5. *Тымчук А.И.* Метод Виолы-Джонса для распознавания объектов на изображении // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2017. – №6. – С. 63-68.

6. *Мищенкова Е.С.* Сравнительный анализ алгоритмов распознавания лиц // Вестник Волгоградского государственного университета. Серия 9. Исследования молодых ученых. – 2013. – № 11. – С. 74-76.

DOI: 10.25728/iccss.2022.52.62.022

Козлов А.Д., Нога Н.Л.

Метод усредненных коэффициентов влияния для формирования нечеткой базы знаний при оценке рисков информационной безопасности

Аннотация: Предложен метод, позволяющий сократить трудозатраты для формирования продукционных правил (нечеткой базы знаний) при определении рисков информационной безопасности с использованием методов нечеткой логики.

Ключевые слова: риски, информационная безопасность, нечеткая логика, продукционные правила, коэффициенты влияния

Широкое внедрение цифровизации в экономику связано с появлением новых вызовов и угроз. Особенно важно учитывать эти вызовы и угрозы в условиях жестких санкций. При эксплуатации информационных систем, особенно КИИ, требуется постоянно мониторить и оценивать риск информационной и кибербезопасности.

Принципы руководства и технологии обеспечения менеджмента риска определены нормативными документами [1, 2].

Методов оценки риска существует достаточно много. Все они имеют свои плюсы и минусы. У большинства из них присутствует существенный недостаток – они плохо работают в условиях неопределенности. В работе [3] предложена методика оценки риска с использованием методов нечеткой логики. Данная методика

позволяет осуществлять оценки поиска информационной безопасности по множеству параметров в условиях неочевидности взаимосвязи между параметрами.

Указанная методика подразумевает построение нечеткой базы знаний (совокупности продукционных правил). При оценке риска по шести и более параметрам количество этих правил может достигать нескольких тысяч. Что в свою очередь вызывает определенные трудности при расчетах рисков.

В дальнейшем данная база знаний может быть использована как для оценки риска средствами пакета Matlab [4], так и для последующей обработки методами регрессионного анализа [5] для определения наиболее критичных для оценки риска показателей.

Чтобы облегчить задачу создания нечеткой базы знаний на первичном этапе оценки риска авторы предлагают использовать метод усредненных коэффициентов влияния.

В общем виде риск можно представить как некоторую функцию R из (1), зависимую от N параметров.

$$R = R\,(y_1, \ldots, y_i, \ldots, y_N) \qquad (1)$$

Каждый параметр, включая риск, можно охарактеризовать как качественно, так и количественно. Количественное значение для удобства сравнения различных параметров лучше нормировать, т.е. чтобы их значения изменялись в пределах от 0 до 1. При этом в определенных границах терма качественное значение (значение лингвистической переменной) будет постоянным.

Значения лингвистической переменной могут быть разными, но они должны характеризовать переменную в пределах указанного терма. Например, лингвистическая переменная – уровень затрат может принимать значения: *низкий, средний, высокий, значительный.* Или лингвистическая переменная – уровень износа оборудования может принимать значения: *незначительный, низкий, средний, высокий, критический*.

Количество термов для разных переменных может быть различным. Чем их больше, тем точнее получается конечный результат, но усложняются вычисления. Будем считать в нашем примере количество нечетких переменных в терм-множестве для всех лингвистических переменных равным T. Пример терм-

множества для лингвистических переменных приведен в таблице 1, где Ly_{lt} представляет собой нечеткую переменную для y_i-й лингвистической переменной, а $[y'_{it}; y''_{it}]$ – границы значений терма.

Следует обратить внимание, что при использовании метода усредненных коэффициентов влияний необходимо, чтобы все параметры, по которым оценивается риск информационной безопасности, были однонаправленными, т.е. при увеличении уровня любого из параметров риск либо увеличивался, либо уменьшался.

Практически всегда любому параметру можно найти соответствующий антипод, при котором риск бы увеличивался с ростом уровня, а не уменьшался. Например, для лингвистической переменной *импортозамещение* (процент использования отечественного ПО) антиподом будет *использование зарубежного ПО*.

Таблица 1 – Терм-множество для лингвистических переменных

Лингвистические переменные	Нечеткие переменные	Границы терма
Риск, R	LR_1	$[R'_1; R''_1]$
	…	
	LR_t	$[R'_t; R''_t]$
	…	
	LR_T	$[R'_T; R''_T]$
y_1	Ly_{11}	$[y'_{11}; y''_{11}]$
	…	
	Ly_{1t}	$[y'_{1t}; y''_{1t}]$
	…	
	Ly_{1T}	$[y'_{1T}; y''_{1T}]$
…		
y_i	Ly_{i1}	$[y'_{i1}; y''_{i1}]$
	…	
	Ly_{it}	$[y'_{it}; y''_{it}]$
	…	
	Ly_{iT}	$[y'_{iT}; y''_{iT}]$
…		
y_N	Ly_{N1}	$[y'_{N1}; y''_{N1}]$

Лингвистические переменные	Нечеткие переменные	Границы терма
	…	
	Ly_{Nt}	$[y'_{Nt}; y''_{Nt}]$
	…	
	Ly_{NT}	$[y'_{NT}; y''_{NT}]$

На основе значений переменных в таблице 1 можно создать нечеткую базу (таблица 2), представляющую некоторую матрицу размерностью $M \times (N+1)$, где N – число показателей (лингвистических переменных), по которым рассчитывается риск, а M – количество строк в матрице, равное количеству вводимых продукционных правил.

Последний столбец представляет собой уровень риска.

