Хмельницького національного університету. Технічні науки. – 2009. – № 5. – С. 116-130.

4. Восприятие и его свойства. Виды восприятия (часть 1) // http://psylesson.ru/node/33, http://coma.su/content/ view/99/30/.

5. Восприятие // http://add.net.ru/dictionary/vospriyatie.html

6. Сознание. Восприятие. Бесплатное обучение // http://www.ai-trening.ru/soznanie.htm.

7. Орнатский П.П. Теоретические основы информационно-измерительной техники. – К.: Вища шк., 1976. – 432 с.

8. Свойства восприятия // http://psyznaiyka.net/view-vospriyatie.html?id=svoistva-vospriyatiya.

9. Мир словарей // http://mirslovarei.com/content_psy/VOSPRIJATIE-1218.html].

10. Восприятие и его свойства. Виды восприятия (часть 2) // http://psylesson.ru/ node/58.

11. Татур В.Ю. О Диалектике и Триалектике // http://www.trinitas.ru/rus/doc/0216/ 002a/02160000.htm.

12. Метод // http://ru.wikipedia.org/wiki/Метод.

13. Массивы информации. Физические эффекты // http://www.metodolog.ru/00751/ 00751.html.

14. Орнатский П.П. Общенаучные методы познания. – К.: О-во «Знание», 1984. – 35 с.

15. Операции в языках программирования. Операции сравнения. http://prg.vede-nin.ru/4.php.

Надійшла 7.12.2009 р.

УДК 004.492.3

Р.П. ГРАФОВ, Р.О. ЛАДУНЕЦ, С.О. ШЕПАРСКИЙ
Хмельницкий национальный университет

РАЗРАБОТКА МЕТОДА ПРИНЯТИЯ РЕШЕНИЯ НА ОСНОВЕ НЕЧЕТКОГО ЛОГИЧЕСКОГО ВЫВОДА И ЗНАНИЙ ЭКСПЕРТА

У роботі запропоновано новий підхід до проблеми прийняття рішень в системах, які характеризуються не чіткою інформацією про протікання процесів і методів реалізації на основі механізма нечіткого логічно-го виводу і знань експертів, наведено методику використання на прикладі пошуку шкідливого програмного забезпечення в обчислювальних системах. Отримані результати можуть бути використані розробкичиками антивірусного діагностування.

In work new approach is offered to the problem of decision-making in the systems, characterized not-clear information about flowings processes and method of realization on basis mechanism of unclear logichesko-go conclusion and knowledges of experts, the method of the use is resulted on the example of search of the vredonosnogo programm-nogo providing in the computer systems. Can be drawn on got results razrabot-chikami of the anti-virus diagnosing.

Ключевые слова: Нечетная логика; нечёткие множества; нечеткий вывод; лингвистическая переменная; фаззификация; дефаззификация; база знаний;

Введение

Известно, что при построении различных систем, характеризующихся нечеткой информацией о протекающих процессах, возникает ряд проблем, связанных с трудностью формализации решаемых задач. В связи с этим существует ряд задач, решение которых довольно проблематично. Например: проведения быстрого моделирования сложных динамических систем и их сравнительный анализ с заданной степенью точности; проведение нечеткой формализации критериев оценки и сравнения; оперирование критериями "большинство", "возможно", преимущественно" и т.д.; проведение качественных оценок как входных данных, так и выходных результатов. Перечисленные задачи относятся к классу fuzzy (нечетких) систем и решаются методами нечеткой логики [1].Для решения задач нечеткими методами разработано в настоящее время ряд программных и аппаратных средств.

Рассмотрим некоторые из них:

- CubiCalc 2.0 RTC – одна из мощных коммерческих экспертных систем на основе нечеткой логики, позволяющая создавать собственные прикладные экспертные системы;
- RuleMaker – программа автоматического извлечения нечетких правил из входных данных;
- FuziCalc – электронная таблица с нечеткими полями, позволяющая делать быстрые оценки при неточных данных без накопления погрешности;
- OWL – пакет, содержащий исходные тексты всех известных видов нейронных сетей, нечеткой ассоциативной памяти и т.д.

