МЕТОДОЛОГИЧЕСКИЙ ПОДХОД
к построению системы комплексной безопасности

Часть I

А.Пинчук, директор ООО "НТЦ ПРОТЕЙ",
В.Секереш, директор ООО "ПРОТЕЙ СпецТехника",
Н.Соколов, доктор технических наук, технический директор ООО "ПРОТЕЙ СпецТехника"

В статье обсуждается методологический подход к созданию системы комплексной безопасности (СКБ) для субъекта Федерации. Авторы постарались обобщить результаты исследований, проведенных ими в последние годы по различным аспектам безопасности. Эти результаты стимулировали разработку концепции СКБ.

Терминологические аспекты

Термины, используемые ниже, базируются в основном на трех определениях, которые приведены в стандарте [1]: безопасность – отсутствие недопустимого риска; риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба; ущерб – нанесение физического повреждения или другого вреда здоровью людей, или вреда имуществу, или окружающей среде.

Слово "комплекс" в современных толковых словарях трактуется как сложная система, охватывающая группу предметов, объектов, явлений, процессов и т.п. СКБ уместно связать с пирамидой потребности Абрахама Маслоу [3], которая отображает пять ключевых потребностей человека. На рис.1 пирамида Маслоу дополнена блоком СКБ, который иллюстрирует важность функций безопасности для поддержки безопасности всех аспектов жизни каждого человека и общества в целом.

Таким образом, СКБ предназначена для поддержки всех функций безопасности, определяемых перечнем потенциальных видов риска и градациями возможного ущерба. Классифицировать СКБ в ряде случаев удобнее не при помощи пирамиды Маслоу, а за счет выделения основных видов безопасности. Такой подход использован, например, в презентации "Применение ИКТ для обеспечения безопасности жизнедеятельности региона", которую разработали специалисты Республики Коми. Авторы презентации предлагают акцентировать внимание на восьми основных видах безопасности субъекта Федерации – экономической, экологической, технологической, энергетической, информационной, физической, социальной, продовольственной.

Можно выделить большее или меньшее количество видов безопасности, что не меняет сути понятия "система комплексной безопасности". Например, в [3] для гипотетической компании рассматриваются следующие виды безопасности: инвестиционная, кредитная, имущественная и ряд других. В любом случае каждый вид безопасности может быть ассоциирован с одноименной подсистемой, входящей в состав СКБ.

Модель системы комплексной безопасности

Предлагаемая модель СКБ приведена на рис.2. Она состоит из набора автоматических и автоматизированных систем, представляющих

Рис.1. Пирамида потребностей и система комплексной безопасности

собой совокупность источников информации о состоянии контролируемых объектов и/или процессов, средств обмена информацией, ситуационных центров и экспертных групп.

Предлагаемую модель можно считать идеализированной в том смысле, что она включает в свой состав набор элементов, которые – теоретически – позволяют достичь максимально возможного уровня безопасности. Очевидно, что эта модель не будет реализована в полном объеме в силу объективных и субъективных факторов. Тем не менее ее анализ интересен с практической точки зрения. По этой причине ниже кратко рассматриваются характеристики основных элементов модели и их эволюция с учетом ожидаемых технологических изменений.

Автоматические системы представлены пятью примерами. Каждый из этих примеров имеет специфические особенности.

Первый пример касается сенсорных датчиков, объединяемых при помощи алгоритмов, которые приняты для самоорганизующихся сетей [4]. Чаще всего такие датчики ассоциируются с концепцией "интеллектуальное жилище" [5]. Функции, выполняемые датчиками, можно разделить на несколько классов. Один из классов – функции безопасности. В частности, к ним относятся операции, выполняемые счетчиками электроэнергии (резкое повышение расхода тока свидетельствует о вероятности возникновении пожара), устройствами контроля доступа (частое применение неверного пароля может быть связано с попыткой взлома), дымоуловителями (их назначение практически полностью определяется требованиями безопасности) и другими приборами.

Второй пример связан с решением Европейского Союза (ЕС) по созданию системы eCall [6] для организации оперативной помощи автомобилистам при аварии в любой точке континента. Ожидается, что система eCall будет введена на всей территории ЕС к 2015 году. На территории Российской Федерации создается система "ЭРА ГЛОНАСС", которая основана на принципах, схожих с концепцией eCall. При оценке ее эффективности была получена "стоимость жизни" россиянина в 4 млн. руб. в ценах 2018 года на основе расходов страховых компаний.

Третий пример представляет собой один из вариантов мониторинга транспортных средств. Простейший случай – выбор разумного режима работы светофора с учетом интенсивности движения автомобилей. Такие светофоры обычно называют интеллектуальными. Они регулируют транспортные потоки с учетом сложившейся ситуации на дорогах.

