

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет радіоелектроніки і телекомунікацій

Кафедра захисту інформації

Пояснювальна записка

до магістерської роботи

на тему: «Аналіз загроз захищеності інформації

від спам-повідомлень»

Виконав: студент 6 курсу, групи РТз-813м
напряму підготовки (спеціальності)

125 «Кібербезпека» («Безпека
інформаційних і комунікаційних систем»)

Єленич Андрій Олександрович

Керівник: к.ф-м.н. доцент Романенко С.М.

Рецензент _____

(прізвище та ініціали)

Запорізький національний технічний університет

Факультет Радіoeлектроніки та телекомунікацій
Кафедра Захисту інформації
Рівень вищої освіти (освітньо-кваліфікаційний рівень) Магістр
Спеціальність 125 Кібербезпека
Напрямок підготовки Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри ЗІ

проф. Л.М. Карпуков

« » 2018 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ
Єленичу Андрію Олександровичу

1. Тема проекту (роботи): Аналіз загроз захищеності інформації від спам-повідомлень
керівник проекту (роботи): доц., к.ф.-м.н. Романенко Сергій Миколайович
затверджені наказом вищого навчального закладу
від “07” лютого 2018 року № 330
2. Строк подання студентом проекту (роботи) 10 грудня 2018 р.
3. Вихідні дані до проекту (роботи): захист інформації, спам-повідомлення, література по темі
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) аналіз принципів і методів захисту інформації від спам-повідомлень
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) слайди з основних результатів проведеного аналізу
6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основна частина	доц., к.ф-м.н. Романенко С.М.		
Економічна частина	доц., к.е.н. Лівовшко Т.В.		
Охорона праці	ст. викл.Писарський А.О.		
Нормоконтроль	ст. викл. Нікуліщев Г.І.		

7. Дата видачі завдання « 03 » вересня 2018 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Складання та затвердження ТЗ, підбір літератури	03.09-16.09.2018	
2	Аналіз різних видів спам-повідомлень	17.09-07.10.2018	
3	Аналіз достоїнств й недоліків відомих підходів до протидії загрозам захищеності інформації, що одержується, зберігається й опрацьовується в системах електронного поштового зв'язку.	08.10-21.10.2018	
4	Розробка алгоритму багатоетапної класифікації й детектування спам- повідомлень	22.10-28.10.2018	
5	Розробка економічної частини	29.10-04.11.2018	
6	Розробка заходів з охорони праці	05.11-11.11.2018	
7	Оформлення графічної частини	12.11-25.11.2018	
8	Оформлення пояснювальної записки	26.11-09.12.2018	

Студент _____ Єленич А.О.
(підпис)

Керівник проекту (роботи) _____ Романенко С.М.
(підпис)

РЕФЕРАТ

ПЗ: 127 стр., 7 рис., 15 табл., 137 источников.

Цель магистерской работы – анализ угроз защищенности информации от спам-сообщений.

Поставленная цель предполагает решение следующих взаимосвязанных задач:

- произвести анализ различных видов спам-сообщений;
- произвести анализ достоинств и недостатков известных подходов к противодействию угрозам защищенности информации, которая получается, хранится и обрабатывается в системах электронной почтовой связи;
- разработать алгоритм многоэтапной классификации и детектирования спам-сообщений.

