ПУТИ РЕШЕНИЯ НЕКОТОРЫХ ПРОБЛЕМ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ МЕТОДАМИ СИСТЕМНОЙ ИНЖЕНЕРИИ

[1,2,3]Костогрызов А.И.

[1]*Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», 119333, Россия, Москва, ул. Вавилова 44, корп.2,*

[2]*ГНИИЦ робототехники МО РФ, 125167 Москва, ул. Серегина, 5,*

[3]*Российской академии ракетных и артиллерийских наук, 107564 Москва, 1-я Мясниковская 3, стр.3*

e-mail: Akostogr@gmail.com

Сформулированы приоритетные проблемы комплексной безопасности критически важных объектов и систем. Предложены пути решения проблем в виде актуальных законодательных, нормативно-правовых, научно-методических, организационных, опытно-конструкторских, эксплуатационно-производственных и квалификационно-кадровых задач системной инженерии.

Ключевые слова: анализ, безопасность, качество, модель, процесс, риск, система.

THE WAYS OF SOLVING SOME PROBLEMS OF COMPLEX SAFETY BY METHODS OF SYSTEM ENGINEERING

[1,2,3]Kostogryzov A.I.

[1] *Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS), Vavilova Street 44, bld. 2, 119333 Moscow, Russia*

[2] *Main Scientific Research Test Center (MSRTC) of the Russian Ministry of Defence, Seriogina Street 5, 125167 Moscow, Russia*

[3] *Russian Academy of Rockets and Artillery Sciences, 1-st Miasnicovskaya 3, bld.3, 107564 Moscow, Russia*

e-mail: Akostogr@gmail.com

The priority problems of complex safety of critically important objects and systems are formulated. The ways of the solving these problems in the form of actual legislative, standard&legal, scientific&methodical, organizational, developmental, operating and qualifying -personnel problems of system engineering are proposed.

Key words: analysis, model, quality, process, risk, safety, system

1. АНАЛИЗ ТЕНДЕНЦИЙ И ВЫЯВЛЕНИЕ ПРОБЛЕМ

Сегодня наблюдается серьёзный перекос в информационном и техническом прогрессе РФ, обострившийся в последнее время из-за санкций Запада, технологического отставания РФ в области информационных технологий (ИТ), социально-экономических кризисов и распространения терроризма, ведущих к росту разнородных неопределенностей. В итоге процесс создания и эксплуатации критически важных объектов и систем (КВОС) в России и за рубежом оказывается совмещенным с утратой согласованной подконтрольности отдельных элементов и систем.

Это приводит к недооценке роста рисков нарушения комплексной безопасности и нерациональности в решении связанных с этим системных проблем.

Под комплексной безопасностью понимается безопасность важных объектов и систем в условиях разнородных угроз (включая угрозы промышленной, энергетической, пожарной, информационной, экологической, транспортной, антитеррористической безопасности, безопасности зданий и сооружений,

ядерной и радиационной безопасности).[1]

Впереди России предстоит не только выход из кризиса, подъем отечественной промышленности, важные международные мероприятия, построение электронного государства, сложные технические проекты в странах содружеств БРИКС, ШОС, ЕАЭС, но и освоение Арктики, международные антитеррористические операции в Сирии и других горячих точках мира и иные крупные задачи в технологическом и социально-экономическом развитии. Учитывая, что потенциальные ущербы и затраты на ликвидацию последствий критичных нарушений безопасности важных объектов и систем в условиях разнородных угроз на порядок превышают затраты на превентивные меры, необходим поиск эффективных решений по комплексной безопасности. Несмотря на то, что многочисленные предпринятые в России меры противодействия угрозам разработаны на уровне федеральных законов (ФЗ), федеральных норм и правил (ФНП), руководств по безопасности (РБ), «ручное» управление комплексной безопасности продолжает оставаться главенствующим, причем так, как это субъективно понимается на ведомственном и корпоративном уровне. В свою очередь, мировые тенденции развития современных систем различного функционального назначения свидетельствуют о необходимости кардинального разворота от «ручного» управления отдельными видами безопасности (основанного на выполнении устоявшихся инструкций и на экспертных оценках складывающихся ситуаций) к реализации научно обоснованных эффективных упреждающих мер в жизненном цикле важных объектов и систем на основе прогнозирования рисков. Это позволяет на основе прогнозного взгляда вперед превентивно предпринимать эффективные упреждающие воздействия. Такая идея красной линией проходит через все западные концепции и последние стандарты системной инженерии. Но как это сделать – остается за кадром. В мире еще нет универсального подхода к реализации этой идеи. В поиске – все ведущие страны мира, а находки, которых не так много, обращаются в государственные, коммерческие или военные решения «ноу-хау», предопределяющие выгоды от их применения. У России уже есть фундаментальные наработки в этом направлении, которые должны быть обращены на пользу делу.

