УДК 004.056
ГРНТИ 78.25.33.37.19

МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ КОМПЬЮТЕРНЫХ АТАК

Д.В. ГОЛОВАНОВ
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
О.Н. ЕЛЬЦОВ, кандидат технических наук, старший научный сотрудник
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
Э.Б. ХАНОВ, кандидат технических наук
ООО «СТЦ» (г. Санкт-Петербург)

В статье представлена методика расчета значения показателя защищенности элементов автоматизированных систем от компьютерных атак, определяемого на основе оценки риска информационной безопасности автоматизированных систем, учитывающего вероятности возникновения угрозы, реализации уязвимости и ценность информационного ресурса автоматизированных систем. Методика основана на использовании математического аппарата нечетких продукционных когнитивных карт. Приводится пример расчета указанного показателя при реализации компьютерной атаки на информационный ресурс, размещенный на сервере локальной вычислительной сети автоматизированной системы.

Ключевые слова: компьютерная атака, нечеткие продукционные когнитивные карты, фаззификация, дефаззификация.

METHODOLOGY FOR ASSESSING THE AUTOMATED SYSTEMS PROTECTION AGAINST COMPUTER ATTACKS

D.V. GOLOVANOV
MESC AF «N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh)
O.N. ELTSOV, Candidate of Technical sciences, Senior Researcher
MESC AF «N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh)
`E.B. KHANOV , Candidate of Technical sciences
OOO «STC» (Saint Petersburg)

The article presents the method of calculating the value of the protection elements automated systems from computer attacks, based on risk assessment information security automated systems, taking into account the threat realization vulnerability occurrence probability and value of the information resource automated systems. The method is based on the use of the mathematical apparatus of fuzzy production cognitive maps. An example of calculating this indicator when implementing a computer attack on an information resource located on the server of the local computer network of an automated system is given.

Keywords: computer attack, fuzzy production cognitive maps, fuzzification, defuzzification.

Введение. В настоящее время разработка и использование автоматизированных систем (АС) различного назначения находит все большее применение в системах управления, связи, производства и научных исследований. При этом данные АС могут быть подвержены компьютерным атакам (КА) различных типов на используемый в них информационный ресурс. Основным направлением постоянного совершенствования АС является повышение защищенности их информационного ресурса от КА. Оценка защищенности АС от КА является одной из задач, являющейся приоритетной при их создании.

Актуальность. При создании АС различного назначения требования к их защищенности от КА должны задаваться в тактико-техническом (техническом) задании (ТТЗ (ТЗ)) на их разработку. На сегодняшний день данные требования задаются, как правило, на качественном

СОДЕРЖАНИЕ

уровне (класс системы антивирусной защиты, класс системы обнаружения вторжений и др.), причем выбор средств защиты от КА определяется не характером существующих угроз и возможностью их реакции, а уровнем конфиденциальности обрабатываемой в АС информации. Численные значения показателя защищенности АС от КА не задаются, что приводит к необоснованно завышенным требованиям к средствам защиты, с одной стороны, и сложностью оценки комплексной защищенности АС от КА при проведении их испытаний. Вышесказанное определяет актуальность разработки методики оценки защищённости АС от КА, позволяющей определять численные значения показателя защищенности.

Настоящая методика устанавливает порядок подготовки исходных данных и их обработки с целью определения показателя защищенности АС от КА.

В качестве математического аппарата при оценке защищенности АС от КА используется аппарат нечетких множеств и продукционных когнитивных карт (НПКК) [2–5].

НПКК называется ориентированный граф $K=\{C,F\}$, где $C=\left\{C_i : i=\overline{1,n}\right\}$ задается множеством узлов (концептов) ориентированного графа, а $F=\left\{F_{ij} : i,j=\overline{1,n}\right\}$ задается множеством связей между концептами. При этом совокупность значений лингвистической переменной X_i состояния каждого концепта C_i составляет терм-множество $\{T_{i1},T_{i2},\ldots,T_{im}\}$ этой переменной, подмножества (термы) которого $T_{ik}\ (k=1,2,\ldots,m)$ задаются функциями принадлежности: $T_{ik}=\left\{\left(\mu_{ik}(X_i)/X_i\right)\right\}$, $\mu_{ik}: X_i\to[0,1]$, где $X_i\in[0,1]$.

