СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. На сегодняшний день рабочее место практически любого человека является автоматизированным. Автоматизированное рабочее место (АРМ) - программно-технический комплекс автоматизированной системы (АС) предназначенный для автоматизации деятельности определенного вида [8]. В связи с широкой распространенностью АРМ во всех сферах деятельности человека, существует множество угроз безопасности информации, обрабатываемой на таких рабочих местах. Для разработки эффективной системы защиты информации и подбора необходимых средств защиты информации (СЗИ) необходимо проводить риск-анализ защищаемого объекта.

В ходе риск-анализа происходит выявление существующих уязвимостей, актуальных угроз и расчет величины возможного ущерба при реализации конкретной угрозы. В завершение риск-анализа получается полная картина риска для исследуемого объекта, также составляются рекомендации по управлению риском. Основываясь на результатах риск-анализа, строится эффективная система защиты информации [11, 12]. В данной работе риск-анализ проводится на основе методов экспертных оценок и теории нечетких множеств. Так как в данной работе риск-анализ проводится на основе экспертных оценок, была выбрана именно теория нечетких множеств, так как задачи, стоящие перед человеком в различных областях знаний являются по своей природе слишком сложными и многогранными для того, чтобы использовать для их решения только точные, хорошо определенные модели и алгоритмы.

Многие понятия вследствие человеческого мышления, приближенного характера умозаключений и лингвистического их описания являются нечеткими по своей природе и требуют для своего описания соответствующего аппарата, в частности, аппарата теории нечетких множеств [16].

В отличие от традиционной математики, требующей на каждом шаге вычислений точных и однозначных описаний закономерностей, нечеткая логика предлагает совершенно иной уровень мышления, благодаря которому творческий процесс

моделирования происходит на наивысшем уровне абстракции, при котором постулируется лишь минимальный набор закономерностей.

Нечеткие числа, получаемые в результате «не вполне точных измерений», во многом аналогичны распределениям теории вероятностей, но свободны от присущих последним недостатков: малое количество пригодных к анализу функций распределения, необходимость их принудительной нормализации, соблюдение требований аддитивности, трудность обоснования адекватности математической абстракции для описания поведения фактических величин. В пределе, при возрастании точности, нечеткая логика приходит к стандартной, Булевой. По сравнению с вероятностным методом, нечеткий метод позволяет резко сократить объем производимых вычислений, что, в свою очередь, приводит к увеличению быстродействия нечетких систем [15, 20].

ЗАКЛЮЧЕНИЕ

Преимущество модели оценки рисков информационной безопасности на основе нечетких множеств состоит в применении аппарата нечеткой логики, т.к. процесс защиты информации не всегда можно описать однозначно, особенно это касается поведения персонала. Метод оценки рисков информационной безопасности на основе теории нечетких множеств даже при недостаточном объеме входных данных позволяет построить адекватную модель воздействия угроз на объект, который подлежит защите. При этом возможно рассматривать несколько ветвлений реализации угрозы или множества угроз на объект. Таким образом, можно оценить наиболее вероятные угрозы на объект защиты и, на базе полученной информации, создать или модернизировать систему защиты информации.

Преимуществом экспертных оценок является индивидуальный подход к каждой организации, так как привлекая к оценке экспертов из организации, можно адаптировать модель под специфику конкретной компании.

В данной работе рассматриваются два новых метода ранжирования применительно к анализу рисков информационной безопасности.

Методом на основе взвешенного коэффициента корреляции ранжируется множество существующих для объекта угроз, для того, чтобы выявить направленность наиболее опасных угроз: конфиденциальность, целостность или доступность информации. Затем по результатам ранжирования выбирается адекватная для объекта защиты СЗИ.

После применения СЗИ ранжирование производится повторно для проверки работоспособности системы защиты. Повторное ранжирование производится двумя разными методами для сравнения результатов, так как данные методы применяются в области информационной безопасности в первые.

Примечательно, что результаты расчетов по обоим методам получились схожими с небольшими отклонениями в области рисков среднего значения. Схожесть результатов доказывает работоспособность методов.