Пренебрежительное отношение к аналитическому прогнозированию рисков ведет к многомиллиардным ущербам. Для КВОС злоумышленные нарушения могут маскироваться под технические неисправности, ошибки от «человеческого фактора» или под «облачные» воздействия. Независимо от рода реализуемых угроз это может наносить непоправимый ущерб, вредить конкурентоспособности России, вести к обострению социальной напряженности.

Острота перечисленных угроз усугубляется отсутствием в России требований и применяемых мер обеспечения информационной безопасности открытой служебной информации. Возрастают риски нарушения информационной безопасности и связанных с этим других видов безопасности - промышленной, энергетической, пожарной, экологической, транспортной, антитеррористической безопасности, безопасности зданий и сооружений, ядерной и радиационной безопасности с использованием ИТ-систем.

В современных условиях антироссийских санкций и противостояния с США и странами Запада возникла острая необходимость импортозамещения программного обеспечения (ПО). Так, в нефтегазовом комплексе России используется прикладное ПО около 30 зарубежных компаний, таких, как Schlumberger, Emerson Electric, Halliburton, Honeywell (все - США), Shell Global Solution (Великобритания-Голландия); Alstom (Франция) и др. Анализ возможностей отечественных пакетов программ показал, что функциональность систем в нефтегазовом комплексе может быть обеспечена на базе отечественного инженерного ПО в области

---

[1] Примечание. К критически важным объектам и системам относятся:

стратегически и критически важные объекты РФ, особо опасные, потенциально опасные и опасные производственные объекты, включая действующие и проектируемые объекты топливно-энергетического комплекса (ТЭК), атомные и гидроэлектростанции, объекты химической и металлургической промышленности;

информатизированные техногенные и логистические системы в промышленности (в т.ч. АСУ технологическими процессами, системы диспетчерского управления, компьютеризированное производство), энергетике, строительстве, на транспорте, в крупных коммерческих структурах;

информатизированные объекты и системы инфраструктуры для проведения международных мероприятий в России (в т.ч. чемпионаты мира по футболу-2018, хоккею-2016, Универсиады-2019, Олимпиад, фестивалей, научно-технических форумов, выставок);

важные информатизированные объекты и системы социальной инфраструктуры РФ, системы электронного государства, электронного Правительства и информационного общества в РФ, в т.ч. государственной информационно-аналитическая система мониторинга состояния национальной безопасности Российской Федерации (информационно-аналитические системы мониторинга национальной безопасности), государственная информационная система (ГИС) ТЭК, информационные системы МЧС, ГАС «Выборы», ситуационно-аналитические центры, системы поддержки принятия решений в органах государственного управления, социальную медиа-среду с использованием Интернет;

военно-политические, военно-технические и охранные системы РФ, важные информатизированные объекты и системы инфраструктуры РФ за рубежом в условиях информационного противоборства;

объекты и системы, участвующие в освоении подводных месторождений углеводородов Северного Ледовитого океана;

проекты содружеств БРИКС, ШОС, ЕАЭС.

геологоразведки, разработки, добычи лишь при строгой целенаправленности работ по импортозамещению. В других коммерчески выгодных областях ситуация во многом аналогична.

Тенденции таковы, что перечисленные разнородные угрозы расширяются при дальнейшем развитии России и стран содружеств БРИКС, ШОС, ЕАЭС, включая создание и эксплуатацию важных объектов и систем РФ, в т.ч. объектов ТЭК, систем, участвующих в освоении Арктики, инфраструктуры для проведения в России различных международных форумов.

Вышеперечисленные факторы в условиях террористических угроз ведут к возрастанию рисков нарушения промышленной, энергетической, пожарной, информационной, экологической, транспортной, антитеррористической безопасности, безопасности зданий и сооружений, ядерной и радиационной безопасности и порождают противоречия между информационно-техническими потребностями во всестороннем развитии России и реальными возможностями по обеспечению комплексной безопасности и эффективности важных объектов и систем.