ЗАЩИТА ИНФОРМАЦИИ, СПАМ-СООБЩЕНИЯ, УГРОЗЫ И
УЯЗВИМОСТИ, ЭЛЕКТРОННАЯ ПОЧТОВАЯ СВЯЗЬ

СОДЕРЖАНИЕ

Перечень сокращений	7
Введение	8
1 Анализ задачи автоматической фильтрации сообщений, как задачи обеспечения информационной безопасности	10
1.1 Анализ понятия спама	10
1.2 Признаки, классифицирующих спам - сообщения	11
2 Основные угрозы информационной безопасности	14
2.1 Основные угрозы информационной безопасности от различных видов спам - сообщений	14
2.2 Основные методы борьбы со спамом	17
2.3 Концепция построения системы фильтрации спама	47
3 Разработка архитектуры интеллектуальной системы фильтрации спам - сообщений	48
3.1 Рассмотрение задачи классификации электронной информации, передаваемой по каналам связи, на примере фильтрации спама	48
3.2 Разработка архитектуры интеллектуальной системы фильтрации спам- сообщений	49
3.3 Разработка алгоритма заполнения системы фильтрации	64
3.4 Разработка алгоритма фильтрации документа	67
4 Экономическое обоснование магистерской работы	76
4.1 Планирование разработки	76
4.2 Построение сетевого графика	79
4.3 Расчет параметров сетевого графика	81

4.4	Определение затрат на разработку и проектирование	83
4.5	Расчет основной и дополнительной заработной платы	84
4.6	Расчёт эксплуатационных расходов	85
4.7	Накладные расходы	88
4.8	Эффективность разработки	89
5	Охрана труда и безопасность в чрезвычайных ситуациях	95
5.1	Анализ потенциальных опасностей	96
5.2	Мероприятия по обеспечению производственной санитарии, безопасности и гигиены труда	99
5.3	Мероприятия по пожарной безопасности	103
5.4	Мероприятия по обеспечению безопасности в чрезвычайных ситуациях	106
	Заключение	114
	Список литературы	115

СПИСОК ЛИТЕРАТУРЫ

1. Abadi, M., Burrows, M., Manasse, M. and Wobber, T.: 2003, Moderately Hard, Memory-Bound Functions, Proceedings of the 10th Annual Network and Distributed System Security Symposium, pp. 25-39.
2. Allman, E.: 2003, Spam, Spam, Spam, Spam, Spam, The FTC and Spam, ACM queue 1(6), p. 92.
3. Alonso Eduardo, Kudenko Daniel, Kazakov Dimitar: Adaptive Agents and Multi-Agent Systems: Adaptation and Multi-Agent Learning (Lecture Notes in Computer Science), Springer, 2003, pp. 135-137.
4. Androutsopoulos, I., Magirou, E. and Vassilakis, D.: 2005, A Game Theoretic Model of Spam E-Mailing, Proceedings of the 2nd Conference on Email and Anti-Spam (CEAS 2005), pp. 12-15.
5. Anti-Spam Technical Alliance (ASTA): 2004, Anti-spam technical alliance technology and policy report, Technical report, pp. 223-226.
6. Anti-Spam Technical Alliance (ASTA): 2004, Anti-spam technical alliance technology and policy report, Technical report, pp. 62-63.
7. Back, A.: 2002, Hashcash - A Denial of Service Counter-Measure, <http://www.hashcash.org/papers/hashcash.pdf>, p. 2.
8. BBC: 2003, E-mail vetting blocks mps' sex debate, <http://news.bbc.co.Uk/1/hi/uk politics/2723 85 1.stm>, pp. 1-2.
9. Bless, R., Conrad, M. and Hof, H.-J.: 2005, Spam Protection by using Sender Address Verification Extension (SAVE). <http://doc.tm.uka.de/2005/SAVE.pdf>, p. 1.
10. Bundesamt f.ur Sicherheit in der Informationstechnik (BSI): 2005, Antispam -Strategien: Unerw.unschte E-mails erkennen und abwehren, p. 75.
11. Callas, J., Donnerhacke, L., Finney, H. and Thayer, R.: 1998, OpenPGP Message Format, RFC 2440, IETF Network Working Group, pp. 78-81.
12. Campbell, K.: 1994, A NET.CONSPIRACY SO IMMENSE...Chatting With Martha Siegel of the Internet's Infamous Canter & Siegel,

[http://www.eff.org/legal/cases/Canter Siegel/c-and-s summary.article](http://www.eff.org/legal/cases/Canter_Siegel/c-and-s_summary.article), p. 23.

13. Carreras, X. and Mrquez, L.: 2001, Boosting Trees for Anti-Spam Email Filtering, in T. Chark (ed.), Proceedings of the International Conference on Recent Advances in Natural Language Processing, p. 126.

