

ЭКСПЕРТНАЯ ОЦЕНКА ЖИВУЧЕСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И КОМПЬЮТЕРНЫХ СЕТЕЙ (ТСКС) В УСЛОВИЯХ НЕПОЛНОТЫ ИНФОРМАЦИИ

М.В. Тюрин (МАИ)

Методологический базис – важнейший компонент анализа и обеспечения живучести ТСКС. Рассматривается метод расчета показателей живучести ТСКС в условиях неполноты информации на основе применения методов нечеткой логики.

Бурный рост информационных технологий привел к такому же стремительному развитию деструктивных факторов, влияние которых на работу ТСКС, зачастую, оценить в явном виде не представляется возможным по причине *неполноты информации* об источниках угроз, проявлениях их активности и т. д. В связи с этим обстоятельством наиболее универсальной характеристикой состояния ТСКС может стать понятие живучести, то есть способность получать, хранить, обрабатывать и передавать информацию, несмотря на влияние деструктивных воздействий. Понятие *живучести* объединяет ряд категорий: *надежность* оборудования; *функциональность* ПО; *информационная безопасность* технологий. Поскольку понятие живучести комплексное, то для определения характеристик живучести ТСКС применяют метод логико-лингвистических экспертных оценок.

Известно множество методов организации коллективной работы экспертов: мозговой атаки, сценариев, деловых игр, совещаний, суда. Все эти методы отличаются способами организации возможности экспертов высказать свое мнение наиболее эффективным образом, при этом сохраняется *неопределенность* в подсчете их голосов в условиях неполноты информации по причине наличия сомнений, неоднозначности трактовки тех или иных терминов, определений, показаний и измерений. Основу этой неопределенности составляет *лингвистическая неопределенность*. В случае представления *лингвистической неопределенности* в виде стохастических процессов, вероятностные методы оказываются неэффективны, поскольку они помогают выбирать наилучшие из множества возможных решений лишь в условиях одного конкретного вида неопределенности или в условиях полной определенности. Повысить достоверность экспертизы живучести ТСКС в условиях неполноты информации способно применение специализированных подходов и методов, основанных на теории *нечетких множеств* [1].

Экспертная оценка угроз живучести ТСКС

Как правило, экспертная оценка живучести строится на основе анализа модели угроз и нарушителей [2]. Например, угрозами, влияющими на живучесть ТСКС, могут быть: снижение аппаратной надежности ТСКС по причине наличия оборудования из так называемых "серых сборок" (неподтвержденное качество сборки); уязвимости ПО; ошибки программирования и недостатки технической поддержки производителя; отказ систем энергоснабжения и электропитания и т.п. [2].

Как основное допущение, предположим, что ТСКС состоит из надежного, хорошо себя зарекомендовавшего оборудования с использованием резервирования, находящегося на гарантийном обслуживании и эксплуатируемого подготовленным персоналом. Решение о критичности того или иного ресурса принимается на основе SLA (Service Level Agreement) – соглашения об уровне сервиса, определяющем взаимные ответственности провайдера ИТ сервиса и его пользователей.

Определение базового экспертного запроса и формирование лингвистических термов

На *первом этапе* на основе анализа модели угроз и нарушителей формулируются лингвистические оценки, образующие множество исходных данных – ID_{ij} ($i = \overline{1, n}$; $j = \overline{1, m}$) где, n – число возможных угроз; m – общее число экспертов.

Своеобразной *шкалой* для формирования единых мнений экспертов может служить таблица определения риска (табл. 1) разработки компании *Gartner Group* [2].

Такие таблицы используются как в "бумажных", так и в аппаратных методиках оценки рисков.

На *втором этапе* выполняется ранжирование исходных данных через определение коэффициентов важности $KB_j = [KB_1, \dots, KB_j]$. Для примера, возьмем шесть основных угроз, оцениваемые шестью независимыми экспертами. Эксперты указывают свои субъективные мнения в виде численных значений от 0 (максимально необходимая, оптимальная, живучесть – точка "горизонта") до 1 (полный крах системы). Оценки (коэффициенты важности угроз) образуют матрицу базового экспертного запроса (табл. 2).

Множества экспертных оценок угроз живучести образуют *нечеткие числа* $X_i = \{x_1, \dots, x_6\}$, что обусловлено распылчатостью понятий (лингвистических термов).

Результатом их ранжирования может стать функция принадлежности (ФП): $\mu_{KB}(x_i)$ – отображение множества угроз X_i в единичный отрезок $[0, 1]$, $X \rightarrow [0, 1]$.

