И. М. Ажмухамедов

ДИНАМИЧЕСКАЯ НЕЧЕТКАЯ КОГНИТИВНАЯ МОДЕЛЬ ВЛИЯНИЯ УГРОЗ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ СИСТЕМЫ

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 могут привести к возникновению угроз. Реализация этих угроз, в свою очередь, оказывает негативное влияние на состояние безопасности системы, что вызывает различные деструктивные процессы. Нарушается нормальное функционирование системы, и это находит свое отражение в значениях различных критериев и показателей, используемых для оценки безопасности [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 осреднение (пусть и неявное) при оценке комплексной безопасности, неприемлемы.

Комплексная оценка уровня безопасности не может быть больше минимальной оценки, полученной для различных частей 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 именно *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 [2].

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 [3].

Когнитивная модель влияния угроз на безопасность системы

Уровень комплексной безопасности — это интегральная оценка, основанная на наборе показателей и критериев, характеризующая состояние системы в плане защищенности критичных для нее 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:

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

Здесь:

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

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

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); $F_0 = K_0$ — корневая вершина, отвечающая уровню комплексной безопасности в целом (интегральному критерию безопасности — целевому концепту).

L — набор качественных оценок уровней каждого фактора в иерархии (терм-множество):

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:

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

где F_i и F_j — факторы одного уровня иерархии, $>$ — отношение предпочтения, $\approx$ — отношение безразличия. Такая система может быть получена, например, изложенным в работе [4] модифицированным методом нестрогого ранжирования, позволяющим определить обобщенные на случай предпочтения/безразличия факторов по отношению друг к другу веса Фишберна S_{ij} для каждой дуги D_{ij} (веса связей).

Пример наложения системы отношений предпочтения типа (3): E={U_1>U_2; U_2>U_3≈U_4; N_4≈U_5} на фрагмент графа изображен на рис. 1.

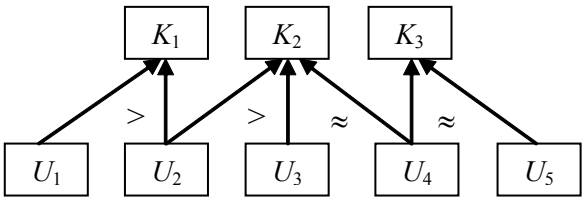

Рис. 1. Пример системы отношений предпочтения на одном из уровней иерархии

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.

Чтобы оценить уровень фактора количественно и качественно, необходимо произвести агрегирование данных, собранных в рамках иерархии G по направлению дуг графа. При этом агрегированию подлежит не отдельное значение выбранной функции принадлежности в структуре лингвистической переменной «Уровень фактора», а вся функция принадлежности целиком. Подробно методика расчетов применительно к задаче оценке уровня безопасности приведена в работе [4].

Состояние системы можно охарактеризовать вектором безопасности (ВБ)

$$\vec{K} = (K_1, K_2, ..., K_N),$$

где K_i — показатель уровня безопасности по i-му частному критерию.

Частные критерии K_i можно сгруппировать по соответствующим направлениям обеспечения безопасности, например: информационные, экономические, экологические, социальные, технические и т. п. Каждый компонент ВБ характеризует в динамике текущее состояние безопасности по определенному критерию.

Показатели уровня безопасности K_i тесно связаны с возникновением внешних и внутренних угроз, мерами предотвращения реализаций этих угроз и мерами, направленными на локализацию и устранение последствий, если таковые все же возникли.

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.

С первичными угрозами мы боремся, не имея возможности повлиять на сам факт их появления. Вторичные угрозы мы должны пытаться вообще не допустить, т. е. должны бороться с вызывающими их причинами.

В рамках биосистемной аналогии, предложенной в работе [6], данный факт можно описать следующим образом. Угроза заражения какой-либо инфекцией или получения травмы (вирусная атака на компьютерную сеть или нарушение физической целостности) является первичной и возникает с определенной безусловной вероятностью, не зависящей от конкретного человека (информационной системы — ИС). Будет ли эта угроза реализована и приведет ли это к болезни (нарушению функционирования ИС), зависит от превентивных мер, предпринятых для профилактики заболевания (например, вакцинации (применения средств антивирусной защиты) или закаливания организма (настройки политики безопасности)). Однако если последствия все же наступили, то это может повлечь за собой появление других угроз здоровью (функционированию ИС), к примеру возникновение болезней, связанных с ослаблением иммунной системы (антивирусной и иной защиты), неверным лечением (неадекватными действиями антивирусных пакетов) или отказом критичных систем вследствие продолжительной высокой температуры биологического организма (потеря доступности системы и/или критичное падение производительности вследствие того, что большая часть ресурсов отвлечена на борьбу с атаками).