СПИСОК ЛИТЕРАТУРЫ

1 Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646) // Доступ из справ.-правовой системы «КонсультантПлюс».

2 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации,информационных технологиях и защите информации». М.: Кремль, 2006. // Доступ из справ.-правовой системы «КонсультантПлюс».

1 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК РФ, 2008. // Доступ из справ.-правовой системы «КонсультантПлюс».

2 Классификация автоматизированных систем и требования по защите информации // Сборник руководящих документов по защите информации от несанкционированного доступа. М.: Гостехкомиссия России, 1998.

3 Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

4 ГОСТ Р ИСО/МЭК 17799—2005. Информационная технология. Практические правила управления информационной безопасностью.

5 ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

6 ГОСТ 34.003-90 С. 4. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения.

7 Щербаков В. Б. Безопасность беспроводных сетей: стандарт IEEE 802.11 / Щербаков В. Б., С. А. Ермаков. - М: РадиоСофт, 2010. - 256 с.

8 Бельфер Р. А. Сравнительный анализ моделей оценки уровня риска угроз ИБ сети связи / Р. А. Бельфер // Сборник трудов всероссийской научно-технической конференции «Безопасные информационные технологии» НИИ РЛ МГТУ им. Н.Э.Баумана. - 2013. - С. 12-15.

9 Домарев В. В. Управление информационной безопасностью / В. В. Домарев, Д. В. Домарев – Донецк: Велстар, 2012. – 146 с.

10 Корниенко М. А. Модель оценки рисков информационной безопасности на основе теории нечетких множеств / М. А. Корниенко, Е. А. Островерхова // Материалы XVIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». Т. 4 – Х.: ХНУРЭ, 2014. – С. 279.

11 Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH / А. В. Леоненков. – СПб.: БХВ-Петербург, 2005. – 292 с.

12 Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. — К.: «МК-Пресс», 2006 - 320 с.

13 Борисов В. В. Нечеткие модели и сети / В. В. Борисов, В. В. Круглов, А. С. Федулов. – М.: Горячая линия-Телеком, 2007. – 236 с.

14 Заде Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. А Заде. – М.: Мир, 2003. – 157 с.

15 Зефиров С. Л. Как измерить информационную безопасность организации? Объективно о субъективном / С. Л. Зефиров, В. Б. Голованов. – М.: Защита информации INSIDE. – 2006. – № 3.– С. 28–36.

16 Воробьев А. А. Оценивание защищенности автоматизированных систем на основе методов теории игр / А. А. Воробьев, Г. В. Куликов, А. В. Непомнящих // Приложение к журналу «Информационные технологии». – 2007. – № 1. – С. 1–24.

17 Белов В. М. Информационные системы и технологии: проблемы и перспективы / Под ред. А.В. Бабкина. - СПб.: Изд-во Политехн. ун-та, 2007. – С. 300–331.

18 Соколов А. М. Методы и алгоритмы нечеткого моделирования механических систем / А. М. Соколов // Информационные технологии. – 2007. – № 3. – С. 13–20. 21.

19 Чернов В. Г. Модели поддержки принятия решений в инвестиционной деятельности на основе аппарата нечетких множеств / В. Г. Чернов. – М.: Горячая линия – Телеком, 2007. – 312 с.

20 Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский. - М: Горячая линия-Телеком, 2006. - 388 с.

21 Моёров А.С. Общие положения и математический аппарат для определения характеристики вероятности угроз в транспортной сети VANET / А. С. Моёров, Р. А. Бельфер // Сборник трудов всероссийской научно-технической конференции «Безопасные информационные технологии» НИИ РЛ МГТУ им. Н.Э.Баумана. - 2012. - С. 132-134.

22 Петухов Г. Б. Теоретические основы и методы исследования эффективности операционных целенаправленных процессов / Г. Б. Петухов. – М.: МО, 2002. – 176 с.