Таблица 1. Оценочная таблица разработки компании *Gartner Group*

Цена потери (степень серьезности угрозы)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Н	С	В	Н	С	В	Н	С	В
Низкая	0	0,1	0,2	0,1	0,2	0,3	0,2	0,3	0,4
Ниже средней	0,1	0,2	0,3	0,2	0,3	0,4	0,3	0,4	0,5
Средняя	0,2	0,3	0,4	0,3	0,4	0,5	0,4	0,5	0,6
Выше средней	0,3	0,4	0,5	0,4	0,5	0,6	0,5	0,6	0,7
Высокая	0,4	0,5	0,6	0,5	0,6	0,7	0,6	0,7	0,8

Таблица 2. Коэффициенты важности угроз

		Коэффициент Важности (KB_j)						Функция принадлежности
		KB_1	KB_2	KB_3	KB_4	KB_5	KB_6	
Угрозы X_i	x_1 Угроза отказа доступа	0,7	0,6	0,6	0,5	0,5	0,6	$\mu_{KB}(x_1)$ 0,58
	x_2 Выход из строя активного сетевого оборудования	0,5	0,4	0,4	0,6	0,5	0,5	0,48
	x_3 Нарушение электропитания	0	0,4	0,6	0,2	0,3	0,3	0,3
	x_4 Угроза нарушения целостности	0,3	0,2	0,2	0,1	0,5	0,3	0,26
	x_5 Угроза нарушения конфиденциальности	0,3	0,2	0	0,2	0,3	0,2	0,2
	x_6 Выход из строя пассивного сетевого оборудования	0,2	0,2	0,3	0,1	0	0,2	0,16

Для определения значения ФП нечеткого множества экспертных оценок каждой из угроз живучести предлагается использовать метод построения экспоненциальной ФП.

Этот метод целесообразнее всего использовать при решении задач *выработки и оценки альтернатив*, а также представления *нормально* распределенных случайных величин таких, как угрозы (возмущения) информационной безопасности. Соответственно, реакция экспертов на рассматриваемые угрозы также представляет собой нормально распределенную случайную величину, что может упростить дальнейший переход к стохастическим методам оценки.

$$\mu_{KB}(x_i) = e^{-\alpha(KB_j - x_i)^2}, \quad (1)$$

где $\alpha = -4 \ln(0,5)/\beta^2$, значения α и β — границы толерантности нечеткого числа (расстояние между точками перехода, в которых функция приобретает значение 0,5).

Найденное значение базовой функции принадлежности $\mu_{KB}(x_i)$ оценок угроз живучести ТСКС, представлено в табл. 2 в отдельном столбце.

Очень часто в практике экспертизы одним термином описываются различные характеристики живучести ТСКС и ее элементов, или, наоборот, одно и то же свойство объекта можно описать различными синонимами. В этом случае могут сформироваться множества экспертных оценок, перекрывающиеся друг друга и требующие дополнительных разъяснений (экспликаций), для чего на основании идей, изложенных в [3], предлагается ввести понятие *цвет* нечеткого множества оценок и рассматривать его как экспликацию (разъяснение) понятий: *свойство, атрибут, характеристика*. Следовательно, нечеткое множество экспертных оценок, в совокупности с подмножествами их характеристик (толкований в стиле "ДА-НЕТ", образующими совокупность булевых матриц) составит нечеткое полихроматическое множество PS_x .

На *третьем этапе* в нечетком полихроматическом множестве PS_x , моделирующем живучесть оцениваемой ТСКС, каждому элементу $x_i \in X$ ставится в соот-

ветствие множество персональных цветов или раскрасок $F(x_i)$ разъясняющее эти свойства, а множеству X в целом — множество унитарных цветов или раскрасок $F(X)$ самого PS -множества.

При этом на основании идей, изложенных в [4], телом (носителем) $X_i(F_i)$ унитарного цвета $F_i(X)$ будет называться набор элементов, $X_i(F_i) \subseteq X$ персональных цвета которых обеспечивают существование унитарного цвета $F_i(X)$. Так например, телом унитарного цвета (комплексного понятия) "информационная безопасность" будут являться персональные цвета (простые понятия) "конфиденциальность", "целостность", "доступность" и "апеллируемость" (аутентичность) — свойства информации, характеризующие способность ТСКС применяться для ее безопасной обработки.

