанного и согласованного комплекса специальных мероприятий, связанных с организацией полномасштабной сферы безопасности на государственно значимых объектах. Данная статья предлагает новый подход к обозначенной проблеме, акцентируя основное внимание на комплексном противодействии терроризму.

КЛЮЧЕВЫЕ СЛОВА: национальная и общественная безопасность, военное и гражданское строительство, ядерно-, радиационно-, химически-, биологически-, техногенно-, пожаро-, взрыво-, гидродинамически-опасные объекты, информационные и телекоммуникационные системы, системный проект.

THE PARADIGM OF SECURING THE COUNTER-TERRORIST SAFETY OF STATE-OWNED IMPORTANT OBJECTS (SYSTEM PROJECT “SAFE STATE-OWNED IMPORTANT OBJECT”)

Makhutov Nikolai Andreevich, Head of the Working Group under the President of the Russian Academy of Sciences on Risk Analysis and Security Problems "RISK AND SECURITY", Head of the Working Group of the Section on Security and Law Enforcement of the Expert Council under the Committee of the Council of Federation on Defense and Security, Corresponding Member of the Russian Academy of Sciences, Doctor of Technical Sciences, Professor

Balanovskiy Vladimir Leonidovich, executive secretary of the working group of the section on security and law enforcement activities of the Expert Council under the Committee of the Council of Federation on Defense and Security, deputy chairman of the Committee for Integrated Security, professor of the Academy of Military Sciences, full member of the Academy of Quality Problems and the All-Russian Academy of Complex Safety Sciences

Gabour Sergey Pavlovich, Corresponding Member of the Academy of Quality Problems and the Russian Academy of Engineering, Ph.D. in economics, Deputy Chairman of the Committee for Complex Security, Deputy Head of the Secretariat of the WG "Hidden Safety Reserves" of the Expert Council of the Chairman of the Board of the Military Industrial Commission of the Russian Federation

Abstract

At present, there is an urgent need in Russia to ensure the guaranteed security of state-owned important objects (SOIO). The solution of this problem has certain (objective and subjective) difficulties. It is necessary to implement an interconnected and coordinated set of special measures related to the organization of a full-scale security sector at state-owned important objects. This article offers a new approach to the problem, focusing on the comprehensive counteraction to terrorism.

KEYWORDS: national and public security, military and civil construction, nuclear, radioactive, chemical, biological, technical, fire, explosive, hydrodynamically-dangerous objects, information and telecommunication systems, system project.

Обостряющаяся международная и внутренняя обстановка диктует острую необходимость обеспечения гарантированной безопасности государственно значимых объектов (ГЗО). Безопасность функционирования ГЗО прямо сказывается на общественно-политической жизни страны, ее социально-экономическом развитии и обеспечении национальной безопасности.

В России насчитывается 100 тыс. опасных производств и объектов. Особенно высока опасность 1500 ядерных и 3000 химических объектов **(всего примерно 4500 критически важных объектов (КВО))**. В первых сосредоточено около 10^{13}, а во вторых – около 10^{12} смертельных токсических доз. Уже сейчас накоплено радиоактивных отходов с суммарной активностью 2,73 млрд Ки, что соответствует 55 Чернобыльским выбросам. Интересен факт, что 4500 КВО, около 8000 пожаро-взрывоопасных объектов и более 30000 гидротехнических сооружений располагаются на территориях, на которых проживают не менее 90 миллионов человек. **Поэтому любые деструктивные воздействия террористической направленности на объекты инфраструктуры РФ** (в том числе на 1200-1300 объектов оборонного комплекса) **способны привести к глобальной катастрофе** [1].

Решение данной постановочной проблемы имеет свои объективные и субъективные сложности. В настоящее время затруднены в реализации единые комплексные подходы по согласованному решению вопросов обеспечения безопасности подобных объектов. Различные аспекты общей системы безопасности находятся в ведении различных ведомственных структур, не обеспечивая необходимую координацию решения вопросов на разных уровнях и в разных зонах ответственности, что провоцирует появление «слабых звеньев» в системе защищенности, нерациональность и дисбаланс затрат при построении отдельных сегментов системы безопасности. Отсутствует системная возможность отбора наиболее рациональных решений из имеющегося множества приемлемых вариантов в каждом конкретном случае с получением синергетических эффектов [2].

Основные предложения по решению проблемы в создавшейся ситуации могут быть следующими. Необходимо осуществление взаимосвязанного и согласованного комплекса специальных мероприятий, связанных с организацией полномасштабной сферы безопасности на государственно значимых объектах, таких как объекты основного и вспомогательного назначения Министерства обороны (МО), военно-промышленного комплекса (ВПК), критически важных объектов (КВО) и стратегически важных объектов (СВО) (объекты МВКС). **Данные мероприятия должны быть реализованы в системном проекте** «Безопасный объект МО, ВПК, КВО и СВО РФ (СП БО МВКС)».