Четвертый пример – мониторинг промышленных объектов. В первую очередь, актуальны

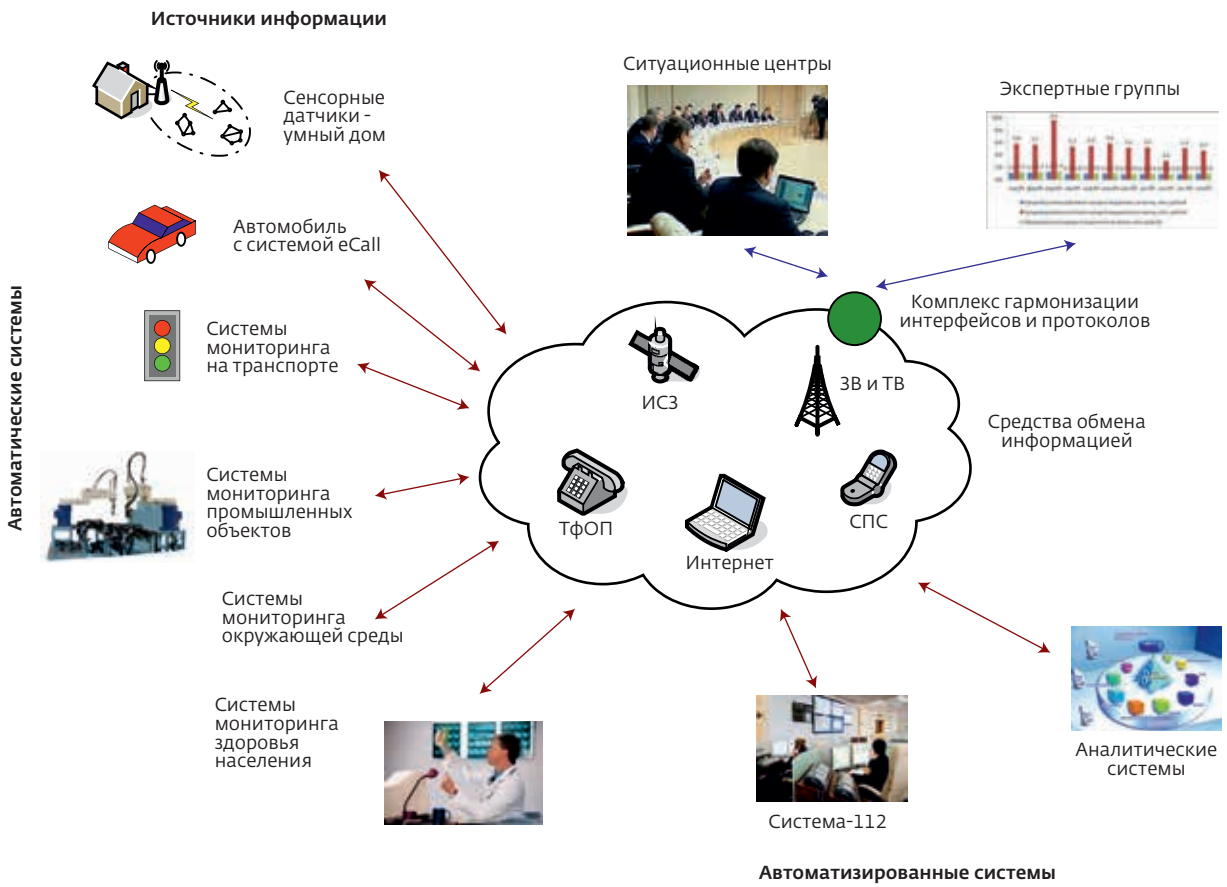

Рис.2. Модель системы комплексной безопасности

задачи мониторинга тех промышленных предприятий, которые могут стать источником повышенной опасности. Из всех примеров, рассмотренных выше, координация развития соответствующих систем безопасности для промышленных объектов представляется наиболее сложной. Это утверждение объясняется наличием специфических ведомственных требований, заметных различий в технологических процессах, а также исторически сложившейся практикой разработки систем мониторинга. Тем не менее для СКБ источники угроз, которые свойственны промышленным объектам, могут стать самыми существенными. Данное положение стимулирует разработку своего рода медиаторов, позволяющих представить информацию от самых разных систем мониторинга промышленных объектов в единой форме для последующей обработки в СКБ.

Пятый пример относится к системам мониторинга окружающей среды. Это понятие связано, в первую очередь, с предупреждением природных катастроф и мониторингом экологических параметров. Данные аспекты безопасности тщательно изучаются рядом международных организаций. Причем каждая международная организация рассматривает задачи мониторинга и сохранения окружающей среды с двух точек зрения. Во-первых, в каждом виде деятельности человека необходимо минимизировать выбросы вредных веществ и расходы ресурсов (электроэнергии, топлива, воды и др.). Во-вторых, в процессе мониторинга окружающей среды следует стремиться не только к раннему предупреждению чрезвычайных ситуаций и оперативной передаче необходимой информации, но и к прогнозу ситуации на основе обработки поступающих данных и имеющегося опыта.

Пять приведенных выше примеров относятся к автоматическим системам, которые функционируют без участия человека.

Автоматизированные системы предусматривают участие в процессе получения и обработки информации человека – оператора. Их относят к классу эргатических систем управления [7], в которых одним из важных элементов становится оператор. Автоматизированные системы представлены в предложенной модели тремя примерами.

Первый пример – системы мониторинга здоровья человека. Существующие и вновь создаваемые системы такого рода существенно различаются по своему назначению и функциональным возможностям. По всей видимости, важнейшим направлением эволюции для систем мониторинга здоровья человека станет когнитивная медицина [8]. Она, основанная на знаниях, накопленном опыте и учете индивидуальных особенностей каждого человека, способна предложить оптимальное решение возникшей проблемы и прогноз тех ситуаций, которые ожидаются в перспективе.

Второй пример связан с Системой-112 [9]. В подобных системах решающая роль в принятии решений отводится оператору. Тем не менее, эффективность принимаемых решений в значительной мере зависит от интеллектуальных возможностей используемых аппаратно-программных средств.