На *четвертом этапе*, во избежание некорректности нечетких моделей в описании PS -множества, предлагается указывать условия существования *персональных* цветов элементов и *унитарных* цветов самого PS -множества, а также учитывать возможность их влияния друг на друга. Для этого персональные раскраски всех элементов PS -множества описываются матрицей бинарных отношений вида $[X_i \in F(x_i)]$ между элементами X и их цветами $F(x_i)$. Причем, пара (x_i, F_j) существует, если $F_j \in F(x_i)$, и не существует, если $F_j \notin F(x_i)$. Получаемая бинарная матрица характеризует *наличие* физического влияния угроз на состояние живучести ТСКС. Идеальным является случай, когда все угрозы равноценные, однако для реальных систем существуют более или менее опасные и значимые угрозы, которые, в свою очередь, могут быть доминирующими и доминируемыми. В связи с этим принято рассматривать [4] позитивное, негативное и нейтральное взаимодействие раскрасок.

При *позитивном* взаимодействии персональные цвета рассматриваемого элемента расширяют унитарную раскраску PS -множества за счет появления новых тел унитарных цветов, в которые входит рассматриваемый элемент. При *негативном* взаимодействии персональные цвета рассматриваемого элемента отрицательно влияют и на соответствующие персональные цвета других элементов, и на унитарные цвета PS -множества, что приводит к прекращению их существования. При *нейтральном* взаимодействии условия существования цветов других элементов и унитарных цветов PS -множества остаются неизменными.

Так, например, реализация угрозы "выход из строя активного сетевого оборудования" может повлечь за собой возникновение угрозы "отказа доступа", демонстрируя позитивное влияние своей персональной окраски (чистого свойства). Или попытка нарушения "конфиденциальности" (хакерская атака на ресурс с целью хищения информации) на малопроизводительный и перегруженный сервер способна вызвать его физический выход из строя (повисание, "синий экран"), локализуя, тем самым, инцидент за счет реализации менее критичной угрозы "отказа доступа",

Таблица 3. Мнемоническое представление
Булевой матрицы вариантов тел унитарных цветов

		Тела унитарных цветов					
		$X_1(F)$	$X_2(F)$	$X_3(F)$	$X_4(F)$	$X_5(F)$	$X_6(F)$
Персональные цвета	$F(x_1)$	(±)	(-)	(-)	(+)	(+)	(-)
	$F(x_2)$	(+)	(±)	(-)	(+)	(+)	(±)
	$F(x_3)$	(+)	(+)	(±)	(+)	(+)	(+)
	$F(x_4)$	(-)	(-)	(-)	(±)	(+)	(-)
	$F(x_5)$	(-)	(-)	(-)	(-)	(±)	(-)
	$F(x_6)$	(+)	(±)	(-)	(+)	(+)	(±)

где (+) – позитивное, (-) – негативное,
(±) – нейтральное воздействие элемента

при этом демонстрируется *негативное* влияние своей персональной окраски.

Составы элементов всех вариантов тел, обеспечивающих существование унитарных цветов $F(X)$ ПС-множества, представляются булевой матрицей:

$$\|C_i(j)\| = [X_i \times X_j(F)], \quad (2)$$

где элементы x_i – логические переменные:

$$x_i = \begin{cases} 1, & \text{если } x_i \in X_i(F_j), \\ 0, & \text{если } x_i \notin X_i(F_j). \end{cases}$$

Причем, $X(F)$ есть объединение всех вариантов тел унитарных цветов $F(X)$. Мнемонически полученная конструкция будет выглядеть в виде, представленном в табл. 3.

На *пятом этапе* предлагается на основании [4] считать *степенью влияния* в унитарной раскраске ее персональных составляющих меру близости между "соседними" раскрасками элементов полихроматического множества – ПС_x. Способы определения *меры близости* основаны на определении расстояния Хемминга:

$$d_h(F(x_{i-1}), F(x_i)) = \sum_{j=1}^{n^*} |\mu_{x_{i-1}}(F_j) - \mu_{x_i}(F_j)|, \quad (3)$$

где, n^* – число цветов (реакций экспертов на n угроз) в объединении $F(x_1) \dots F(x_i)$, а степень принадлежности к раскраске равна:

$$\mu_x(F_j) = \begin{cases} 1, & \text{если } F_j \in F(x_i), \\ 0, & \text{если } F_j \notin F(x_i). \end{cases}$$

Также может быть удобно в расчетах использовать относительное расстояние Хемминга.