В итоге состояние дел может быть охарактеризовано следующими положениями. Ограниченные возможности России распределяются по отдельным видам безопасности. Количественный прогноз рисков для отдельных видов безопасности не делается (например, для информационной, экологической и антитеррористической безопасности, исключение – прогноз рисков в интересах МЧС РФ и в некоторых случаях- для Росатома путем имитационного моделирования), а там, где делается (например, для промышленной безопасности) – в подавляющем большинстве случаев осуществляется при структурных и методических упрощениях, свойственных достижениям 20-30-летней давности . Отсюда из-за недопонимания требуемой глубины анализа идут грубые ошибки и подгонка результатов – для сложных систем ошибки составляют сотни-тысячи процентов! В общем случае «допустимые риски» рассматриваются лишь как пограничная полоса. Разнородность угроз и их системное влияние на комплексную безопасность не анализируются. В подавляющем большинстве случаев требования к «допустимым» рискам научно не обосновываются или предъявляются формально для демонстрации того, что риски при таких-то условиях «не превышают допустимых» (прогнозы и устойчивость для разнородных угроз – не рассматриваются, задачи синтеза с обоснованием «что делать?» - не решаются в реальном времени). Для сложных структур предпринимаемые меры контроля, мониторинга и противодействия угрозам научно не обосновываются, хотя понятие «допустимых рисков» в мире используется в первую очередь для решения обратных задач и обоснования упреждающих мер противодействия угрозам. Эффективность отдельных упреждающих мер в комплексе мер не оценивается в терминах снижения рисков. Узкоспециализированные (и за счет этого зачастую разнонаправленные и дезинтегрированные) методические решения ведут к различающимся несравнимым интерпретациям и невозможности соизмерить результаты из различных приложений применительно к разнородным угрозам. Междисциплинарный опыт используется крайне редко. Междисциплинарные знания по прецедентам для эффективных упреждающих действий не систематизируются и не доводятся до заинтересованных лиц для учета и недопущения повторных или аналогичных ошибок. Приобретение и внедрение импортного ПО разобщено (отсюда - дублирующиеся государственные расходы, расходование средств и ресурсов нерационально). Доказательствам эффективности систем в терминах прогнозируемых рисков в условиях разнородных угроз на всех стадиях жизненного цикла (особенно на ранних) не уделяется должного внимания. Именно здесь находится источник принципиальных противоречий между требуемой и достигаемой комплексной безопасностью. Если сейчас не повернуться лицом к выявленным противоречиям, то по мере усложнения создаваемых важных объектов и систем тупиковые решения приведут к полной потере конкурентоспособности России. И наоборот, своевременное разрешение накопившихся проблем на основе прогнозирования рисков приведет к долговременной и обоснованной реализации скрытых эффектов для важных объектов и систем различного функционального назначения.

Складывающееся положение дел неоднократно анализировалось на различных научно-технических форумах. Это позволило выявить следующие принципиальные проблемы обеспечения комплексной безопасности, требующие приоритетного решения. В общем случае для ожидаемых условий неопределенности и разнородных угроз в приложении к объекту, системе или системному элементу или их совокупности таковыми проблемами являются – см. рис.1:

1) проблема адекватного аналитического прогнозирования рисков нарушения комплексной безопасности на заданный период прогноза для сложных объектов и систем;

2) проблема аналитического обоснования эффективных упреждающих мер в обеспечение комплексной безопасности важных объектов и систем (по результатам прогнозирования рисков);

3) проблема обеспечения информационной безопасности открытой служебной информации для важных объектов и систем в России и за рубежом;

4) проблема рационального импортозамещения программного обеспечения для важных объектов и систем коммерческих структур (в первую очередь для критически важных объектов и систем);

5) проблема эффективного управления рисками в жизненном цикле системных элементов, важных объектов и систем по критериям «безопасность-эффективность-стоимость».

В качестве научно-теоретической и практической основы решения проблем предлагаются основы системной инженерии, определяемой в современных международных стандартах как сосредоточение научно-технических усилий по рациональному построению и эффективному применению сложных систем.

Рисунок 1 Проблемы и направления их решения для системы и для каждого из системных элементов (в общем случае)

Рассматриваемые системы состоят из множества составных подсистем и системных элементов (их могут быть десятки-сотни-тысячи и более), для каждой из которых в общем случае должны решаться идентичные по своему содержанию проблемы 1-5 в условиях разнородных угроз нарушения комплексной безопасности – см. рис. 2. Прогнозируемые риски должны быть соизмеримыми и в жизненном цикле системных элементов и систем позволять решение прямых и обратных задач по критериям «безопасность-эффективность-стоимость».