Задание функций принадлежности термов T_{ik} лингвистической переменной X_i осуществляется в соответствии с нижеприведенными правилами [6].

Пусть $T=\left\{T_i : i=\overline{1,m}\right\}$ – базовое терм-множество лингвистической переменной $\langle\beta,T,X\rangle$, тройка $\left\langle T_i, X, \tilde{C}_i\right\rangle$ – соответствующая терму $T_i\in T$ нечеткая переменная, C_i – носитель нечеткого множества $\tilde{C}_i=\left\{\left\langle\mu_{C_i}(x)/x\right\rangle\right\}$ на X ($X\subseteq R_i$, где R_i – действительная ось) с функцией принадлежности $\mu_{C_i}(x)$. Упорядочим множество T в соответствии с выражением $(\forall T_i\in T)(\forall T_j\in T)\left(i>j\Leftrightarrow(\exists x\in C_i)(\forall y\in C_j)(x>y)\right)$, при котором терм, имеющий носитель нечеткого множества, расположенный левее на числовой оси, имеет меньший номер. Присвоив $\inf X$ значение x_1, а $\sup X$ значение x_2, получим, что терм-множество лингвистической переменной должно удовлетворять следующим условиям.

Функции принадлежности термов с минимальными и максимальными номерами (термы T_1 и T_5 на рисунке 1а) не могут иметь вид колоколообразных кривых

$$\mu_{C_1}(x_1)=1,\quad \mu_{C_m}(x_2)=1. \tag{1}$$

В базовом множестве термов T запрещается использование определенных пар термов (типа T_1 и T_2, T_2 и T_3), представленных на рисунке 1а. В первом случае (термы T_1 и T_2) отсутствует естественное разграничение понятий, представленных соседними термами, во втором случае (термы T_2 и T_3) образуются такие участки (типа $[a,b]$) области определения, которым не поставлено в соответствие какое-либо понятие

$$\left(\forall T_i\in T\setminus\{T_m\}\right)\left(0<\sup_{x\in X}\mu_{C_i\cap C_{i+1}}(x)<1\right). \tag{2}$$

СОДЕРЖАНИЕ

Данное условие запрещает наличие в множестве T термов типа T_4 (рисунок 1а), поскольку каждое понятие имеет хоты бы один типичный объект, обозначаемый этим понятием

$$(\forall T_i \in T)(\exists x \in X)\left(\mu_{C_i}(x) = 1\right). \quad (3)$$

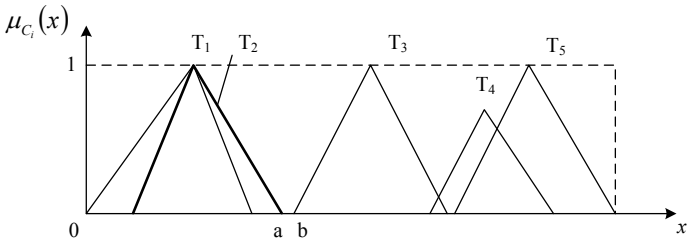
Область определения X должна быть ограничена конечным множеством точек

$$(\forall \beta)(\exists x_1 \in R_i)(\exists x_2 \in R_i)\left((\forall x \in X)(x_1 < x < x_2)\right). \quad (4)$$

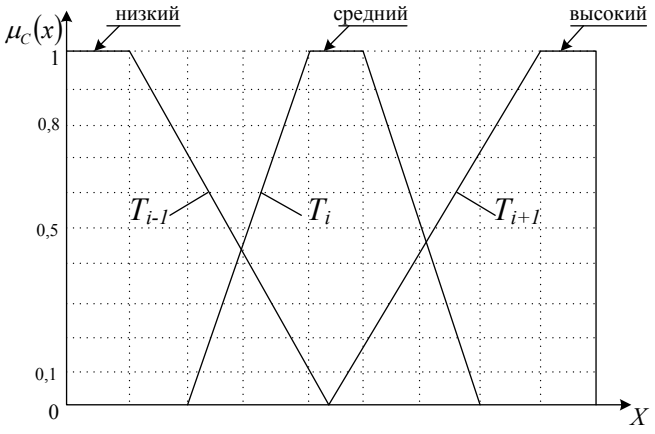
Термы, примыкающие к терму T_i, не должны иметь более одной точки при их пересечении (рисунок 1б)

$$(\forall i \in I, i \neq 1 \wedge i \neq m)\left(card(T_{i-1} \cap T_{i+1}) = 0 \vee ((card(T_{i-1} \cap T_{i+1}) = 1) \wedge \mu(T_{i-1} \cap T_{i+1}) = 0)\right), \quad (5)$$

где $card\, X$ – мощность множества X.



