УДК 004.056
ББК 05.25.05

АНАЛИЗ И УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

Ажмухамедов И.М.[1]
(ФГОУ Астраханский государственный технический университет, Астрахань)

Предложена схема построения когнитивной модели, позволяющая унифицировать подходы к управлению комплексной безопасностью различных систем.

Ключевые слова: нечеткая когнитивная модель, уровень безопасности, нестрогое ранжирование, веса Фишберна.

1. Введение

В современном понятийно-категориальном аппарате под безопасностью понимается 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 угрозы в свою очередь оказывает негативное влияние на состояние безопасности системы, что вызывает различные деструктивные процессы. Нарушается нормальное функционирование системы, что находит свое отражение в значениях различных критериев и показателей, используемых для оценки безопасности [2].

[1] *ИскандарМаратович Ажмухамедов*, *кандидат технических наук*, *доцент* (*aim_agtu@mail.ru*).

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 осреднение (пусть и неявное) при оценке комплексной безопасности неприемлемы.

Комплексная оценка уровня безопасности (КОУБ) не может быть больше минимальной оценки, полученной для различных аспектов системы.

Безопасность не существует сама по себе, в отрыве от человека. Она обеспечивается для человека и им же оценивается. Поэтому, 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 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 [4].

2. Когнитивная 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 (НКМ) объект исследования обычно представляют в виде знакового ориентированного графа. В качестве такой модели при оценке комплексной безопасности системы (KBS) может быть принят кортеж:

(1) $KBS = <G, L, E>$

Здесь:

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

(2) $G = <\{F_i\};\{D_{ij}\}>$,

где $\{F_i\}$ – множество вершин графа (факторов или концептов в терминологии НКМ); $\{D_{ij}\}$ – 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 = {Низкий,Ниже среднего,Средний,Выше среднего,Высокий}.

E - система отношений предпочтения одних факторов другим по степени их влияния на заданный элемент следующего уровня иерархии:

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

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).

Пример наложения системы отношений предпочтения типа (3) $E=\{N_1 \succ N_2;\ N_2 \succ N_3 \approx N_4;\ N_4 \approx N_5\}$ на фрагмент графа изображен на рис.1.

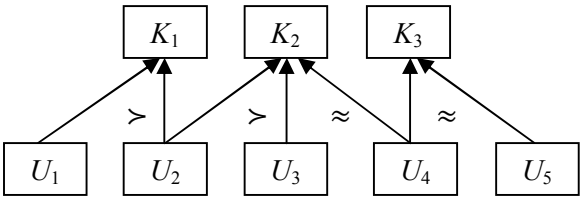

Рис.1. Пример системы отношений предпочтения на одном из уровней иерархии.

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 НКМ нижнего уровня. Такой иерархический способ позволяет упростить построение НКМ для систем высокой степени сложности.

Состояние системы с точки зрения безопасности можно охарактеризовать следующей матрицей:

$$B = \begin{pmatrix} K_1 & F_1 & V_1 & T_1 & S_1 \\ K_2 & F_2 & V_2 & T_2 & S_2 \\ K_3 & F_3 & V_3 & T_3 & S_3 \\ K_4 & F_4 & V_4 & T_4 & S_4 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ K_n & F_n & V_n & T_n & S_n \end{pmatrix},$$

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.

Матрицу вида B будем называть в дальнейшем *матрицей безопасности* (МБ).

Критерии можно сгруппировать 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 особо 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:

$\overline{U_i}$ и $\widetilde{U_j}$ $(i, j = 1,2,3, \dots)$ - совокупность первичных и вторичных угроз, возникающих с вероятностями $\overline{PU_i}$ и $\widetilde{PU_j}$, соответственно, и оказывающих влияние $\bar{n}_{km}$ и $\tilde{n}_{km}$ на элемент (k,m) матрицы безопасности B (k=1,2,3,…; m = 1,2,3,4,5).

Влияние каждой из первичных или вторичных угроз можно описать соответствующими *матрицами влияния* (МВ) $\overline{N_i}$ и $\widetilde{N_i}$, имеющими вид:

$$N_i = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} & n_{15} \\ \underline{n_{21}} & \underline{n_{22}} & \underline{n_{23}} & \underline{n_{24}} & \underline{n_{25}} \\ n_{n1} & n_{n2} & n_{n3} & n_{n4} & n_{n5} \end{pmatrix}$$

Кортеж $\overline{R_i} = \{\overline{N_i}; \overline{PU_i}\}$ назовем *риском реализации i-й первичной угрозы*.

Данный кортеж отражает появление с вероятностью $\overline{PU_i}$ негативных факторов, которые изменяют состояние системы через соответствующие матрицы влияния $\overline{N_i}$.