Рисунок 2 - Декомпозиция сложной системы до элементов для решения проблем

2. ПУТИ РЕШЕНИЯ ПРОБЛЕМ

Западный мир в той или иной степени уже приступил к решению сформулированных выше проблем. Так, США сформулировали подходы системной инженерии к обеспечению национальной безопасности после 11 сентября 2001 года. Например, реализуемые ими концепции гибридных войн настоящего и будущего предусматривают не столько чисто военные решения, сколько использование уязвимостей важных объектов и систем противника к разнородным угрозам и их неспособность противостоять явным или скрытым нарушениям промышленной, энергетической, пожарной, информационной, экологической, транспортной, антитеррористической безопасности, безопасности зданий и сооружений и/или ядерной и радиационной безопасности.

Особенности разнородных угроз для важных объектов и систем России связаны с необходимостью преодоления технологического отставания в различных областях (в первую очередь – в области информационных технологий) и важностью всемерного развития научно-технологического комплекса, с рассредоточенностью в ряде случаев важных объектов и систем на громадной территории РФ с различными условиями и угрозами, с поиском и освоением новых источников энергии (например, в Арктике) и расширение рынков сбыта своей продукции во взаимодействии со странами стран БРИКС, ШОС, ЕАЭС.

Для обеспечение комплексной безопасности важных объектов и систем России в качестве основных задач предлагаются:

<u>по законодательному и нормативно-правовому направлению</u>

гармонизация, совершенствование, дополнение и создание новых законов РФ - для обеспечения эффективного функционирования КВОС в условиях угроз промышленной, энергетической, пожарной, информационной, экологической, транспортной, антитеррористической безопасности, безопасности зданий и сооружений, ядерной и радиационной безопасности и др. критичных видов безопасности;

гармонизация, совершенствование, дополнение и создание новых федеральных норм и правил и руководств по безопасности в части прогнозирования и эффективного управления рисками, обеспечения информационной безопасности служебной информации;[2]

формирование нормативной базы для определения типового множества возможных угроз, уязвимостей, формальных условий нарушений комплексной безопасности для важных объектов и систем и типовых функций противодействия угрозам;

разработка стандартов, определяющих требования ТЗ, содержание технических проектов, показатели рисков для прогноза комплексной безопасности, долгосрочного и среднесрочного планирования и импортозамещения, аналитические методы оценки и испытаний по требованиями комплексной безопасности КВОС, меры государственного контроля и удержания рисков в допустимых пределах;

разработка нормативных документов по созданию микроэлектронной базы и инфраструктуры для выпуска и применения отечественных криптографических средств защиты служебной информации;

<u>по научно-методическому направлению</u>

разработка принципов и научно обоснованных методов структурной декомпозиции систем, создание базовых сценариев нарушения комплексной безопасности и ведения гибридных войн;

разработка и стандартизация вероятностных моделей для адекватного аналитического прогнозирования рисков в системах сложной структуры;

разработка методов прогнозного анализа, системного контроля, мониторинга и восстановления нарушенного качества функционирования КВОС и информационной безопасности служебной информации;

разработка методов аналитического обоснования допустимых рисков и эффективных упреждающих мер в обеспечение комплексной безопасности;

разработка методов долгосрочного, среднесрочного и краткосрочного планирования по показателям прогнозных рисков;

разработка методов эффективного управления рисками в жизненном цикле типовых системных элементов, критически важных объектов и систем по критериям «безопасность-эффективность-стоимость»;

<u>по опытно-конструкторскому направлению</u>

---

[2] Примечание. В качестве совершенствуемых могут выступать ФНП «Правила безопасности в нефтяной и газовой промышленности», ФНП «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств», ФНП «Общие требования к обоснованию безопасности опасного производственного объекта», ФНП "Методика установления допустимых уровней риска аварий на опасных производственных объектах нефтегазового комплекса", ФНП «Правила безопасности для опасных производственных объектов магистральных трубопроводов», РБ «Методика анализа риска аварий на сухопутных объектах нефтегазодобычи и промысловых трубопроводах», РБ «Методика анализа риска аварий на опасных производственных объектах морского нефтегазового комплекса», РБ «Методические рекомендации по разработке обоснования безопасности опасных производственных объектов нефтегазового комплекса», РБ «Методические рекомендации по обеспечению безопасности критической информационной инфраструктуры Российской Федерации» (подлежит созданию), РБ «Методические рекомендации по системному противодействию угрозам в условиях гибридных войн» (подлежит созданию) и др.