Таблица 2 – Нечеткая база знаний, продукционные правила

y_1	…	y_i	…	y_N	R
Ly_{11}	…	Ly_{i1}	…	Ly_{N1}	LR_1
…					
Ly_{1T}	…	Ly_{iM}	…	Ly_{NM}	LR_M

Как правило, уровень риска в нечеткой базе определяется экспертным путем по каждой строке. Когда переменных много, а строк несколько тысяч, то такая работа становится очень трудоемкой, а подчас и совсем невыполнимой.

Авторами предложено провести экспертную оценку для каждой нечеткой переменной и указать усредненный коэффициент влияния K_{it} для каждого интервала значений (терма) (таблица 3).

Проведенные авторами исследования показали, что вполне достаточно, чтобы значения этих коэффициентов лежали в интервале от 0 до 10. Это позволяет получить значение уровня риска с приемлемой точностью.

Таблица 3 – Соответствие нечетких переменных усредненным коэффициентам влияния (для i-ой лингвистичекой переменной)

Лингвистическая переменная	Нечеткая переменная	Границы терма	Коэффициент влияния
y_i	Ly_{i1}	$[y'_{i1}; y''_{i1}]$	K_{i1}
	…		
	Ly_{it}	$[y'_{it}; y''_{it}]$	K_{it}
	…		
	Ly_{iT}	$[y'_{iT}; y''_{iT}]$	K_{iT}

Далее в таблице 2 заменим значения нечетких переменных на соответствующие значения коэффициентов влияния (таблица 4).

Таблица 4 – Нечеткая база знаний с коэффициентами влияния

	y_1	…	y_i	…	y_N	$\sum K$	Уровень риска, R
1	K_{11}	…	K_{i1}	…	K_{N1}	$\sum_{i=1}^{N} K_{i1}$	R_1
…	…						
M	K_{1M}	…	K_{iM}	…	K_{NM}	$\sum_{i=1}^{N} K_{iM}$	R_M

По каждой строке определяем суммарный коэффициент влияния $\sum K$ и находим максимум из этих сумм равный $\max\limits_{1 \le m \le M} \sum\limits_{i=1}^{N} K_{im}$.

Считаем, что этому максимуму соответствует и максимальное значение риска. Нечеткая переменная риска по каждой строке m ($1 \le m \le M$) будет определяться по формуле (2).

$$LR_m = \begin{cases} LR_T, & \text{если } \dfrac{\sum\limits_{i=1}^{N} K_{im}}{\max\limits_{1\le m\le M}\sum\limits_{i=1}^{N} K_{im}} > \dfrac{R'_T}{R''_T}; \\ LR_{T-1}, & \text{если } \dfrac{R'_T}{R''_T} \ge \dfrac{\sum\limits_{i=1}^{N} K_{im}}{\max\limits_{1\le m\le M}\sum\limits_{i=1}^{N} K_{im}} > \dfrac{R'_{T-1}}{R''_T}; \\ \ldots & \\ LR_1, & \text{если } \dfrac{R'_2}{R''_T} \ge \dfrac{\sum\limits_{i=1}^{N} K_{im}}{\max\limits_{1\le m\le M}\sum\limits_{i=1}^{N} K_{im}}. \end{cases} \quad (2)$$

Вывод

Предлагаемый метод позволяет существенно снизить трудоемкость по созданию нечеткой базы знаний при оценке рисков информационной или кибербезопасности, а соответственно сделать процедуру оценки рисков с использованием методов нечеткой логики более доступной.

Метод также легко реализуется в системах электронных таблиц (например, MS Excel) и пригоден для первичной оценки риска в различных информационных системах, включая сетевые структуры.

Литература:

1. ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2020. – 14 с.

2. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска. – М.: Стандартинформ, 2020. – 86 с.

3. *Козлов А.Д., Нога Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском. – 2019. – № 3. – С. 31-46.

4. *Штовба С.Д.* Проектирование нечетких систем средствами MATLAB. – М.: Горячая линия-Телеком, 2007. – 288 с.

5. *Kozlov A., Noga N.* Applying the Methods of Regression Analysis and Fuzzy Logic for Assessing the Information Security Risk of Complex Systems / Proceedings of the 14th International Conference "Management of Large-Scale System Development" (MLSD). – M.: IEEE, 2021. – URL: https://ieeexplore.ieee.org/document/9600245 (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.48.34.023

Абдулова Е.А.

Оценка критической информационной инфраструктуры: киберцели и оценка критичности

Аннотация: В работе рассмотрены кибер-цели и их характеристики, приведено сопоставление целей в физическом и кибер-пространствах и принципы их преобразования, рассмотрены уровни кибер-целей, показана разница в методологических подходах к оценке критичности и риска.

Ключевые слова: критическая информационная инфраструктура, киберсистема, кибер-цели, оценка риска, оценка критичности

Современное общество – это общество, основанное на знаниях, которое в значительной степени полагается на технологии для выполнения или поддержки выполнения задач или функций. В результате современное общество гораздо более уязвимо даже по сравнению с началом века.

Масштабы уязвимости обусловлены тем, что очень много выполняемых операций в какой-то момент поддерживается вводом, хранением и поиском данных и информации во взаимосвязанной сети жестких дисков и серверов данных. Более того, в каждом из этих моментов существует возможность кражи информации, обхода защит, манипулирования или диверсии. При этом не учитывается риск, связанный с непреднамеренными инцидентами, связанными с человеческим фактором, системными сбоями, несовместимостью или другими неожиданными проблемами, а также «стихийными бедствиями». Все больше и больше экспертов по безопасности