ПЕРЕЛІК ДЖЕРЕЛ

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.

2. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.

3. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.

4. Закон України «Про інформацію». Верховна Рада України. Постанова від 02.10.1992 № 2658-XII.

5. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.

6. Правила посиленої сертифікації, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3, зареєстровані в Міністерстві юстиції України 27.01.2005 за № 104/10384 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50).

7. *Горбенко І.Д., Гриненко Т.О.* Захист інформації в інформаційно-телекомунікаційних системах. Част. 1. Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. – 367 с.

8. *Бессалов А., Телиженко А.* Криптосистемы на эллиптических кривых. – К.: «Політехніка», 2004. – 224 с.

9. *Задірака В., Олексик О.* Комп'ютерна криптологія. – К., 2002. – 502 с.

10. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты та языке СИ. – М.: «Триумф», 2002. – 797 с.

11. N. Koblitz. Hyperelliptic cryptosystems. Journal of cryptology, No 1. Pp 139-1501989.

12. I. Blake, G. Seroussi, and N. Smart. Elliptic Curves in Cryptography. Cambridge Universiti Press, 1999. London Mathematical Societi Lecture Note Series 265.

13. ISO/IEC 9594-8 | ITU-T Rec. X.509:2005. Information technology – Open systems interconnection – The Directory: public-key and attribute certificate frameworks.

14. ДСТУ ITU-T Rec. X.509 | ISO/IEC 9594-8:2006 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів».

15. ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures.

16. ДСТУ ISO/IEC 15946-2:2006 (проект) «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 2: Електроні цифрові підписи».

17. ISO/IEC 13888-1:2004, IT security techniques – Non-repudiation – Part 1: General.

18. ДСТУ ISO/IEC 13888-1:1997 «Інформаційні технології. Методи захисту. Неспростовність. Частина 1: Загальні положення» (переглянуто у 2004 році).

19. ISO/IEC 13888-3:1998, Information Technology – Security Techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.

20. ДСТУ ISO/IEC 13888-3:1998. «Інформаційні технології. Методи захисту. Неспростовність. Частина 3: Методи, що ґрунтуються на використанні асиметричних алгоритмів».

21. ISO/IEC 11770-3: 2008 Information technology – Security techniques – Key management Part 3: Mechanisms using asymmetric techniques.

22. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3: Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях».

23. ISO/IEC 9798-3 Information technology – Security techniques – Entity authentication – Part3: Mechanisms using digital signature techniques.

24. ДСТУ ISO/IEC 9798-3 «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 3: Механізми, що ґрунтуються на використанні алгоритмів цифрового підпису».

25. ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers.

26. ДСТУ ISO/IEC 18033-2 (проект) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2: Асиметричні шифри».

27. ISO/IEC 15946-4:2004 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery.

28. ДСТУ ISO/IEC 15946-4 (проект) «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 4: Цифрові підписи із відновленням повідомлень».

29. ISO/IEC 9796-3:2006 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms (містить 5 механізмів з ISO/IEC 15946-4:2004).

30. ISO/IEC 15946-1:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.

31. ДСТУ ISO/IEC 15946-1:2006 «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 1. Основні положення».

32. ISO/IEC 15946-1:2008 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.

33. ISO/IEC CD 15946-5:2008 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation.

34. ISO/IEC 14888-3:2006 Information technology – Security techniques – Digital signatures with appendix Part 3: Discrete logarithm based mechanisms (містить 3 механізми з ISO/IEC 15946-2:2002).

35. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».

36. ISO/IEC 15946-3:2002 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.

37. ДСТУ ISO/IEC 15946-3:2006 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3: Установлення ключів».

38. ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

39. ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. Геш-функції. Частина 3: Спеціалізовані геш-функції».

40. ГОСТ 34.310-95 «Информационные технологии. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма».

41. ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хеширования».

42. IEEE P 1363-2000. Standard Specification for public key cryptography. 2000.

43. FIPS PUB 186-1994. Digital signature standard. National Institute of standard and technology, 1994.

44. American National Standard X9.62-1999. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm, 1999.

45. FIPS PUB 186-2-2000. Digital signature standard. National Institute of standard and technology, 2000.

46. FIPS PUB 186-3-2009. Digital signature standard: 2009. National Institute of standard and technology. – 2009.

47. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи. – М.: Госстандарт России, 2001. – 20 с.

48. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

49. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

50. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

51. Столлингс В. Криптография и защита сетей. – Изд-во «Вильямс». М., 2001. – 669 с.

52. American National Standard X9.63-2000. Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography, 2000.

53. A. Menezes, Y. Wu, R. Zuccherato. An Elementary Introduction to Hyperelliptic Curves. Springer – Verlag, Berlin, Germany, 1998.

