004.056:004.89

ПРИМЕНЕНИЕ МЕТОДОВ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сахно В. В., Маршаков Д. В., Айдинян А. Р.
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
8903461w@mail.ru
daniil_marshakov@mail.ru
aydinian.andrey@yandex.ru

В работе проводится разработка модели оценки рисков информационной безопасности в компьютерной системе, источником которых является множество признаков внешнего характера. Предлагается методика оценки состояния системного блока компьютера на основе технологии инженерии знаний и механизма нечеткого вывода.

Ключевые слова: информационная безопасность, угрозы безопасности, оценка рисков, экспертные системы, нечеткая логика, алгоритм Мамдани.

004.056:004.89

USE OF FUZZY LOGIC METHODS TO SOLVE THE PROBLEM OF INFORMATION SECURITY

Sakhno V. V., Marshakov D. V., Aydinyan A. R.
Don State Technical University, Rostov-on-Don, Russian Federation
8903461w@mail.ru
daniil_marshakov@mail.ru
aydinian.andrey@yandex.ru

The paper considers the risk assessment model of information security in the computer system. The source of risks is a number of external factors. The technique for estimation of the state of the computer system unit based on the engineering knowledge technology and the fuzzy inference is proposed.

Keywords: information security, security threats, risk assessment, expert systems, fuzzy logic, Mamdani algorithm.

Введение. Важнейшей проблемой в вопросах надежного функционирования компьютерных систем является обеспечение их информационной безопасности (ИБ). Существует несколько подходов к оценке уровня ИБ в условиях реализации потенциальных угроз их информационным ресурсам. Ключевыми этапами построения систем защиты информации является анализ актуальных угроз и оценка рисков ИБ. Процесс анализа угроз безопасности подразумевает идентификацию лиц, событий или явлений, в результате воздействия которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и возникновение неприемлемых негативных последствий (ущерба). Оценка рисков требует системного подхода, который включает в себя их количественную оценку и последующее сравнение рисков с критериями для определения их значимости [1].

Определяющим фактором при анализе угроз ИБ и последующей оценке рисков является выявление источников этих угроз. В большинстве случаев нарушение безопасного функционирования компьютерной системы происходит по физическим причинам — отказ аппаратуры, стихийные бедствия и т.п., после чего уже следуют ошибки пользователей, действия вредоносных программ или злоумышленников.

Описание предметной области и постановка задачи. Для компьютерных систем случайные сбои и отказы практически неизбежны [2]. Их возникновение может быть обусловлено

как внутренними технологическими причинами, так и внешними воздействующими факторами (механическими, климатическими, электромагнитными, биологическими, термическими и др.). В результате сбоев или отказов может произойти искажение и даже уничтожение данных, хранящихся и обрабатываемых в системе.

Для снижения рисков безопасности с целью минимизации негативного влияния среды в процессе проработки концепции ИБ необходимо учитывать внешние факторы. На практике это достигается применением различных технических мер, таких как использование специальных покрытий или герметизация оборудования [3]. Однако технологические меры предосторожности применяются, как правило, только для специализированных компьютерных систем. Учитывая, что корпоративные компьютерные системы конструктивно менее защищены, они могут быть подвержены различного рода внешним воздействиям как естественного, так и искусственного происхождения. Важным является отслеживание их физического состояния на этапе хранения и обработки информации.

Целью настоящей работы является разработка модели оценки рисков ИБ в компьютерной системе, источником которых является множество воздействующих внешних факторов, с возможностью ее последующей программно-аппаратной реализации.

Определение стратегии решения задачи. Рассмотрим объекты, понятия и отношения в данной предметной области. Для компьютерной системы на целостность информации и аппаратного обеспечения оказывают влияние: температуры центрального процессора (ЦП), системного блока и жесткого диска, а также влажность в корпусе.

В общем случае температура ЦП в режиме простоя составляет до 45°С, а при нагрузке доходит до 65°С. При этом температура 70°С и выше считается для процессора критической, так как возможно снижение производительности и перезагрузка компьютера. Данный показатель зависит от технологии изготовления и, в зависимости от производителя, допустимый тепловой диапазон может в простое составлять 30–35°С, а при нагрузке — 70–75°С. В то же время при других обстоятельствах нормальная температура ЦП может быть 50–55°С, а рабочая температура при нагрузке доходить до 80–85°С в зависимости от используемой системы охлаждения.

