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.

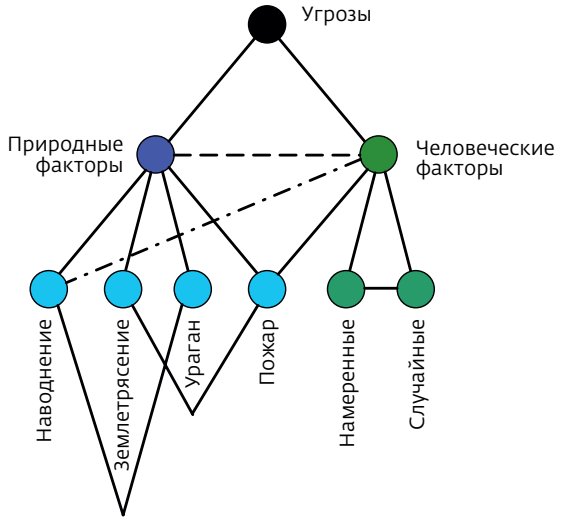

Рис.1. Классификация угроз для населения субъекта федерации

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:

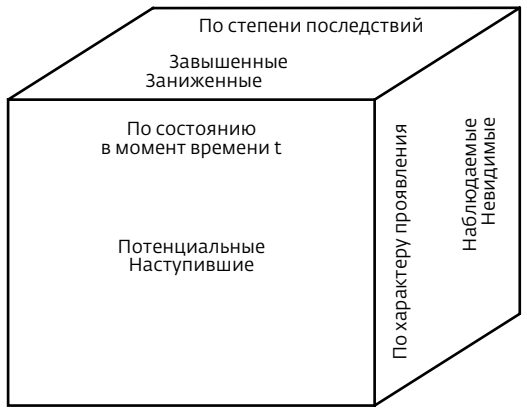

Рис. 2. Классификация угроз по трем классам

- 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;

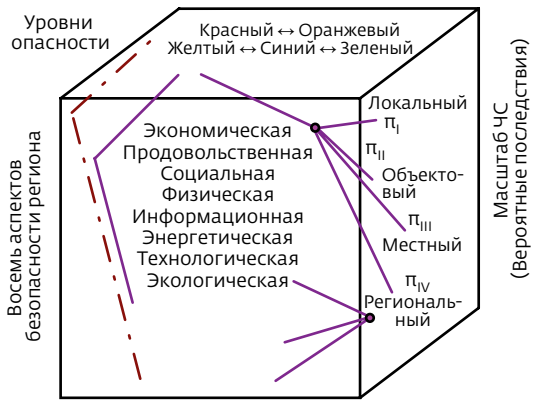

Рис.3. Модель взаимосвязи различных видов безопасности

- 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

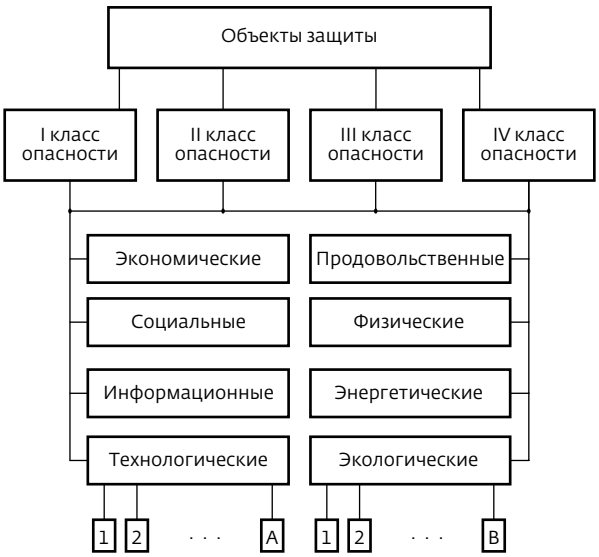

Рис.4. Иерархические уровни объектов защиты

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.

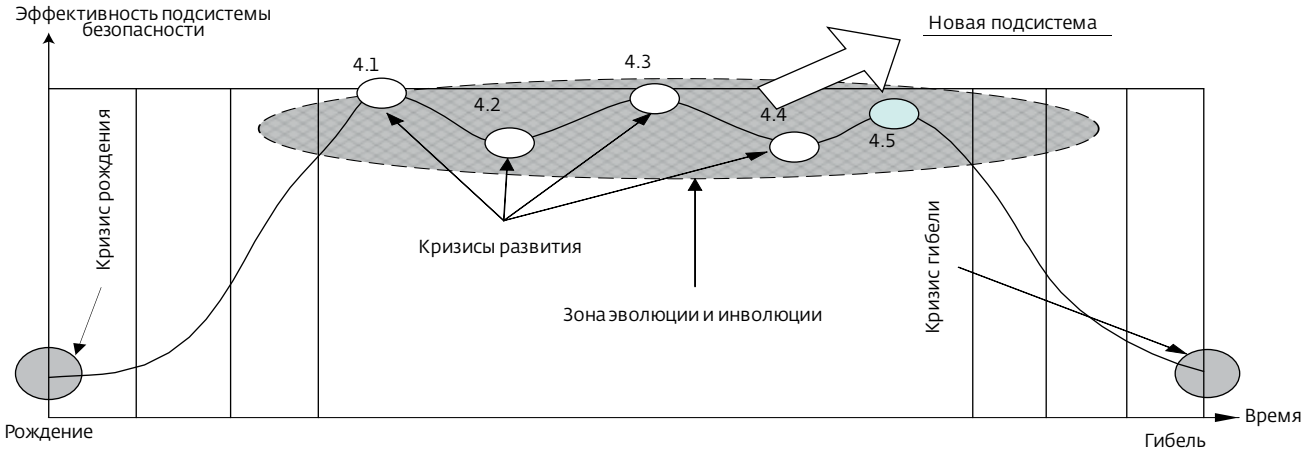

Рис.6. Типичный жизненный цикл подсистемы безопасности

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.

NEC впервые внедрила технологию CPRI в России

Компания **"NEC Нева Коммуникационные Системы"** (NEC Нева), дочернее предприятие корпорации NEC, поставила Сибирскому филиалу оператора "МегаФон" новую модель радиорелейных станций iPASOLINK EX с общим открытым интерфейсом (Common Public Radio Interface, CPRI), что стало первым коммерческим развертыванием NEC технологии CPRI в России. Системы iPASOLINK EX работают в нелицензируемом диапазоне частот 71–86 ГГц и способны обеспечить скорость передачи данных до 3 Гбит/с.

iPASOLINK EX – компактная радиорелейная система, работающая в E-диапазоне спектра миллиметровых волн, которая обеспечивает высокие емкости сети и низкие затраты на лицензирование станций по сравнению с другими радиорешениями. Благодаря внедрению интерфейса CPRI система может быть также использована для передачи беспроводного трафика в облачной сети радиодоступа (Cloud Radio Access Network, C-RAN).

По информации компании "NEC Нева"