разработка систем дистанционного контроля комплексной безопасности (как информационно-аналитических систем КВОС), ориентированных на:

- раннее распознавание и оценку развития предаварийных ситуаций, обеспечение возможностей принятия в реальном времени мер по предотвращению аварий, прогнозирование временного ресурса, имеющегося для принятия упреждающих мер;
- внедрение на предприятиях риск-ориентированного подхода, позволяющего системное прогнозирование рисков,
- выявление узких мест, обоснование допустимых рисков и оперативных мер в обеспечение комплексной безопасности;
- обоснование сбалансированных мер обеспечения комплексной безопасности
- при средне- и долгосрочном планировании;
- создание баз знаний;

опытная реализация функций автоматизированного сбора, учета и анализа информации, необходимой для аналитического прогнозирования рисков в рамках создаваемых и модернизируемых систем мониторинга национальной безопасности, ГИС ТЭК России, государственных и ведомственных информационных систем, систем мониторинга, управления и экстренного реагирования в чрезвычайных и кризисных ситуациях в интересах МЧС, в системах государственных и акционерных структур и хозяйствующих субъектов РФ;

по опыту оборонно-промышленного комплекса (ОПК) - использование аппарата Генеральных конструкторов для координации работ по согласованию ТЗ, технических проектов, программ по импортозамещению, проведению испытаний по требованиям комплексной безопасности;

разработка микроэлектронной базы и инфраструктуры для выпуска и применения отечественных криптографических средств защиты служебной информации;

разработка испытательных полигонов, формирование банков данных и баз знаний для КВОС;

разработка интегрированной системы контроля, эффективного управления рисками и обеспечения комплексной безопасности критически важных объектов России;

<u>по организационному направлению</u>

разработка типовых организационных структур систем дистанционного контроля, требований к инструментально-технической оснащенности и функциональных обязанностей должностных лиц КВОС;

разработка организационным мер взаимодействия, разделения полномочий и разграничения доступа к информации при создании, внедрении и эксплуатации систем дистанционного контроля для различных КВОС (в первую очередь для эффективной реализации мер контроля, мониторинга, прогнозирования рисков, обоснования допустимых рисков и оперативных мер в обеспечение комплексной безопасности, анализа и восстановления целостности реализуемых процессов в жизненном цикле отдельных системных элементов);

<u>по эксплуатационно-производственному направлению</u>

<u>(с использованием результатов по опытно-конструкторскому направлению)</u>

внедрение на критически важных объектах России систем дистанционного контроля комплексной безопасности (как информационно-аналитических систем КВОС), реализующих:

- раннее распознавание и оценку развития предаварийных ситуаций, обеспечение возможностей принятия в реальном времени мер по предотвращению аварий, прогнозирование временного ресурса, имеющегося для принятия упреждающих мер;
- внедрение на предприятиях риск-ориентированного подхода, позволяющего системное прогнозирование рисков,
- выявление узких мест, обоснование допустимых рисков и оперативных мер в обеспечение комплексной безопасности;
- обоснование сбалансированных мер обеспечения комплексной безопасности
- при средне- и долгосрочном планировании;
- создание баз знаний;

внедрение функций автоматизированного сбора, учета и анализа информации, необходимой для аналитического прогнозирования рисков в рамках создаваемых и модернизируемых систем мониторинга национальной безопасности, ГИС ТЭК России, государственных и ведомственных информационных систем, систем мониторинга, управления и экстренного реагирования в чрезвычайных и кризисных ситуациях в интересах МЧС, в системах государственных и акционерных структур и хозяйствующих субъектов РФ;

использование аппарата Генеральных конструкторов для координации работ по осуществлению государственного контроля и надзора в области комплексной безопасности эксплуатируемых КВОС и рационального применения интегрирующей базы знаний для научного обоснования допустимых рисков, повышения адекватности используемых методов и моделей и оптимизации применения систем дистанционного контроля в интересах обеспечения комплексной безопасности всего множества КВОС в России и за рубежом;

внедрение, адаптация и эксплуатация технологий эффективного управления рисками в КВОС России;