Разработка системного проекта базируется на работах, выполненных в тесном взаимодействии РАН и Академии военных наук РФ, в соответствии с Планом подгруппы «Рабочей группы при Президенте РАН по анализу риска и проблем безопасности РГ РАН «Риск и безопасность»», утвержденным 12 декабря 2016 г. п.5 «Разработка проекта общей концепции безопасности (с использованием лучших практик и наилучших доступных технологий), а также ее элементов».

Далее определим общие требования и цели проекта. Системный проект должен базироваться на фундаментальных научных основах, создаваться на новых концептуальных научно-технологических принципах и обеспечивать на долгосрочный период необходимую защищенность всей системы [3] объектов МВКС от террористических воздействий с учетом всех взаимосвязанных факторов (природные, техногенные и социальные). **Необходим гарантированный переход от информационно-аналитических (квазиинтеллектуальных) систем к информационно-интеллектуальным системам поддержки принятия решений**, как основы всего организационного-технологического комплекса защищенности (ОТКЗ) объектов МВКС с введением нового термина «цифровая безопасность». **Структура проекта должна включать мероприятия по созданию Государственной программы «Цифровая безопасность ГЗО», её исполнение и развитие на базе формирования технологической платформы «Цифровая безопасность ГЗО».** Необходимы финансово доступные к реализации комплексные всесторонние подходы в борьбе с актами террористического характера и незаконного вмешательства (АНВ) против персонала, систем жизнеобеспечения, поддержки функционирования этих объектов и смежных ведомств (организаций).

Полномасштабная сфера безопасности МВКС должна достигаться с учетом основного и важного аспекта - фокус решений локализации и предотвращения возможных деструктивных воздействий террористической направленности на объект

должен формироваться с учетом того, что они могут носить взаимосвязанные социальный, природный и техногенный характеры.

В системном проекте должны использоваться результаты проведенных фундаментальных исследований РАН во взаимодействии с головными НИИ ведущих отраслей (ИМАШ, ИПМ, ЦАГИ, НИКИЭТ, ЦНИИМАШ, НИЦ КИ, ВНИКТИ, ВНИИ ГОЧС, ИГЭ, ИБРАЭ, МФТИ, ИФТИ и других организаций). При подготовке к разработке системного проекта были проанализированы более 150 законодательных и нормативных актов, 83 лучшие практики и наилучшие доступные технологии в области безопасности, разработанные и внедренные в период 2013-2017 гг. на объектах всех отраслей и ведомств РФ.

При построении ОТКЗ необходимо в обязательном порядке учитывать возможное применение новых видов оружия: лазерное, источники некогерентного света, СВЧ оружие, инфразвуковое, средства радиоактивной борьбы, оружие электромагнитного импульса, биотехнологическое (экологическое), средства информационной борьбы, информационно-технологическое, информационно-психологическое (открытые психотехнологии, манипулятивные психотехнологии, психофизическое (психотронное, суггестивное, парапсихологические методы воздействия), высокоточное оружие нового поколения («интеллектуальные» боеприпасы), метеорологическое, геофизическое, биологическое оружие нового поколения (включая психотропные средства), химическое оружие нового поколения [1].

Проект должен разрабатываться на базе систематизации достигнутых научно-технических, инженерных решений и результатов в этом направлении для постановки краткосрочных и долгосрочных целей, понимания и организации этапов реализации достижения целей. СП БО МВКС представляет собой интеллектуальный механизм, постоянно интегрированный в систему национальной и общественной безопасности государства. Поэтому жизненный цикл системного проекта «безопасный объект МВКС» совпадает с жизненным циклом организации национальной безопасности государства.

Реализация системного проекта предполагает достижение следующих целей:

– обеспечение гарантированной безопасности МВКС, в том числе на базе рассмотрения функционирования сложных технических систем в более жесткой взаимосвязи и влиянии друг на друга военной и гражданской сфер государства;

– консолидацию усилий гражданских предприятий, выпускающих продукцию двойного назначения, в том числе способных выпускать данную продукцию;

– **решение системных вопросов применения двойных технологий** в организации технологических комплексов защищенности объектов МВКС. Основная задача - создание комплексов в соотношении оптимальной цены и качества;

– **достижение постоянного научно-технологического прорыва и мирового первенства**. Наука и техника (новые технологии) должны быть интегрированы в текущие проекты строек капитального и некапитального строительства. Формирование эффективных систем безопасности МВКС реализуется при наличии в технических заданиях на проектирование объектов отдельного пункта – проведение научно-исследовательских и экспериментальных работ, тогда наука будет встроена в процесс основной деятельности профильных министерств и ведомств;

– **создание условий бурного развития двойных технологий**, в том числе на базе организации интеллектуальной безопасности разработчиков новых технологий;

– **создание важнейших механизмов реализации** всего системного проекта - межотраслевой, межведомственной, государственной программы РФ «Цифровая безопасность ГЗО» и технологической платформы «Цифровая безопасность ГЗО», как важнейших факторов реализации всего системного проекта и взаимным влиянием на все сферы государства.