Основными потребителями нечеткой логики являются банкиры и финансисты, а также специалисты в области политического и экономического анализа. Без применения нечеткой логики немыслимы современные ситуационные центры руководителей, где принимаются ключевые политические решения и моделируются разные кризисные ситуации.

Сегодня элементы нечеткой логики можно найти в десятках промышленных изделий – от систем управления электропоездами и боевыми вертолетами до пылесосов и стиральных машин. В качестве примера известных микроконтроллеров, использующих нечеткую логику можно назвать 68HC11, 68HC12 фирмы "Motorola", MCS-96 фирмы "Intel", а также некоторые другие.

Постановка задачи и ее решение

В данной работе рассматривается задача принятия решения о наличии вредоносных программных продуктов (ВП) в информациионных системах. Анализ современных существующих средств принятия решения относительно ВП содержит в себе зачатки искусственного интеллекта и формирует решение относительно ВП на основе тонкого анализа данных или системы не по жестко заданному набору параметров, а по результатам многосторонней оценки всей совокупности параметров в целом, с присвоением каждому из событий веса “потенциальной вредоносности” и расчетом общего результата.Однако им присущи ряд недостатков [2].

В отличие от существующих методов поиска и идентификации неизвестных ВП, разработан подход который сочетает элементы технологии поиска аномалий и экспертных систем. Для его реализации использован математический аппарат нечеткой логики (НЛ), который в последнее время эффективно используется для решения ряда задач со слабоструктурированными данными

Механизмы нечеткой логики позволяют строить модели предметной области, адекватные реальным, на основе семантического описания объекта исследования и знаний экспертов, что на много проще разработки сложных математических моделей. При этом, с помощью специализированных методов обработки нечисловой информации обеспечиваются достаточно точные решения.

Рассмотрим некоторые понятия теории нечетких множеств, необходимые для дальнейшего изложения. Нечеткое множество А определяется как множество упорядоченных пар (кортежей) вида: (μ_A (u),u), где μ_A (u) – степень принадлежности элемента множества $u \in U$ нечеткому множеству А, u- является элементом универсального множества U. Следовательно,

$$A = \{\mu_A(u_i), u_i\};\ i=1,\ldots,k. \qquad (1)$$

Степень принадлежности определяется некоторым действительным числом из интервала [0,1]. Функция принадлежности позволяют для произвольного элемента универсального множества вычислить степень принадлежности его нечеткому множеству.

Нечеткое множество связано с лингвистической переменной и их нечеткими переменными, которые позволяют определить ее значение с помощью функции принадлежности.

Например, лингвистическая переменная: “ Категория программы “. Ее значениями могут быть нечеткие переменные, образуемые с помощью модификаторов (или, не, очень и др) в виде: не опасная, немного опасная, очень опасная и т.д. Функция принадлежности, если она задана, позволяет оценить далее лингвистическую переменную. Применительно к высказываниям в нечеткой логике применимы функции алгебры логики, которые имеют не численные, а лингвистические значения истинности, которые адекватны степени принадлежности.

Основой семантического описания исследуемой модели является выбор и анализ входных и выходных лингвистических переменных, а также их значений, которые получаются с помощью мониторинга и экспертных оценок. Лингвистическая переменная считается заданной, если для нее определены: наименование N, универсальное множество А (область рассуждений), базовое терм – множество Т (нечеткие переменные- значения лингвистической переменной), функция принадлежности μ и семантические процедуры преобразования (модификации) переменных термов лингвистической переменной.

Основой исследования нечетких моделей является механизм нечеткого логического вывода, который содержит следующие этапы [3,4]:

- фаззификация;
- нечеткий логический вывод;
- дефаззификация.

Фаззификация-процесс перевода входных четких величин, полученных на основе экспертного анализа исследуемого объекта , в нечеткие переменные. На этапе логического вывода используются нечеткие продукционные (if – then) правила, заложенные в базу знаний, для преобразования нечетких входных данных после фаззификации в выходные, которые также носят нечеткий характер. Дефаззификация-композиция и приведение к четкости нечетких множеств логического вывода для принятия решения.