а) варианты некорректного распределения термов



б) ограничение на функции принадлежности рассматриваемых термов лингвистической переменной

Рисунок 1 – Условия, которым должно удовлетворять терм-множество лингвистической переменной X

Данное ограничение позволяет уменьшить количество продукционных правил максимум до 4 и при логическом выводе использовать таблицы решений размерностью максимум 2x2.

Вычислительный процесс на НПКК состоит в выполнении следующей последовательности, представленной на рисунке 2, и включающей в себя пять действий для каждой пары концептов $C_j \to C_{j+1} \to \cdots$, следующей за предыдущей на пути следования в НПКК.

СОДЕРЖАНИЕ

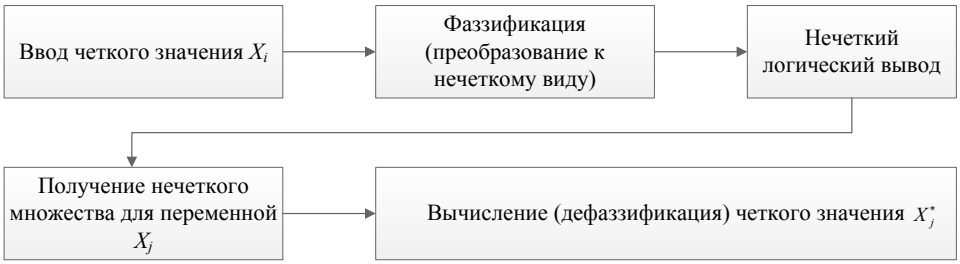


Рисунок 2 – Организация вычислительного процесса на НПКК

Взаимное влияние концептов $C_i \to C_j$ определяется с использованием нечетких продукционных правил, задаваемых в виде матриц риска [1] (рисунок 3). Переменные X_i и X_j состояния концептов C_i и C_j принимают следующие нечеткие значения из терм-множества $T = \{(L)$ Низкое, (M) Среднее, (MH)Выше_среднего, (H) Высокое, (VH) Очень_высокое$\}$, которые задаются с помощью соответствующих функций принадлежности.

X_i \ X_j	L	M	MH	H	VH
VH	MH	H	H	H	VH
H	M	MH	H	H	H
MH	M	M	MH	MH	H
M	L	M	M	M	MH
L	L	L	L	M	M

Рисунок 3 – Вид матрицы риска

Основным недостатком применения НПКК является значительное число продукционных правил, используемых при определении нечеткого значения выходной переменной состояния концепта. Так при двух предшествующих концептах C_i и C_j, описываемых соответствующими переменными X_i и X_j, для определения состояния концепта C_k, описываемого выходной переменной X_k (рисунок 4), имеем $k = 2$ (количество предшествующих концептов) и $M=5$ (число термов в множестве T) общее число правил $M^2 = 25$:

$П_1$: Если $X_i = VH$ и $X_j = L$, то $X_k = MH$;

…

$П_{25}$: Если $X_i = L$ и $X_j = VH$, то $X_k = M$.

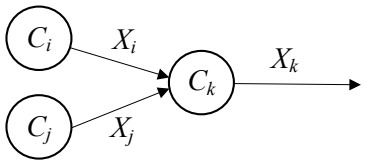


Рисунок 4 – Определение состояния концепта C_k, описываемого выходной переменной X_k

СОДЕРЖАНИЕ

Однако, введение дополнительного ограничения (5) на функции принадлежности термов позволяет оставлять активными не более четырех правил.

В качестве показателя защищенности АС от КА используется вероятность непоражения локальной вычислительной сети (ЛВС) АС $P_{непор.}$, рассчитываемая на основе определения риска информационной безопасности АС при КА [1]:

$P_{непор.} = 1 - П_{риск}$, $П_{риск} = P_{угр} \cdot P_{уязв} \cdot S_{Црес.}$,

где $P_{угр}$ – вероятность возникновения угрозы КА; $P_{уязв}$ – вероятность существования уязвимости АС; $S_{Црес}$ – ценность информационного ресурса АС.