Перед тем как перейти к новой парадигме, задачам, практической реализации, составу и результатам СП БО МВКС, необходимо рассмотреть существующее положение дел и подходов к КВО и СВО на современном этапе. Анализ техногенных аварий и катастроф последних десятилетий во многих промышленно развитых странах показал, что наиболее тяжелые последствия возникающих при этом угроз и чрезвычайных ситуаций (ЧС) имеют место в тех случаях, когда не обеспечивается безопасность крупных, уникальных объектов инфраструктуры. Выполненные в XX веке исследования и прикладные разработки с участием специалистов Совета Безопасности РФ, РАН, МЧС подтвердили данные выводы и показали, что задачи предупреждения и предотвращения данных угроз и ЧС являются одной из наиболее сложных научно-технических, социально-экономических и экологических проблем. В связи с этим после обращения в 2001 году президента РАН академика Ю.С. Осипова и министра МЧС России С.К. Шойгу к президенту РФ В.В. Путину, **учитывая возрастающее количество ЧС (рис.1 и рис.2),** решением совместного заседания Совета Безопасности РФ и Президиума Госсовета РФ от 13 ноября 2003 года (протокол №4) **проблема повышения защищенности КВО была определена как один из важнейших элементов государственной политики в сфере безопасности страны [1].**

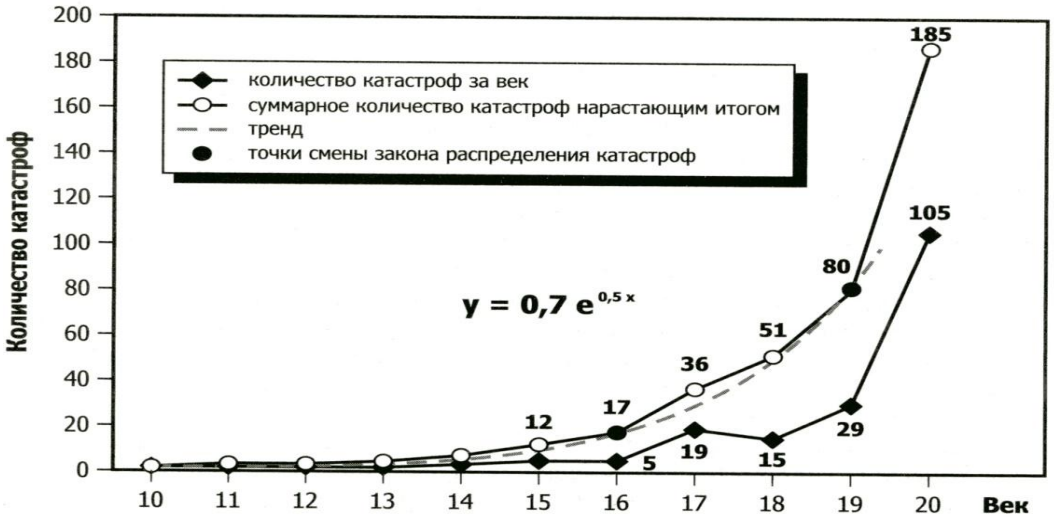

Рис. 1. Динамика проявления крупнейших природных катастроф на современной территории России за десять веков

Закономерности по анализу, прогнозу возникновения и ликвидации последствий природных, техногенных и социальных ЧС **взаимосвязаны и имеют единую фундаментальную основу**.

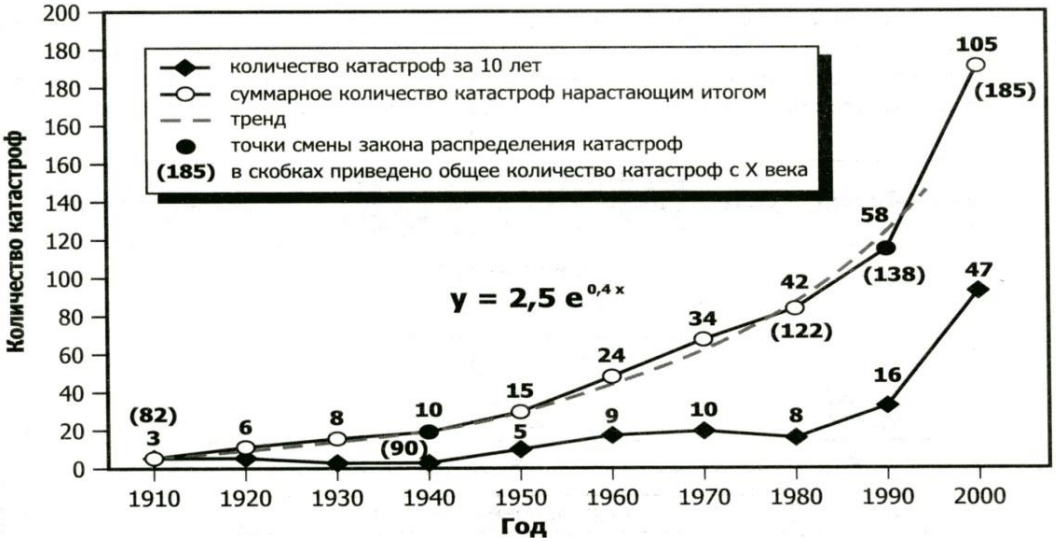

Рис. 2. Динамика проявления крупнейших природных катастроф на современной территории России в XX веке

Анализ большинства техногенных и природно-техногенных катастроф на КВО показывает, что они определяются тремя основными параметрами и опасными процессами: неконтролируемым выбросом веществ, неконтролируемым выделением опасной энергии (механической, тепловой, электромагнитной, световой), неконтролируемым созданием или разрушением потоков информации. Для защиты критически важных объектов (КВО) от инициирующих воздействий и развивающихся ЧС в их конкретном приложении должны исследоваться и разрабатываться следующие типы защиты: жесткая защита, постоянно действующая функциональная защита, естественная защита, комбинированная защита [1].