54. *Горбенко І.Д., Мелецький А.П., Погребняк К.А., Шевченко Д.В.* Билинейное спаривание точек эллиптических кривых и его теоретические основы. // Прикладная радиоэлектроника. – 2006. Том 5. № 1. – С. 3–13.

55. *Горбенко І.Д., Мелецький А.П., Погребняк К.А., Шевченко Д.В.* Методы выполнения билинейных спариваний точек эллиптических кривых в крипто-

графических приложениях. // Прикладная радиоэлектроника. – 2006. Том 5. – № 1. – С. 13–18.

56. ДСТУ ISO/IEC 15946-3:2002 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів».

57. Національна система електронного цифрового підпису. Технічні специфікації форматів представлення базових об'єктів. Формат підписаних даних.

58. Національна система електронного цифрового підпису. Технічні специфікації протоколів взаємодії. Протокол визначення статусу сертифікату.

59. Національна система електронного цифрового підпису. Технічні специфікації протоколів взаємодії. Протокол фіксування часу.

60. Національна система електронного цифрового підпису. Технічні специфікації форматів криптографічних повідомлень. Захищені дані.

61. *Бондаренко М.Ф., Горбенко И.Д., Черных С.П., Потий А.В.* Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих ИТ-систем // Радиотехника. – 2002. – Вып. 126. – С. 5–17.

62. *Горбенко І.Д., Демехін В.А., Горбенко Ю.І., Потій О.В., Онопрієнко В.В., Батюшко С.С.* Стан та проблемні питання створення та розвитку національної інфраструктури відкритих ключів. Прикладна радіоелектроніка. – 2006. Том 5. – № 1. – С. 41–51.

63. *Рембо Мао.* Современная криптография. Теория и практика. Компания Hewlett-Packard. – Санкт-Петербург–Киев, 2005. – 763 с.

64. *Горбенко И.Д., Збитнев С.И. Поляков А.А.* Сравнительный анализ ЦП в группах точек эллиптических кривых. // Радиотехника: Всеукр. Межвед. Научн.-техн. Сб. – 2002. – Вып. 126. – С. 71–84.

65. D.Richard Kuhn, Vincent C. Hu, W.Timothy Polk, Shu-Jen Chang. "Introduction to Public Key Technology and the Federal PKI Infrastructure". NIST SP 800-32, 2001.

66. W.Burr, D.Dodson, N.Nazario, W.Timothy Polk. Minimum Interoperability Specification for PKI Components. V.1 (MISPC). NIST SP 800-15, 1997.

67. Advanced and Remaining Challenges to Adopting of Public Key Infrastructure Technology. U.S. General Accounting Office. GAO-01-277, 2001.

68. X. 509 Certificate Policy for the Federal Bridge Certification Authority (FBCA). V.1.06, 2000.

69. Status of Federal Public Key Infrastructure Activities of Major Federal Departament and Agencies. U.S. General Accounting office, GAO-04-157. 2003.

70. Government of Canada Public Key Infrastructure. White Paper. MG-15a, 1998.

71. Certificate Issuing and Management Components Family of Profiles. NIST PKI Team, 2001.

72. Global Status Report on PKI legistation. WP – LEG – 002. – Radicchioo White Paper.

73. G. Endersz Electronic Signature and PKI Standartisation in Europe. – 2000, Tella.

74. Національна система електронного цифрового підпису. Центральний засвідчувальний орган. Регламент роботи (тимчасовий). Версія 1.0. 2006 р.

75. Національна система електронного цифрового підпису. Закрите акціонерне товариство «Інфраструктура відкритих ключів». Регламент роботи Версія 1.0. 2005 р.

76. Національна система електронного цифрового підпису. Центральний засвідчувальний орган. Регламент роботи (тимчасовий). Версія 1.1. 2007 р.

77. Національна система електронного цифрового підпису. Центральний засвідчувальний орган. Політика сертифікації національного мостового центру сертифікації ключів (проект). Версія 1.0. 2007 р.

78. Ukrainian PKI. Certificate Policy (draf). Version 0.1. 2007.

79. Национальна система электронного цифрового підпису. Центральний засвідчувальний орган. Критерії та методологія перехресної сертифікації (проект). Версия 1.0.

80. Національна система электронного цифрового підпису. Центральний засвідчувальний орган. Регламент надання послуги фіксування часу (проект). Версия 1.0.

81. X. 509 Certificate Policy for the Federal Bridge Certification Authority (FBCA). V.2.2. 28.09. 2006.

82. Goverment of Canada Government On-line Certificate. Policies General Purpose.ConfidetialityGeneral Purepose. Digital Signature Limited Purpose.

83. ETSI TS 102 042 – Policy requirements for Certification Authorities issuing public key certificates, v. 1.1.1, dated April 2002.