Вероятности возникновения первичных угроз $\overline{PU_i}$ 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 (МПМ):

$$Z_j = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} & z_{n5} \end{pmatrix},$$

где $j = \overline{1, \mathrm{M}}$, 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 – МОВ) элементы которой находятся из выражения:

$$\hat{n}_{mn} = n_{mn} \otimes \max_{\mathrm{k=1...M}} \mathrm{z}^{\mathrm{k}}_{\mathrm{mn}},$$

где $\mathrm{z}^{\mathrm{k}}_{\mathrm{mn}}$ – элемент (m,n) матрицы превентивных мер Z_k. Символом «⊗» обозначена некоторым образом определенная для двух матриц операция. В случае числовых значений элементов матриц, это может быть, например, операция простого 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 [4].

Под *остаточным риском* будем понимать кортеж:

$$\bar{R} = \{\hat{N}_i;\ \overline{PU_i}\},$$

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 «#» к двум элементам матриц аналогично тому, как это было сделано для операции «⊗»: в случае числовых значений элементов матриц - это операция поэлементного вычитания, в случае лингвистических значений - операция определяется с помощью принципа расширения Л.Заде.

Тогда матрицу $Q = B_S \# \hat{B}$ назовем *матрицей потерь безопасности* (МПБ) на данном этапе.

Элементы МПБ являются входными данными для блока ликвидации последствий (БЛП).

Реализация мероприятий этого блока может быть формализована с помощью матрицы ликвидации последствий (МЛП):

$$L = \begin{pmatrix} l_{11} & l_{12} & l_{13} & l_{14} & l_{15} \\ \underline{l_{21}} & \underline{l_{22}} & \underline{l_{23}} & \underline{l_{24}} & \underline{l_{25}} \\ l_{n1} & l_{n2} & l_{n3} & l_{n4} & l_{n5} \end{pmatrix}.$$

Результат применения БЛП может быть записан следующим образом:

$$\hat{Q} = Q \otimes L = \begin{pmatrix} \hat{q}_{11} & \hat{q}_{12} & \hat{q}_{13} & \hat{q}_{14} & \hat{q}_{15} \\ \underline{\hat{q}_{21}} & \underline{\hat{q}_{22}} & \underline{\hat{q}l_{23}} & \underline{\hat{q}_{24}} & \underline{\hat{q}_{25}} \\ \hat{q}_{n1} & \hat{q}_{n2} & \hat{q}_{n3} & \hat{q}_{n4} & \hat{q}_{n5} \end{pmatrix}$$

Матрицу $\hat{Q}$ назовем матрицей остаточных потерь безопасности (МОПБ).

Если $\hat{Q} \neq B_S$, то подобное состояние системы может инициировать появление вторичных угроз с вероятностями $\widetilde{PU}_i$.

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

Кортеж $\tilde{R}_i = \{\tilde{N}_i ; \widetilde{PU}_i\}$ назовем риском реализации i-й вторичной угрозы.

Заметим, что 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 с 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:

1. 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).
2. Построение когнитивной модели в виде знакового ориентированного графа с наложенной системой отношений предпочтения типа (3).
3. Вычисление весов Фишберна на основании модифицированного метода нестрого ранжирования.
4. Анализ уровня обеспечения безопасности системы (УБС).
5. Если УБС 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 МПМ и МЛП. Данные изменения соответствуют различным стратегиям управления безопасностью: уменьшение рисков, уклонение от рисков, принятие рисков [5].

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.

3. 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.

Литература

1. АЖМУХАМЕДОВ И.М. *Моделирование на основе экспертных суждений процесса оценки информационной безопасности* // Вестник АГТУ 2/2009 г., С.101-109.
2. ДОМАРЕВ В.В. *Защита информации и безопасность компьютерных систем*.- Киев, Изд-во «Диасофт», 2006, 480с.

3. ЗАДЕ Л. *Понятие лингвистической переменной и его применение к принятию приближенных решений* – М.; МИР, 1976 – 165с.
4. МАКСИМОВ В.И., КОРНОУШЕНКО Е.К. *Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач* // Труды ИПУ РАН. - М., 1999. – Т. 2. – С.95-109.
5. ХРУСТАЛЕВ Е.Ю., МАКАРЕНКО Д.И. *Когнитивные технологии в теории и практике стратегического управления (на примере оборонно-промышленного комплекса)* // Проблемы теории и практики управления. - 2007.- № 4. - С. 25-33.

ANALYSIS AND MANAGEMENT OF THE INTEGRATED SECURITY BASED ON COGNITIVE MODELLING

Iskandar Azmuhamedov, Astrakhan State Technical University, Astrakhan, Cand.Sc., assistant professor (aim_agtu@mail.ru).

Abstract: Build cognitive model proposed scheme that allows you to standardize approaches to management of the integrated security systems.

Keywords: fuzzy cognitive model, the level of security, poor ranking, weight of Fishbern.