14. Cavedon Lawrence, Maamar Zakaria, Martin David, Benatallah Boualem: Extending Web Services Technologies: The Use of Multi-Agent Approaches, Springer, 2005, pp. 57-59.

15. Chhabra, S. and Siefkes, C: 2004, Spam Filtering using a Markov Random Field Model with Variable Weighting Schemas, Proceedings of the 4th IEEE International Conference on Data Mining, pp. 347-350

16. Chris van Aart: Organizational Principles for Multi-Agent Architectures (Whitestein Series in Software Agent Technologies), Birkhauser, 2005, pp. 37-39.

17. Coding email links to avoid spam: 2003, <http://www.bronzeage.com/nospam/>, p. 2.

18. Cohen, W.: 1996, Learning rules that classify e-mail, Papers from the AAA! Spring Syposium on Machine Learning in Information Access, pp. 18-25.

19. Commtouch: 2006, Spam statistics, <http://www.commtouch.com/Site/ResearchLab/statistics.asp>, pp. 1-3.

20. Cranor, L. F. and LaMacchia, B. A.: 1998, Spam!, Communications of the ACM 41(9), pp. 74-83.

21. Crawford, E., Kay, J. and McCreath, E.: 2001, Automatic induction of rules for e-mail classification, Proceedings of the Sixth Australasian Document Computing Symposium, pp. 34-35.

22. Crocker, D., Leslie, J. and Otis, D.: 2005, Certified Server Validation (CSV), Internet draft, IETF Network Working Group, pp. 58-59.

23. Damiani, E., De Capitani di Vimercati, S., Paraboschi, S. and Samarati, P.: 2004, P2p-based collaborative spam detection and filtering, Proceedings of the Fourth International Conference on Peer-to-Peer Computing, pp. 176-183.

24. Danish, H.: 2004, The RMX DNS RR and method for lightweight SMTP sender authorization, Internet draft, IETF Network Working Group, pp. 117-119.

25. David P. Buse, Qing-Hua Wu: IP Network-based Multi-agent Systems for Industrial Automation: Information Management, Condition Monitoring and Control of Power Systems, Springer, 2006, pp. 78-80.
26. DECLUDE Internet Security Software: 2005, List of All Known DNSbased SpamDatabases, <http://www.decmde.com/Articles.asp?ID=97>, p. 3.
27. DeKok, A.: 2004, Lightweight MTA Authentication Protocol (LMAP) Discussion and Applicability Statement, Internet draft, IETF Network Working Group, pp. 65-67.
28. Delany, M.: 2005, Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys), Internet draft, IETF Network Working Group, pp. 202-204.
29. Denning, P.: 1982, Electronic junk, Communications of the ACM 25(3), 163-165, pp. 75-77.
30. Directive 2002/58/EC: 2002, Official Journal of the European Communities, L 201/37, pp. 36-37.
31. Doll, J.: n.d., Spam Attack, <http://www.joes.com/spammed.html>, p. 3.
32. Drawes, R.: 2002, An artificial neural network spam classifier, Technical report. www.interstice.com/drewes/cs676/spam-nn/spam-nn.html, p. 2.
33. Drucker, H., Wu, D. and Vladimir N. Vapnik: 1999, Support Vector Machines for Spam Categorization, IEEE Transactions on Neural Networks 10(5), pp. 1048-1054.
34. Dwork, C. and Naor, M.: 2002, Proving via Processing or Combatting Junk Mail, in D. Boneh (ed.), Proceedings of the 22nd Annual International Cryptology Conference (CRYPTO 2002), number 740 in LNCS, Springer, pp. 137-147.
35. Email Service Provider Coalition: 2003, Project Lumos: A Solutions Blueprint for Solving the Spam Problem by Establishing Volume Email Sender Accountability, Technical report, pp. 76-78.
36. Email-policy.com: 2004, Real-time Spam Black Lists (RBL), <http://www.email-policy.com/Spam-black-lists.htm>, p. 4.
37. EU: 2004, Cooperation Procedure Concerning the Transmission of

Complaint Information and Intelligence Relevant to the Enforcement of Article 13 of the Privacy and Electronic Communication Directive 2002/58/EC, or Any Other Applicable National Law Pertaining to the Use of Unsolicited Electronic Communications, pp. 69-71.