23 Терентьев В. М. Теоретические основы управления сетями многоканальной радиосвязи / В. М. Терентьев, И. Б. Паращук. – С.-Пб.: ВАС, 1995. – 195 с.

24 Терентьев В. М. Анализ эффективности функционирования автоматизированных сетей многоканальной радиосвязи / В. М. Терентьев, Ю. В. Санин. – С.-Пб.: ВАС, 2007. – 80 с.

25 Цициашвили Г. Ш. Декомпозиционные методы в задачах устойчивости и эффективности сложных систем / Г. Ш. Цициашвили. – М.: ДВО АН, 2005. – 116с.

26 Ягер Р. Р. Нечеткие множества и теория возможностей. Последние достижения: пер. с англ. / под ред. Р.Р. Ягера. – М.: Радио и связь, 2000. – 408 с.

27 Паращук И. Б. Нечеткие множества в задачах анализа сетей связи / И. Б. Паращук, И. П Бобрик. – С.-Пб.: ВАС, 2001. – 80 с.

28 Дюбуа Д. Теория возможностей. Приложения к представлению

знаний в информатике: пер. с фр. / Д. Дюбуа, А. Прад. – М.: Радио и связь, 2004. – 288 с.

29 Буренин Н. И. Новые сетевые технологии в системах управления военного назначения: под ред. Н.И. Буренина / Н. И. Буренин, С. М. Одоевский, И. Б. Паращук. - СПб.: ВУС, 2000. – 195 с.

30 Воронов М. В. Нечёткие множества в моделях систем организационного управления / М. В. Воронов. - М.: ВМА, 2005. – 231 с.

31 Тэтано Т. Прикладные нечеткие системы: под ред. Асаи К. / Т. Тэтано. - М: Мир, 2006. – 182 с.

32 Марков А. Управление рисками – нормативный вакуум информационной безопасности / А. Марков, В. Цирлов // Открытые системы. СУБД: Журнал для профессионалов в области информационных технологий. – 2007. – №8. – С. 63-67.

33 Долженко А. И. Модель анализа риска потребительского качества проектов экономических информационных систем / А. И. Долженко // Вестник Северо-Кавказского государственного технического университета. – 2009. – №1. – С.129-134.

34 Зайченко Ю. П. Нечеткие модели и методы в интеллектуальных системах: учебник для вузов / Ю. П. Зайченко. – Киев: Слово, 2008. – 344 с.

35 Булдакова Т. И. Реализация методики оценки рисков информационной безопасности в среде Matlab / Т. И. Булдакова, Д. А. Миков // Вопросы кибербезопасности. – 2015. – № 4 (12) – С. 53–61.

36 Космачева И. М. Алгоритм оценки риска нарушения информационных сервисов в организации / И. М. Космачева, И. В. Сибикина, Л. В. Галимова // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2015. – № 2. – С. 58–64.

37 Выборнова О. Н. Онтологическая модель процесса оценки рисков / О. Н. Выборнова // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2015. – № 2. – С. 97–102.

38 Давидюк Н. В. Формирование начальной популяции в процедуре генетического поиска варианта эффективного расположения средств обнаружения на объекте защиты / Н. В. Давидюк, С. В. Белов // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2010. – № 1. – С. 114–118.

39 Ажмухамедов И. М. Динамическая нечеткая когнитивная модель оценки уровня безопасности информационных активов ВУЗа / И. М. Ажмухамедов // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2012. – № 2. – С. 137–142.

40 Усков А. А. Принципы построения систем управления с нечеткой логикой / А. А. Усков // Приборы и системы. Управление, контроль, диагностика. – 2004. – № 6. – С. 7–13.

41 Сибикина И. В. Построение лингвистических шкал в целях выявления важных дисциплин, формирующих компетенцию / И. В. Сибикина, И. Ю. Квятковская // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2012. – № 2. – С. 182–186.

42 Сибикина И. В. Теоретические основы разработки информационных систем и ресурсов на основе модели компетенции для автоматизированных систем управления вузом / И. В. Сибикина, И. Ю. Квятковская. – Астрахань: АГТУ, 2016. – 100 с.