Температура жесткого диска также является относительно иррегулярной величиной, зависящей от ряда обстоятельств. Например, в зимнее время температура может составить 40–45°С, а летом подниматься до 50°С. Считается, что температура ниже 25°С и 45–52°С нежелательны, а температура выше 55°С является уже критической для жесткого диска.

Наиболее трудно формализуемой величиной является влажность в системном блоке. Низкая влажность на уровне 15–20% приводит к накоплению в воздухе статического электричества и, как следствие, электризации пыли, загрязнению аппаратуры и образованию токопроводящих дорожек. Недостаточная влажность (до 30%) приводит к разрушению лака на электронных печатных платах, высыханию и затвердеванию изоляции проводов системного блока с последующим их растрескиванием. Влажность выше 60% является причиной коррозии и окисления контактов, что может вызвать короткое замыкание.

Рассмотренные параметры взаимосвязаны. Температура ЦП может зависеть от состояния термопасты и частоты вращения охлаждающего вентилятора центрального процессора. На температуры жесткого диска и системного блока оказывает влияние установленный в нем вентилятор. Частота вращения вентиляторов зависит от температуры и регулируется материнской платой. Влажность в корпусе зависит от состояния помещения, для ее оценки требуется установка в корпус датчика влажности.

Задача комплексного учета совокупности описанных параметров требует наличия специализированных знаний и эвристического опыта со стороны разработчиков. Поэтому оправданной и разумной стратегией в выработке обоснованных заключений о возможных информационных рисках в компьютерной системе является применение технологии экспертных систем [4]. Многие понятия, связанные с безопасностью, являются сугубо качественными, их оценка на основе количественного измерения в большинстве случаев является затруднительной. В ряде случаев оценка экспертом проводится в виде словесных формулировок, которые затем связывают с числовыми значениями, что ограничивает возможности данной технологии, поскольку уверенность в предлагаемой экспертом оценке может носить субъективный характер. Это обусловливает необходимость оперирования лингвистическими основными структурными единицами естественного языка (лингвистическими переменными), то есть применения аппарата нечеткой логики, успешно себя зарекомендовавшего в схожих задачах обеспечения ИБ [5–7].

В данной работе предлагается методика оценки состояния системного блока компьютера на основе технологии инженерии знаний и механизма нечеткого вывода.

Разработка нечеткой модели. Согласно установленным ранее объектам и понятиям разрабатываемой системы, введем и формализуем необходимые лингвистические переменные: T1 — температура ЦП; T2 — температура жесткого диска; T3 — температура в системном блоке; V1 — скорость вращения вентилятора ЦП; V2 — скорость вращения вентилятора в системном блоке; H — влажность в системном блоке. Выходной лингвистической переменной является R — уровень риска информационной безопасности.

Определим терм-множества для входных и выходной лингвистических переменных. Для входных лингвистических переменных T2, V1, V2, H введем терм-множество {НИЗКАЯ, СРЕДНЯЯ, ВЫСОКАЯ}, для T1, T3 — {КРИТИЧЕСКИ НИЗКАЯ, НИЗКАЯ, СРЕДНЯЯ, ВЫСОКАЯ, КРИТИЧЕСКИ ВЫСОКАЯ}. Терм-множество выходной лингвистической переменной описывает уровень информационных рисков: {ОТСУТСТВУЕТ, МАЛОВЕРОЯТНЫЙ, НИЗКИЙ, ДОСТАТОЧНО ВЫСОКИЙ, КРИТИЧЕСКИ ВЫСОКИЙ}.

Уровень риска оценивается в процессе нечеткого вывода, использующего множество нечетких правил, составляющих в совокупности базу знаний данной предметной области, которые представляются в виде:

ЕСЛИ (x_1 это A) И (x_2 это B), ТО (y это C),

где A, B, C — это лингвистические значения, идентифицированные нечетким способом через соответствующие функции принадлежности для переменных x_1, x_2 и y.

В результате проведенного исследования была определена нечеткая база знаний, представленная на рис. 1.