Механизм нечеткого вывода в данной работе реализуется с помощью нечеткой модели, которая основана на семантическом описании и анализе множества возможных состояний ВП в течении жизненного цикла.

$$НМ \rightarrow \{(X, Y, V, Z)\}, \qquad (2)$$

где X – универсальное множество входных состояний $x \in X$, принимающих ВП в системе пользователя (функции и действия, используемые ВП для проникновения в систему); Y – универсальное множество выходных состояний $y \in Y$ (компоненты, которые потенциально могу быть подвержены действию ВП); V – множество нечетких отношений (x_i, y_j) , характеризующие связи между элементами множеств X и Y; Z –характеристические параметры отношений.

Так как любая ВП представляет собой некоторый файл, реализующий в операционной системе множество различных функций и действий, то для удобства анализа множество состояний ВП представлено в виде трех основных этапов идентификации ВП, которые образуют один трехуровневый жизненный цикл (ЖЦ): проникновение в систему, активизация и деструктивные действия [5].

В связи с этим на множествах X, Y определены нечеткие множества ($X^п$, $X^а$, $X^д$) и ($Y^п$, $Y^а$, $Y^д$)

входных и выходных состояний ВП, соответствующие этапам ЖЦ. В соответствии с (1) множества $X^{п}$, $X^{а}$, $X^{д}$ определяются, как множества упорядоченных пар: $X^{п} = \{\mu_{X^{п}}(x), x\}$; $X^{а} = \{\mu_{X^{а}}(x), x\}$ $X^{д} = \{\mu_{X^{д}}(x), x\}$, где $\mu_{X^{п}}(x)$, $\mu_{X^{а}}(x)$ и $\mu_{X^{д}}(x)$ – функции принадлежности, указывающие на степень принадлежности элемента x множества X множествам $X^{п}$, $X^{а}$, $X^{д}$ соответственно. Значения функции принадлежности определяются на интервале [0,1]. Область значений элементов множеств X, Y выбирается экспертом.

Множества ($Y^{п}$, $Y^{а}$, $Y^{д}$) представляются в виде множеств отношений (x_i, y_j):

$Y^{п} = \{ (x_i, y_j, \mu_V (x_i, y_j) \}$; $Y^{а} = \{ (x_i, y_j, \mu_V (x_i, y_j) \}$; $Y^{д} = \{ (x_i, y_j, \mu_V (x_i, y_j) \}$,где выражения $\mu_{Y^{п}}(x_i, y_j)$, $\mu_{Y^{а}}(x_i, y_j)$ и $\mu_{Y^{д}}(x_i, y_j)$ являются функциями принадлежности нечетких отношений (x_i, y_j) множествам $Y^{п}$, $Y^{а}$, $Y^{д}$ соответственно, которые определяют степень уверенности в существовании причинно – следственной связи (x_i, y_j). Нечеткие отношения множеств $Y^{п}$, $Y^{а}$, $Y^{д}$ представляются соответствующими матрицами: $V_п = |x_i, y_j|$,$V_а = |x_i, y_j|$ $V_д = |x_i, y_j|$, в которых на пересечении x_i, y_j находятся значения функции принадлежности $\mu_{Y^{п}}(x_i, y_j)$, $\mu_{Y^{а}}(x_i, y_j)$ и $\mu_{Y^{д}}(x_i, y_j)$ соответственно.