Третий пример относится к работе аналитических систем различного назначения. Понятие "аналитическая система" с точки зрения рассматриваемых вопросов следует уточнить. В последнее время под аналитической системой чаще всего понимается комплекс средств, предназначенных для сбора и анализа информации, а также представления ее в удобном для пользователей виде. Формально такое определение можно считать приемлемым, но не исчерпывающим. В состав определения аналитической системы целесообразно включить группу специалистов из государственных структур, занимающихся проблемами безопасности.

Средства обмена информацией выполняют функции по надежной доставке сообщений в соответствии с заданными качественными показателями и установленными регламентами. В качестве этих средств используются ресурсы существующих или вновь создаваемых телекоммуникационных сетей. На рис.2 приведены следующие примеры телекоммуникационных сетей, задействованных в облаке "Средства обмена информацией": телефонная сеть общего пользования (ТфОП); интернет; сети подвижной связи (СПС) любых принятых стандартов; сети звукового (ЗВ) и телевизионного (ТВ) вещания; системы связи через искусственные спутники Земли (ИСЗ).

Совокупность качественных показателей включает характеристики и атрибуты, позволяющие нормировать ключевые показатели функционирования средств обмена информацией [10]: время доставки информации (среднее значение, допустимая величина с заранее заданной вероятностью и им подобные параметры); искажение передаваемых сообщений (доля ошибочно принятых и/или потерянных сообщений, количество автоматически исправляемых ошибок и другие параметры); дополнительные характеристики, существенные для эффективной работы СКБ.

Надежность доставки сообщений определяется, в основном, двумя параметрами – коэффициентом готовности и средним временем устранения неисправностей. При необходимости могут вводиться и другие показатели, известные из теории надежности [11].

В верхней части облака "Средства обмена информацией" выделен модуль, названный комплексом гармонизации интерфейсов и протоколов. Задачи, возложенные на этот комплекс, требуют детальной проработки и принятия согласованных организационно-технических решений. В данном разделе статьи достаточно сформулировать решаемые задачи в самом общем виде. Они заключаются в следующем: два важнейших элемента рассматриваемой модели – "Ситуационные центры" и "Экспертные группы" – должны получать в удобном виде точную информацию от автоматических и автоматизированных систем; инструкции, направляемые из "Ситуационных центров" и "Экспертных групп" должны адекватно восприниматься автоматическими и автоматизированными системами при помощи используемых ими интерфейсов и протоколов.

Ключевая роль в успешной работе СКБ отводится ситуационным центрам (СЦ). Количество СЦ, их полномочия и принципы взаимодействия – предмет самостоятельного исследования. Для предложенной модели достаточно рассматривать один СЦ, задачи которого заключаются в анализе всей необходимой информации и разработке решений по ликвидации возникших или ожидаемых последствий.

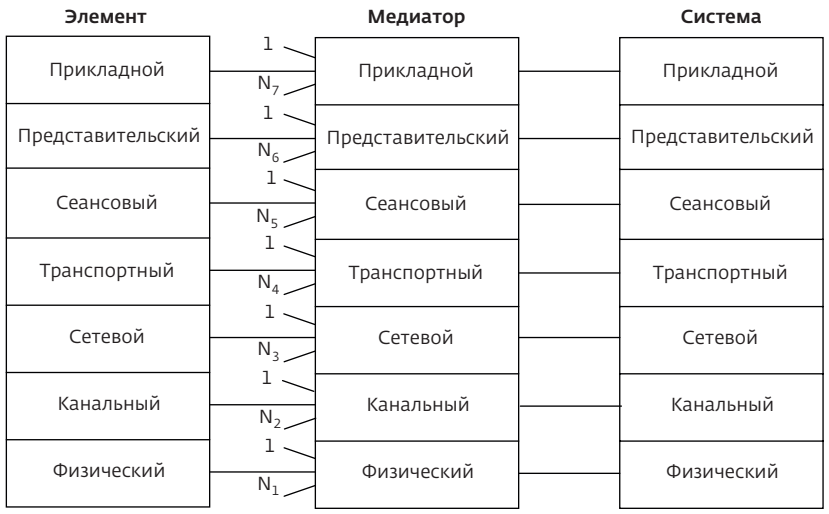

Рис.3. Фрагмент семиуровневой модели

При необходимости специалисты СЦ могут создавать (оперативно или на основании заранее составленных планов) экспертные группы. Задача этих групп состоит в проведении коллективной экспертизы по тем проблемам, которые определяются специалистами СЦ. Для ускорения работы экспертных групп со специалистами СЦ задействуются ресурсы средств обмена информацией.

Модель, предлагаемая для разработки СКБ, позволяет учесть основные функции, выполняемые различными группами людей при возникновении каких-либо угроз. При необходимости модель может быть дополнена новыми элементами. Ряд элементов может быть представлен в виде нескольких компонентов, взаимодействующих между собой. Такой подход, как было отмечено выше, будет весьма полезен для анализа модуля "комплекс гармонизации интерфейсов и протоколов". Именно этот модуль позволит реализовать процессы конвергенции, интеграции и консолидации [12], позволяющие достичь синергетического эффекта при построении и долгосрочной эволюции СКБ.