Управление, регулирование и обеспечение защищенности населения и КВО по критериям рисков сводится к качественному и количественному статистическому и детерминированному анализу на определенном отрезке времени параметра вероятности возникновения аварий и катастроф и математического ожидания ущерба от них, а также к осуществлению комплексных мероприятий по снижению рисков от фактически неприемлемых до приемлемых (допустимых) уровней с формированием цепочки «защищенность→безопасность→риск→живучесть→надежность→ресурс→прочность» [1].

Исходя из цели обеспечения безопасности КВО, при разработке соответствующей методологии решаются следующие задачи: предварительный анализ нарушений с целью отбора событий для определения их значимости для безопасности объекта; детальный анализ с оценкой событий на основе комбинированных моделей и методов (детерминированных, статистических, вероятностных, логико-вероятностных, имитационных), обеспечивающих получение качественных и количественных результатов оценки риска. По значениям рисков оцениваются уровень влияния нарушений на безопасность объекта, а также выявляются причины нарушения эксплуатации и другие условия, характеризующие анализируемую ситуацию [1].

Существующие подходы на сегодня решают главную задачу – прогноз, предотвращение аварий и катастроф, и ликвидация их последствий на объектах КВО и СВО, их влияние на внешнюю среду (территории, государство в целом), т.е. на всё что «вокруг» с учетом природных и социальных факторов исходящих «извне» на объект и техногенной ситуации «внутри» объекта на основе двух подходов:

1. **Нормативные подходы к обеспечению защищенности**, которые базируются на снижении возможности достижения системой различных предельных состояний за счет реализации технических и организационных мер, обеспечивающих соответствующие запасы по основным механизмам достижения предельных состояний.
2. **Подходы, основанные на управлении риском аварий и катастроф на КВО** и предполагающие выработку комплекса технических и организационных мероприятий, направленных на снижение уровня угроз, которым подвергаются КВО, на снижение уязвимости объектов по отношению к угрозам и минимизацию ущербов в случае аварий в КВО [1].

Применение первого подхода оправдано в случаях, когда имеется значительный опыт строительства и эксплуатации систем данного класса. Для уникальных объектов требуется использование второго подхода.

В качестве интегрального показателя защищенности вводится риск-индекс защищенности КВО, представляющий собой отношение законодательно установленного максимального допустимого значения интегрального риска для рассматриваемой системы к текущему значению интегрального риска.

Основанный на управлении риском подход к обеспечению защищенности КВО предусматривает действия по снижению трех факторов риска [1]:

1. Угроз природно-техногенного и террористического характера, которым подвергается КВО (рис. 3);
2. Уязвимости КВО по отношению к указанным угрозам;
3. Ущербов при авариях на КВО.

При этом требуется анализ и оценка риска всех трех факторов с учетом различных концепций (технической, экономической, психологической, социальной), методов (феноменологического, детерминистского, вероятностного), которых несколько десятков. Соответственно для каждого объекта необходимо проводить большую работу по конкретизации применимости тех или иных методов.