В качестве входной лингвистической переменной на множестве X принята: “Степень подозрительности”. Ее характеристикой является терм-множество T, которое содержит три нечетких переменных (значения лингвистической переменной): “Малая подозрительность M (x)”, “Средняя подозрительность C (x)” и “Высокая подозрительность B (x)”, с областью определения [0,1]. На практике число переменных терма не превышает семи. Для физической реализации лингвистической переменной необходимо определить значения переменных терма T при заданных входных переменных x. Для этого должны быть найдены функции принадлежности: $\mu_{Xп}$ (M), $\mu_{Xп}$(C) $\mu_{Xп}$ (B); $\mu_{Xа}$ (M), $\mu_{Xа}$(C) $\mu_{Xа}$(B), а также $\mu_{Xд}$ (M), $\mu_{Xд}$ (C), $\mu_{Xд}$ (B). На практике с этой целью часто используется ряд типовых форм кривых: треугольная, трапецеидальная и гауссова функция принадлежности [4]. Так, на рис. 2, (а) для нечетких переменных M (x), C (x), B (x) на множествах $X^{п}$, $X^{а}$, $X^{д}$ их функции принадлежности определены при входных значениях x_1=2, x_2=5, x_3=9: (0,62, 0,78, 0,37); (0,9, 0,5, 0,75) и (0,42, 0,28, 0,5) соответственно. Входные значения определяются и приводятся к определенному формату экспертом по результату мониторинга.

Таким образом, в результате фаззификации определены лингвистическая переменная, ее нечеткие переменные и степень их принадлежности. При этом использованы треугольные функции принадлежности.

Выходную лингвистическую переменную зададим на множестве Y.

В качестве такой переменной принята: "Опасность поражения", значение которой будет определяться на этапах ЖЦ нечеткой переменной: "Степень поражения" с функциями принадлежности : $\mu_{Y^{п}}(x_i, y_j)$, $\mu_{Y^{а}}(x_i, y_j)$ и $\mu_{Y^{д}}(x_i, y_j)$. В данной постановке задачи, для оценки лингвистической переменной также учитывается вид поражения: зависание системы, потеря и искажение файлов, нарушение реестра и т.д., что учитывается вектором $Z = \{z_k\}$, в котором компонентам z_k, k = 1,..,r, (виды поражения) присваиваются нормированные приоритетные веса $P=\{ p_k \}$, ($\sum p_k = 1$), учитывающие уровень их опасности для системы пользователя.

Рассмотрим содержательную часть матриц отношений построенных с учетом [5, 6]. Так, в матрице отношений $V_п = |x_i, y_j|$ элементы x_i – функции (механизмы) и способы проникновения ВП в систему пользователя, i = 1,…,k; элементы y_j – возможные входы проникновения в систему: порты сетевых протоколов прикладного уровня, j = 1,…,h. (индексы не совпадают с истинными номерами портов).

Например: x_1 – набор функций работы с электронной почтой; x_2 – набор функций работы с системами передачи файлов; x_3 – набор функций отдаленного доступа (через консоль и командные интерпретаторы); x_4 – набор функций работы с web-браузером и т.д. Порт p_{20} – FTP (FileTransferProtocol) – сетевой протокол, предназначенный для передачи файлов в компьютерных сетях; p_{22} – SSH (Secure Shell) – сетевой протокол, который позволяет осуществлять отдаленное управление компьютером и передачу файлов и т.д.

На этапе деструктивных действий используется матрица отношений исследуемого объекта и структурных единиц ОС: $V_д = |x_i, y_j|$, в которой x_i -действия ВП, направленные на структурные компоненты ОС пользователя; i = 1,…,σ; y_j – структурные компоненты ОС пользователя, j = 1,…,τ . Например, x_1 – прием и отправление файлов; x_2 – создание и уничтожение файлов; x_3 – создание, запуск и уничтожение процессов и т.д. К структурным компонентам ОС относятся: y_1- файловая система; y_2 – планировщик процессов (как составляющая ядра операционной системы); y_3 – системные службы (ключи реестра – Windows XP, конфигурационные файлы управления демонами в Unix, Linux-системах); y_4 – функции работы с сетью и т.д.

Из приведенных примеров видно, что поведение ВП на этапах ЖЦ многовариантно, имеет нечеткий характер и, в принципе, не может быть просто прогнозировано. Кроме того, их функции принадлежности не определены, что делает невозможным оценки выходной лингвистической переменной. В работе данные функции определяются, в отличие от типовых подходов, косвенным путем на основе анализа и оптимизации матриц нечетких отношений $V_п$, $V_а$, $V_д$ с привлечением оценок экспертов.