На основании (3) относительное расстояние Хемминга между персональными раскрасками $F(x_{i-1})$, $F(x_i)$ в n -мерном булевом векторном пространстве будет определяться по формуле:

$$d_{h(0)}(F(x_{i-1}), F(x_i)) = d_h(F(x_{i-1}), F(x_i)) \cdot n^{-1}, \quad (4)$$

где $0 \leq d_{h(0)} \leq 1$.

При этом, чем больше относительное расстояние Хемминга, тем меньше одна раскраска влияет на другую в составе этого ПС-множества. На основании булевой матрицы (2) и ее мнемонического представления (табл. 3) получаем численные значения расстояний Хемминга (табл. 4).

Таблица 4. Матрица относительных расстояний Хемминга
между персональными цветами объектов

$d_{h(0)}$	Персональные цвета $F(x_i)$					
	$F(x_1)$	$F(x_2)$	$F(x_3)$	$F(x_4)$	$F(x_5)$	$F(x_6)$
$F(x_1)$	0	0,67	0,5	0,5	0,5	0,67
$F(x_2)$	0,67	0	0,83	0,5	0,5	0,33
$F(x_3)$	0,5	0,83	0	0,67	0,67	0,5
$F(x_4)$	0,5	0,5	0,67	0	0,33	0,83
$F(x_5)$	0,5	0,5	0,67	0,33	0	0,5
$F(x_6)$	0,67	0,33	0,5	0,83	0,5	0

Например, нарушение конфиденциальности информации может сильно сказаться на ее целостности в результате удачной хакерской атаки, демонстрируя небольшое значение расстояния Хемминга между данными понятиями; взаимно противоположные по смыслу понятия конфиденциальности и доступности (чем выше необходимо достичь уровня конфиденциальности информации, тем большему кругу лиц необходимо запретить к ней доступ) имеют *значительное* расстояние Хемминга по причине того, что взаимодействуют между собой через формализованные условия – документированные условия присвоения информации грифа "конфиденциально" и последующие ограничения на доступ к ней и т.д.

Нечеткий вывод занимает центральное место в нечеткой логике и системах нечеткого управления. Нечетким логическим выводом называется получение заключения в виде нечеткого множества, соответствующего текущим значениям входов, с использованием нечеткой базы знаний и нечетких операций. Основу нечеткого логического вывода составляет композиционное правило Заде [1].

Механизм или алгоритм вывода является следующей важной частью базовой архитектуры систем нечеткого вывода. Одним из наиболее широко распространенных алгоритмов нечеткого вывода является алгоритм *Мамдани* (Mamdani) [http://rrc.dgu.ru/res/matlab/mltb/default.html].

Результатом приведения нечетких экспертных оценок будет являться *четкое* значение w_0 переменной x_i определяемое, как центр тяжести кривой результирующей функции принадлежности $\mu_\Sigma(w)$ комбинированного нечеткого множества (5), соответствующий логическому выводу выходной переменной $w(x_i)$:

$$w_0 = \frac{\int_{\Omega} w_i \cdot \mu_\Sigma(w) dw}{\int_{\Omega} \mu_\Sigma(w) dw}, \quad (5)$$

где Ω – область определения функции $\mu_\Sigma(w)$ – $[0;1]$, w_i – уровни "отсечения" для предпосылок каждого из правил (с использованием операций "минимум", "максимум").

Для учета влияния цветности на нечеткие множества оценок $\overline{w_0}$ каждой угрозы необходимо отобразить относительное расстояние Хемминга на множество выходных переменных: $d_{h(0)}^{+1}$, $d_{h(0)}^{-1}$ и $d_{h(0)}^0$ – относительное

Таблица 5. Таблица приведения к четким значениям

	Логический вывод (экспликация) оценки w_{0i}						
	w_{01}	w_{02}	w_{03}	w_{04}	w_{05}	w_{06}	$\bar{w}_{0i}$
Угроза отказа доступа	0	0,89	~1	0,25	0,25	0,89	0,55
Выход из строя активного сетевого оборудования	0,34	0	0,48	0,3	0,25	0,5	0,31
Нарушение электропитания	0	0,33	0	0,13	0,2	0,15	0,14
Угроза нарушения целостности	0,6	0,4	0,3	0	0,33	0,83	0,41
Угроза нарушения конфиденциальности	0,6	0,4	0	0,6	0	0,4	0,33
Выход из строя пассивного сетевого оборудования	0,13	0,2	0,6	0,08	0	0	0,17

расстояние Хемминга (4) при *позитивном, негативном и нейтральном* воздействии персональных цветов.

