УДК 004.056
ББК 05.25.05

АНАЛИЗ И УПРАВЛЕНИЕ 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.

Исследованию в этой области посвящен ряд работ, в которых предлагаются различные подходы.

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

Так, например, в [6] изложен системный подход к построению комплексной защиты информационной системы предприятия и описана методика построения такой системы с применением отечественных технических и криптографических средств защиты. В работе [4] рассмотрены принципы и методы аудита информационной безопасности (ИБ) на основе процессорного подхода, приведены некоторые методы оценивания ИБ.

Наиболее яркое выражение системный подход к решению задач безопасности нашел в работах В. В. Домарева. Им предложена трехмерная модель, включающая в себя основные этапы, направления и методы обеспечения безопасности различных систем [2]. Подчеркнуто, что специфическими особенностями задачи создания систем защиты являются:

– неполнота и неопределенность исходной информации о составе и характере угроз;

– многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей;

– наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения систем защиты;

– невозможность применения классических методов оптимизации.

Поэтому разработка модели, позволяющей унифицировать подходы к управлению комплексной безопасностью системы, является весьма актуальной задачей.

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 [5].

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-ую и j-ую 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) $E = \{F_i(\mathrm{e})\, F_j \mid \mathrm{e} \in (\succ; \approx)\}$,

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).

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 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) $E = \{U_1 \succ U_2;\ U_2 \succ U_3 \approx U_4;\ U_4 \approx U_5\}$ 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 НКМ нижнего уровня. Такой иерархический способ позволяет упростить построение НКМ для систем высокой степени сложности.

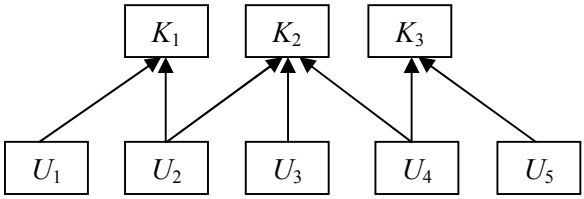

Рис. 1. Пример системы отношений предпочтения на одном из уровней иерархии

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:

$$K_i(t) = K_i(t = 0) + F_i * V_i(t/T_i).$$

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* (МБ).

Критерии можно сгруппировать по соответствующим направлениям обеспечения безопасности, например: экономиче-

ские, 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, …) – совокупность первичных и вторичных угроз, возникающих с вероятностями $P\overline{U}_i$ и $P\widetilde{U}_i$, соответственно и оказывающих влияние $\overline{n}_{km}$ и $\widetilde{n}_{km}$ 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 $N_i = \{n_{ij}\}$.

Кортеж $\overline{R}_i = \{\overline{N}_i; P\overline{U}_i\}$ назовем *риском реализации i-ой первичной угрозы*.

Данный кортеж отражает появление с вероятностью $P\overline{U}_i$ негативных факторов, которые изменяют состояние системы через соответствующие матрицы влияния $\overline{N}_i$.

Вероятности возникновения первичных угроз $P\overline{U}_i$ 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 (МПМ) $Z_j = \{z_{ik}\}$ (i=1,…,n; k=1,…,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 $\widehat{N}_i$ (назовем ее матрицей остаточного влияния – МОВ) элементы которой находятся из выражения:

$$\widehat{n}_{mn} = n_{mn} \otimes \max_{k=1...M} z_{mn}^k$$

где z_{mn}^k – 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 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

$$\widehat{R}_i = \{\widehat{N}_i; P\overline{U}_i\}$$

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 $\widehat{B}$ от безопасного состояния B_S.

Введем понятие разности между двумя матрицами, определив результат применения операции «#» аналогично тому, как это было сделано для операции «⊗»: в случае числовых значений элементов матриц – это операция поэлементного вычитания, в случае лингвистических значений – операция определяет-

ся с помощью принципа расширения Л. Заде.

Тогда матрицу $Q = B_S \# \widehat{B}$ 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) $L=\{l_{ij}\}$, где $i=1,\ldots, n$; $j=1,\ldots, 5$.

Результат применения БЛП может быть записан следующим образом:

$$\widehat{Q} = Q \otimes L = \{\widehat{q}_{ij}\}$$

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

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

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

Кортеж $\widetilde{R}_i = \{\widetilde{N}_i; P\widetilde{U}_i\}$ назовем риском реализации i-ой 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 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:

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 [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.

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. – 2009. – №2. – С. 101–109.
2. ДОМАРЕВ В. В. *Безопасность информационных технологий. Системный подход.* – Киев: изд-во «Диасофт», 2004. – 992 с.
3. ЗАДЕ Л. *Понятие лингвистической переменной и его применение к принятию приближенных решений* – М.: Мир, 1976. – 165 с.
4. КУРИЛО А. П., ЗЕФИРОВ С. Л., ГОЛОВАНОВ В. Б. *Аудит информационной безопасности.* – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
5. МАКСИМОВ В. И., КОРНОУШЕНКО Е. К. *Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач* // Труды ИПУ РАН. – 1999. – Т. 2. – С. 95–109.
6. САДЕРДИНОВ А. А., ТРАЙНЕВ В. А., ФЕДУЛОВ А. А. *Информационная безопасность предприятия: Учебное пособие. 2-е изд*. – М.: Издательско-торговая корпорация «Дашков К°», 2005. – 336 с.
7. 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.

COGNITIVE-MODELING-BASED INTEGRATED SECURITY ANALYSIS AND MANAGEMENT

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

Abstract: The scheme of cognitive model construction is proposed that allows unifying the approaches to the integrated risk management in various systems.

Keywords: fuzzy cognitive model, security level, poor ranking, Fishburn weights.

Статья представлена к публикации членом редакционной коллегии Д. А. Новиковым