84. ETSI TS 101 456 – Policy requirements for Certification Authorities issuing qualified certificates, v.1.2.1, dated April 2002.

85. A. Shamir. Identity-based cryptosystems and signature schemes. In CRYPTO '84, volume 196 of Lecture Notes in Computer Science, pages 47–53. Springer Verlag, 1984.

86. Feng Bao. Security Analysis of a Password Authenticated Key Exchange Protocol. In Colin Boyd and Wenbo Mao, editors, 6th Information Security Conference – ISC 2003, pages 208–217. Springer-Verlag, 2003. Volume 2851/2003 of Lecture Notes in Computer Science.

87. D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer Verlag, 2001.

88. L. Chen, K. Harrison, N. Smart, D. Soldera. Applications of Multiply Trust Authorities in pairing based Cryptosystems, 2002.

89. O.R. Gangishetti, M. Choudary Gorantla, M. Lal Das, A. Saxena. Cryptoanalysis of key issuing protocols in ID-based cryptosystems, 2006.

90. C. Gentry. Certificate-based encryption and the certificate revocation problem, 2003.

91. B.Lee, C.Boyd, E. Dawson, K. Kim, J. Yang, S. Yoo. Secure key issuing in ID-based cryptography, 2004.

92. K. Paterson. Cryptography from pairings: a snapshot of current research, 2002.

93. K.P. Kumar, G. Shailaja, A. Saxena. Secure and efficient threshold key issuing protocol for ID-based cryptosystems, 2006.

94. X. Chunxiang, Z. Junhui, Q. Zhiguang. A note on secure key issuing in ID-based cryptography, 2005.

95. *Тевяшев А.Д., Горбенко Ю.И.* Оценка опасности криптоаналитических атак методом создания коллизий. // Радиотехника. – Вып. 126. – С. 166–172.

96. *Балагура Д.С., Горбенко Ю.И.* Методы оценки сложности криптоанализа для криптографических приложений в группе точек эллиптической кривой, учитывающие вероятность коллизий. // Радиотехника. – 2005. – Вып. 142. – С. 205–214.

97. *Бондаренко М.Ф., Горбенко Ю.І., Батюшко С.С.* Аналіз існуючих ЕЦП від атак на зв'язаних ключах. // Прикладная радиоэлектроника. – 2006. Том 5. – № 1. – С. 52–59.

98. *Бондаренко М.Ф., Горбенко Ю.І., Батюшко С.С.* Аналіз захищеності існуючих ЕЦП від атак на реалізацію. // Прикладная радиоэлектроника. – 2006. – Том 5. – № 1. – С. 59–62.

99. *Бондаренко М.Ф., Денисенко Б.И., Горбенко Ю.И.* Методика сравнения алгоритмов ЕЦП в группе точек эллиптической кривой. // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2008. – № 3. – С. 256– 263.

100. *Потий Александр, Столяр Александр, Горбенко Юрий, Мядковский Даниил.* Анализ особенностей технической реализации программно-аппаратных средств КЗИ «Гряда-31, 41» в соответствии с требованиями стандарта FIPS 140-2 // Безпека інформації в інформаційно-телекомунікаційних системах. 5 Міжнародна науково-практична конференція 20–24 травня 2002 р. – Київ. – С. 45–46.

101. *Гулак Геннадий, Потий Александр, Горбенко Юрий.* Структура и требования безопастности к центру управления сертификатами // Безпека інформації в інформаційно-телекомунікаційних системах. 6 Міжнародна науково-практична конференція 13–16 травня 2003 р. – Київ. – С. 23–25.

102. *Горбенко Юрій, Батюшко Стас.* Застосування PKI при створенні системи електронного документообігу із застосуванням електронного цифрового підпису. // Безопасность информации в информационно-телекоммуникационных системах. 7 Международная научно-практическая конференция 12–14 мая 2004 г. – Киев. – С. 43.

103. *Горбенко Ю., Горбенко И., Потий А., Батюшко С.* Требования к инфраструктуре открытых ключей в части защиты от компроментации личных ключей. // Безопасность информации в информационно-телекоммуникационных системах : 9-я Международная научно-практическая конференция 17–19 мая 2006 г. – Киев. – С. 76.

104. *Горбенко Ю.* Требования к инфраструктуре открытых ключей относительно обеспечения защиты секретных ключей пользователей и их реализация. // Безопасность информации в информационно-телекоммуникационных системах : 9-я Международная научно-практическая конференция 17–19 мая 2006 г. – Киев. – С. 90–91.

105. *Горбенко И., Горбенко Ю., Потий А.* Сравнительный анализ стандартов цифровой подписи инфраструктуры ЭЦП в Украине. // Безопасность информации в информационно-телекоммуникационых системах : 9-я Международная научно-практическая конференция 17–19 мая 2006 г. – Киев. – С. 91–92.