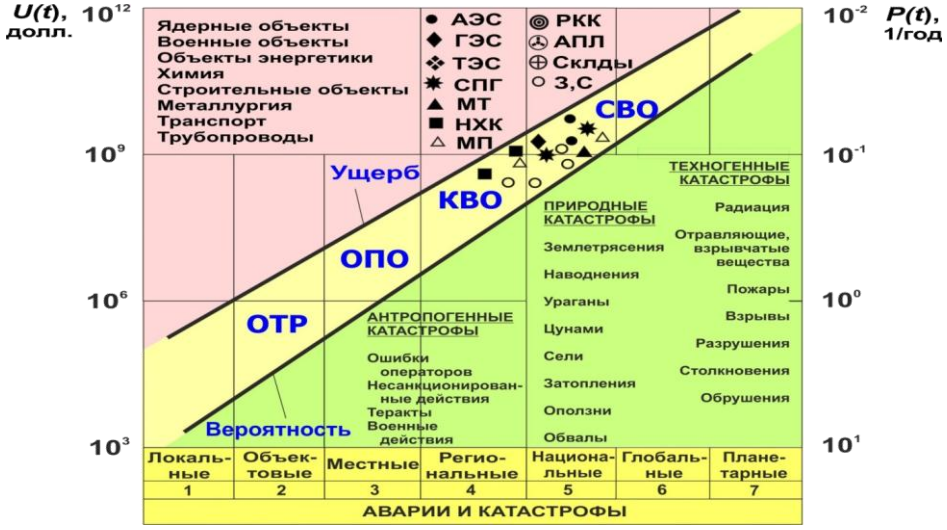

Рис. 3. Ущербы, периодичность тяжелых катастроф на уникальных объектах

Вместе с тем достижение новых приемлемых уровней стратегических рисков для КВО по-прежнему затруднено наличием ряда нерешенных вопросов научно-методологического и организационного характера, связанных с определением и категорированием КВО и потенциально опасных объектов (ПОО) РФ. Пока **отсутствует единая утвержденная на соответствующем уровне методика оценки риска возникновения ЧС на КВО** в зависимости от состояния его защищенности. Отнесение объектов инфраструктуры страны к категории КВО носит заявительный характер, такой параметр, как **допустимый и приемлемый риск, - ещё одна характеристика объекта – не**

содержится в существующих Перечнях КВО. Оформление паспортов безопасности опасных объектов (ОТР, ОПО, КВО, СВО) и разработки планов их защищенности от угроз техногенного, природного характера и террористических актов основаны на использовании разнородных ведомственных методик. Численные значения выходных параметров данных методик, при прочих равных условиях, значительно различаются и не могут быть соотнесены с уровнем допустимого риска конкретного КВО. Вместе с тем **именно это соотношение (приемлемый (допустимый) - неприемлемый риск) характеризует уровень достигнутой защищенности объекта и если оказывается ниже требуемого [1], проводятся специальные мероприятия по повышению уровня защищенности с пониманием финансовых затрат, необходимых для обеспечения безопасности КВО** (собственные ресурсы и меры господдержки). Изменение этого соотношения должно явиться важнейшей характеристикой объекта, контролируемой в рамках федеральной системы защищенности КВО и ПОО инфраструктуры РФ.

Результаты исследований и прикладных межотраслевых разработок отражены в 52 томах издания «Безопасность России. Правовые, социально-экономические и научно-технические аспекты».

Рассмотрим подробнее новую парадигму, задачи, практическую реализацию, состав и результаты СП БО МВКС.

В СП БО МВКС задача схожая относительно существующих подходов, но с учетом основного и важного аспекта - фокус решений локализации и предотвращения возможных деструктивных воздействий террористической направленности на объект должен формироваться с учетом того, что они могут носить взаимосвязанные социальный, природный и техногенный характеры. Именно это данное воззрение (положение) определяет новую парадигму.

Учитывая три вида терроризма (традиционный, технологический, интеллектуальный) - это более сложная задача, имеющая следующие особенности:

1. **Более динамичный характер террористических рисков** – изменение спектра и интенсивности угроз при террористических воздействиях проходит значительно интенсивнее, чем для угроз природно-техногенного характера. Террористы способны постоянно расширять свой арсенал механизмов инициации ЧС, используя современные материалы и технологии; реагировать на изменения систем защиты объекта МВКС и извлекать уроки из ошибок, совершенных при нападении на МВКС в прошлом;

2. **Высокий уровень неопределенности**, связанный с человеческим фактором, сложность оценки системы ценностей и логики поведения террористов;
3. **Сознательный выбор террористами сценариев атаки** (места, времени и типа воздействия) с учетом параметров уязвимости системы и ущерба, ожидаемого в случае успешной реализации атаки. Следует иметь в виду, что террористы способны анализировать матрицу уязвимости и структуру ущербов при различных видах воздействия на систему и выбирать тот сценарий атаки, который максимизирует ущерб для общества (с учетом вторичных и каскадных ущербов). Здесь, дополнительно к вероятностному анализу, необходимо привлечение аппарата теории игр, позволяющего учесть сознательные действия террористов.

Отличительные особенности сценариев аварий, инициированных террористическими атаками на МВКС, по сравнению со сценариями аварий на КВО, инициированными не террористическими угрозами, **обуславливаются способностью террористов осуществлять сознательный выбор сценария атаки**. Этот выбор основывается на рациональной оценке: (1) уязвимости рассматриваемой системы по отношению к различным сценариям атаки и (2) величин ущербов, ожидаемых при их реализации [1].

Выбираемые террористами варианты воздействия на принципе минимакса, заключающемся в стремлении нанести обществу максимальный ущерб при минимальном расходовании ресурсов и минимальном риске обнаружения и ликвидации организации (то есть на стремлении обеспечить максимальную эффективность атаки).

Традиционные методы построения деревьев событий, содержащие только случайные узлы, которые используются при проведении сценарной оценки в технической системе в случае техногенных катастроф, не позволяют описать сценарии террористических атак. Они не учитывают способность террористов делать осознанный выбор сценария – иными словами, не учитывают сознательный и рациональный характер их действий, обеспечивающих максимальную эффективность. Простейший способ учета особенностей террористических сценариев в графовых моделях заключается в дополнении сценарных деревьев специальными узлами решений (построение «деревьев решений»).

Такие **решения ограничены**, поскольку эти модели не позволяют вводить обратные связи, которые присутствуют в задачах терроризма, а также описывать динамику принятия мер и контрмер сторонами защиты и нападения. Для преодоления этих недостатков **необходимо строить многофакторные (многомерные) динамические модели** [1].