38. Evett, D.: 2006, Spam Statistics 2006, <http://spam-filterreview.toptenreviews.com/spam-statistics.html>, pp. 5-6.

39. Fabio Luigi Bellifemine, Giovanni Caire, Dominic Greenwood: *Developing Multi-Agent Systems with JADE* (Wiley Series in Agent Technology), Wiley, 2007, pp. 117

40. Fahmann, S.: 2002, Selling interrupt rights: A way to control unwanted e-mail and telephone calls, *IBM Systems Journal* 41(4), pp. 759-766.

41. Fecyk, G.: 2003, Designated Mailers Protocol, Internet draft, IETF Network Working Group, pp. 91-93.

42. Fenton, J. and Thomas, M.: 2005, Identified Internet Mail, J. fenton and m. thomas, IETF Network Working Group, pp. 165-167.

43. Ferris Research: 2005, The Global Economic Impact of Spam, 2005. Report #409, pp. 172-173.

44. FTC: 2004, National Do Not Email Registry A Report to Congress, Technical report, pp. 83-84.

45. Gabber, E., Jakobsson, M., Matias, Y. and Mayer, A. J.: 1998, Curbing Junk E-Mail via Secure Classification, *Proceedings of the Second International Conference on Financial Cryptography*, pp. 198-213.

46. Garfinkel, S.: 2003, Email-Based Identification and Authentication: An Alternative to PKI?, *IEEE Security & Privacy* 1(6), pp. 20-26.

47. Gauthronet, S. and Etienne, D.: 2001, Unsolicited Commercial Communications and Data Protection, p. 128.

48. Graham, P.: 2003, Better Bayesian Filtering, *Proceedings of the 2003 Spam Conference*, pp. 117-119.

49. Hall, R.: 1996, Channels: Avoiding Unwanted Electronic Mail, *Proceedings of the DIMACS Symposium on Network Threats*, pp. 135-137.

50. Hans-Dieter Burkhard, Gabriela Lindemann, Rineke Verbrugge: Multi-Agent Systems and Applications V: 5th International Central and Eastern European Conference on Multi-Agent Systems, CEEMAS 2007, Leipzig, Germany,... (Lecture Notes in Computer Science), Springer, 2007, pp. 144-146.
51. InfoSec: 2004, Email Spamming (include scam), Technical report, pp. 78-80.
52. Ironport: 2006, Internet Email Traffic Emergency: Spam Bounce Messages are Compromising Networks, <http://www.ironport.com/bouncereport/>, pp. 3.
53. ITU: 2003, Memorandum of Understanding Between the Korea Information Security Agency and the Australian Communications Authority and the National Office for the Information Economy of Australia Concerning Cooperation in the Regulation of Spam, pp. 57-59.
54. ITU: 2005a, A Comparative Analysis of Spam Laws: The Quest for a Model Law, Background Paper for the ITU WSIS Thematic Meeting on Cybersecurity, Geneva, Switzerland, 28 JUNE 1 JULY 2005, pp. 119-120.
55. ITU: 2005b, ITU Survey on Anti-spam Legislation Worldwide, pp. 28-29.
56. Johansson, E.: n.d., Camram, www.camram.org, pp. 2-3.
57. Kocher, J.: 2004, Anti-spam-gesetze, DFN Mitteilungen (64 - 3), pp. 29-30.
58. Katsumi Inoue, Ken Satoh, Francesca Toni: Computational Logic in Multi-Agent Systems: 7th International Workshop, CLIMA VII, Hakodate, Japan, May 8-9, 2006, Revised Selected and Invited Papers (Lecture Notes in Computer Science), Springer, 2007, p. 150.
59. Leibzon, W.: 2005a, Email Security Anti-Spoofing Protection with Path and Cryptographic Authentication Methods, <http://www.metasignatures.org/path> and [cryptographic authentication.htm](http://www.metasignatures.org/cryptographic_authentication.htm), p. 2.
60. Leibzon, W.: 2005b, META Signatures (Message Enhancements for Transmission Authorization), Technical report, http://www.metasignatures.org/meta_signatures_proto-col.htm, pp. 1-2.
61. Lin Hong: Architectural Design of Multi-Agent Systems: Technologies and

Techniques , IGI Global, 2007, pp. 123-125.