Покажем на примере принцип формирования функции принадлежности $\mu_{Y^{п}}(x_i, y_j)$ на этапе проникновения. Рассматриваемая задача представляется как нахождение для каждого x_i матрицы $V_п = |x_i, y_j|$ наиболее вероятного порта проникновения y_j при заданных признаках опасности z_k. Данная задача сводится к задаче ранжирования [7], в которой в отличие от [4], попарное сравнение экспертов производится с учетом

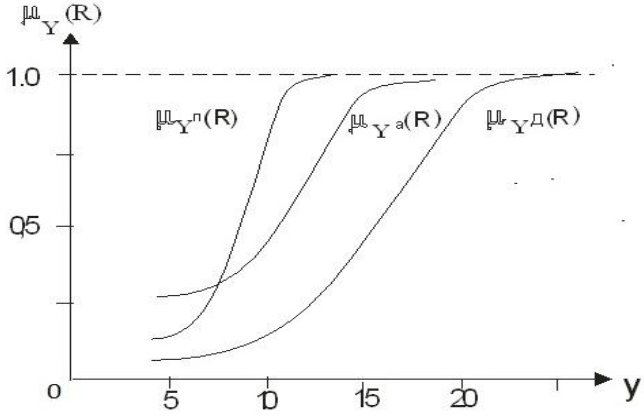
оценочных признаков, позволяющих учесть особенности сравниваемых объектов.

Исходным для решения задачи является построение матрицы превосходства $S=|s_{ij}|$, элементы которой s_{ij} выражаются любым положительным числом ($s_{ij} = s_i/s_j$; $0 < s_{ij} < \infty$; $s_{ji} = 1/ s_{ij}$; $s_{ii} =1$; i, j = 1,…,m, где m- число возможных исходов). Элементы s_{ij} матрицы S определяются вычислением значений парных предпочтений по каждому признаку отдельно с учетом их весов $P=\{p_k\}$; k=1,..,r, с использованием выражения:

$$s_{ij} = \frac{\sum_{k=1}^{r} s_{ij}^k \cdot p_k}{\sum_{k=1}^{r} s_{jk}^k \cdot p_k}; \; s_{ji} = \frac{1}{s_{ij}}; \; s_{ii} = 1; \; i, j = \overline{1,m}.$$

С помощью матрицы S определяется собственный вектор $\Pi = (\pi_1,..., \pi_m)$, который соответствует максимальному положительному корню l характеристического полинома $|S - l \cdot E| = 0; \; S \cdot \Pi = l \cdot \Pi$, где E -единичная матрица. Компоненты вектора Π ($\sum\pi_i=1$) отождествляются с оценкой $\mu_Y^{\text{п}}(x_i, y_j)$, учитывающей принятые признаки опасности. Подобная процедура производится для всей матрицы $V_{\text{п}} = |x_i, y_j|$.

В итоге получаем оптимизированную матрицу отношений $V_{\text{п}} = |x_i, y_j|$, в которой используются лишь отношения x_i, y_j с наиболее выраженным уровнем опасности, определяемым значением, равным π_{max}, ($0 \le \pi_{max} \le 1$).С использованием данной матрицы строится нормированная кривая функция принадлежности $\mu_Y^{\text{п}}(x_i, y_j)$ выходной переменной y, а также таблица, в которой каждому значению $\mu_Y^{\text{п}}(x_i, y_j)$ ставится в соответствие пара (x_i, y_j), позволяющая идентифицировать, в том числе, ресурсы, которые были использованы вредоносной программой на рассматриваемом этапе, рис. 1. Для компактности отношения (x_i y_j) заменены символом R.



R_i	x_i	y_i
x · · x	x · · x	x · · x

Рис. 1. Примерный вид функций принадлежности выходной переменной

Основой для нечеткого вывода служит база знаний, которая содержит множество нечетких продукционных правил (НПП), определяющих стратегию решения задачи. Типичное продукционное правило базы правил состоит из посылки (антецедента): нечеткие высказывания в форме «если…» и заключения (консеквента) – в форме «то…». Антецедент может содержать несколько посылок, которые объединяются в зависимости от стратегии посредством логических связок «и» или «или».