внедрение и эксплуатация в ГИС ТЭК России интегрированной системы дистанционного контроля, системы сбора, учета и обработки статистической информации о своей работе. Внедрение и эксплуатация в интегральном сегменте ГИС ТЭК России «Аналитической подсистемы поддержки принятия решений по управлению рисками» для прогнозирования рисков, обоснования допустимых рисков и выработки эффективных упреждающих воздействий в обеспечение комплексной безопасности ТЭК. Внедрение в ГИС ТЭК России базы знаний и ее эксплуатация для научного обоснования допустимых рисков, повышения адекватности используемых методов и моделей и оптимизации применения систем поддержки принятия решений в интересах обеспечения комплексной безопасности ТЭК;

внедрение, адаптация и эксплуатация интегрирующей системы дистанционного контроля в государственных и ведомственных информационных системах (в части качающейся) по заказам ФСБ России, МВД России, системах мониторинга, управления и экстренного реагирования в чрезвычайных и кризисных ситуациях в интересах МЧС России, важных государственных и акционерных структурах и хозяйствующих субъектах РФ, в других КВОС;

внедрение, адаптация и эксплуатация интегрирующей базы знаний в действующие КВОС для научного обоснования допустимых рисков, повышения адекватности используемых методов и моделей и оптимизации применения систем управления рисками в интересах обеспечения комплексной безопасности всего множества КВОС в России и за рубежом;

выпуск и широкое внедрение в важные объекты и системы отечественных криптографических средств защиты служебной информации, в т. ч. по проектам содружеств БРИКС, ШОС, ЕАЭС;

рациональное внедрение по критериям «безопасность-эффективность-стоимость» и эксплуатация на важных объектах и в системах коммерческих структур программного обеспечения, созданного по программе импортозамещения. Подключение к интегрирующей базе знаний информации, поступающей от важных объектов и систем коммерческих структур в части качества программного обеспечения, поставленного по программе импортозамещения;

внедрение и эксплуатация тренажеров в процесс обучения и повышения квалификации персонала по системам дистанционного контроля и управления рисками в интересах обеспечения комплексной безопасности КВОС;

внедрение, адаптация и эксплуатация дистанционного контроля, реализованных по проектам содружеств БРИКС, ШОС, ЕАЭС;

<u>по квалификационно-кадровому направлению</u>

разработка программ и внедрение системы обучения и повышения квалификации персонала КВОС с использованием тренажеров в России и за рубежом, в т.ч. по проектам стран содружеств БРИКС, ШОС, ЕАЭС;

разработка программ и внедрение системы обучения и повышения квалификации персонала по созданию и применению отечественных криптографических средств защиты служебной информации.

3. ОЖИДАЕМЫЕ ЭФФЕКТЫ

В результате решения обозначенных проблем ожидается инновационно-технологический прорыв. Создание и внедрение предлагаемых технологий будет сопровождаться прогнозами эффектов от их применения в условиях неопределенности и разнородных угроз – причем, не после создания, а, начиная с ранних этапов замысла и разработки технического задания и далее по жизненному циклу. Ожидаемые эффекты оцениваются десятками миллиардов рублей предотвращенного ущерба и/или дополнительного выигрыша, обусловленного научно обоснованным управлением при качественном и безопасном функционировании анализируемых объектов и систем. К примеру, применение на 200 объектах в Калужской и Курской областях и в Заполярье в период 2009-2014гг. специального отечественного комплекса обеспечения техногенной безопасности на объектах газораспределения нефтегазовой отрасли, созданного на принципах системной инженерии и удостоенного в 2014г. премии Правительства РФ в области науки и техники, обеспечило возможность экономии 8,5 млрд рублей, что достигнуто за счет эффективного внедрения в технологического процессы контроля и мониторинга газораспределения функций прогнозирования рисков и обеспечения техногенной безопасности [1].

По опыту развитых стран за счет эффективного управления различными процессами достижим прирост внутреннего валового продукта (ВВП) до 0.5%, аналогичный вклад в прирост ВВП дает только нефтедобыча. Именно такой прагматический эффект от системного широкомасштабного решения сформулированных проблем является ожидаемым и практически достижимым для России в ближайшие годы.

Список литературы

1. Акимов В.А.,…,Костогрызов А.И., Махутов Н.А., Фортов В.Е., Шойгу С.К. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015, - 936с.

References

1. Akimov V.,…,Kostogryzov A., Mahutov N. at al. Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of Mahutov N. – Moskva, “Znanie”, 2015. 936p.