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

Обозначим через $\overline{U}_i$ и $\widetilde{U}_j$ — совокупность первичных и вторичных угроз, возникающих с вероятностями $P\overline{U}_i$ и $P\widetilde{U}_j$ соответственно. Тогда влияние каждой из угроз на состояние безопасности можно описать соответствующими векторами:

$$\bar{\bar{N}}_i = \{\bar{n}_{ik}\} \text{ и } \tilde{\bar{N}}_j = \{\tilde{n}_{jk}\}.$$

Вероятности возникновения первичных угроз, действующих в течение времени $T\bar{U}_i$, от нас не зависят. Однако превентивные меры защиты, количество которых обозначим через M, позволяют ослабить их влияние на степень безопасности системы (стратегия уменьшения рисков).

Поскольку один механизм защиты может оказывать воздействие (иногда противоположное) на характеристики нескольких угроз, влияние этих мер описывается матрицами превентивных мер (МПМ) $Z_m = \{z_{ik}^{\ m}\}$, где $m = 1, 2...M$. Возможны ситуации, когда определенный защитный механизм, ослабляя влияние одних угроз, усиливает действие других либо приводит к возникновению вторичных угроз безопасности, что соответствует понятию «побочный эффект» в биосистемной аналогии.

Остаточное негативное влияние угроз формализуется вектором $\vec{N}_i$, компоненты которого образуют в графе G уровень, предшествующий уровню частных критериев безопасности. Их значения могут быть найдены вышеупомянутым способом агрегирования данных по направлению дуг графа.

Если, несмотря на превентивные меры защиты, реализация определенного множества первичных угроз привела к возникновению последствий, то необходимо предпринять меры для их локализации и устранения (стратегия принятия рисков).

Прежде всего, необходимо оценить отклонение вектора текущего состояния безопасности системы $\widetilde{K} = (\widetilde{K}_1, \widetilde{K}_2, ..., \widetilde{K}_N)$ от вектора безопасного состояния $K^B = (K_1^B, K_2^B, ..., K_N^B)$, а также найти интегральный критерий безопасности, согласно методике, изложенной в работе [4].

Введем понятие разности между двумя векторами, обозначив эту операцию символом «#» и определив ее результат следующим образом: в случае числовых значений компонентов вектора это операция поэлементного вычитания, в случае лингвистических значений данная операция определяется с помощью принципа расширения обычных (четких) математических функций на нечеткие числа, предложенного Л. Заде [2].

Вектором потерь безопасности (ВПБ) на текущем этапе назовем вектор $\vec{R} = (K_i^B \# \widetilde{K}_i)$.

Наличие ненулевых компонентов ВПБ является условием принятия решения о необходимости активизации блока ликвидации последствий (БЛП).

Реализация мероприятий этого блока может быть формализована с помощью вектора ликвидации последствий (ВЛП): $\vec{LP} = (l_k)$. Компенсаторные механизмы БЛП действуют до тех пор, пока в них есть необходимость, но не дольше, чем будет исчерпан запас сил и средств, имеющихся у лица, принимающего решения (ЛПР).

Следует заметить, что значения l_k, так же как и $\bar{n}_{ik}$, $\tilde{n}_{ik}$, zn_{ik}^m, зависят от времени, т. е. являются динамически изменяющимися величинами. В общем случае для l_k можно записать, что:

$$l_k^t = l_k^0 - l_k^{out}(t) + l_k^{in}(t),$$

где l_k^t, l_k^0 — текущее и начальное значения ресурса l_k соответственно; $l_k^{out}(t)$ и $l_k^{in}(t)$ — законы изменения по времени соответственно расхода и поступления в распоряжение ЛПР ресурса l_k.

С учетом вышеизложенного общую схему анализа и управления комплексной безопасностью на основе динамического 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 нестрогого ранжирования;

4. Вычисление ВПБ и 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 ВЛП. 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 критерия безопасности K_i и интегрального критерия K_0 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

Построенная динамическая нечеткая когнитивная модель позволяет унифицировать подходы к управлению комплексной безопасностью и приступить к разработке соответствующих вычислительных процедур и модулей, которые могут быть в дальнейшем использованы в системах поддержки принятия решений.

СПИСОК ЛИТЕРАТУРЫ:

1. *Домарев В. В.* Защита информации и безопасность компьютерных систем. Киев: Диасофт, 2006. – 480 с.
2. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: МИР, 1976. – 165 с.
3. *Максимов В. И., Корноушенко Е. К.* Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач // Труды ИПУ РАН. 1999. Т. 2. С. 95–109.
4. *Ажмухамедов И. М.* Моделирование на основе экспертных суждений процесса оценки информационной безопасности // Вестник АГТУ. 2009. № 2. С. 101–109.
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.
6. *Суханов А. В., Нестерук А. Г., Нестерук Ф. Г.* Мониторинг безопасности информационных систем на основе модели адаптивной защиты // Безопасность информационных технологий. 2008. № 3. С. 33–38.