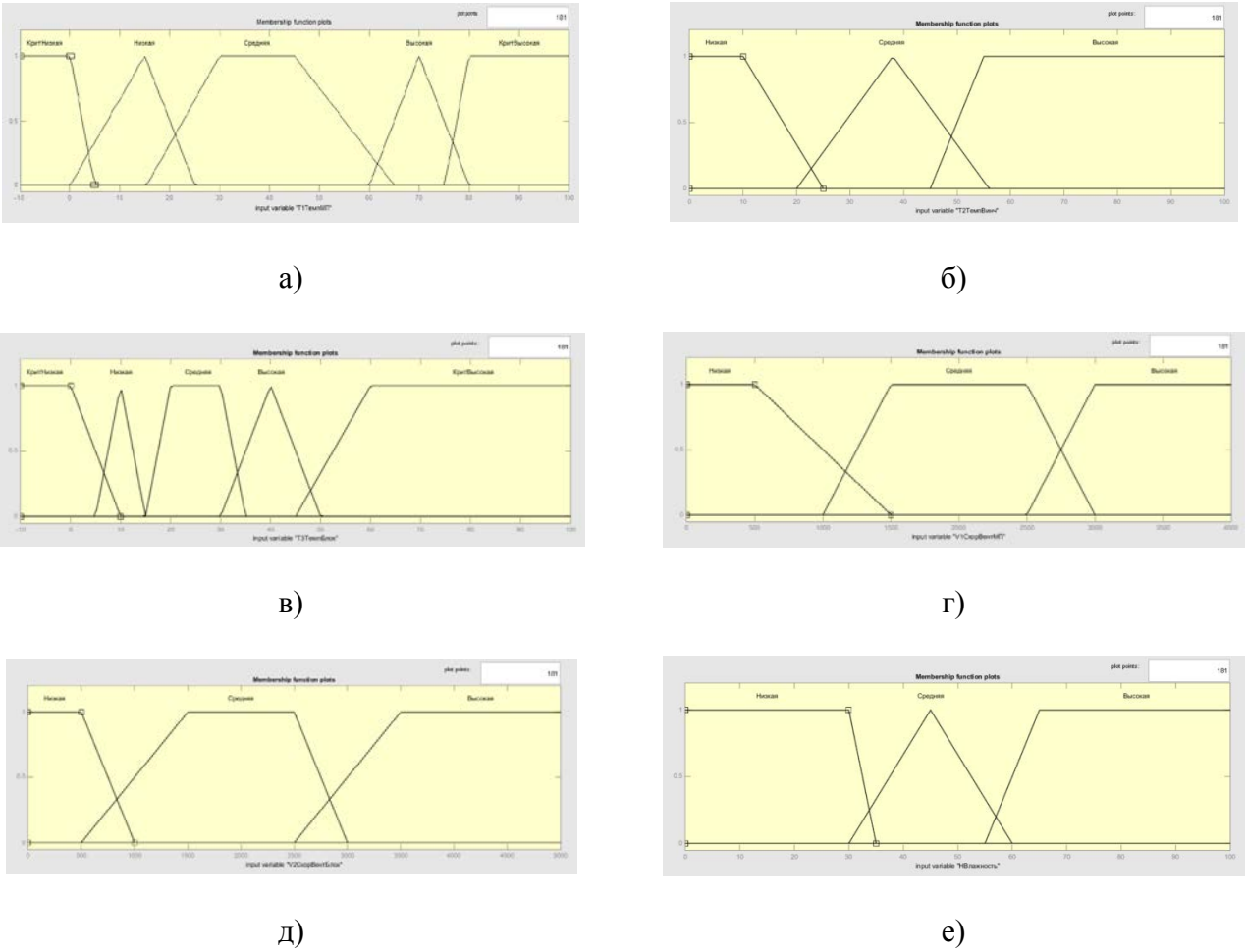
1. ЕСЛИ T1= «КРИТИЧЕСКИ НИЗКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
2. ЕСЛИ T1= «КРИТИЧЕСКИ ВЫСОКАЯ» ТО R= «КРИТИЧЕСКИ ВЫСОКИЙ
3. ЕСЛИ T1= «НИЗКАЯ» ТО R=«ОТСУТСТВУЕТ»
4. ЕСЛИ T1= «СРЕДНЯЯ» И V1=«НИЗКАЯ» ТО R=«ОТСУТСТВУЕТ»
5. ЕСЛИ T1= «СРЕДНЯЯ» И V1=«СРЕДНЯЯ» ТО R=«ОТСУТСТВУЕТ»
6. ЕСЛИ T1= «СРЕДНЯЯ» И V1=«ВЫСОКАЯ» ТО R=«МАЛОВЕРОЯТНЫЙ»
7. ЕСЛИ T1= «ВЫСОКАЯ» И V1=«НИЗКАЯ» ТО R=«ДОСТАТОЧНО ВЫСОКИЙ»
8. ЕСЛИ T1= «ВЫСОКАЯ» И V1=«СРЕДНЯЯ» ТО R=«НИЗКИЙ»
9. ЕСЛИ T1= «ВЫСОКАЯ» И V1=«ВЫСОКАЯ» ТО R=«МАЛОВЕРОЯТНЫЙ»
10. ЕСЛИ H= «СРЕДНЯЯ» ТО R=«ОТСУТСТВУЕТ»
11. ЕСЛИ H= «ВЫСОКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
12. ЕСЛИ H= «НИЗКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
13. ЕСЛИ T3= «КРИТИЧЕСКИ НИЗКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