Методика расчета $П_{риск}$ включает следующие шаги.

Шаг 1. Построение НПКК для рассматриваемой КА на элементы АС. Пример построения НПКК приведен на рисунке 5, где C_i – наименование концепта, X_i – наименование переменной состояния концепта.

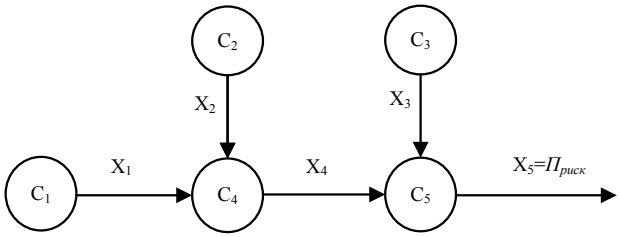


Рисунок 5 – Пример построения НПКК

Шаг 2. Задание термов переменных состояния X в виде лингвистических переменных, которые могут принимать значения: L (Low) – Низкий уровень; M (Medium) – Средний уровень; MH (Medium High) – Уровень выше среднего; H (High) – Высокий уровень; VH (Very High) – Очень высокий уровень.

Построение функций принадлежности для введенных термов.

Шаг 3. Построение совокупности нечетких продукционных правил и матрицы риска, которые описывают состояние концепта C_i в виде:

$П_1$: Если $X_1 = L$ и $X_2 = L$, то $X_4 = L$;

…

$П_{25}$: Если $X_1 = VH$ и $X_2 = VH$, то $X_4 = VH$.

Задание коэффициента определенности правил для построенной матрицы риска.

Пример построения матрицы риска представлен на рисунке 6.

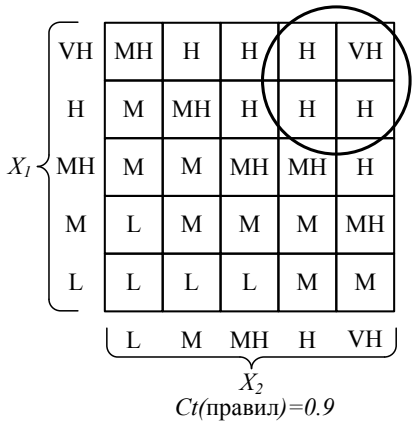


Рисунок 6 – Матрица риска

СОДЕРЖАНИЕ

Шаг 4. Задание экспертно или экспериментально полученных четких значений входных переменных состояния концептов и построение схемы нечеткого логического вывода (рисунок 7).

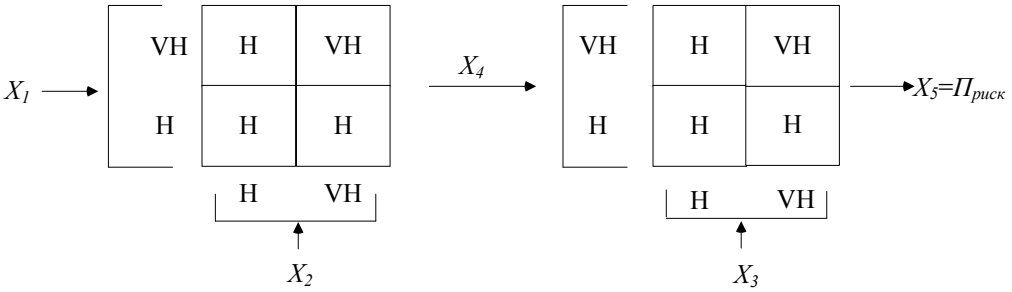


Рисунок 7 – Пример нечеткого логического вывода

Шаг 5. Нахождение значений промежуточных переменных состояния концептов и переменной риска по алгоритму, представленному на рисунке 8.