62. Loder, T., van Alstyne, M. and Walsh, R.: 2004, Information Asymmetry and Thwarting Spam, Technical report, University of Michigan, pp. 52-54.

63. Lyon, J. and Wong, M.: 2005, Sender III: Authenticating E-Mail, Internet draft, IETF Network Working Group, pp. 160-161.

64. Lyon, J.: 2005, Purported Responsible Address in E-Mail Messages, Internet draft, IETF Network Working Group, pp. 29-31.

65. Metzger, J., Schillo, M. and Fischer, K.: 2003, A Multiagent-Based Peer-to-Peer Network in Java for Distributed Spam Filtering, in V. Mark, J. Miller and M. Pechoucek (eds), Proceedings of the 3rd International Workshop of Central and Eastern Europe on Multi-Agent Systems (CEEMAS), pp. 616-625.

66. Microsoft: 2004, Email Postmarks, pp. 119-121.

67. Moreno Antonio, Pavon Juan: Issues in Multi-Agent Systems (Whitestein Series in Software Agent Technologies and Autonomic Computing), Birkhauser Basel, 2007, pp. 112-114.

68. Moustakas, E., Ranganathan, C. and Duquenoy, P.: 2005, Combating Spam through Legislation: A Comparative Analysis of US and European Approaches, Proceedings of the Second Conference on Email and Anti-Spam (CEAS 2005), pp. 126-129.

69. Myers, J.: 1997, Simple Authentication and Security Layer (SASL), RFC 2222, IETF Network Working Group, pp. 117-119.

70. Myers, J.: 1999, SMTP Service Extension for Authentication, RFC 2554, IETF Network Working Group, p. 92.

71. Ngoc Thanh Nguyen, Adam Grzech, Lakhmi C. Jain: Agent and Multi-Agent Systems: Technologies and Applications: First KES International Symposium, KES-AMSTA 2007, Wroclaw, Poland, May 31-June 1, 2007, Proceedings (Lecture Notes in Computer Science), Springer, 2007, pp. 94-97.

72. Ngoc Thanh Nguyen, Geun Sik Jo, Robert J. Howlett, Lakhmi Jain: Agent and Multi-Agent Systems: Technologies and Applications: Second KES International Symposium, KES-AMSTA 2008, Incheon, Korea, March 26-28, 2008, Proceedings

(Lecture Notes in Computer Science), Springer, 2008, pp. 78-81.

73. Nikitin A. P. Multi-Agent Anti-Spam System. P. 227-229. Proceeding of the Workshop on Computer Science and Information Technologies (CSIT'2005), Ufa, September 18-21, 2005. Volume 2, pp. 227-229.

74. Nikitin A.P., Valeev S.S. Intellectual Anti-Spam System. 9th International Workshop on Computer Science and Information Technologies CSIT'2007, Ufa-Krasnounsolsk, Russia, 2007, pp. 57-59.

75. NOIE: 2003, Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered, Technical report. [www.noie.gov.au/publications/NOIE/spam/final report/SPAMreport.pdf](http://www.noie.gov.au/publications/NOIE/spam/final%20report/SPAMreport.pdf), p. 1.

