

УДК 504.06

В.Н. Федирко

Управление комплексной безопасностью социо-эколого-экономического развития региона

В статье исследована сущность безопасности; обоснована необходимость количественного измерения уровня комплексной безопасности как основы эффективного управления; предложены этапы и модель анализа и управления комплексной безопасностью.

Ключевые слова: комплексная безопасность, социо-эколого-экономическое развитие, когнитивная модель.

Введение

В современном понятийно-категориальном аппарате под безопасностью понимаются состояние и тенденции развития защищенности жизненно важных элементов системы от внешних и внутренних негативных факторов.

Любые неконтролируемые внешние или внутренние процессы потенциально могут привести к возникновению угроз. Реализация этих угроз, в свою очередь, оказывает негативное влияние на состояние безопасности системы, что вызывает деструктивные процессы. Нарушается нормальное функционирование системы, что находит свое отражение в значениях различных критериев и показателей, используемых для оценки безопасности.

Экономическая безопасность территориального образования – совокупность условий и факторов, характеризующих текущее состояние экономики, стабильность, устойчивость, поступательность ее развития, степень ее самостоятельности и интеграции с экономическим развитием страны.

Если экономическая безопасность характеризует оптимальное соотношение экономических интересов субъектов экономических отношений, то конкуренция устанавливает пределы возможностей для реализации субъектами рынка своих интересов. В связи с этим экономическая безопасность региона непосредственно влияет на способность региональной экономики конкурировать в различных отраслях и на конкретных товарных рынках [1].

Безопасность – понятие комплексное и не может рассматриваться как простая сумма составляющих ее частей. Эти части взаимосвязаны и взаимозависимы. Кроме того, каждая часть критично значима. Следовательно, никакие методы, предусматривающие усреднение при оценке комплексной безопасности, неприемлемы.

Понятие безопасности имеет не только объективную, но и субъективную сторону, поскольку оценка ее уровня проводится в конечном итоге человеком. При этом оценка уровня безопасности всегда относительна. Попытки напрямую приписать этой оценке численное значение в большинстве случаев бесперспективны в плане дальнейшей интерпретации результатов.

Это весьма важный аспект, который приводит к слабой формализованности задачи оценки уровня безопасности и к необходимости оперирования лингвистическими

Федирко Владимир Николаевич, совместитель кафедры управления Сумского государственного университета.

© В.Н. Федирко, 2011

переменными (основными структурными единицами в языке людей) и, как следствие, к применению аппарата нечеткой логики [3].

Для решения широкого круга задач, связанных с моделированием плохо формализованных процессов, их прогнозированием и поддержкой принятия решений, часто используются нечеткие когнитивные модели. Неоспоримыми их достоинствами по сравнению с другими методами являются возможность формализации численно неизмеримых факторов, использования неполной, нечеткой и даже противоречивой информации [5].

Когнитивная¹ модель управления уровнем комплексной безопасности

Уровень комплексной безопасности – это интегральная оценка, основанная на наборе показателей и критериев, характеризующая состояние системы в плане защищенности критичных для неё элементов.

При построении нечеткой когнитивной модели объект исследования обычно представляют в виде знакового ориентированного графа. В качестве такой модели при оценке комплексной безопасности системы (*KBS*) может быть принят кортеж²:

$$KBS = \langle G, L, E \rangle, \quad (1)$$

где *G* – ориентированный граф, имеющий одну корневую вершину и не содержащий петель и горизонтальных ребер в пределах одного уровня иерархии:

$$G = \langle \{F_i\}; \{D_{ij}\} \rangle, \quad (2)$$

где $\{F_i\}$ – множество вершин графа (факторов или концептов в терминологии когнитивного моделирования); $\{D_{ij}\}$ – множество дуг, соединяющих *i*-ю и *j*-ю вершины (множество причинно-следственных связей между концептами); $F_0 = K$ – корневая вершина, отвечающая уровню комплексной безопасности в целом (интегральному критерию безопасности – целевому концепту); *L* – набор качественных оценок уровней каждого фактора в иерархии: $L = \{\text{низкий, ниже среднего, средний, выше среднего, высокий}\}$; *E* – система отношений предпочтения одних факторов другим по степени их влияния на заданный элемент следующего уровня иерархии:

$$E = \{F_{i(e)} F_j \mid e \in (\succ; \approx)\}, \quad (3)$$

где F_i и F_j – факторы одного уровня иерархии; \succ – отношение предпочтения; \approx – отношение безразличия. Такая система может быть получена, например, изложенным в [1] модифицированным методом нестрогого ранжирования, позволяющим определить обобщенные на случай предпочтения/безразличия факторов по отношению друг к другу веса Фишберна для каждой дуги D_{ij} (веса связей).