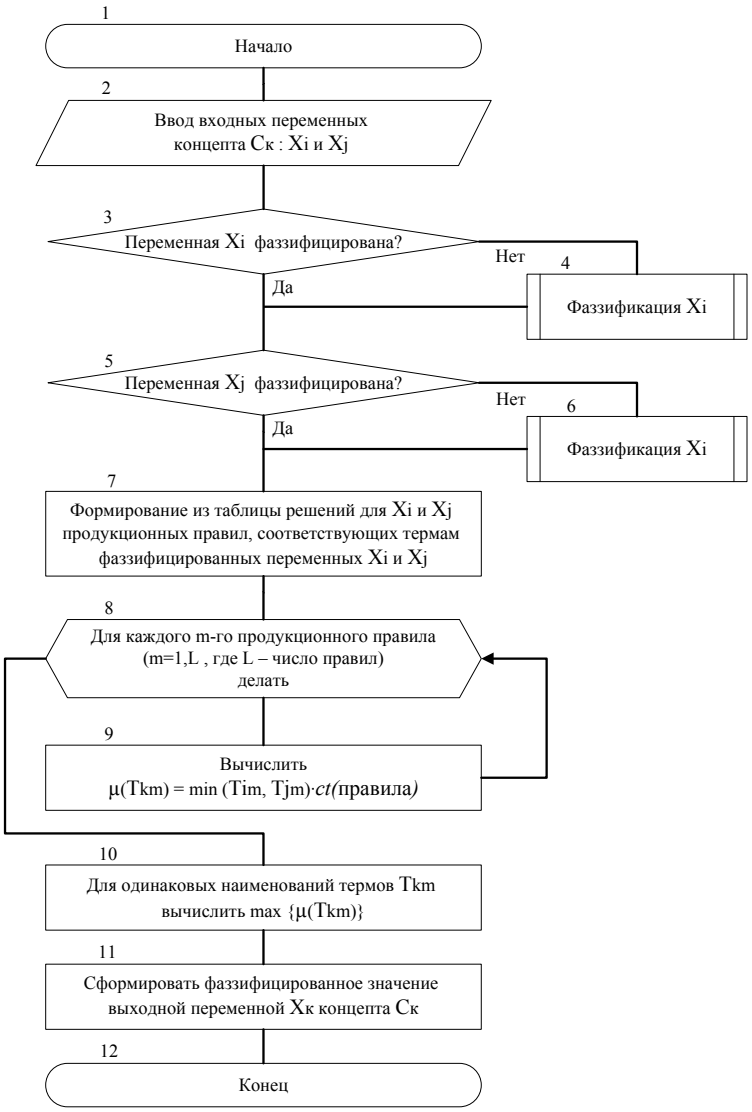


Рисунок 8 – Алгоритм вычисления промежуточных переменных состояния концептов и переменной риска (алгоритм логического вывода)

СОДЕРЖАНИЕ

Шаг 6. Вычисление значения выходной переменной риска методом взвешенного среднего:

$$X_R = П_{риск} = \frac{\sum_{i=1}^{m} \alpha_i X_{Ri}^0}{\sum_{i=1}^{m} \alpha_i}, \quad (6)$$

где $X_{Ri}^0 \left(i = 1, 2, \ldots, m\right)$ – центральные значения термов функций принадлежности (m – количество термов лингвистической переменной X_R), α_i – уровень активности i-го правила, определяющий значение степени принадлежности i-го терма переменной X_R.

В качестве примера расчета значения показателя $П_{риск}$ рассматривается воздействие КА на некоторый информационный ресурс, который размещен на сервере ЛВС АС. Отсутствие обновления программного обеспечения антивирусной защиты на сервере ЛВС АС рассматривается в качестве уязвимости.

Шаг 1. Построение НПКК для рассматриваемой КА на элементы АС (рисунок 5), где: C_1 – угроза КА; C_2 – уязвимость АС; C_3 – информационный ресурс на сервере ЛВС АС; C_4 – реализация КА; C_5 – потенциальный ущерб от реализации КА; X_1 – вероятность возникновения угрозы КА; X_2 – вероятность наличия уязвимости АС; X_3 – ценность информационного ресурса на сервере ЛВС АС; X_4 – вероятность успешной реализации КА; $X_5 = П_{риск}$ – значение ожидаемого потенциального ущерба от воздействия КА.

Шаг 2. Каждая из этих переменных состояния является лингвистической переменной, которая принимает одно из значений, определенных на шаге 2 методики. Каждое из этих нечетких подмножеств задается на шаге 2 собственной функцией принадлежности (с учетом введённых ограничений (1) – (5)), построенной экспертным путем. Вид функций принадлежности показан на рисунке 9.