76. Nucleus Research: 2003, Spam: The Silent ROI Killer, pp. 117-118.

77. OECD: 2004a, Background Paper for the OECD Workshop on Spam, pp. 40-41.

78. OECD: 2004b, Report of the 2nd OECD Workshop on Spam, pp. 17-18.

79. OECD: 2004c, Report on non-OECD Countries' Spam Legislation, pp. 205-206.

80. OECD: 2005a, Anti-Spam Law Enforcement Report, pp. 107-112.

81. OECD: 2005b, Anti-Spam Regulation, pp. 29-32.

82. OECD: 2005c, Spam Issues in Developing Countries, pp. 39-41.

83. Otis, D., Crocker, D. and Leslie, J.: 2005, Client SMTP Authorization (CSA), Internet draft, IETF Network Working Group, pp. 72-74.

84. Postel, J.: 1975, On the Junk Mail Problem, RFC 706, IETF Network Working Group, p. 11.

85. Rafael H. Bordini, Jomi Fred Hubner, Michael Wooldridge: Programming Multi-Agent Systems in AgentSpeak using Jason (Wiley Series in Agent Technology), Wiley-Interscience, 2007, pp. 46-48.

86. Rafael H. Bordini, Mehdi Dastani, Jurgen Dix, Amal El Fallah Seghrouchni: Programming Multi-Agent Systems: 4th International Workshop, ProMAS 2006, Hakodate, Japan, May 9, 2006, Revised and Invited Papers (Lecture Notes in Computer Science), Springer, 2007, pp. 56-59.

87. Ramsdell, B.: 2004, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, RFC 3851, IETF Network Working Group, pp. 52-54.
88. Raz, U.: n.d., How do spammers harvest email addresses, <http://www.private.org.il/harvest.html>, p. 1.
89. Ron Sun: Cognition and Multi-Agent Interaction : From Cognitive Modeling to Social Simulation, Cambridge University Press, 2005, p. 103.
90. Schryen, G. and Hoven, R.: 2004, Appropriateness of Lightweight MTA Authentication Protocols for Fighting Spam, Proceedings of IPSI International Conference on Advances in the Internet, Processing, Systems, and Interdisciplinary Research, pp. 98-
91. Schryen, G.: 2004b, Approaches addressing spam, Proceedings of the HHCCII, pp. 41-43.
92. Sester, P. and Mutschler, S.: 2006, Neue Kooperationen und rechtliche Entwicklungen im Kampf gegen Spam, Informatik-Spektrum 29(1), pp. 14-22.
93. Shamma Jeff: Cooperative Control of Distributed Multi-Agent Systems, Wiley-Interscience, 2008, pp. 89-91.
94. Sophos: 2005a, CAN-SPAM Act can do better, <http://www.sophos.com/pressoffice/news/articles/2005/12/canspam05.html>, p. 2.
95. Spamhaus: 2006, Spamhaus Statistics : The Top 10, <http://www.spamhaus.org/statistics/countries.lasso>, p. 1.
96. Spamhaus: n.d., The Definition of Spam, <http://www.spamhaus.org/definition.html>, p. 1-2.
97. Spammer-X: 2004, The SPAM Cartel Why Spammers Spam, Syngress Media, p. 56.
98. Stumpf, M. and Hoehne, S.: 2005, Marking Mail Transfer Agents in Reverse DNS with TXT RRs, Internet draft, IETF Network Working Group, pp. 15-19.
99. Tanase, M.: 2003, IP Spoofing: An Introduction, <http://www.securityfocus.com/infocus/1674>, pp. 1-2.
100. Templeton, B.: n.d.a, E-stamps,

<http://www.templetons.com/brad/spam/estamps.html>, pp. 1.

101. Templeton, B.: n.d.b, Origin of the term "spam" to mean net abuse, <http://www.templetons.com/brad/spamterm.html>, p. 54.

102. The Government of Hongkong: n.d., Nigerian letters, <http://www.mfo.gov.hk/police/pda/con-tricks/con7.htm>, pp. 2-3.

103. THE LONDON ACTION PLAN On International Spam Enforcement Cooperation: 2004, <http://www.londonactionplan.org>, p. 4.