43 Белов С. В. Процедура оценки показателей злоумышленного проникновения в составе автоматизированной системы контроля физической безопасности объекта защиты / С. В. Белов, А. В. Мельников // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2014. – № 2. – С. 28–37.

44 Белов С. В. Оценка степени злоумышленного интереса к различным компонентам объекта защиты / С. В. Белов, Б. Р. Досмухамедов // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2013. – № 1. – С. 14–20.

45 Симонов С. С. Методология анализа рисков в информационных системах / С. С. Симонов // Защита информации. – 2002. - №2. - С.12-18.

46 S.H. Nasseri, M.M. Zadeh, M. Kardoost, E. Behmanesh Ranking fuzzy quantities based on the angle of the reference functions, Applied Mathematical Modelling, no. 37, 2013, pp. 9230–9241.

47 Jun Ye Fuzzy decision-making method based on the weighted correlation coefficient under intuitionistic fuzzy environment, European Journal of Operational Research, no. 205, 2011, pp. 202–204.

48 Risk Management Guide for Information Technology Systems. – NIST, Special Publication 800-30. // http:csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

49 Shyi-Ming Chen, Kata Sanguansat Analyzing fuzzy risk based on a new fuzzy ranking method between generalized fuzzy numbers, Expert Systems with Applications, no. 38, 2013, pp. 2163–2171.

50 Sivanandam S. N. Introduction to fuzzy logic using Matlab / S. N. Sivanandam, S. Sumathi, S. N. Deepa. – Berlin: Springer, 2007. – 430 p.

51 Fakariah Hani Mohd Ali, Wan Mohd Nadzir Hadzril Wan Ismail. Network Security Threat Assessment Model Based on Fuzzy Algorithm, IEEE, no. 11, 2011.

52 Maxwell Dondo, A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System, Defence R&D Canada – Ottawa, Technical Memorandum DRDC Ottawa TM 2007-090, May 2007.

53 Матрица знаний информационной безопасности. Безопасность информационных технологий [Электронный ресурс]. – Режим доступа: http://domarev.com.ua.

54 Оценка СЗИ. Безопасность информационных технологий [Электронный ресурс]. – Режим доступа: http://domarev.com.ua.

55 Jin-fu Wang E-government Security Management: Key Factors and Countermeasure, IAS, vol. 2, Fifth International Conference on Information Assurance and Security, 2009, pp.483-486

56 Arnold F. Shapiro, Marie-Claire Koissi Risk Assessment Applications of Fuzzy Logic, Casualty Actuarial Society, 2015, pp. 58-102

57 Hwang J. and Syamsuddin I. Information Security Policy Decision Making: An Analytic Hierarchy Process Approach, Proceeding of IEEE Third Asia International Conference on Modelling & Simulation, AMS 2009, pp.158-163

58 Syamsuddin I. and Hwang J. The Application of AHP Model to Guide Decision Makers: A Case Study of E-banking Security, Proceeding of IEEE Fourth Interna-

tional Conference on Computer Sciences and Convergence Information Technology IC-CIT 2009, pp.1469-1473

59 Backhouse J. and G. Dhillon Current Directions in IS Security Research: Toward Socio Organizational Perspectives", Information Systems Journal, 11 (2), 2011, pp. 127-153

60 Dhillon G. and Torkzadeh G. “Value Focused Assessment of Information System Security in Organizations”. Information Systems Journal. Vol 16. No 3, 2006

61 Siponen M.T and Kukkonen H.O. “A review of information security issues and respective research contributions”. DATA BASE 38(1): 2006, pp. 60-80

62 Anderson R. Why Information Security is Hard: An Economic Perspective, Proceedings of 17th Annual Computer Security Applications Conference, 2011, pp.10-14

63 von Solms B. Information Security — A Multidimensional Discipline Computers & Security, Vol. 20, Issue 6, 1, 2011, pp. 504-508

64 Bishop M. Introduction to Computer Security Information Security Risk Analysis, 2nd ed. CRC Press, 2005, pp. 15-21

65 NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, September? 2012, 95 pp.

66 The Security Risk Management Guide, Microsoft Corporation, 2006.

67 The OCTAVE Approach to Information Security Risk Assessment, ISACA Journal, Vol. 4, 2009, pp. 1-5.

68 T. L. Saaty Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World”, RWS Publications; 3rd Revised edition, 2001, 323 pp.