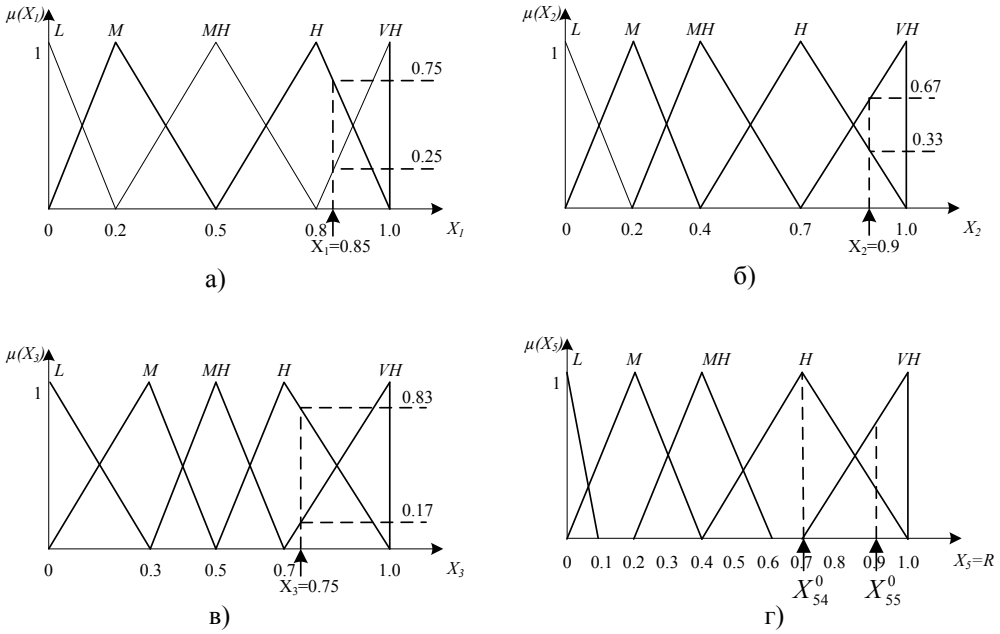


Рисунок 9 – Вид функций принадлежности рассматриваемых термов лингвистических переменных нечетких множеств: а) (C_1) – угроза КА, б) (C_2) – уязвимость АС, в) (C_3) – ценность информационного ресурса, г) (C_5) – потенциальный ущерб от реализации КА

СОДЕРЖАНИЕ

Шаг 3. Построение совокупности нечетких продукционных правил для концептов C_4 и C_5, а также матриц риска, которые описывают состояние данных концептов:

концепт C_4:

$П_1$: Если $X_1 = L$ и $X_2 = L$, то $X_4 = L$;

…

$П_{25}$: Если $X_1 = VH$ и $X_2 = VH$, то $X_4 = VH$.

концепт C_5:

$П_{26}$: Если $X_3 = L$ и $X_4 = L$, то $X_5 = L$;

…

$П_{50}$: Если $X_3 = VH$ и $X_4 = VH$, то $X_5 = VH$.

Коэффициенты определенности правил для матриц риска приняты равными 1.

Матрицы риска, описывающие состояние концептов C_4 и C_5, приведены на рисунке 10.

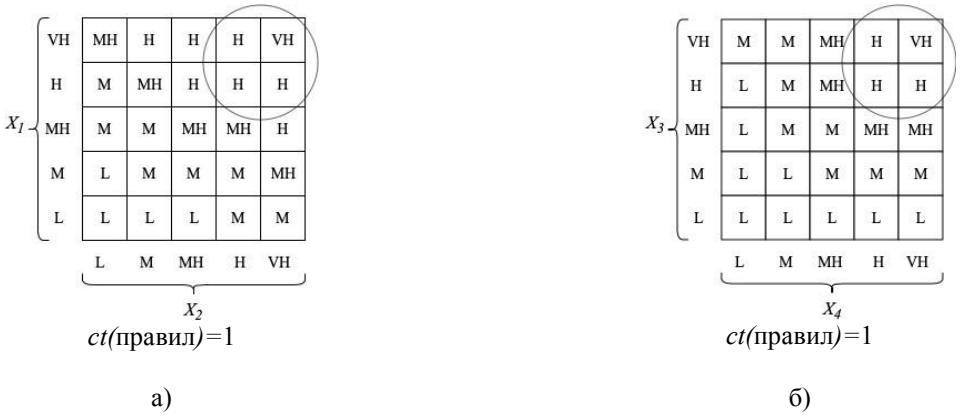


Рисунок 10 – Матрицы риска, описывающие состояние концептов: а) реализация угрозы (концепт C_4), б) потенциальный ущерб (концепт C_5)