Каждое из правил нечетких продукций может иметь некоторый вес F_i= [0,1], который определяет значимость правила или уверенность в степени истинности заключения, получаемого по отдельному нечеткому правилу. В общем виде база, содержащая m правил, имеет вид:

Π_1: если x_1 это A_{11} … и (или) … x_n это A_{1n}, то y это R_1;

Π_i: если x_1 это A_{i1} … и (или) … x_n это A_{in}, то y это R_i;

Π_m: если x_1 это A_{i1} … и (или) … x_n это A_{mn}, то y это R_m,

где: x_k – входные переменные, k=1,…,n; y – выходная переменная;

A_{ik} – заданные нечеткие множества с функциями принадлежности (i=1,…,m; k=1,…,n).

На основе нечетких высказываний, истинность которых установлена в результате фаззификации, оценивается степень истинности нечетких высказываний, являющихся заключением соответствующих НПП. Далее выполняется процедура (агрегирование) определения степени истинности левых частей (уровней отсечения – a_i) по каждому из правил системы нечеткого вывода. Так, дизъюнкцией нечетких высказываний является логическая операция, результатом которой является нечеткое высказывание, определяемое как:

$$a_i = \max_i (A_{ik}(X_k)).$$

В рассматриваемой задаче приведем для примера фрагмент базы правил (три переменные и три правила), в которой для каждого правила использованы связки «или» и значения F_i равны единице:

П1: если x_1 = М, или x_2 = С, или x_3 = В, то y = $R^{п}$;

П2: если x_1 = М, или x_2= С, или x_3 = В, то y = $R^{а}$;

П3: если x_1 = М, или x_2 =С, или x_3 = В, то y = $R^{д}$.

Возможны и другие стратегии базы правил.

В работе используется стратегия на основе правила max-min композиции и нечеткой операции max – дизъюнкции для оценки одинаковых заключений.

В рассматриваемом фрагменте при заданных x_1, x_2 , x_3 правила 1-3 позволяют получить нечеткое заключение о степени истинности подозрительности на исследуемых этапах:

$\mu_1 = \max\{ \mu_x^{п}(М); \mu_x^{п}(С); \mu_x^{п}(В)\} = \max\{0,62; 0,78; 0,37 \} = 0,78.$

$\mu_2 = \max\{\mu_x^{а}(М); \mu_x^{а}(С); \mu_x^{а}(В)\} = \max\{ 0,9; 0,5; 0,25 \} = 0,90.$

$\mu_3 = \max\{\mu_x^{д}(М); \mu_x^{д}(С); \mu_x^{д}(В)\} = \max\{ 0,42; 0,28; 0,5\} = 0,5.$

Далее для нечеткого вывода выполняется процесс активизации: процесс нахождения степени истинности каждого из заключений нечетких продукционных правил, который осуществляется усечением функций принадлежности выходной переменной на уровнях μ_1, μ_2, μ_3, рис. 2, (б):

$$\mu_Y^{п}(R)= 0,78;\ \mu_Y^{а}(R) =0,90;\ \mu_Y^{д}(R) =0,5.$$

Для композиции (объединения) полученных усеченных функций используется максимальная композиция нечетких множеств

$$M_y(R) = \max_i (\mu_y(R))$$

где $M_y(R)$ – функция принадлежности итогового нечеткого множества.

На рис.2 показана графическая интерпретация нечеткого вывода для трех входных переменных и трех нечетких правил.