Веса Фишберна отражают тот факт, что системе убывающего предпочтения *N* альтернатив наилучшим образом отвечает система снижающихся по правилу арифметической прогрессии весов.

Поэтому эти веса представляют собой рациональные дроби, в знаменателе которых

¹ Методология когнитивного моделирования, предназначенная для анализа и принятия решений в плохо определенных ситуациях, была предложена Аксельродом (Axelrod R. The Structure of Decision: Cognitive Maps of Political Elites. – Princeton. University Press, 1976). Она основана на моделировании субъективных представлений экспертов о ситуации и включает: методологию структуризации ситуации; модель представления знаний эксперта в виде знакового орграфа (когнитивной карты) (*F*, *W*), где *F* – множество факторов ситуации; *W* – множество причинно-следственных отношений между факторами ситуации; методы анализа ситуации.

² В математике кортеж – последовательность конечного числа элементов.

стоит сумма N первых членов натурального ряда (арифметической прогрессии с шагом 1), а в числителе – убывающие на единицу элементы натурального ряда, от N до 1 (например, $3/6$, $2/6$, $1/6$). Таким образом, предпочтение по Фишберну выражается в убывании на единицу числителя рациональной дроби весового коэффициента более слабой альтернативы.

Пример наложения системы отношений предпочтения типа (3) $E = \{U1 \succ U2; U2 \succ U3 \approx U4; U4 \approx U5\}$ на фрагмент графа изображен на рис. 1.

Связь между любыми двумя вершинами (концептами) при необходимости можно также представить в виде нечеткой когнитивной модели более низкого уровня. При этом на верхний уровень будет передаваться максимальное значение связи, выявленное в ходе анализа когнитивной модели нижнего уровня. Такой иерархический способ позволяет упростить построение когнитивной модели для систем высокой степени сложности.

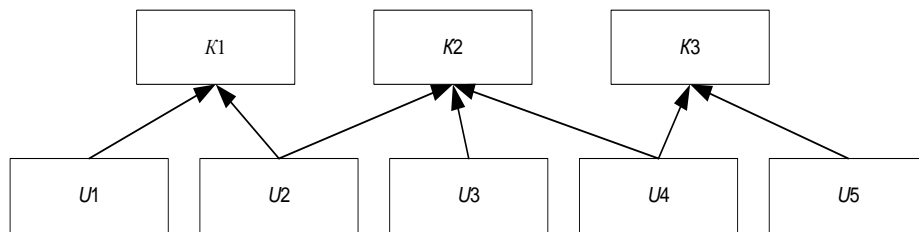


Рис. 1. Пример системы отношений предпочтения на одном из уровней иерархии

Состояние системы с точки зрения безопасности можно охарактеризовать матрицей B , строки которой состоят из элементов $(K_i, F_i, V_i, T_i, S_i)$, где K_i – показатель уровня безопасности по i -му критерию; F_i – тенденция изменения i -го критерия (возрастает (+1), убывает (-1), нейтрален (0)); V_i – скорость изменения i -го критерия (например: низкая, ниже среднего, средняя, выше среднего, высокая); T_i – характерное для i -го критерия время, которое, в частности, позволяет правильно интерпретировать значения параметра V_i ; S_i – степень критичности негативных последствий при реализации рисков, ухудшающих значение i -го критерия.

В этом случае текущее значение K_i в произвольный момент времени t может быть найдено по формуле

$$K_{i(t)} = K_{i(t=0)} + F_i V_i(t/T_i). \quad (4)$$

Показатели же степени критичности негативных последствий S_i фактически представляют собой веса, с которыми частные критерии безопасности K_i влияют на комплексный показатель безопасности системы в целом.

Матрицу вида B будем называть в дальнейшем матрицей безопасности.

Критерии можно группировать по соответствующим направлениям обеспечения безопасности, например: экономические, экологические, социальные, технические и т.п.

Таким образом, каждый кортеж $(K_i, F_i, V_i, T_i, S_i)$ характеризует состояние безопасности по i -му критерию.

Частичные матрицы, состоящие из строк, представляющих определенное направление обеспечения безопасности, описывают состояние в соответствующей области.

Показатели уровня безопасности K_i тесно связаны с последствиями от возможной

реализации имеющихся в системе угроз, мерами предотвращения таких последствий и мерами, направленными на локализацию и устранение последствий, если таковые все же возникают.