Предположим, что три основных риск-фактора потенциальной угрозы, являющихся входными переменными для НПКК, принимают следующие значения: $X_1^* = 0,85$, $X_2^* = 0,9$, $X_3^* = 0,75$. Используя функции принадлежности нечетких множеств для рассматриваемых входных переменных НПКК (рисунок 9), а также матрицы риска, которые описывают состояние концептов C_4 и C_5 (рисунок 10), определяем, что переменные X_1, X_2, X_3, X_4 принимают только значения H и VH и активными остаются только восемь правил, которые соответствуют выделенным на рисунке 10 блокам из четырех соседних ячеек в матрицах рисков.

Шаг 4. Для принятых значений входных переменных строим схему нечеткого логического вывода (рисунок 11).

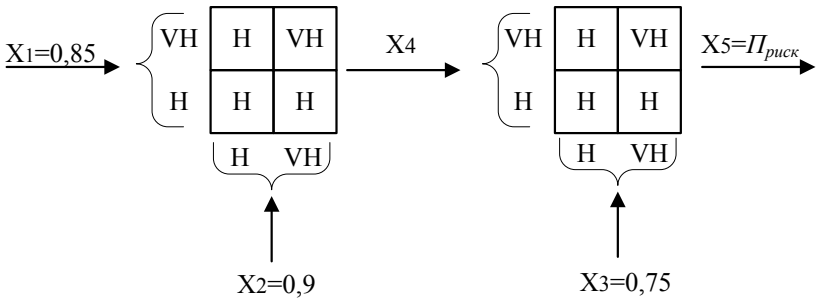


Рисунок 11 – Схема нечеткого логического вывода

СОДЕРЖАНИЕ

Шаг 5. Рассчитаем значение промежуточной переменной X_4 состояния концепта C_4 (рисунок 10а) по алгоритму, который представлен на рисунке 8.

Если $X_1 = H$ и $X_2 = H$, то $X_4 = H$;

Если $X_1 = H$ и $X_2 = VH$, то $X_4 = H$;

Если $X_1 = VH$ и $X_2 = H$, то $X_4 = H$;

Если $X_1 = VH$ и $X_2 = VH$, то $X_4 = VH$.

Значения функций принадлежности $\mu(x_1^*)$ и $\mu(x_2^*)$ (рисунок 9 а, б) соответственно равны $\langle\langle 0,75 / H\rangle, \langle 0,25 / VH\rangle\rangle$ и $\langle\langle 0,33 / H\rangle, \langle 0,67 / VH\rangle\rangle$.

Далее в соответствии с алгоритмом (рисунок 8) для каждого правила применяется операция MIN:

правило 1: min (0,75; 0,33) = 0,33;
правило 2: min (0,75; 0,67) = 0,67;
правило 3: min (0,25; 0,33) = 0,25;
правило 4: min (0,25; 0,67) = 0,25.

С учетом значения коэффициента определенности правил для матрицы риска (рисунок 10а) полученные значения не изменятся.

Для одинаковых наименований термов продукционных правил, стоящих в заключении продукций (H (Высокий уровень) и VH (Очень высокий уровень)) применяется операция MAX:

– max (0,33; 0,67; 0,25) = 0,67;
– max (0,25) = 0,25.

Переменная X_4 состояния концепта C_4 следовательно принимает следующее нечеткое значение $\langle\langle 0,67 / H\rangle, \langle 0,25 / VH\rangle\rangle$.

Таким же образом вычисляется значение переменной X_5 состояния концепта C_5, которое составит $\langle\langle 0,67 / H\rangle, \langle 0,17 / VH\rangle\rangle$.

Шаг 6. Применяя формулу (6) для следующих исходных данных: α_1 (Очень высокий уровень)=0,17; α_2 (Высокий уровень)=0,67; X^0_{55}(Очень высокий уровень)=0,91; X^0_{54}(Высокий уровень)=0,7 (рисунок 9 г), вычисляется дефаззифицированное («четкое») значение переменной X_5^*=0,74. Следовательно, искомое значение потенциального ущерба $X_5 = П_{риск} = 0,74$.