14. ЕСЛИ T3= «КРИТИЧЕСКИ ВЫСОКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
15. ЕСЛИ T3= «НИЗКАЯ» И V2=«НИЗКАЯ» ТО R=«ОТСУТСТВУЕТ»
16. ЕСЛИ T3= «СРЕДНЯЯ» И V2=«НИЗКАЯ» ТО R=«МАЛОВЕРОЯТНЫЙ»
17. ЕСЛИ T3= «СРЕДНЯЯ» И V2=«СРЕДНЯЯ» ТО R=«ОТСУТСТВУЕТ»
18. ЕСЛИ T3= «СРЕДНЯЯ» И V2=«ВЫСОКАЯ» ТО R=«МАЛОВЕРОЯТНЫЙ»
19. ЕСЛИ T3= «ВЫСОКАЯ» И V2=«НИЗКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ
20. ЕСЛИ T3= «ВЫСОКАЯ» И V2=«СРЕДНЯЯ» ТО R=«НИЗКИЙ»
21. ЕСЛИ T3= «ВЫСОКАЯ» И V2=«ВЫСОКАЯ» ТО R=«НИЗКИЙ»
22. ЕСЛИ T2= «КРИТИЧЕСКИ НИЗКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
23. ЕСЛИ T2= «ВЫСОКАЯ» ТО R=«КРИТИЧЕСКИ ВЫСОКИЙ»
24. ЕСЛИ T2= «НИЗКАЯ» И V2=«НИЗКАЯ» ТО R=«ОТСУТСТВУЕТ»
25. ЕСЛИ T2= «СРЕДНЯЯ» И V2=«НИЗКАЯ» ТО R=«МАЛОВЕРОЯТНЫЙ»
26. ЕСЛИ T2= «СРЕДНЯЯ» И V2=«СРЕДНЯЯ» ТО R=«ОТСУТСТВУЕТ»
27. ЕСЛИ T2= «СРЕДНЯЯ» И V2=«ВЫСОКАЯ» ТО R=«МАЛОВЕРОЯТНЫЙ»