69 J. Anderson, R. Narasimhan Assessing project implementation risk: a methodological approach, Management Science 25(6) (1979) 512–521.

70 R. Anderson, A. Homer, S. Robinson, Beginning Components for ASP, Wrox Press, Birmingham, 2002.

71 S. M. Bass, H. Kwakernaak, Rating and ranking of multipleaspect alternatives using fuzzy sets, Automatica 1 (1), 2005, pp. 47–58.

72 J. C. Bennett, G. A. Bohoris, E. M. Aspinwall, R. C. Hall, Risk analysis techniques and their application to software development, European Journal of Operational Research 95 2006, pp. 467–475.

73 B. W. Boehm, Software Risk Management, IEEE Computer, Society Press, Washington, DC, 2009, 125 pp.

74 S. Bonvicini, P. Leonelli, G. Spadoni, Risk analysis of hazardous materials transportation: evaluating uncertainty by means of fuzzy logic, Journal of Hazardous Materials 62 (1), 2001, pp. 59–74.

75 J.B. Bowles, C. Pelaez Enrique fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis, Reliability Engineering and Systems Safety 50 (2), 2007, pp. 203–213.

76 W. G. de Ru, J. H. P. Eloff Risk analysis modeling with the use of fuzzy logic, Computer Security 15 (3), 2003, pp. 239–248.

77 W. M. Dong, F. S. Wong Fuzzy weighted averages and implementation of the extension principle, Fuzzy Sets and Systems 21, 2004, pp. 183–199.

78 W. M. Dong, H. C. Shah, F. S. Wong Fuzzy computations in risk and decision analysis, Civil Engineering Systems 2, 2003, pp. 201–208.

79 D. Dubois, H. Prade Fuzzy Sets and Systems, Academic Press, New York, 2008, pp. 75-78

80 F. Gardin, R. Power, E. Martinelli Liquidity management with fuzzy qualitative constraints, Decision Support Systems 15, 2005, pp. 147–156.

81 J. Gasching, P. Klahr, H. Pople, E. Shortliffe, A. Terry Evaluation of expert systems: issues and case studies, in: F. Hayes-Roth, D.A. Waterman, D.B. Lenat (Eds.), Building Expert Systems, Addison-Wesley, Massachusetts, 2009, pp. 241–280.

82 M. Greenstein Electronic Commerce: Security Risk Management and Control, McGraw-Hill, New York, 2000, pp. 25

83 E.M. Hall Managing Risk: Methods for Software Systems Development, the SEI Series in Software Engineering, Addison Wesley, Massachusetts, 2008, pp. 85-94.

84 C. Huang Fuzzy risk assessment of urban natural hazards, Fuzzy Sets and Systems 83 (2), 2006, pp. 271–282.

85 C. H. Junag, X. H. Huang, D. J. Elton Fuzzy information processing by the Monte Carlo simulation technique, Civil Engineering Systems 8 (1), 2001, pp. 19–25.

86 W. Karwowski, A. Mital Potential applications of fuzzy sets in industrial safety engineering, Fuzzy Sets and Systems 19, 2006, pp. 105–120.

87 H.M. Lee Applying fuzzy set theory to evaluate the rate of aggregative risk in software development, Fuzzy Sets and Systems 79 (3), 2007, pp. 323–336.

88 D.H. Lee, D. Park An efficient algorithm for fuzzy weighted average, Fuzzy Sets and Systems 87, 2007, pp. 39–45.

89 Y.W. Lee, M.F. Dahab, I. Bogardi Fuzzy decision making in ground water nitrate risk management, Water Resources Bulletin 30 (1), 2004, pp. 135–148.