106. *Козак В., Горбенко Ю.* Анализ требований к средствам КЗИ в соответствии с международными стандартами и возможности их выполнения. // Безопасность

информации в информационно-телекоммуникационных системах. 10 Международная научно-практическая конференция 15–18 мая 2007 г. – Киев. – С. 13–15.

107. *Оноприенко В., Горбенко Ю., Тоцкий А., Чичмар С.* Опыт внедрения и применения ЕЦП в информационных технологиях. // Безопасность информации в информационно-телекоммуникационных системах. 10 Международная научно-практическая конференция 15–18 мая 2006 г. – Киев. – С. 86–87.

108. ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security. Part 1: Introduction and general model. Part 2: Security functional requirements. Part 3: Security assurance requirements.

109. *Саати Т.* Принятие решений: Метод анализа иерархий. / Пер. с англ. – М.: Радио и связь, 1993.

110. Li C. M., Hwang T., Lee N. Y. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders, Advanced in Cryptography – Eurocrypt'94, pp. 194-204, Springer-Verlag, 1994.

111. Nessie public report D20. Nessie security report : http://cryptonessie.org

112. Долгов В.И., Неласая А.В., Погорелый А.Н. К вопросу применения и совершенствования стандарта электронной цифровой подписи в Украине // Прикладная радиоэлектроника. – 2008. – Т. 7. – № 3. – С. 263–267.

113. *Клименко І.В., Линьов К.О., Горбенко І.Д., Онопарієнко В.В.* Електронний документообіг в державному управлінні. Навчальний посібник. – К.: НАДУ, 2009.; Х.: Вид-во «ФОРТ», 2009. – 232 с.

114. El Gamal T. A public key cryptosystems and a signature scheme based on discrete logarithms. // IEEE Trans. on Information Theory. – 1985. vol.31. – P.469-472.

115. *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда. // Радиотехника: Всеукр. Межвед. Научн.-техн. сб. – 2001. – Вып. 119. – С. 43–50.

116. Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.

117. Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999.

118. National Institute of Standards and Technology, FIPS 140-3 (DRAFT), Security for cryptographis modules : http://www.nist.gov/cmvp

119. NIST special Publication 800-56A. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. March, 2006.

120. NIST special Publication 800-57 Draft. Recommendation for Key Management-Part 2: Best Pracnices for Key Manageme Jrganizationsnt. April, 2005.

121. ISO/IEC FCD 19790: Information technology– Security requirements for cryptographicmodules. Proect: 1.27.40.

122. Looking over the horszon: FIP 140-3. Jean Campbell. Communications Security Establisment.CMVP Symposium, 2004.

123. FIPS 140-3. Satus fnd Schedules. Allen Roginsry. CMVP NIST, 2005.

124. X 9-42 Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric Algorithm Keys Using Diffie-Hellman, 1996.

125. *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда. / Всеукр. межвед. науч.-техн. сб. Радиотехника. – Вып. 119. – 2001. – С. 43–50.

126. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Шнайер Б. – Изд-во «Триумф», 2002. – 1160 с.

127. *Васильцов І.В.* Атаки спеціального виду на криптопристрої та методи боротьби з ними. / За науковою редакцією проф. В.П. Широчина. – Кременець: Видавничий центр «КОГПІ», 2009. – 264 с.

128. *Оноприенко В.В., Горбенко Ю.І.* Электронная цифровая подпись. Состояние и перспективы использования. // 12 межународная научно-практическая конференция «Проблемы и перспективы инновационного развития экономики» (ИНКОН X11). – Журнал об инновационной деятельности «Инновации». – Вып. «Инновации в странах СНГ». – № 8 (106), август 2007, Санкт-Петербург. – С. 119–120.

129. *Горбенко Ю.И.* Сравнительный анализ стандартов ЭЦП по критериям стойкости. / НАНУ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова. Збірка наукових праць «Моделювання та інформаційні технології». Спеціальний випуск. – Київ, 2008. – С. 11–20.

130. *Горбенко Ю.И., Бобух В.А.* Требования к средствам КЗИ в ИОК в соответствии с международными и региональными стандартами. / НАНУ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова. Збірка наукових праць «Моделювання та інформаційні технології». Спеціальний випуск. – Київ, 2008. – С. 20–33.

131. *Горбенко Ю.И., Оноприенко В.В.* Состояние национальной системы ЕЦП в Украине и проблемы ее развития. / НАНУ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова. – Збірка наукових праць «Моделювання та інформаційні технології». Спеціальний випуск. – Київ, 2008. – С. 34–35.

132. *Горбенко И.Д., Погребняк К.А.* Классы сложностей алгоритмов на основе билинейных отображений. // Радіоелектронні і комп'ютерні системи. – Х.: ХАІ, 2007. – № 7. – С. 125–128.