Рис. 1. База правил нечетких продукций

Для создания методики оценки рисков необходимо разработать экспертную систему, которая была бы реализована в виде системы нечеткого вывода и позволяла определять величину риска на основе субъективных оценок всех уровней ИБ. Для последующего моделирования такого рода системы используется программный инструментарий Fuzzy Logic Toolbox, представляющий собой пакет расширения MATLAB, содержащий инструменты для проектирования систем нечеткой логики.

При определении форм кривых функций принадлежности учитывается, что они строятся субъективно по результатам опроса экспертов, поэтому являются, в некотором смысле, «приближенными». На практике форма кривых функции принадлежности выбирается исходя из сложности проведения расчетов. Наибольшее распространение получили треугольная и трапецеидальная функции принадлежности из-за их универсальности и меньших требований к вычислительным ресурсам при их аппаратной реализации [8].

Для отображения выделенных нечетких подмножеств лингвистических переменных воспользуемся ими. Параметры входных функций принадлежности приведены на рис. 2.



а) б)

в) г)

д) е)

Рис. 2. Параметры входных лингвистических переменных:

а — температура ЦП; б — температура жесткого диска; в — температура в системном блоке; г — скорость вращения вентилятора ЦП; д — скорость вращения вентилятора в системном блоке; е — влажность в системном блоке

В качестве механизма нечеткого логического вывода разрабатываемой системы применяется алгоритм Мамдани, получивший наибольшее практическое применение в задачах нечеткого моделирования и заключающийся в применении минимаксной композиции нечетких множеств.

Процесс обработки нечетких правил вывода в этом случае состоит из четырех этапов.

1. Фаззификация, состоящая в определении степени истинности, т.е. значения функции принадлежности для предпосылок (левых частей) каждого правила.

2. Нечеткий вывод, состоящий в применении к заключениям (правой части) правил вычисленного значения истинности для предпосылок каждого правила. В качестве правил логического вывода в алгоритме Мамдани используется операция минимум (min), «отсекающая» функцию принадлежности заключения правила по высоте, соответствующей вычисленной степени истинности предпосылки правила.

3. Композиция, объединяющая с использованием операции максимум (max) все нечеткие подмножества, определенные для каждой переменной вывода, и формирующая одно нечеткое подмножество для каждой переменной вывода.

4. Дефаззификация, реализующая скаляризацию результата композиции, т.е. переход от нечеткого подмножества к скалярным значениям.

Реализованная в среде MATLAB схема описанной системы нечеткого вывода приведена на рис. 3.

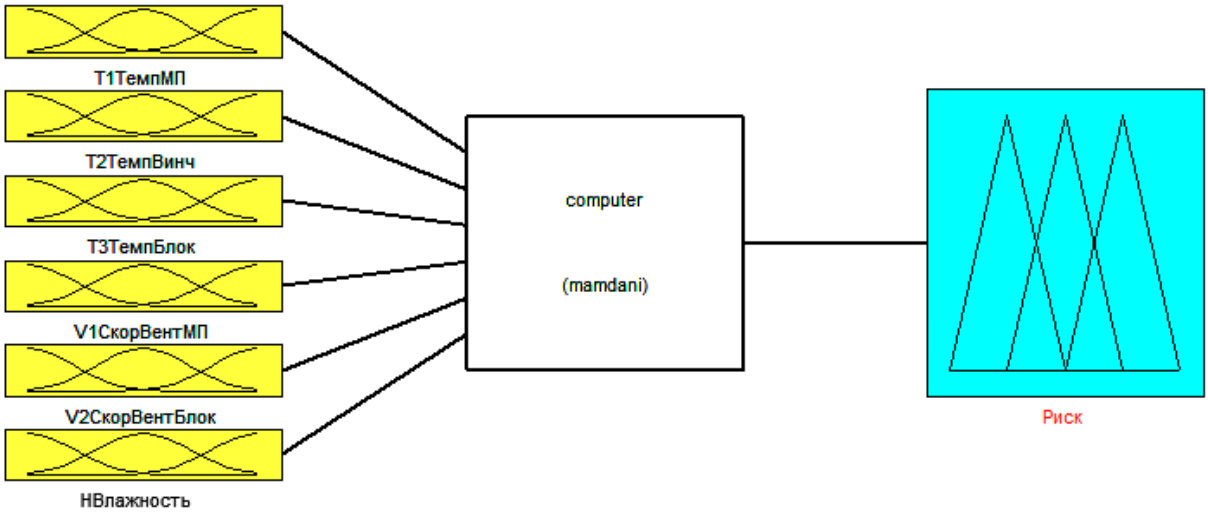


Рис. 3. Схема системы нечеткого вывода в среде MATLAB

Данная система позволяет оценить риск ИБ в компьютерной системе на основании введенной выходной лингвистической переменной, параметры которой представлены на рис. 4.