Совместная работа отдельных подсистем безопасности

Полноценное функционирование СКБ подразумевает совместную работу всех ее подсистем. Задачи совместной работы существующих подсистем безопасности можно разделить на технические и организационные. В этом разделе рассматриваются технические аспекты. По отношению к СКБ все существующие средства обеспечения безопасности (от самых простых устройств мониторинга до сложных аппаратно-программных комплексов) следует рассматривать как самостоятельно функционирующие элементы [13]. Основными задачами технических средств, названных на рис.2 "комплексом гармонизации интерфейсов и протоколов", становятся: обеспечение взаимодействия между элементами в тех случаях, когда это необходимо; поддержка функций по обмену информацией между каждым элементом и теми техническими средствами, которые используются в ситуационных центрах и в экспертных группах. Обе задачи – теоретически – могут быть решены на разных уровнях модели взаимодействия открытых систем [14]. С практической точки зрения изменения на нижних уровнях модели не представляются реальными.

Существующие средства мониторинга следует рассматривать как элементы, построенные по принципу As Is – как есть. При создании перспективной СКБ следует руководствоваться принципом As Should Be – как должно быть. Комплекс гармонизации интерфейсов и протоколов должен выполнять все функции, свойственные своего рода медиатору (посреднику) между двумя разными состояниями СКБ: As Is и As Should Be.

Результаты перехода к принципу As Should Be стимулируют появление в СКБ так называемых “эмерджентных свойств” [15]. Этот термин представляет собой “кальку” словосочетания emergent properties в английском языке. Под эмерджентными понимаются такие свойства целостной системы, которых нет в ее элементах (пока они функционируют раздельно). Обычно свойства такого рода и порождают синергетический эффект.

Для достижения такого эффекта следует использовать концепцию G3 [16] – Giant Global Graph. Она основана на том, что информация снабжена точно определенным смыслом, что позволяет организовать эффективную работу ситуационных центров и экспертных групп.

На рис.3 приведена семиуровневая модель [14], которая отражает суть операций, выполняемых комплексом гармонизации интерфейсов и протоколов. Предполагается, что изменения могут потребоваться на всех уровнях модели. Если же никакие изменения не нужны, то соответствующие функции рассматриваются как нулевые.

На входе медиатора – с точки зрения каждого уровня – может использоваться $N_i=(i=1,7)$ различных интерфейсов и протоколов. Причем, рассматривая процесс развития СКБ во времени, можно ввести набор из семи функций вида $N_i=(t)$. В момент времени $t_2 > t_1$ могут наблюдаться соотношения такого рода: $N_i=(t_2) \le N_i=(t_1)$ и $N_i=(t_2) \ge N_i=(t_1)$. Это означает, что "со стороны" элементов медиатор должен обеспечивать наращивание и количества интерфейсов, и набора используемых протоколов.

С системой медиатор обменивается посредством одного протокола на каждом функциональном уровне рассматриваемой модели. Аналогично, для каждого уровня применяется только один интерфейс, стандартизуемый для СКБ. Конечно, такой подход представляется некоторой идеализацией. Не исключено, что потребуется введение дополнительных протоколов и интерфейсов (например, для повышения живучести СКБ), но их количество должно быть ограничено.

В большинстве эксплуатируемых систем мониторинга используются средства вычислительной техники, в которых собирается и обрабатывается текущая информация. Это означает, что разработка медиатора сводится к созданию аппаратно-программного комплекса, в котором основные задачи решаются на трех верхних уровнях рассматриваемой модели: сеансовом, представительском и прикладном.

Для разработки медиатора необходимо тщательно проанализировать характеристики используемых устройств мониторинга, выбрать оптимальные решения по интерфейсам и протоколам в системе (в ситуационных центрах и в экспертных группах). Полученные сведения позволят сформулировать техническое задание на разработку медиатора. После установки медиатора отдельные подсистемы безопасности смогут работать совместно для достижения максимальной эффективности СКБ.

ЛИТЕРАТУРА

1. ГОСТ Р 51898 – 2002 "Аспекты безопасности. Правила включение в стандарты". – Введен 01 января 2003 года.
2. **Маслоу А.Г.** Мотивация и личность. – СПб.: Евразия, 2001.
3. **Тихоненко В.В.** Основные стандарты безопасности. Информационный ресурс: http://www.cfin.ru/management/manufact/safety_aspects.shtml.
4. **Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А.** Саморганизующиеся сети. – СПб.: Любавич, 2011.
5. **Богданов С.В.** Умный дом. – СПб.: Наука и техника, 2003.
6. **Скворцова С.А.** У M2M драйверы глобальные // ИКС. 2011. № 10.
7. **Климов Е.А.** Введение в психологию труда // Учебное пособие для студентов и аспирантов психологических факультетов. – М.: МГУ, 1998.
8. **Комашинский В.И., Соколов Н.А.** Когнитивные системы и телекоммуникационные сети // Вестник связи. 2011. № 10.
9. **Гольдштейн Б.С., Леваков А.К., Соколов Н.А.** Доступ к центру обработки вызовов номера "112" // Вестник связи. 2012. № 1.
10. **Битнер В.И., Попов Г.Н.** Нормирование качества телекоммуникационных услуг. – М.: Горячая линия – Телеком, 2004.
11. **Острейковский В.А.** Теория надежности. – М.: Высшая школа, 2003.
12. **Соколов Н.А.** Процессы конвергенции, интеграции и консолидации в современной телекоммуникационной системе // Connect! Мир связи. 2007. № 10.
13. **Тарасенко Ф.П.** Прикладной системный анализ. – М.: КноРус, 2010.
14. МСЭ-Т. Эталонная модель взаимосвязи открытых систем. – Рекомендация X.200. – Женева, 1994.
15. **Луценко Е.В.** Количественные меры возрастания эмерджентности в процессе эволюции систем (в рамках системной теории информации) // Научный журнал КубГАУ. 2006. № 5 (21).
16. **Бородакий Ю.В., Лободинский Ю.Г.** Эволюция информационных систем (современное состояние и перспектива). – М.: Горячая линия – Телеком, 2011.