Учитывая вышеизложенное, для успешной реализации системного проекта необходимо решение следующих задач:

- **организация осуществления комплекса мероприятий** на новом научно-технологическом и инженерном уровне. Применение новых технологий и оборудования на разных этапах их готовности и наилучших практик сразу на этапе проектирования в программах капитального строительства и ремонта объектов МВКС;
- **реализация пилотных проектов** по созданию организационно-технологического комплекса защищенности (ОТКЗ) объектов МВКС на базе Центра компетенции (инновационного кластера) с переходом к Технологической платформе «Цифровая безопасность МВКС»;
- **организация специальных работ** (в том числе проведения проектных, строительно-монтажных, пусконаладочных, экспериментальных, поисковых, аналитических и т.д.);
- **разработка комплексной методологии** создания и совершенствования (модернизации) систем безопасности объектов на основе единого подхода комплексной оценки угроз с учетом приемлемого и допустимого риска, выработки и обоснования рациональной совокупности взаимодополняющих мер обеспечения безопасности, оптимизация затрат с учетом конкретной специфики каждого объекта;
- **гарантированный переход** от квазиинтеллектуальных систем **к информационно-интеллектуальным системам поддержки принятия решений**, как ядра всей системы безопасности;
- **формирование нормативно-правовой**, методологической базы процесса обеспечения безопасности объектов МВКС;
- организация **комплексной психофизиологической безопасности** личного состава на базе применения инновационных медицинских технологий;
- организация многоуровневого **процесса обучения и повышения квалификации**.

Практическая реализация СП БО МВКС условно базируется на двух этапах. Определение и запуск конкретных пилотных проектов в ведомствах. Далее, используя результаты пилотных проектов, переход к созданию межотраслевой, межведомственной, государственной программы РФ и технологической платформы «Цифровая безопасность ГЗО», как важнейшим механизмам реализации всего системного проекта и взаимным влиянием на все сферы государства.

На первоначальных этапах движения, опорой системного проекта является Инновационный кластер Национальное агентство «Наука и Безопасность». Работа Центра

компетенции участников на единой правовой площадке необходима для решения распределенных организационно-технологических задач, синхронизации научно-технических и инженерных решений с учетом «лучших практик», в том числе для выполнения ряда поисковых, аналитических и проектных работ.

На разных стадиях реализации проекта **конечные продукты (организационно-технологические комплексы защищенности (ОТКЗ)) будут представлять собой единый комбинированный, многоуровневый комплекс для решения разнонаправленных задач, состоящий из совокупности интегрированных программ в области безопасности, с учетом тесной взаимосвязи (в том числе нормативно-правовой) объектов МВКС с другими ведомственными и отраслевыми организациями, транспортным комплексом страны**.

СП БО МВКС интегрирует как уже созданные системы безопасности этих объектов, так и планируемые к внедрению новейшие системы и комплексы. В проекте предусматривается детальный анализ системы безопасности для определения соответствия ее существующему и планируемому характеру и уровню соответствующих угроз. Потребуется полная синхронизация действий и решений по обеспечению безопасности объекта с текущей работой правоохранительных органов, специальных служб, служб министерств и ведомств, занимающихся вопросами комплексной безопасности и влияющих на конкретный объект МВКС. Понимание всего комплекса «проблем» социальной, природной и техногенной обстановки «вокруг» объекта важно для интеграции этой информации в ОТКЗ в автоматическом режиме. **Необходимо на каждом объекте МВКС «собрать» в единый интеллектуальный комплекс службу безопасности (охраны), комплекс инженерно-технических средств охраны (КИТСО), часть средств технологических систем инженерно-технических служб, службу охраны труда и промышленной безопасности, экологическую службу, метеорологическую службу, службу радиационного и химического контроля и другие (всего минимум двадцать видов опасностей), новые технологии обнаружения и противодействия террористическим актам, которые могут структурно входить в выше перечисленные составляющие, исходя из трёх видов терроризма (традиционный, технологический, интеллектуальный)**.

Суммарно применяемых в проекте технологий может быть достаточно большим. Применяемость технологий будет определяться требованиями к защищенности конкретного объекта (в т.ч. совокупностью неприемлемых и допустимых рисков (методикой)). **Основу ОТКЗ будет составлять интеллектуальное ядро системы, на которое будут**

«наматываться» применяемые технологии. По согласованию с Заказчиком определяется перечень аналитического инструментария, например: когнитивное моделирование, эволюционные вычисления, иммунные вычисления, муравьиные алгоритмы, сетевая экспертиза, анализ иерархий, визуальная аналитика, контент и коннект анализ, квантовая семантика, некорректные задачи на топологиях, фундаментальные основы мониторинга рисков и управления стойкостью [4].