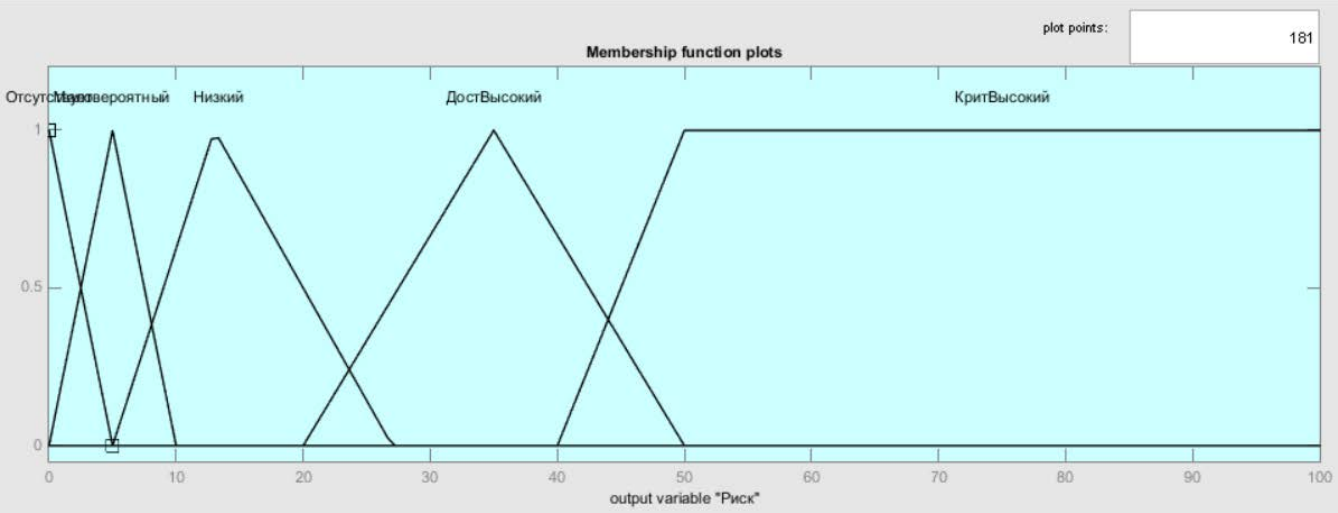


Рис. 4. Параметры выходной лингвистической переменной
«уровень риска информационной безопасности»

Рассмотрим пример проведения подобной оценки. Для этого предположим, что на основании измерений в системном блоке были получены следующие входные данные: температура ЦП составила 45°C, температура жесткого диска — 44°C, температура в системном блоке — 45°C, при этом скорость вращения вентилятора ЦП — 2000 RPM, скорость вращения вентилятора в системном блоке — 2500 RPM, влажность в системном блоке — 50%.

Особенностью нечеткой экспертной системы является одновременное срабатывание всех заданных правил, с различной степенью их влияния на выходное значение. Результаты вычислений нечеткого вывода для 27 заданных ранее правил приведены на рис. 5.