Тогда, *четкое* значение $\bar{w}_0$ с учетом влияния цветности будет представлено формулой вида (6):

$$\bar{w}_0 = \sum_{i=1}^m (d_{h(0),i}^{+1} \cdot w_{0i}) / m. \quad (6)$$

Для результатов базового экспертного запроса (табл. 2) с учетом влияния всех вариантов тел, унитарных цветов получаем таблицу приведения к четким значениям (табл. 5).

Для наглядности сравнения результатов до и после экспликации (разъяснения) экспертных оценок запишем таблицу сравнений (табл. 6).

Таблица 6. Таблица сравнений результатов до и после экспликации экспертных оценок

	Функция принадлежности $m_{KB}(x_i)$ (экспертная оценка живучести) w_{0i}	
	Функция принадлежности $m_{KB}(x_i)$ (экспертная оценка живучести)	Разъясненное значение оценки живучести $\bar{w}_{0i}$
Угроза отказа доступа	0,58	0,55
Выход из строя активного сетевого оборудования	0,48	0,31
Нарушение электропитания	0,3	0,14
Угроза нарушения целостности	0,26	0,41
Угроза нарушения конфиденциальности	0,2	0,33
Выход из строя пассивного сетевого оборудования	0,16	0,17
Средняя оценка риска всех угроз	0,33	0,318
Средняя оценка живучести ТСКС на этапе внедрения	0,67	0,682

знаний, минуя промежуточные результаты) и может в некоторой степени учитываться и прогнозироваться с помощью нечетких методов.

3) Применение методов нечеткой логики в условиях неполноты информации позволяет разложить исходную задачу на этапы и находить решения для систем с большим числом состояний, что позволяет экономить время экспертов, вычислительные ресурсы и расставлять приоритеты.

4) Рассмотренный метод экспертной оценки живучести телекоммуникационных систем и компьютерных сетей (ТСКС) может являться основой для создания целого класса систем принятия решений в условиях неполноты (нечеткости, неточности) информации.

Список литературы

1. Заде Л.А. Тени нечетких множеств // Проблемы передачи информации. Москва, 1966.
2. Петренко С.А., Петренко А.А. Аудит информационной безопасности Интернет // Академия Ай-Ти. Москва, 2002.
3. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Киев, 2006.
4. Павлов В.В. Полихроматические множества в теории систем. CALS – технологии. Наука. Москва, 2006.
5. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб, 2003.

Тюрин Михаил Вячеславович – инженер Московского авиационного института.

E-mail: mturin@mail.ru

Выпущен сервисный пакет обновления SCADA "КРУГ-2000" версии 3.0

Практический опыт разработки и результаты эксплуатации АСУТП на базе SCADA "КРУГ-2000" версии 3.0 нашли отражение в развитии SCADA "КРУГ-2000" и были оформлены как Сервисный пакет обновления (СПО) №4 для версии 3.0. Сервисный пакет обновлений включает ряд изменений в ПО SCADA "КРУГ-2000":

1. *Сервер базы данных и генератор БД*: произведена общая оптимизация работы; оптимизирован алгоритм обработки простоя трендов при запуске Сервера БД; произведена оптимизация запуска резервного Сервера БД и работы зеркализации для архивного протокола событий; модифицирован протокол обмена "Сервер БД – СРВК"; оптимизирован алгоритм регистрации событий Сервером БД; добавлено сохранение пользовательских словарей по каналам;
2. *Генератор Динамики и Графический интерфейс*: произведена общая оптимизация работы; реализована новая опция для мемо-

схем – "Кэширование мнемосхем"; изменен алгоритм поддержки двухмониторного режима при различных настройках видеокарты; изменен интерфейс и функциональные возможности обновления и импортирования мнемосхем в Генераторе Динамики;

3. *OPC-клиент*: оптимизирована работа OPC-клиента Сервера БД; обеспечена возможность работы с удаленным OPC-сервером SNMP;

4. *Менеджер Задач*: оптимизирован алгоритм вывода сигнализации для некоторых типов процессоров и материнских плат;

5. *Сервис перезапуска*: оптимизирован алгоритм перезагрузки компьютера; добавлено формирование списка запущенных процессов и его запись в системный журнал при старте сервиса;

Модуль диагностики Сервера Единого Времени: откорректирован алгоритм вычитки сообщений, относящихся к синхронизации времени, из системного журнала ОС Windows XP.

[Http://www.krug2000.ru](http://www.krug2000.ru)