Заключительным является этап дефаззификация- приведение к четкости (получение численного значения для принятия решения), рис. 2, (в). Существует ряд методов дефаззификации. В нашем случае используется метод центра тяжести. При дефаззификации методом центра тяжести значение выходной переменной равно абсциссе центра тяжести площади, ограниченной графиком функции принадлежности итогового нечеткого множества $M_y(R)$.

$$y = \frac{\sum_{i=1}^{n} y_i M_y(R)i}{\sum_{i=1}^{n} M_y(R)i} = \frac{9,0\cdot0,9+7,5\cdot0,78+4,2\cdot0,5}{0,90+0,78+0,5} = 7,36$$

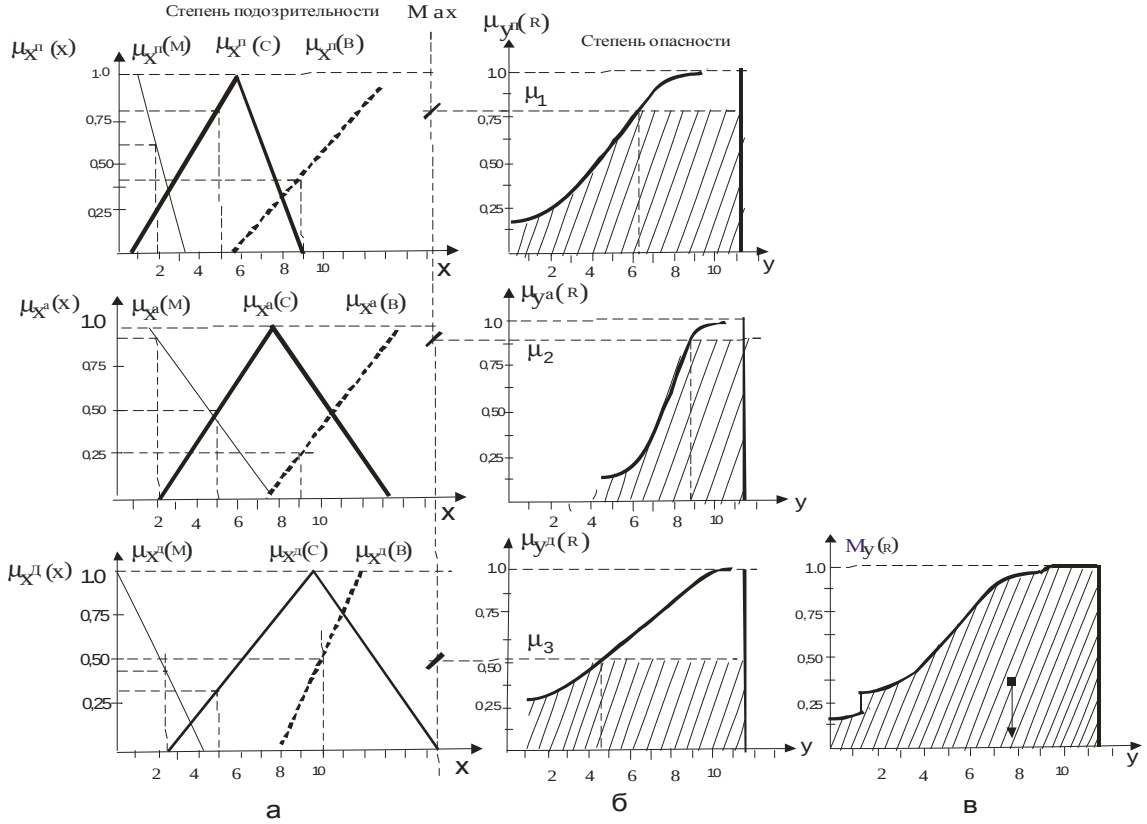


Рис. 2. Графическая интерпретация нечеткого вывода

Полученный результат интерпретируется как коэффициент опасности поражения системы со стороны ВП, который сравнивается с некоторым нормированным коэффициентом, определяемым принятой стратегией безопасности. Окончательное решение (предупредить, в карантин, удалить) принимается в зависимости от соотношения этих коэффициентов.

Обобщенная схема реализации методологии приведена на рис. 3. Подсистема мониторинга отслеживает текущие события в системе, реагирует на программы, действия которых отвечают жизненному циклу ВП, выполняет мониторинг выполнения системных функций, которые могут реализовать проникновение ВП, выполняет блокирование подозрительных функций. Результаты мониторинга передаются на вход аналитической системы, реализующей нечеткий логический вывод и принимающей решение относительно присутствия в системе ВП.