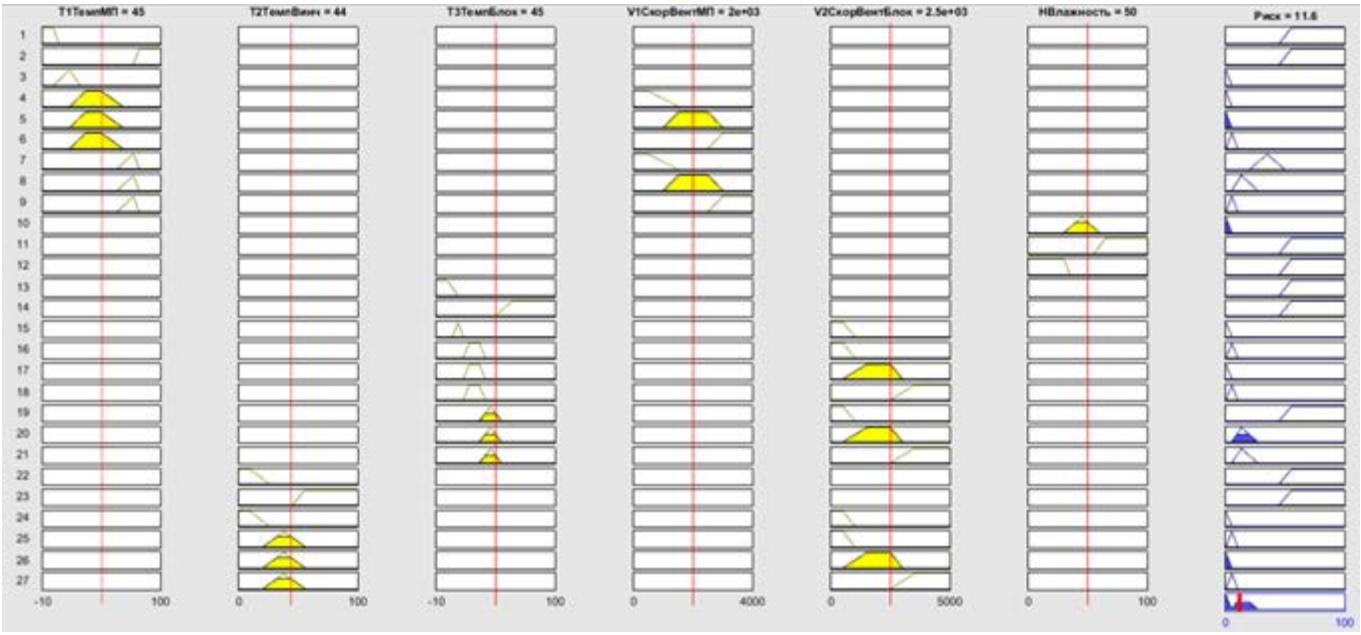


Рис. 5. Результаты вычислений нечеткого вывода для 27 заданных правил

Согласно выполненному расчету уровень риска ИБ при измеренных параметрах является НИЗКИМ, что соответствует исходным входным данным.

Проведенные аналогичные исследования представленной нечеткой модели для различных наборов исходных данных также показали приемлемые результаты.

Заключение. Рассмотренная в данной работе реализация в среде MATLAB нечеткой модели оценки состояния системного блока компьютерной системы является адекватной происходящим в компьютерной системе физическим процессами, позволяет оценить риски ИБ, источником которых является множество воздействующих внешних факторов.

В дальнейшем планируется программно-аппаратная реализация предложенной модели на базе микроконтроллера с целью оценки рисков информационной безопасности компьютерных систем в масштабе реального времени.

Библиографический список

1. ГОСТ Р ИСО/МЭК 27 002–2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002 [Электронный ресурс] / Электронный фонд правовой и нормативно-технической документации. — Режим доступа :http://docs.cntd.ru/ document/1200103621 (дата обращения : 24.04.2018).

2. Семененко, В. А. Информационная безопасность / В. А. Семененко. — Москва : МГИУ, 2010. — 276 с.

3. Морозов, Д. И. Защита радиоэлектронных средств от влияния климатических факторов / Д. И. Морозов, П. Г. Андреев, И. Ю. Наумова // Радиоэлектронная техника. — №1 (4). — 2011. — С. 255–261.

4. Маршаков, Д. В. Экспертные системы информационной безопасности / Д. В. Маршаков, В. А. Фатхи. — Ростов-на-Дону: Издательский центр ДГТУ, 2015. — 223 с.

5. Ажмухамедов, И. М. Оценка повреждений безопасности информационной системы на основе нечетко-когнитивного подхода / И. М. Ажмухамедов // Вопросы защиты информации. — 2012. — №1. — С. 57–60.

6. Булдакова, Т. И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели / Т. И. Булдакова, Д. А. Миков // Наука и образование: МГТУ им. Н.Э. Баумана. — 2013. — № 11. — С. 295–310.

7. Баранова, Е. К. Методика анализа рисков информационной безопасности с использованием нечеткой логики на базе инструментария MATLAB / Е. К. Баранова, А. М. Гусев // Образовательные ресурсы и технологии. — 2016. — №1(13). — С. 88–96.

8. Schrieber M.D. Hardware Implementation of a Novel Inference Engine for Interval Type-2 Fuzzy Control on FPGA / Schrieber M.D., Biglarbegian M. // IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 6-11 July 2014, Beijing, China. — USA, Piscataway, NJ: IEEE, 2014. — P. 640–646.