Следует отметить, что угрозы можно разделить на первичные и вторичные. Первичные угрозы существуют вне зависимости от состояния системы и имеют априорно заданную безусловную вероятность появления. Вероятность появления вторичных угроз является условной и зависит от внутреннего состояния системы и состояния внешней среды.

В частности, некоторые состояния системы могут спровоцировать возникновение угроз, появление которых в иных условиях было бы невозможным.

Введем следующие обозначения: \bar{U}_i и \tilde{U}_j , ($i, j = 1, 2, \dots$) – совокупность первичных и вторичных угроз, возникающих с вероятностями $P\bar{U}_i$ и $P\tilde{U}_j$ соответственно и оказывающих влияние \bar{n}_{km} и \tilde{n}_{km} на элемент (k, m) матрицы безопасности B , ($k = 1, 2, 3, \dots; m = 1, 2, 3, 4, 5$).

Влияние каждой из первичных или вторичных угроз можно описать соответствующими матрицами влияния \bar{N}_i и \tilde{N}_i , имеющими вид $N_i = \{n_{ij}\}$.

Кортеж $\bar{R}_i = \{\bar{N}_i; P\bar{U}_i\}$ назовем риском реализации i -й первичной угрозы. Данный кортеж отражает появление с вероятностью $P\bar{U}_i$ негативных факторов, которые изменяют состояние системы через соответствующие матрицы влияния \bar{N}_i .

Вероятности возникновения первичных угроз $P\bar{U}_i$ от нас не зависят. Однако совокупность превентивных мер защиты позволяет ослабить влияние первичных угроз на степень безопасности системы.

Этот факт может быть описан с помощью матриц превентивных мер $Z_j = \{z_{ik}\}$ ($i=1, \dots, n; k=1, \dots, 5$). Здесь j меняется от 1 до M , где M – общее количество превентивных мер.

Элементы матрицы Z_i назовем демпфирующими коэффициентами. Тогда под остаточным влиянием будем подразумевать матрицу \hat{N}_i (назовем ее матрицей остаточного влияния), элементы которой находятся из выражения

$$\hat{n}_{mn} = n_{mn} \otimes \max_{k=1 \dots M} Z_{mn}^k, \quad (5)$$

где Z_{mn}^k – элемент (m, n) матрицы превентивных мер Z_k . Символом \otimes обозначена некоторым образом определенная для двух матриц операция. В случае числовых значений элементов матриц это может быть, например, операция обычного поэлементного умножения или сложения. В случае лингвистических значений данная операция определяется с помощью принципа расширения обычных (четких) математических функций на нечеткие числа, предложенного Л. Заде [3].

Под *остаточным риском* будем понимать кортеж

$$\hat{R}_i = \{\hat{N}_i; P\bar{U}_i\}. \quad (6)$$

Если все же, несмотря на превентивные меры защиты, реализация определенного множества первичных угроз привела к возникновению последствий, то необходимо предпринять меры для их локализации и устранения.

Прежде всего необходимо оценить отклонение текущего состояния системы \hat{B} от

безопасного состояния B_s .

Введем понятие разности между двумя матрицами, определив результат применения операции « \oplus » аналогично тому, как это было сделано для операции « \otimes »: в случае числовых значений элементов матриц – это операция поэлементного вычитания, в случае лингвистических значений – операция определяется с помощью принципа расширения Л. Заде.

Тогда матрицу $Q = B_s \oplus \hat{B}$ назовем матрицей потерь безопасности на данном этапе.

Элементы матрицы потерь безопасности являются входными данными для блока ликвидации последствий.

Реализация мероприятий этого блока может быть формализована с помощью матрицы ликвидации последствий $L = \{l_{ij}\}$, где $i = 1, \dots, n; j = 1, \dots, 5$.

Результат применения матрицы ликвидации последствий может быть записан следующим образом:

$$\hat{Q} = Q \otimes L \{ \hat{q}_{ij} \}. \quad (7)$$

Матрицу \hat{Q} назовем матрицей остаточных потерь безопасности. Если $\hat{Q} \neq B_s$, то подобное состояние системы может инициировать появление вторичных угроз с вероятностями $P\tilde{U}_i$.

Таким образом, кроме первичных угроз, в зависимости от текущего состояния системы и ее окружения возможно возникновение вторичных угроз, вероятность появления которых равна $P\tilde{U}_i$.