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД
к построению системы комплексной безопасности

Часть 2

А.Пинчук, директор ООО "НТЦ ПРОТЕЙ",
В.Секереш, директор ООО "ПРОТЕЙ СпецТехника",
Н.Соколов, доктор технических наук, технический директор ООО "ПРОТЕЙ СпецТехника"

Для повышения безопасности работы систем электросвязи необходимо предварительно тщательно продумать основные сценарии реагирования на нештатные ситуации.

Модель угроз для населения субъекта Российской Федерации

Разработку модели угроз, существенных для населения субъекта федерации, следует начать с классификации, которая учитывает источники опасности, возникающие риски и возможные последствия. Предлагаемая классификация, показанная на рис.1, не претендует на универсальность, но позволяет изложить основные решения по реализации системы комплексной безопасности (СКБ).

Все источники опасности можно разделить на две большие группы: стихийные бедствия, обусловленные природными явлениями, и угрозы со стороны человека. Кроме того, следует учесть возможность совместного влияния природных и человеческих факторов, что иллюстрируется в рассматриваемой модели пунктирной линией. В левой нижней части графа приведены четыре типичных примера проявления природных факторов. Ориентированные ребра указывают на возможные причинно-следственные связи между этими факторами. В частности, землетрясение может вызвать пожары, а ураган – привести к наводнению. Штрихпунктирной линией отмечена ситуация, когда из-за ошибок человека возникает наводнение. Каждый из четырех факторов при необходимости может быть детализирован с использованием различных классификационных признаков – таксонов.

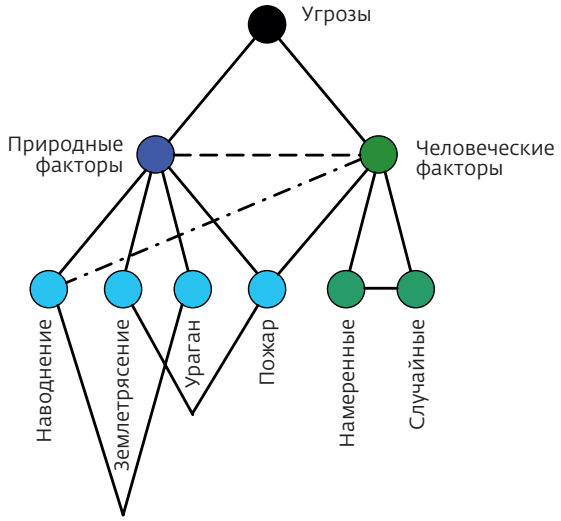

Рис.1. Классификация угроз для населения субъекта федерации

В качестве таксонов используются такие атрибуты, как количество пострадавших, размер материального ущерба и др.

Классификация человеческих факторов ограничена двумя ключевыми группами – намеренные и случайные. К намеренным относятся угрозы, которые, безусловно, следует отнести к противоправным действиям. Они охватывают широкий диапазон явлений, от военных действий до хакерских атак. Характерным примером случайных угроз можно считать неточное выполнение должностных инструкций на особо опасных объектах.

На основании таксонов, рассматриваемых в [1], можно предложить модель, характеризующую угрозы по трем важным характеристикам. Эта модель показана на рис.2 в виде куба. Каждая грань содержит два основных признака для каждого таксона. В принципе, на каждой грани можно указать большее количество видов угроз, если такой подход будет признан целесообразным. При необходимости, куб можно заменить многогранником, что позволит ввести требуемое количество характеристик угроз.

Предположим, что количество граней, позволяющее описать все возможные характеристики угроз, равно D. Допустим, что для каждой i-й характеристики угроз ($i = \overline{1,D}$) количество необходимых признаков составляет k_i. Таким образом, общая численность угроз может быть оценена некой конечной величиной L. Значение величины L будет измеряться сотнями или даже тысячами. По этой причине разработка модели для всех возможных угроз не представляется возможной, но уместно ввести универсальную модель для каждой j-ой угрозы ($j = \overline{1,L}$) в виде m-мерного вектора $\vec{U}_m(j)$. Такую модель следует рассматривать как статическую. Ее целесообразно дополнить динамической моделью, которая описывает каждую j-ою угрозу с учетом времени $W_j(t)$. Вектор $\vec{U}_m(j)$ и функция $W_j(t)$ позволяют с максимальной полнотой охарактеризовать j-ю угрозу. Пара $\vec{U}_m(j)$ и $W_j(t)$ представляет собой формализованную модель j-й угрозы.

Выбор векторов $\vec{U}_m(j)$ и функций $W_j(t)$ – самостоятельная задача, требующая проведения трудоемкой работы. Эту задачу можно решать на основе принципа "от простого к сложному". Иными словами, на первом этапе можно ввести упрощенные метрики для определения векторов $\vec{U}_m(j)$ и функций $W_j(t)$. По мере накопления опыта метрики будут уточняться и дополняться.