104. The New York Times: 2003, We Hate Spam, Congress Says (Except Ours), <http://www.nytimes.com>, p. 3.

105. Tom Wagner, Omer F. Rana: Infrastructure for Agents, Multi-Agent Systems, and Scalable Multi-Agent Systems, Springer, 2001, pp. 117-119.

106. Tompkins, T. and Handley, D.: 2003, Giving E-mail Back to the Users: Using Digital Signatures to Solve the Spam Problem, *FirstMonday* 8(9), pp. 34-36.

107. Toru Ishida, Les Gasser, Hideyuki Nakashima: Massively Multi-Agent Systems I: First International Workshop, MMAS 2004, Kyoto, Japan, December 10-11, 2004, Revised Selected and Invited Papers (Lecture Notes in Computer Science), Springer, 2005, p. 27.

108. Turner, D. A. and Havey, D. M.: 2004, Controlling Spam through Lightweight Currency, *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, pp. 70-72.

109. Turner, D. and Ross, K.: 2003, A Lightweight Currency Paradigm for the P2P Resource Market, pp. 107-109.

110. Valeev S.S., Nikitin A.P. Multi-agent system of filtering of the spam, *CSIT-2008. -Уфа.-2008*, pp. 224-227

111. von Ahn, L., Blum, M. and Langford, J.: 2004, Telling Humans and Computers Apart Automatically, *Communications of the ACM* 47(2), pp. 57-60.

112. von Ahn, L., Blum, M., Hopper, N. and Langford, J.: 2003, CAPTCHA: Using hard AI problems for security, *Proceedings of Eurocrypt*, pp. 294-311.

113. Wong, M. and Schlitt, W.: 2005, Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, version 1, Internet draft, IETF Network

Working Group, pp. 52-54.

114. Zhou, F., Zhuang, L., Zhao, B., Huang, L., Joseph, A. and Kubiawicz, J.: 2003, Approximate object location and spam filtering on peer-to-peer systems, Proceedings of ACM/FIP/USENIX International Middleware Conference, pp. 22-26.

115. Анношкина Ж.Г. Морфологический процессор русского языка // Альманах "Говор". - Сыктывкар, 1995.-стр. 17-23.

116. Аралбаев Т. 3. Особенности синтеза оптимальной мажоритарной функции в задаче распознавания образов // Проблемы управления и информатики. - 2002. -№5.-С. 98-102

117. Основы информационной безопасности. / Белов Е.Б., Лось Р.В., Мещеряков Р. В., Шелупанов А. А. - М.: Горячая линия-Телеком, 2006. - 544 с.

118. Богуславский И.М., Семантический компонент лингвистического процессора // И.М. Богуславский, Л.Л Цинман. Семантика и информатика. - М., 1990. - Вып. 30. - стр. 5-30.

119. Валеев С.С. Многоуровневая система фильтрации спама на основе технологий искусственного интеллекта. Валеев С.С., Никитин А. П Вестник УГАТУ, - Уфа. - 2008, стр. 215-219.

120. Валеев С.С., Система автоматической интеллектуальной классификации текстов. / С.С.Валеев, А. П Никитин Самара. - 2008, стр. 44-46

121. Волкова И.А., Адаптивный синтаксический анализатор // [И.А.Волкова, М.Г.Мальковский, Н.В.Одинцев] Труды Международной конференции ДИАЛОГ-2003. - Протвино, 2003.-стр. 476-480.

122. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. -М.: Энергоатомиздат, 1994.

123. Горелик А. Л., Скрипкин В. А. Методы распознавания. - М.: Высшая

школа, 2004.-261 с.

124. Городецкий Б.Ю. Компьютерная лингвистика: моделирование языкового общения // Новое в зарубежной лингвистике. - М., 1989. — Вып. 24, стр. 125-127.

125. Гурькин, Ю. Н. Модельный прогноз для числа сетевых вторжений на будущие годы /Ю.Н.Гурькин, Ю.А.Семенов // Труды XLVI научной конференции МФТИ 25-26 ноября 2005 года, [Электронный ресурс]—Режим доступа: http://saturn.itep.ru/intr_forecast.htm

126. Демьянков В.З. Основы теории интерпретации и ее приложения в вычислительной лингвистике. - М., 1985, стр. 136-138.