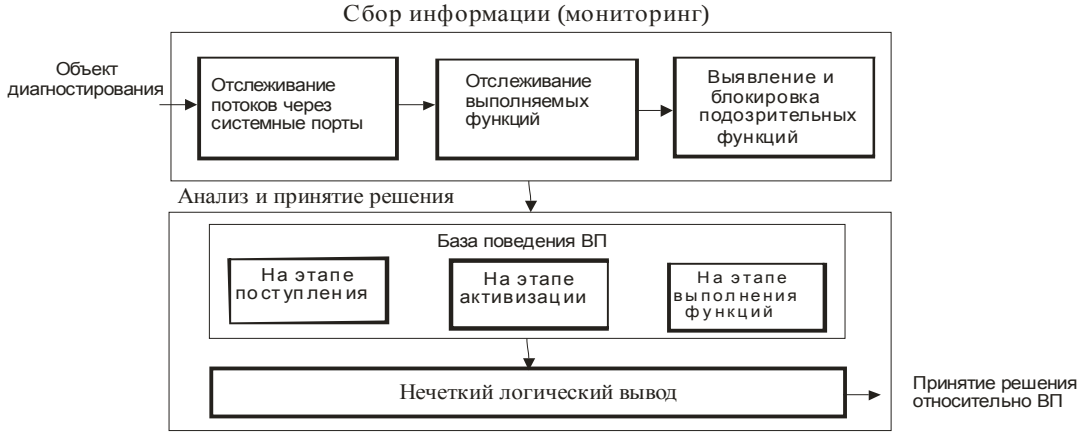


Рис. 3. Обобщенная схема поиска вредоносных программ

Выводы

Анализ существующих методов поиска ВП показал, что им присущи следующие недостатки: невысокое быстродействие, низкая вероятность идентификации новых ВП, высокие требования отдельных методов к аппаратному обеспечению, сложность модели и ее реализации.

В работе предложен новый подход и метод поиска и идентификации ВП на основе нечеткой логики, позволяющей получать достаточно точные решения на основе семантического описания задачи и нечетких продукционных правил, что упрощает решение задачи поиска ВП по сравнению с существующими методами.

Установлено, что применение нечеткой логики открывает большие возможности для адаптации к любым моделям ВП а также принятия оптимального решения путем проектирования соответствующей базы продукционных правил и стратегии их обработки.

Результаты исследования показали возможность идентификации ВП при невысоких требованиях к аппаратным и программным средствам. При этом обеспечивается повышение быстродействия за счет исключения из алгоритмов поиска достаточно сложных компонент и процедур (баз сигнатур, эвристических анализаторов, использование контрольных сумм и т.д.), свойственных существующим методам, а также достаточно высокая реакция и незначительная вероятность пропуска неизвестных ВП. Результаты работы могут быть использованы разработчиками антивирусного диагностирования, эксплуатирующих распределенные информационные системы. Рабочей средой для разработки и исследования предложенной методологии является программная оболочка FUZZY EXPERT.

Литература

1. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. М: Мир, 1976, 165с.

2. Шевченко Алиса. Технологии обнаружения вредоносного кода / Viruslist_com

3. Леоненков А.В. Нечеткое моделирование в среде MATLAB в fuzzyTECH. – СПб.: БХВ – Петербург, 2005. – 736 с.

4. Штовба С.Д. Проектирование нечетких систем средствами МАТЛАБ. – М.: Горячая линия-телеком. – 2007, 290 с.

5. Савенко О.С., Лысенко С.М. Модель процесса поиска троянских программ в персональном компьютере // Радиоэлектронные и компьютерные системы. – Харьков: НАУ "ХАІ", 2008. – № 7. – С. 87-92.

6. Х-релиз: исходники трояна // Информационный портал Хакер.Ру. – Режим доступа: http://www.xakep.ru/post/17223/

7. Берников А.Р., Графов Р.П. Согласование экспертных оценок для формирования модели деятельности оператора в тренажерах. – М., Сб.: Информационные технологии, 2003. – № 6.

Надійшла 23.12.2009 р.