Вычисляем значение показателя $P_{непор} = 1 - П_{риск}$. Оно составит 0,26.

Выводы. Представленная методика расчета показателя защищенности автоматизированных систем от компьютерных атак основана на использовании математического аппарата нечетких продукционных когнитивных карт, в основе построения которых лежит описание взаимодействия между концептами с использованием совокупности нечетких продукционных правил и является развитием подхода, предложенного в [1]. В отличие от существующих подходов использования НПКК введено новое ограничение на построение функций принадлежности термов лингвистических переменных, характеризующих процесс КА (угроза, уязвимость, ценность ресурса, потенциальный ущерб), позволивших уменьшить временную сложность алгоритма нечеткого логического вывода на НПКК и устранить потенциальную противоречивость данных при построении функций принадлежности. Введение коэффициента определенности продукционных правил для матриц риска позволило снизить влияние субъективного мнения экспертов на правильность их построения.

СПИСОК ЛИТЕРАТУРЫ

1. Васильев В.И., Вульфин А.М., Гузаиров М.Б. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. 2018. Т. 24. № 4. С. 266–272.

СОДЕРЖАНИЕ

2. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: ДМ К Пресс, 2005. 384 с.

3. Борисов В.В., Федулов А.С., Устиненков Е.С. Анализ динамики состояния сложных систем на основе обобщенных нечетких продукционных когнитивных карт // Нейрокомпьютеры: разработка, применение. 2007. № 1. С. 17–23.

4. Гузаиров М.Б., Васильев В.И., Кудрявцева Р.Т. Системный анализ информационных рисков с применением нечетких когнитивных карт // Инфокоммуникационные технологии. 2007. Т. 5. № 4. С. 42–48.

5. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. Изд. 2-е, стереотип. М.: Горячая линия – Телеком, 2012. 284 с.

6. Мелихов А.Н., Бернштейн Л.С., Коровин С.Я. Ситуационные советующие системы с нечеткой логикой. М.: Наука, 1990. 272 с.

REFERENCES

1. Vasil'ev V.I., Vul'fin A.M., Guzairov M.B. Ocenka riskov informacionnoj bezopasnosti s ispol'zovaniem nechetkih produkcionnyh kognitivnyh kart // Informacionnye tehnologii. 2018. T. 24. № 4. pp. 266–272.

2. Petrenko S.A., Simonov S.V. Upravlenie informacionnymi riskami. `Ekonomicheski opravdannaya bezopasnost'. M.: DM K Press, 2005. 384 p.

3. Borisov V.V., Fedulov A.S., Ustinenkov E.S. Analiz dinamiki sostoyaniya slozhnyh sistem na osnove obobschennyh nechetkih produkcionnyh kognitivnyh kart // Nejrokomp'yutery: razrabotka, primenenie. 2007. № 1. pp. 17–23.

4. Guzairov M.B., Vasil'ev V.I., Kudryavceva R.T. Sistemnyj analiz informacionnyh riskov s primeneniem nechetkih kognitivnyh kart // Infokommunikacionnye tehnologii. 2007. T. 5. № 4. pp. 42–48.

5. Borisov V.V., Kruglov V.V., Fedulov A.S. Nechetkie modeli i seti. Izd. 2-e, stereotip. M.: Goryachaya liniya - Telekom, 2012. 284 p.

6. Melihov A.N., Bernshtejn L.S., Korovin S.Ya. Situacionnye sovetuyuschie sistemy s nechetkoj logikoj. M.: Nauka, 1990. 272 p.

Голованов Дмитрий Викторович, старший научный сотрудник отдела научно-исследовательского испытательного института (радиоэлектронной борьбы), Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А. dmitry1801@bk.ru.

Ельцов Олег Николаевич, кандидат технических наук, старший научный сотрудник, главный научный сотрудник научно-исследовательского испытательного института (радиоэлектронной борьбы), Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А.

Ханов Эдуард Борисович, кандидат технических наук, заместитель директора, ООО «СТЦ», Россия, 195220, г. Санкт-Петербург, ул. Гжатская, 21, hansonpiter@yandex.ru.