Учитывая, что применяемые технологии будут определять облик и наполнение ОТКЗ, в качестве примера перечислим **некоторые из них:**

- Технологии **ситуационного моделирования** - процесс построения и анализа формализованных моделей (в т.ч. факторная модель) реальных ситуаций, возникающих в технических, организационных, социально-экономических и других сферах функционирования объектов;
- Технологии **виртуального полигона**, визуализации информации, виртуального окружения на основе виртуального повествования (компьютерные приложения, сочетающие черты виртуального тренажёра, интерактивной модели, компьютерной игры в которых участники виртуального повествования выступают не в качестве пассивных слушателей, а в роли активных действующих лиц, непосредственно влияющих на процесс развёртывания интерактивного виртуального повествования; виртуальное повествование - новая форма взаимодействия пользователя и персонала объекта МВКС, как объекта с информационной системой)[2];
- Технологии **3D ГИС** в интересах мониторинга кризисных ситуаций;
- Технологии **прогнозирования**, выявления тенденций и рисков;
- Технологии **подготовки решений руководителей объектов** МВКС на основе поддержки коллективного принятия решения - формальных методов (кооперативные игры, согласованные решения, голосование и коллективный выбор, генетический консилиум);
- Технологии **автоматизированного решения** информационных, информационно-расчетных, информационно-аналитических и интеллектуальных **задач** в распределенных системах (мониторинг рисков и управление стойкостью);
- Технологии **анализа данных** (в реальном масштабе времени, в краткосрочном и долгосрочном периодах времени);
- Технологии по **организации** межведомственного и межотраслевого **взаимодействия;**
- Технологии **работы в информационном пространстве** (социальные сети, интернет);

- Технологии, обеспечивающие **мониторинг** безопасности (**технического состояния**) зданий и сооружений;
- Технологии **локального и дистанционного контроля состояния** комплекса средств автоматизации (**КСА**);
- Технологии, использующие **методы управления функциональной безопасностью** электрических, электронных, программируемых электронных систем, связанных с безопасностью объектов и комплексов МВКС, их аппаратных средств и программного обеспечения;
- Технологий создания сложных технических объектов на основании методов информационной поддержки жизненного цикла продукции (CALS-технологии);
- Технологии **сбора и передачи** больших и **интеллектуальных объемов информации**;
- Технологии формирования и ведения больших баз данных (информационного хранилища), **Big Data**;
- Технологии и инженерно-технические решения, применяемые в транспортном комплексе, энергетике и других отраслях и ведомствах;
- Технологии, **обеспечивающие** приемлемый уровень защищённости (**безопасности) периметра объекта**, формирования **зон безопасности**;
- Технологии, обеспечивающие **информационную и кибернетическую безопасность**;
- **Технологии обнаружения, идентификации, сопровождения множественных беспилотных транспортных средств (БТС)**;
- Технологии комплексной мультирадарной обработки и выдачи целеуказаний на АРМ оператора и наземные/воздушные системы блокировки/поражения **БТС**;
- Технологии блокировки инфо-управляющих каналов **БТС** и перехвата управления, включая спуферы каналов спутниковых навигационных и связных систем;
- **Технологии уничтожения БТС, включая обычное и лучевое воздействие;**
- Технологии электромагнитного уничтожения **БТС**;
- Технологии кинетического воздействия и физического перехвата **БТС**, включая **использование БТС-перехватчиков**;
- Технологии снижения последствий несанкционированного применения **БТС**;
- Технологий **мониторинга и противодействия реализации АНВ** (в том числе террористических актов) с применением **взрывчатых веществ, отравляющих химических и бактериологических веществ**;
- Технологий мониторинга и противодействия распространению обширных **инфекционных заболеваний**;

- Технологий **противодействия паническим настроениям и связанных с ними последствиям** во время деструктивных воздействий;
- Технологии закрытой **помехоустойчивой связи**;
- Технологии **мониторинга электромагнитных излучений** для определения фактов проведения пробных разведывательных действий перед деструктивным воздействием на системы и рубежи защиты объектов МВКС:
- Технологии по **организации комплексной психофизической безопасности** личного состава на базе применения инновационных медицинских технологий;
- Технологии по организации мониторинга окружающей среды (в т.ч. **технологические решения по экологической безопасности**) [5, 6];

Моделирование процессов противодействию деструктивных воздействий на объектах МВКС будет осуществляться с использованием всех выше перечисленных инструментов, в том числе математических, имитационных моделей, методов прогнозирования потенциальных опасностей и угроз, использования проактивных, интерактивных методов, методов блокирования и нейтрализации угроз. Будет учтен опыт и накопленный объем многолетней статистической информации транспортной инфраструктуры, ТЭК, других отраслей и ведомств. Это позволит надежно прогнозировать значения соответствующих показателей и вероятности реализации того или иного сценария развития обстановки на объектах МВКС на долговременный период [7].

С учетом выше сказанного необходимо в мероприятиях предусмотреть взвешенные, плановые организационно-штатные мероприятия на объекте, принятие новых управленческих решений для перехода на другой качественный уровень управления объектами без боязни и оглядки на сложившиеся управленческие стереотипы [8].

Для подготовки, функционирования и пополнения кадров необходима организация комплексной психофизиологической безопасности личного состава на базе применения инновационных медицинских технологий. Особое внимание необходимо уделить операторам дежурных смен.