127. Кобзарева Т.Ю. Принципы сегментационного анализа русского предложения // Московский лингвистический журнал. - М., 2004. - Т. 8. - № 1, стр. 23-24.

128. Мельчук И.А. Опыт теории лингвистических моделей "Смысл «-> Текст". -М., 1999, стр. 65-66.

129. Никитин А. П. Интеллектуальная система фильтрации сообщений. А.П. Никитин С.С.Валеев Стр. 246-247. Восьмая Международная научно-техническая конференция «Проблемы техники и технологии телекоммуникации», 26-28 ноября 2007 г. Уфимск. гос. авиац. техн. ун-т. - Уфа, 2007 -382 с, стр. 246-247.

130. Никитин А. П. Интеллектуальная система автоматической классификации информации. Стр. 18-19. Мавлютовские чтения: Всероссийская молодежная научная конференция, посвященная 75-летию УГАТУ: сборник трудов. Т. 3. Уфимск. гос. авиац. техн. ун-т, - Уфа, 2007. -232 с, стр. 18-19

131. Никитин А. П. Модульная система классификации электронных

сообщений. Стр. 95-96. Туполевские чтения: международная молодежная научная конференция, посвященная 1000-летию города Казани, 10-11 ноября 2005 г.: Материалы конференции. Том III. Казань: Изд-во Казан, гос. техн. ун-та. 2005. 178 с, стр. 95-96

132. Никитин А. П. Система интеллектуальной фильтрации спама. Труды I международной заочной научно-технической конференции «Актуальные проблемы безопасности информационных технологий» (АПроБИТ-2007) Красноярск -2007.

133. Журавель М. О., Методичні вказівки до виконання розділу «Охорона праці та безпека у надзвичайних ситуаціях» в магістерських дипломних роботах зі спеціальності 141 - «Електроенергетика, електротехніка та електромеханіка» з спеціалізації – «Електричні машини і апарати», «Електричні та електронні апарати», «Електромеханічні системи автоматизації та електропривод», «Електротехнічні системи електроспоживання», «Електромеханічне обладнання електроємних виробництв» / Укл. : М. О. Журавель – Запоріжжя: ЗНТУ, 2018

134. Спам и фишинг в 2017 году Д.Гудкова, [и другие] [Электронный ресурс]—Режим доступа: <https://securelist.ru/spam-and-phishing-in-2017/88630/>

135. Методичні вказівки до виконання економічного розділу дипломних та магістерських проектів для студентів спеціальності 7.05090301, 8.05090301 «Інформаційні мережі зв'язку» всіх форм навчання. / Укладачі: Бобровникова Р.Г., Круглікова В.В. – Запоріжжя: ЗНТУ, 2012 – 18 с.

136. Методичні вказівки до практичної роботи «Визначення повітрообміну у виробничих та адміністративних приміщеннях» з дисципліни «Охорона праці в галузі» для студентів всіх форм навчання / Укл. О.Л. Скуйбіда – Запоріжжя: ЗНТУ, 2011. – 18 с.

137. Методичні вказівки до виконання розділу «Охорона праці та безпека у надзвичайних ситуаціях» у дипломних проектах (роботах) студентів спеціальностей 7(8).05090101 «Радіотехніка», 7(8).05090301 «Інформаційні мережі зв'язку», 7(8).05080101 «Мікро- та наноелектронні прилади і пристрої», 7.18010010 «Якість, стандартизація та сертифікація», 7(8).05090201 «Радіоелектронні апарати та засоби», 7(8).05090203 «Інтелектуальні техно-логії мікросистемної радіоелектронної техніки», 7(8).17010201 «Системи технічного захисту інформації, автоматизація її обробки», 7(8).17010101 «Безпека інформаційних і комунікаційних систем» усіх форм навчання / Укл.: О.В. Коробко, А.Є. Островська – Запоріжжя: ЗНТУ, 2014. – 22 с.