133. *Горбенко И.Д., Погребняк К.А.* Классы сложностей криптосистем на основе билинейных отображений. // Прикладная радиоэлектроника, Х.: ХНУРЭ, 2007. – № 2.

134. *Горбенко И.Д., Поляков А.А.* Метод анализа структуры группы точек эллиптической кривой на содержание подгрупп малого порядка над расширениями поля характеристики 2. // Прикладная радиоэлектроника – Х.: ХНУРЭ, 2007. – № 2.

135. *Горбенко И.Д., Шевченко Д.В., Козак В.Ф.* Порівняльний аналіз групових та кільцевих підписів, методи побудови кільцевих підписів. // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2007. – № 3. – С. 329.

136. *Горбенко И.Д., Погребняк К.* Классы сложностей алгоритмов на основе билинейных от ображений. // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2007. – № 3. – С. 329.

137. *Бондаренко М.Ф., Горбенко І.Д., Кравченко П.А., Мелецкий О.П.* Аналіз та перспективи сучасних протоколів видання та генерації ключів для інфраструктури на базі ідентифікаторів. // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2007.– № 3. – С. 356.

138. *Горбенко І., Качко О., Волощук О., Балагура Д., Головашич С.* Основні принципи побудови центрів сертифікації ключів. Центр сертифікації ключів «Джерело» та його можливості. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Київ, 2005. – № 10. – С.143–151.

139. *Збитнев С.И.* Проективная геометрия – не все так гладко. // Радиотехника: Всеукр. Межвед. Научн.-техн. сб., 2002. – Вып. 126. – С. 123–131.

140. Постанова КМУ від 26.05.2004 № 680 «Порядок засвідчення наявності электронного документа (електронних даних) на певний момент часу».

141. Постанова КМУ від 13.06.2004 № 903 «Порядок акредитації центру сертифікації ключів».

142. Постанова КМУ від 28.10.2004 № 1451 «Положення про центральний засвідчувальний орган».

143. Постанова КМУ від 28.10.2004 № 1452 «Порядок застосування електронного цифрового підпису органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності».

144. Постанова КМУ від 28.10.2004 №1453 «Типовий порядок здійснення електронного документообігу в органах виконавчої влади».

145. Постанова КМУ від 28.10.2004 №1454 «Порядок обов'язкової передачі документованої інформації».

146. RFC 2631 "Diffie-Hellman Key Agreement Method", June 1999.

147. RFC 2785 Methods for Avoiding the «Small-Subgroup» Attacks on the Diffie-Hellman Key Agreement for S/MIME, March 2000.

148. RFC 3279 "Algorithms and Identifiers for the Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.

149. RFC 3281 "An Internet Attribute Certificate Profile for Authorization", April 2002.

150. RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002.

151. RFC 3394 "Encryption Standard (AES) Key Wrap Algorithm", September 2002.

152. RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004.

153. RFC 4490 – Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001.

154. Algorithms with Cryptographic Message Syntax (CMS), May 2006.

155. RFC 5008 "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)", September 2007.

156. RFC 5480 "Elliptic Curve Cryptography Subject Public Key", March 2009.

157. RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009.

158. L. Martin, M. Schertler, G. Appenzeller, «Identity-Based Encryption Architecture and Supporting Data Structures», RFC 5408, January 2009.

159. X. Boyen, L. Martin, «Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems», RFC 5091, December 2007.

160. D. Boneh and M. Franklin, «Identity-based encryption from the Weil pairing,» in Proc. of CRYPTO 01, LNCS 2139, pp. 213-229, 2001.

161. G. Appenzeller, L. Martin, and M. Schertler, «Identitybased Encryption Architecture», Work in Progress.

162. Klensin, J., «Simple Mail Transfer Protocol», RFC 5321, October 2008.

163. L. Martin, and M. Schertler, «Using the Boneh-Franklin Identity-Based Encryption Algorithm with the Cryptographic Message Syntax (CMS)», RFC 5409, January 2009.

164. Hoes Lane, «Draft Standard for Identity-based Public-key Cryptography Using Pairings», IEEE P1636.3™/D1, April 2008.

165. Ф. Оорт, Ж. де Ионг, «Гиперэллиптические кривые в абелевых многообразиях». Алгебраическая геометрия-5. – Итоги науки и техн. Сер. соврем. мат. и ее прил. Темат. обз. 34. – М.: ВИНИТИ, 2001. – С. 149–163.

166. http://www.rsa.com/node.aspx

167. *Шевченко Д.В.* Кільцеві підписи та їх властивості // Радіоелектронні і комп'ютерні системи. – 2007. – № 8 (27). – С. 139–144. "Radio-electronic and Computer Systems".