В качестве примера рассмотрим определение вектора $\vec{U}_7(1)$ и функции $W_1(t)$, которые соответствуют пожару (угроза №1). Предполагается, что для описания пожара достаточно семь признаков, то есть m=7:

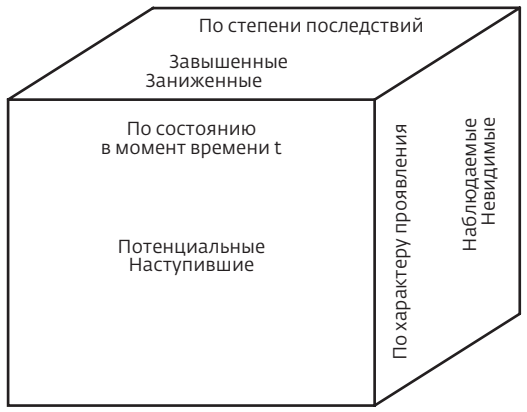

Рис. 2. Классификация угроз по трем классам

- 501 – номер объекта в субъекте федерации, на котором (предположительно!) произошло возгорание;
- 2 – категория пожара, присвоенная на основании имеющейся информации;
- 13/48/35 – местное время (часы, минуты и секунды) при фиксации пожара;
- 1 – способ получения информации о возгорании (сигнал из системы мониторинга, звонок по номеру "112", SMS и т.п.);
- 479/598/062 – перечень объектов, расположенных поблизости от предполагаемого очага возгорания;
- 07/76/E02 – температура, влажность, направление и скорость ветра;
- 4 – дополнительная информация об объекте 501, существенная для тушения пожара.

Тогда вектор $\vec{U}_7(1)$ представляет собой однозначно заданный кортеж следующего вида:

<501; 2; 13/48/35; 1; 479/598/062; 07/76/E02; 4>.

Этот кортеж используется аппаратно-программными средствами Системы-112 и другими средствами безопасности для получения из соответствующих баз данных всей необходимой информации для оптимального тушения пожара и эффективной ликвидации возможных последствий. Эта же информация позволяет определить вид и параметры функции $W_1(t)$. Форма и параметры векторов $\vec{U}_m(j)$ и функций $W_j(t)$ должны уточняться по мере накопления опыта работы всех компонентов в составе СКБ. Такая процедура может быть реализована, например, как процесс обучения нейронной сети [2].

Оценки уровня опасности

Для интегральной оценки уровня опасности чаще всего используется цветовая гамма. Предположим, что установлено пять уровней опасности:

- отсутствие причин для тревоги – зеленый цвет;
- очень низкая вероятность опасности – синий цвет;
- возрастание вероятности опасности – желтый цвет;
- возникновение существенной опасности – оранжевый цвет;
- высокая степень опасности – красный цвет.

Для каждой угрозы могут использоваться от двух до пяти цветов. Два цвета используется для указания на двоичное состояние объекта. Например, для подледного лова выход на лед разрешен (зеленый цвет) или запрещен (красный цвет). Большее количество цветов применяется для сложных объектов или ситуаций. Например, для движения автомобилей по магистрали может использоваться зеленый цвет (отсутствие ограничений), желтый цвет (ограничение скорости из-за погодных условий), красный цвет (проезд закрыт для проведения ремонтных работ).

Для дифференциальной оценки уровня опасности, задаваемой для каждого самостоятельно функционирующего объекта, вводится несколько параметров. Их количество и смысл определяются спецификой объекта. Можно назвать, по крайней мере, один параметр, который важен для всех объектов – вероятность отказа [3]. Часто вероятность отказа рассматривается как мера риска [4]. Величина риска для функционирования объекта, который не представляет опасности для жизни людей и окружающей среды, на уровне 10^{-4}(вероятность отказа) представляется, в среднем, допустимой. Для объектов, напрямую определяющих жизнь и здоровье граждан, а также экологическую безопасность, вероятность отказа на уровне 10^{-8} не всегда рассматривается как приемлемый риск.

Следует подчеркнуть, что мера риска может резко меняться со временем. Типичным примером служит информационная безопасность. Средства нарушения информационной безопасности постоянно совершенствуются. Это стимулирует ужесточение требований к системам защиты. Следовательно, оценки уровня опасности постоянно меняются. Данный вывод справедлив и для большинства других видов безопасности.

Связь между разными видами безопасности

Модель, предназначенная для описания взаимных связей между разными видами безопасности, показана на рис.3. Она основана на введенном выше представлении отдельных свойств безопасности в виде куба. Масштаб чрезвычайной ситуации (ЧС) определяется нормативными документами, принятыми в Российской Федерации [5–7].

В качестве примера ниже рассматривается цепочка, порождаемая повышением уровня энергетической безопасности до "желтого". В этом случае – автоматически или при помощи экспертной группы – прогнозируются потенциальные риски для возможных ЧС четырех масштабов. Эти риски выражаются вероятностями наступления угрозы π_i ($i = \overline{1,4}$). Обычно соблюдается такое неравенство:

$$\pi_1 > \pi_2 > \pi_3 > \pi_4.$$

Далее для ЧС i-го масштаба определяются те аспекты безопасности, для которых могут возникнуть угрозы. Предполагается (в качестве примера), что возникают реальные угрозы следующим аспектам безопасности:

- информационному – вследствие длительного нарушения системы электропитания телекоммуникационного и информационного оборудования, приводящего к их переходу в состояние "отказ";
- технологическому – из-за прекращения энергоснабжения жизненно-важных мониторингов систем на время, превышающее запас работы аккумуляторных батарей;

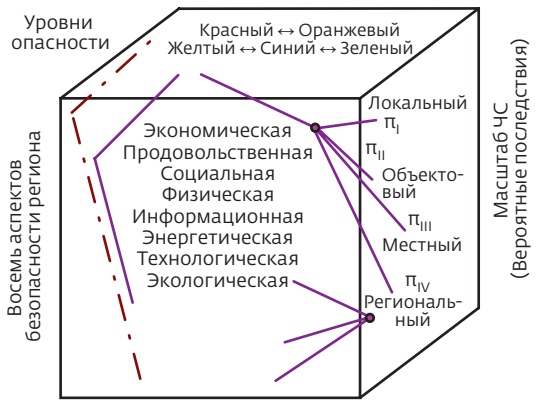

Рис.3. Модель взаимосвязи различных видов безопасности

- экологическому – по причине отказа очистных сооружений из-за отсутствия гарантированного энергоснабжения.