Кортеж $\tilde{R}_i = \{ \hat{N}_i; P\tilde{U}_i \}$ назовем риском реализации i -й вторичной угрозы. Вероятности появления вторичных угроз не являются безусловными, как для первичных угроз. Они зависят от текущего состояния системы. С первичными угрозами мы начинаем бороться еще до их наступления, т. е. фактически пытаемся свести к минимуму их последствия, не имея возможности повлиять на сам факт их появления. В случае со вторичными угрозами мы должны пытаться вообще не допустить их, т. е. должны бороться с вызывающими их причинами. Это принципиальное различие в блоках мероприятий, воздействие которых формализовано множеством матриц Z_j и матрицей L .

На основании вышеизложенного общую схему анализа и управления комплексной безопасностью на основе нечеткого когнитивного моделирования можно представить в следующем виде:

- сбор информации об объекте защиты, выбор критериев, характеризующих состояние различных сторон обеспечения безопасности, определение их приемлемого уровня (возможно, в виде интервальных оценок или лингвистических термов);
- построение когнитивной модели в виде знакового ориентированного графа с наложенной системой отношений предпочтения типа (3);
- вычисление весов Фишберна на основании модифицированного метода нестрогого ранжирования;
- анализ уровня обеспечения безопасности системы;
- если управление безопасностью некоторой системы не находится в приемлемом диапазоне значений, то производятся изменения в составе концептов, участвующих в построении когнитивной модели, в составе связей между концептами, изменяются их веса посредством введения защитных мероприятий, влияния которых отражаются матрицей потерь безопасности и матрицей ликвидации последствий. Данные изменения соответствуют различным стратегиям управления безопасностью: уменьшение рисков,

уклонение от рисков, принятие рисков [7].

Таким образом, процесс обеспечения безопасности системы подразумевает решение двух взаимосвязанных задач: прямой (анализ состояния системы) и обратной задачи управления (воздействие на систему). При решении первой задачи требуется определить значения критериев безопасности K_i и интегрального критерия K при заданных значениях всех влияющих на них концептов. Если полученные значения находятся вне диапазона приемлемости, то при решении обратной задачи необходимо подобрать такие управляющие воздействия Z_i и L , которые обеспечат возвращение целевых критериев в безопасный диапазон.

Если существует не единственный набор необходимых управляющих воздействий, то на этом этапе может возникнуть задача оптимизации, состоящая в нахождении такой комбинации Z_i и L , которая обеспечивает максимальное воздействие на негативные факторы при заданных или минимальных затратах на реализацию способов и средств защиты.

Выводы

Схема построения когнитивной модели позволяет унифицировать подходы к управлению комплексной безопасностью и приступить к разработке соответствующих вычислительных процедур и модулей, которые могут быть в дальнейшем использованы при построении систем поддержки принятия решений.

1. *Ажмухамедов И. М.* Моделирование на основе экспертных суждений процесса оценки информационной безопасности / И. М. Ажмухамедов // Вестник АГТУ. – 2009. – № 2. – С. 101–109.
2. *Домарев В. В.* Безопасность информационных технологий. Системный подход / В. В. Домарев – К. : Изд-во «Диасофт», 2004. – 992 с.
3. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – М. : Мир, 1976. – 165 с.
4. *Аудит информационной безопасности.* [Электронный ресурс] – Режим доступа : <http://www.technoserv.ru/ru/solutions/is/services/audit/>
5. *Максимов В. И.* Целеполагание и стратегическое управление развитием сложных социально-экономических объектов в нестабильной внешней среде / В. И. Максимов, С. В. Коврига : материалы тр. 5-й междунар. науч.-практ. конф. [Анализ систем на рубеже тысячелетий: теория и практика – 2001]. – М., 2001. – Т. 2. – 2001. – С. 23–36.
6. *Садердинов А. А.* Информационная безопасность предприятия / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. – М. : Дашков К°, 2005. – 336 с.
7. *Хрусталева Е.* Когнитивные технологии в теории и практике стратегического управления (на примере оборонно-промышленного комплекса) / Е. Хрусталева // Проблемы теории и практики управления. – 2007. – № 4. – С. 25–33.

Получено 21.12.2010 г.

В.М. Федірко

Управління комплексною безпекою соціо-еколого-економічного розвитку регіону

У статті досліджена сутність безпеки; обґрунтована необхідність кількісного вимірювання рівня комплексної безпеки як основи ефективного управління; запропоновані етапи і модель аналізу та управління комплексною безпекою.

Ключові слова: комплексна безпека, соціо-еколого-економічний розвиток; когнітивна модель.

V.M. Fedirko

Management of complex security of socio-ecological and economic development of the region

The safety essence has been explored; the need of quantitative measurement of complex security level based as the basis of effectively management has been justified; steps and model of analysis and management of complex security have been offered in the article.

Keywords: complex security, socio-ecological and economic development, cognitive model.