168. Sherman S.M. Chow, Richard W.C. Lui, Lucas C.K. Hui, and S.M. Yiu Identity Based Ring Signature:Why, How and What next // http://www.springerlink.com/content/f44t56873132g2ht/

169. Chih-Yin Lin and Tsong_Chen Wu AnIdentity-based Ring Signatures Scheme form Bilinear Pairings // Advanced Information and Communications Security –ICICS 2004, LNCS 3269, pp. 459-507.

170. Fanguo Zhang and Kwangjo Kim ID-based Blind Sugnature and Ring signature from pairing // Advances in Cryptology – AsiaCrypt2002, LNCS 2501, pp. 533-647.

171. *Горбенко И.Д., Качко Е.Г., Свинарев А.В.* Стандарт ЦП ГОСТ 34.10-95 на эллиптических кривых. // Безопасность информации в информационно-телекоммуникационных системах. 3 Международная научно-практическая конференция 17–19 мая 2000 г. – Киев.

172. Key Management Usign ANSI X 9.17. U.S. DEPFRTMENT OF COMMERCE. NIST.

173. Советский энциклопедический словарь. Главный редактор А.М. прохоров. Изд. Третье. Москва, советская энциклопедия, 1985.

174. J. Neehvatal, E. Berker, et. al. Report on the development of the advanced encryption standard (AES) / computer security division, NIST : http://cryptonessie.org

175. Положення про порядок розроблення. Виробництва та екусплуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису. Наказ департамента спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України 30.04.2004 № 31.

176. *Андрейчиков А.В., Андрейчикова О.Н.* Анализ, синтез, планирование решений в экономике. – М.: «Финансы и статистика», 2002. – 359 с.

177. *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. – К.: «МК-Пресс», 2006. – 320 с.

178. *Орловский С.А.* Проблемы принятия решений при нечёткой исходной информации. – М.: Наука, 1981. – 208 с.

179. *Окунев Ю.Б., Плотников В.Г.* Принципы системного подхода к проектированию в технике связи. – М.: «Связь», 1976.– 184 с.

180. [2] M. ABE and T. OKAMOTO, "A signature scheme with message recovery as secure as discrete logarithm," Advances in Cryptology – Asiacrypt'99, Lecture Notes in Computer Science 1716, pp. 378–389, Springer-Verlag, 1999.

181. [6] C. H. LIM and P. J. LEE, "A study on the proposed Korean digital signature algorithm," Advances in Cryptology – Asiacrypt'98, Lecture Notes in Computer Science 1514, pp. 175-186, Springer-Verlag,1998.

182. [7] A. J. MENEZES, P. C. VAN OORSCHOT and S. A. VANSTONE, "Handbook of applied cryptography," CRC Press, 1997.

183. [8] A. MIYAJI, "Another Countermeasure to Forgeries over Message Recovery Signature," IEICE Trans., Fundamentals, vol. E80-A, No.11, pp. 2192-2200, 1997.

184. [9] K. NYBERG and R. A. RUEPPEL, "Message recovery for signature schemes based on the discrete logarithm problem," Designs, Codes and Cryptography, 7, pp. 61-81, 1996.

185. L. PINTSOV and S. VANSTONE, "Postal Revenue Collection in the Digital Age," Proceedings of the.

186. *Горбенко Ю.І., Шевчук О.А.* Аналіз властивостей та областей застосування цифрових підписів стандарту ISO/IEC 9796-36:2006 // Прикладная радиоэлектроника. – 2009. Том 8. – № 3. – С. 304 – 314.

187. [13] Miyaji, Atsuko. Weakness in message recovery signature schemes based on discrete logarithm problems 2. – 2002.

188. [14] Вступ у теорію γ-мірних колізій та її застосування / Сінаюк Л.В. Горбенко Ю.І., Фролов О.С. // Прикладная радиоэлектроника. – 2006.

189. *Горбенко Ю.І., Бойко А.В., Герцог А.М.* Мета, стан та попередні підсумки проекту SHA-3. // Прикладная радиоэлектроника. – 2009. Том 8. – № 3. – С. 315–321.

190. ISO/IEC 10118-1. Information technology – Security techniques – Hash-functions – Part 1: General.

191. ISO/IEC 10118-2. Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher.

192. ISO/IEC 10118-3 Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.

193. ISO/IEC 10118-4 Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic.

194. *Горбенко Ю.І., Бойко А.В., Герцог А.М.* Порівняння перспективних швидкодіючих функцій гешування // Прикладная радиоэлектроника. – 2009. Том 8. – № 3. – С. 321–327.

195. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функции хеширования. – М.: Госстандарт России, 1994.

196. Federal Register Notice published on November 2, 2007.– http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf

197. FIPS PUB 180-1/ Federal Information Processing Standards Publication. 1995April 17.

198. FIPS PUB180-2/ Federal Information Processing Standards Publication 180-2.

199. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu Finding Collisions in the Full SHA-1.

200. Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD.

201. Bob Hattersley NIST SHA-3 Competition Waterfall Hash Algorithm Specification and Analysis http://ehash.iaik.tugraz.at/uploads/1/19/Waterfall_Specification_1.0.pdf

202. Mihir Bellare, Daniele Micciancio A New Paradigm for Collision-free Hashing: Incrementality at Reduced Cost.

203. Palash Sarkar, Paul J. Shellenberg A Parallelizable Design Principle for Cryptographic Hash Functions.

204. Ewan Fleischmann1, Christian Forler, and Michael Gorski Classification of the SHA-3 Candidates.

205.http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo/

206. NIST Computer security resource center. Announcing request for Candidate algorithm nominations for a new cryptographic hash algorithm nominations for a new cryptographic hash algorithm (SHA-3) family.

207. Damgård I. A Design Principle for Hash Functions. In Advances in Cryptology – CRYPTO '89 Proceedings, Lecture Notes in Computer Science Vol. 435, G. Brassard, ed, Springer-Verlag, 1989, pp. 416–427.

208. Bellare M. A new paradigm for collision-free hashing: incrementaly at reduced cost.

209. Sarkar P. A parallelizable design principe for cryptographic hash functions.

210. ISO/IEC 10181-2:1996 Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.

211. ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

212. ISO/IEC 9797-2, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function.

213. ДСТУ ISO/IEC 9798 – 3: 2002. Інформаційні технології. Методи захисту. Автентифікація обєктів. Частина 3: Механізми, що ґрунтуються на цифровому підписі (ISO/IEC 9798 – 3: 2002, IDT).

214. Симонс Г.Дж. Обзор методов аутентификации информации // ТИИЭР. 11988.76(5). С. 105-125.

215. Бабенко Л.К., Ищуков С.С., Макапевич О.Б.. Защита информации с использованием смарт-карт и электронных брелоков. Москва. Гелиос АРВ, 2003.– С. 351.

216. Смирнов С.Н. Безопасность систем баз даних.-М.: Гелиос АРВ, 2007.

217. Knobloch Hans Joachim. A smart Card Implementation of the Fiat Shamir Identificatsjn Scheme, Proc. Of EUROCRYPT 88. Pp. 87-94.

218. Biometrics Deployment of EU-Passports. EU – Passport Specification. Working document (EN) – 28/06/2006.

219. *Горбенко Ю.І., Тоцький О.С.* Аналіз та удосконалення криптографічних протоколів автентифікації та встановлення ключів між серверами ЛОМ. // Прикладная радиоэлектроника. – Т. 8. – № 3. – С. 405–412.

220. Основи інформаційної безпеки та захисту інформації у контексті Євроатлантичної інтеграції України. / За загальною редакцією академіка НАН України В.П. Горбуліна. – ДП «НВЦ» Євроатлантикінформ». – Київ, 2006. – 103 с.

221. Public Key Infrastructure Study. Final Report. NIST. MITRE Corp. 1994.

222. *D.Richard Kuhn, Vincent C. Hu, W.Timothy Polk, Shu-Jen Chang.* "Introduction to Public Key Technology and the Federal PKI Infrastructure". NIST SP 800-32. 2001.

223. Government of Canada Public Key Infrastructure. White Paper. MG-15a. 1998.

224. Security Target Entrust/Authority 5.1 Entrust Technologies Lim. 2000.

225. Security Target Entrust/RA 5.1 Entrust Technologies Lim. 2000.

226. Work-plan for ETSI ESI WG, electronic signature standartisation. EISI, 2001.

227. *G. Endersz* Electronic Signature and PKI Standartisation in Europe. – 2000, Tella.

228. www.pki-forum.ru/doc/aspekty.doc (http://www.pki-page.info/eu/). Юридические и коммерческие аспекты ввода в действие Директивы 1999/93/ЕС и практическое применение электронных подписей в странах-членах ЕС, ЕЭЗ, странах, вступающих в ЕС и странах-кандидатах.

229. *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI. – М.: Горячая линия – Телеком, 2004. – 246 с.

230. www.aladdin.ru/press-center/.../publication2280.php

231. dehack.ru/metod_infbezop/szi_v_OS/pki/

232. ank-pki.ru/index.php/press-center-ank/posts-ank/108-regionsystems

233. eprints.qut.edu.au/4406/

234. www.verisign.com.au/gatekeeper/customs/

235. www.iit.com.ua/

236. United States Department of Defense X.509 Certificate Policyю . Version 10. 2 March 2009.Prepared by: DoD Public Key Infrastructure Program Management Office Approved.