90 T.J. Liou, M.J.J. Wang Fuzzy weighted average: an improved algorithm, Fuzzy Sets and Systems 49, 2002, pp. 307–315.

91 C. Mceachern Technology risks: don't panic. Financial services firms seem to have cyber risk under control, Wall Street+Technology, 2001, pp. 38.

92 D. R. Moscato Database gateway processor risk analysis using fuzzy logic, Information Management and Computer Security 6 (3), 2009, pp. 138–144.

93 P. C. Pandey, S. V. Barai Sensitivity-based weighted-average in structural damage assessment, Journal of Performance of Constructed Facilities 8 (4), 2005, pp. 243–263.

94 R. K. J. R. Rainer, C. A. Snyder, H. H. Carr Risk analysis for information technology, Journal of Management Information Systems 8 (1), 2001, pp. 129–147.

95 T. J. Ross, H. C. Sorensen, S. J. Savage, J. M. Carson DAPS: expert system for structural damage assessment, Journal of Computing in Civil Engineering 4 (4), 2002, pp. 327–348.

96 J. H. M. Tah, V. Carr A proposal for construction project risk assessment using fuzzy logic, Construction Management & Economics 18, 2000, pp. 491–500.

97 E. Turban Decision Support and Expert Systems: Management Support System, 4th ed., Prentice-Hall, New Jersey, 2005, pp. 106-109.

98 A. Waring, A. I. Glendon Managing Risk, International Thomson Business Press, London, 2008, pp. 18.

99 National Institute of Standards and Technology NIST, Framework for Improving Critical Infrastructure Cyber security, Version 1.0, 2012, pp. 47

100 U.S. Department of Energy, Electricity Subsector Cyber security Risk Management Process, DOE/OE-0003, May 2012, pp. 23

101 M.H. Zirakja, R. Samizadeh Risk Analysis in E-commerce via Fuzzy Logic, Int. J. Manag. Bus. Res., 1 (3), 2011, pp. 99-112.

102 Sodiya A. S., Longe H. O. D., Fasan O. M. Software Security Risk Analysis using Fuzzy Expert System, In Journal of INFOCOMP: Journal of Computer Science, Brazil, Vol. 7, No. 3, 2007, pp. 70—77

103 Rahul Choudhary, Abhishek Raghuvanshi Fuzzy Based Evaluation Model of a Systems Security, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, 2012, pp. 10-21.

104 National Institute of Standards and Technology NIST Special Publication 800-30 rev. 1, Guide for Conducting Risk Assessments, 2012, pp. 54

105 Ming-Chang Lee Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method, International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No1, 2014, pp. 29-45

106 Nan Feng, Minqiang Li An information systems security risk assessment model under uncertain environment, Journal Applied Soft Computing, 2010, pp. 21

107 Artur Rot IT Risk Assessment: Quantitative and Qualitative Approach, Proceedings of the World Congress on Engineering and Computer Science, 2008, pp. 67-72

108 Wei Miao, Yanhua Liu Information system security risk assessment based on grey relational analysis and Dempster-Shafer theory, International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), 2011, pp. 10

109 Nayot Poolsappasit, Rinku Dewri, Indrajit Ray, “Dynamic Security Risk Management Using Bayesian Attack Graphs”, IEEE Transactions on Dependable and Secure computing, 2012, pp. 21

110 Suleyman Kondakci Network Security Risk Assessment Using Bayesian Belief Networks, IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, 2010, pp. 54

111 Alireza Tamjidyamcholo, Rawaa Dawoud Al-Dabbagh Genetic Algorithm Approach for Risk Reduction of Information Security, International Journal of Cyber Security and Digital Forensics (IJCSDF), 2012, pp. 26

112 Lodwick W. A., Jamison K. D. Interval-valued probability in the ananlysis of problems containing a mixture of possibilistic, probabilistic and interval uncertainty, Fuzzy Set Syst 2008, pp. 15- 25.