Если, в частности, последствия для экологии расцениваются как критические, то уровень опасности может перейти к порогу "красный". Такая возможность показана на рис.3 штрихпунктирной линией. Этот пример иллюстрирует сложность задач, которые возложены на СКБ. С другой стороны, он свидетельствует о возможности упреждать возникновение масштабных ЧС за счет оперативной обработки всей поступающей информации.

Следует отметить, что превентивные меры для повышения безопасности позволяют получить ощутимый эффект. В частности, в [8] показана возможность улучшения работы системы электросвязи в ЧС при условии, что предварительно тщательно продуманы основные сценарии реагирования на нештатные ситуации.

Практическая реализация модели для взаимосвязи различных видов безопасности потребует разработки большого объема программного обеспечения. Оно может наращиваться модульно, чтобы уже на первом этапе построения СКБ можно было минимизировать возникающие риски, характерные для всех аспектов безопасности. Еще одна важная задача реализации рассматриваемой модели – постоянное обучение персонала, занимающегося вопросами безопасности.

Объекты и субъекты защиты в системе безопасности

В нормативной и научно-технической литературе используются различные подходы к классификации объектов и субъектов защиты. Новая версия закона "О промышленной безопасности опасных производственных объектов" [9] предусматривает четыре класса опасности, что

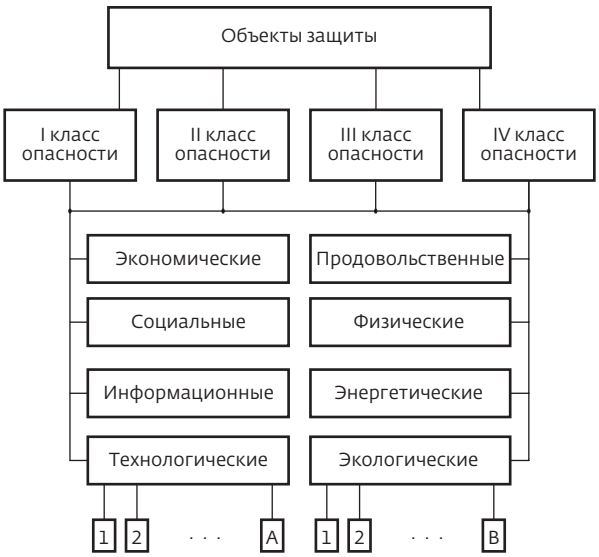

Рис.4. Иерархические уровни объектов защиты

представляется авторам статьи наиболее удачным методологическим подходом:

I класс – объекты чрезвычайно высокой опасности;
II класс – объекты высокой опасности;
III класс – объекты средней опасности;
IV класс – объекты низкой опасности.

Такой способ классификации представляется очень полезным для распределения всех объектов защиты по уровням иерархии. Этот подход иллюстрируется рис.4. Он не позволяет выделить все объекты защиты, но отражает предлагаемый подход к их ранжированию.

На первом уровне иерархии выполнено деление по четырем классам опасности. На втором уровне представлены восемь аспектов безопасности.

Рис.5. Классификация субъектов защиты

Для каждого из них предусмотрена возможность соотнесения объекта с любым из четырех классов опасности. На третьем уровне для технологического и экологического аспектов изображены два множества из A и B объектов. Они соответствуют тем реальным объектам, которые должны быть защищены.

Ряд объектов может быть отнесен более чем к одному аспекту безопасности. Если в качестве классификационного признака выбрать наиболее важный таксон, то любой объект можно отобразить при помощи кортежа <X, Y, Z>. Параметр "X" принимает значения I, II, III или IV. Величина "Y" меняется от единицы до восьми. Число "Z" определяет номер объекта. В частности, для технологического аспекта Z=A, а для экологического – Z=B. Следует подчеркнуть, что к объектам защиты относятся также и люди.

К субъектам защиты относятся структуры государственной власти и, в некоторых случаях, добровольные формирования граждан – волонтеров. Предлагаемая классификация показана на рис.5. Она учитывает сложившуюся практику функционирования органов исполнительной власти и ряда ведомств. Координация работы органов исполнительной власти и ведомственных структур с технической точки зрения осуществляется посредством ситуационного центра. Для реализации такой возможности должен быть разработан (а при его наличии – уточнен) соответствующий регламент.

Вероятные направления дальнейших работ

Дальнейшие работы по реализации СКБ уместно разделить на два направления. Первое подразумевает решение задач, которые были сформулированы в обеих частях данной статьи. Исследование проблем, которые напрямую не рассматривались ни в первой, ни во второй частях статьи, образуют второе направление дальнейших работ.