237. *Wollinger T.* Software and Hardware Implementation of Hyperelliptic Curve Cryptosystem. Dissertation for the Degree of Doctor-Ingenious / Wollinger T. – Bochum, Germany, 2004.–201p.

238. Pelzl J., Wollinger T., Paar C. High Performance Arithmetic for Hyperelliptic Curve Cryptosystems of Genus Two, International Conference on Information Technology: Coding and Computing – ITCC, April 5-7, 2004, (postscript) Cryptology ePrint Archive, Report 2003/212, 2003, http://eprint.iacr.org/2003/212.pdf

239. Thomas Wollinger, Christof Paar, "Hardware Architectures proposed for Cryptosystems Based on Hyperelliptic Curves", To be presented at the 9th

IEEE International Conference on Electronics, Circuits and Systems – ICECS 2002, September 15-18, 2002, Dubrovnik, Croatia. (gzipped postscript)

240. T. Wollinger, V. Kovtun. Fast explicit formulae for genus 2 hyperelliptic curves using projective coordinates (Updated), available at http://eprint.iacr.org/2008/056.pdf

241.V. Kovtun, J. Pelzl, A. Kuznetsov. Software Implementation of Genus-2 Hyperelliptic Curve Cryptosystems Over Prime Fields, available at http://eprint.iacr.org/2008/057.pdf

242. *Долгов В.И., Неласая А.В.* Геометрический подход к сложению дивизоров гиперэллиптической кривой. // Радіоелектроніка. Інформатика. Управління. – № 2 (18). – Запоріжжя, 2007. – С. 44–50.

243. *Неласая А.В.* Стойкость криптографических алгоритмов на гиперэллиптических кривих. / Долгов В.И., Неласая А.В. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации: ХНУРЭ, 2006. – Том 5. – № 1. – С. 30–34.

244. *Неласая А.В, Козина Г.Л, Молдовян Н.А.* Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых. // Радіоелектроніка. Інформатика. Управління. – № 1(19). – Запоріжжя, 2008. – С. 127–133.

245. Cantor, D. G. Computing in the Jacobian of a hyperelliptic curve. Math. Comp. 48, 177 (1987), 95-101.

246. P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In Bart Preneel, editor, Advances in Cryptology — EUROCRYPT 2000, volume LNCS 1807, Berlin, Germany, Springer-Verlag, 2000, pp. 19–34.

247. Анна Неласая Протокол цифровой подписи на гиперэллиптических кривых//Радіоелектроніка. Інформатика. Управління. №1(15).-Запоріжжя, 2006, с.113–118.

248. 210. Hoes Lane, "Draft Standard for Identity-based Public-key Cryptography Using Pairings", IEEE P1636.3™/D1, April 2008.

249. X. Boyen, L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, December 2007.

250. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in Proc. of CRYPTO 01, LNCS 2139, pp. 213-229, 2001.

251. D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles", In Proc. of EUROCRYPT 04, LNCS 3027, pp. 223-238, 2004.

252. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol-HTTP/1.1", RFC 2616, June 1999.

253. Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)", RFC 3987, January 2005.

254. *Горбенко І.Д., Погребняк К.А.* Схема цифрового підпису із використанням парних відображень на основі стандарту ДСТУТ 4145 – 2002// Прикладная радиоэлектроника. – 2009. – Том 8. – № 3. – С. 290–296.

255. *Бондаренко М.Ф., Кравченко П.О.* Комбінована інфраструктура відкритих ключів // Прикладная радиоэлектроника. – 2009. – Том 8. – № 3. – С. 327–330.

256. *Бондаренко М.Ф., Горбенко І.Д., Кравченко П.О., Мелецький О.П.* Аналіз та перспективи сучасних протоколів видання та генерації ключів на базі ідентифікаторів // Прикладная радиоэлектроника. – 2007. – Том 3. – № 3. – С. 256–263.

257. *Горбенко І.Д., Погребняк К.А.* Классы сложностей алгоритмов на основе билинейных отображений. Радіоелектронні і комп'ютерні системи. – Х.:ХАІ, 2007. – № 7. – С. 125–158.

258. Diffie-Hellman problems and bilinear maps. Cryptology ePrint Archive: Report 2002/117 (2001). by J H Cheon, D H Lee.

259. Martin, M. Schertler, G. Appenzeller, "Identity-Based Encryption Architecture and Supporting Data Structures", RFC 5408, January 2009

260. A. Joux. A one ro protocol for tripartite Diffi Hellman. In W/ Bosma, editor, Algoritmic Number Theory, IV – th Simposium. Pages 385 – 394. Springer – Verlag, 2000.

261. *Горбенко Ю.И.* Инфраструктура ЭЦП в Украине: проблемы становлення и перспективы развития // Информационно-аналитический журнал Карт-бланш. – № 6. – 2009. – С. 26–35.