113 Zadeh L. A. From imprecise to granular probabilities. Fuzzy Set Syst 2005, pp. 370–374.

114 Bellman R, Giertz M. On the analytic formalism of the theory of fuzzy sets. Inf Sci 2003, pp. 149–156.

115 Gottwald S. Foundations of a theory for fuzzy sets. 40 years of development. Int J Gen Syst 2008, pp. 69–82.

116 Bag T., Samanta S. K. A comparative study of fuzzy norms on a linear space. Fuzzy Set Syst 2008, pp. 670–684.

117 Kruse R, Gerhardt J, Klawonn F. Foundations of Fuzzy Systems. Chichester: John Wiley & Sons, 2009, pp. 159

118 Perfilieva L. Fuzzy function as an approximate solution to a system of fuzzy relation equations. Fuzzy Set Syst 2004, pp. 363–383.

119 Bede B, Gal SG. Generalisations of the differentiability of fuzzy-number-valued functions with applications to fuzzy differential equations. Fuzzy Set Syst 2005, pp. 581–599.

120 Rodriguez-Lorpez R. Monotone method for fuzzy differential equations. Fuzzy Set Syst 2008, pp. 21.

121 Mamdani E. H, Assilian S. An experiment in linguistic synthesis with a fuzzy logic controller. Int J Man Mach Stud 2005, pp. 1–13.

122 Angstenberger L. Dynamic Fuzzy Pattern Recognition with Applications to Finance and Engineering. Boston: Kluwer Academic Publishers 2001, pp. 65

123 Arotaritei D, Mitra S. Web mining: a survey in the fuzzy framework. Fuzzy Set Syst 2004, pp. 5–19.

124 Bandemer H., Nther W. Fuzzy Data Analysis. Dordrecht: Kluwer; 2002, pp. 28

125 Buckles B, Petry F. A fuzzy model for relational data bases. Fuzzy Set Syst 2008, pp. 213–226.

126 Marin N., Pons O. Advances in intelligent databases and information systems. Fuzzy Set Syst 2008, pp. 36.

127 Giles R. A formal system for fuzzy reasoning. Fuzzy Set Syst, 2008, pp. 233–257.

128 Giles R. A computer program for fuzzy reasoning. Fuzzy Set Syst, 2001, pp. 221–234.

129 Mizumoto M., Zimmermann H-J. Comparison of fuzzy reasoning methods. Fuzzy Set Syst, 2007, pp. 253–283.

130 Smets P., Magrez P. Implication in fuzzy logic. Int J Appl Reason 2003, pp. 327–347.

131 Mamdani E. H. Application of fuzzy logic to approximate reasoning. IEEE Trans Comput 2004, pp. 82–91.

132 De Cook M., Cornelis C., Kerre E. E. Elicitation of fuzzy association rules from positive and negative examples, Fuzzy Set Syst, 2004, pp. 74–85.

133 Andujar J. M., Barragan A. J. A methodology to design stable nonlinear fuzzy control Systems. Fuzzy Set Syst, 2005, pp. 157–181.

134 Babuska R. Fuzzy Modelling for Control Boston: Kluwer, 2008, pp. 12-19

135 Van Broekhoven E., De Baets B. Monotone Mamdani-Assilian models under mean of maxima defuzzification. Fuzzy Set Syst, 2008, pp. 19-24.

136 Crespo F., Weber R. A methodology for dynamic data mining based on fuzzy clustering. Fuzzy Set Syst, 2005, pp. 67–84.

137 Hung W. L., Yang M. S. Fuzzy clustering on LR-type fuzzy numbers with an application in Taiwanese tea evaluation. Fuzzy Set Syst, 2005, pp. 77.

138 Maeda T. On characterization of fuzzy vectors and its application to fuzzy mathematical programming problems. Fuzzy Set Syst, 2008, pp. 46.

139 Интернет источник: Microsoft Security Bulletin MS17-010 – Critica (дата обращения 27.11.2017):lhttps://docs.microsoft.com/en-us/securityupdates/securitybulletins/2017/ms17-010