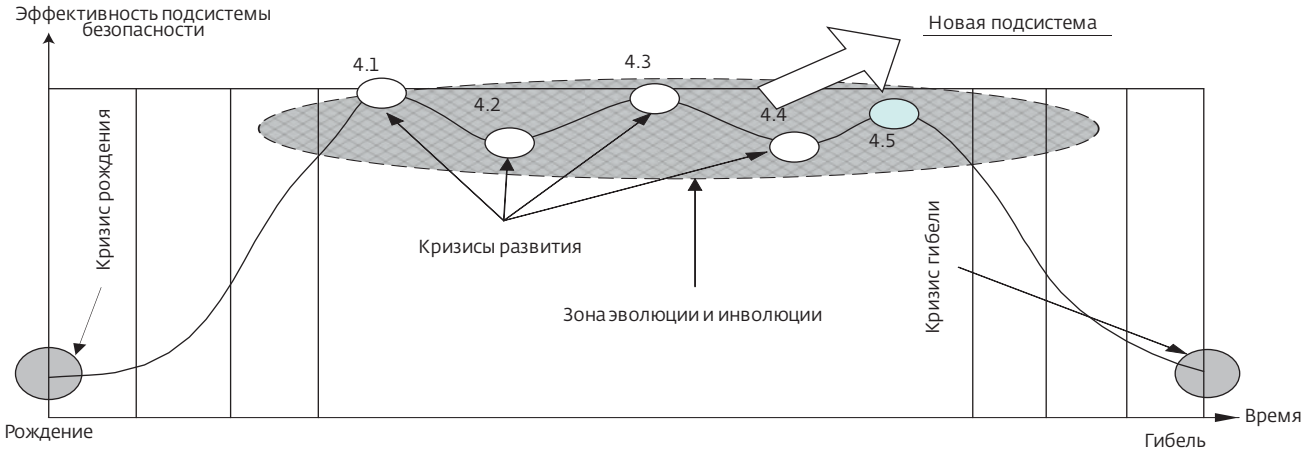

Рис.6. Типичный жизненный цикл подсистемы безопасности

Перечень новых исследований, которые должны быть проведены, в настоящее время можно составить только в самом общем виде. В качестве одной из первоочередных крупных тем для дальнейшей работы следует выделить изучение жизненного цикла СКБ и входящих в ее состав подсистем безопасности.

Типичный жизненный цикл подсистемы безопасности показан на рис.6, который составлен на основе моделей, рассмотренных в [10]. На оси "Время" выделено семь основных стадий в жизненном цикле подсистемы безопасности: зарождение (1), становление (2), развитие (3), расцвет (4), регресс (5), упадок (6) и гибель (7). Стадии 1, 2 и 3 соответствуют периоду эволюции. На фазах 5, 6 и 7 наблюдается период инволюции. Для области 4 на рисунке выделено пять этапов. В пределах этой области происходит смена периодов эволюции и инволюции.

Начало практической реализации подсистемы безопасности относится к этапу 4.1. Изменение требований пользователей к подсистеме безопасности и иные факторы определяют характер рассматриваемой функции кривой до этапа 4.5. Он отражает важное административно-техническое решение – создание новой подсистемы. Подсистема безопасности, существовавшая к началу этапа 4.5, постепенно движется к фазе гибели.

С точки зрения преемственности актуальным вопросом становится возможность использования ряда компонентов (в основном, дорогостоящих) в составе конкретной подсистемы безопасности, а также в СКБ в целом на этапах 4.1 и 4.5. В качестве численной оценки преемственности к моменту времени t можно использовать функцию $f_i(t)$, которая определяет долю стоимости компонентов подсистемы безопасности, которые сохранились на i-ом этапе модернизации СКБ.

Сложность изучения жизненного цикла самой СКБ заключается в том, что ее компоненты (отдельные подсистемы безопасности) имеют различные значения длительности этапов 1–7. Это значит, что жизненный цикл СКБ будет иметь более сложный характер, чем кривая на рис.6. Более того, длительность i-го этапа модернизации СКБ по своей сути становится случайной величиной, закон распределения которой установить очень сложно. Не исключено, что для эффективной работы СКБ придется управлять (в широком смысле этого слова) длительностью этапов 1–7 для отдельных подсистем безопасности.

ЛИТЕРАТУРА

1. **Прохожев А.А.** Общая теория национальной безопасности. – М.: РАГС, 2005.
2. **Рутковская Д., Пилиньский М., Рутковский Л.** Нейронные сети, генетические алгоритмы и нечеткие системы. – М.: Горячая линия – Телеком, 2008.
3. **Острейковский В.А.** Теория надежности. – М.: Высшая школа, 2003.
4. **Королев В.Ю., Бенинг В.Е., Шоргин С.Я.** Математические основы теории риска. – М.: Физматлит, 2011.
5. О классификации чрезвычайных ситуаций природного и техногенного характера. – Постановление Правительства Российской Федерации №304 от 21 мая 2007 года.
6. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера. – Федеральный закон №68-ФЗ от 21 декабря 1994 года.
7. О внесении изменений в Федеральный закон "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера". – Федеральный закон №23-ФЗ от 1 апреля 2012 года.
8. **Леваков А.К.** Особенности функционирования сети следующего поколения в чрезвычайных ситуациях. – М.: ИРИАС, 2012.
9. Федеральный закон от 21 июля 1997 года № 116-ФЗ "О промышленной безопасности опасных производственных объектов" (с изменениями и дополнениями).
10. **Новосельцев В.И., Тарасов Б.В.** Теоретические основы системного анализа. – М.: Майор, 2013.