Полученные в системном проекте результаты будут являться системно-технической основой, обеспечивающей возможность ускоренного и гармонизированного выполнения последующих стадий работ по проектированию и построению качественно новой системы безопасности объектов МВКС, даст возможность определить облик будущего ОТКЗ (непрерывное устойчивое развитие), намечает перечень необходимых к созданию стандартов и нормативных документов.

Разработка СП БО МВКС обеспечит:

- **экономическую выгоду производства современной наукоёмкой продукции двойного назначения**. Сегодняшний суммарный мировой **эффект этого рынка** превышает **1 (один) триллион долларов**. **Доля России** на этом рынке пока не превышает **1-1,5% [1]**;
- **исключение (экономию) затрат на восстановление** после деструктивных воздействий в размере **не менее 5% ВВП** в среднесрочной перспективе и доведением до **7,5% ВВП** в долгосрочной перспективе. Решение данного вопроса позволит исключить деградацию производительных сил и приведет к росту экономики России в целом;
- возможность разработки **единой методики оценки риска возникновения деструктивных воздействий террористической направленности и ЧС на МВКС с учётом** комплексного анализа **приемлемых, неприемлемых рисков**, который характеризует законодательно установленную защищенность объекта;
- **реально обоснованное финансирование** (оптимизацию затрат (экономию)), **напрямую увязанное** с пониманием этого процесса (единая методика оценки риска) по **объему организационно-технических мероприятий** для достижения приемлемого уровня риска и обеспечения законодательно установленной защищенности объектов;
- **создание высокоэффективной единой службы защиты объекта на базе ОТКЗ**;
- **решение задачи информационно-интеллектуальной поддержки принятия решений** для лиц принимающих управленческие решения по предупреждению и ликвидации деструктивных воздействий террористической направленности и ЧС на объектах МВКС;
- **гарантированную безопасность объектов МВКС**, в том числе на основе «управления стойкостью (уязвимостью, безопасностью)», которая будет достигаться путем управления существующими уязвимостями и доступными адаптационными возможностями, дополняя «анализ и управление рисками». Установление приоритетов управления безопасностью объектов МВКС: по видам безопасности и типам систем защиты (жесткая, постоянно действующая функциональная, естественная, комбинированная), по степени воздействий опасности, по приоритетам действий органов регулирования и управления;
- **укрепление обороноспособности страны** за счет участия в планах мобилизационной готовности государства.

Результатом системного проекта будет являться создание взаимоувязанного единого организационного-технологического комплекса защищенности (ЕОТКЗ) всей страны, создание искусственного интеллекта специализированного назначения, использующий

данные ЕОТКЗ, для борьбы с различными видами существующих и потенциальных угроз террористической направленности с учетом воздействия социальных, природных и техногенных деструктивных факторов на государственно значимые Министерства обороны, военно-промышленного комплекса, критически и стратегически важные объекты РФ.

Литература

1. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. 52 тома. Научный руководитель издания: член-корреспондент РАН Махутов Н.А. — М., 1998-2015.
2. Клименко С.В., Балановский В.Л., Габур С.П. Комплексное обеспечение безопасности объектов транспортной инфраструктуры: от управления риском к управлению стойкостью // Вопросы радиоэлектроники: №5, 2016.
3. Махутов Н.А., Куприков М.Ю., Балановский В.Л., Куприков Н.М. О современных подходах к процессу формирования облика эффективных систем безопасности сложных объектов в полярных регионах // Известия Тульского государственного университета. Технические науки: № 9-1, 2017. — С. 389-395.
4. Клименко А.С., Кириллов И.А., Клименко С.В., Балановский В.Л., Габур С.П. Проблемы формирования управления стойкостью // Труды Международной научной Школы-семинара «Ситуационные центры и ИАС-4i для мониторинга и безопасности», 21-24 ноября 2015 г., Протвино. — М.: Изд-во ИФТИ, 2016.
5. Балановский В.Л., Габур С.П., Плотников Н.И. Безопасный регион (город): устойчивое развитие и новые доступные технологии // Труды Международной конференции и Школы по стойкости социо-технических систем Resilience 2014, 25-28 ноября 2014 г., Протвино. — М.: Изд-во ИФТИ, 2015. — С. 148-153.
6. Балановский В.Л., Габур С.П. Технологии обеспечения комплексной безопасности транспорта // Труды Международной научной Школы-семинара «Ситуационные центры и ИАС-4i для мониторинга и безопасности», 21-24 ноября 2015 г., Протвино. – М.: Изд-во ИФТИ, 2016.
7. Махутов Н.А., Клименко С.В., Балановский В.Л., Габур С.П., Любимов К.М., Юсупов М.Р. Формирование понимания концепции управления стойкостью в составе сети распределенных ситуационных центров // Радиопромышленность: №3, 2016.
8. Балановский В.Л., Габур С.П. Совершенствование систем комплексной безопасности на основе управления качеством безопасности // Труды Международной научной Школы-семинара «Ситуационные центры и ИАС-4i для мониторинга и безопасности», 21-24 ноября 2015 г., Протвино. — М.: Изд-во ИФТИ, 2016.