ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
НАУЧНАЯ БИБЛИОТЕКА
ОТДЕЛ СПРАВОЧНО-БИБЛИОГРАФИЧЕСКОЙ
И ИНФОРМАЦИОННОЙ РАБОТЫ

ОСНОВЫ КРИПТОГРАФИИ

(Письменная справка)

1999-2014 гг.

Донецк-2015

Письменная справка «Основы криптографии» составлена по заявке кафедры радиофизики.

В нее включены книги, статьи из периодических и продолжающихся изданий, авторефераты диссертаций на русском, украинском и английском языках за период 1999-2014 гг.

Для отбора материала были использованы библиографические и информационные издания, имеющиеся в фонде библиотеки ДонНУ, электронный каталог библиотеки, базы информационных центров России и Украины, а также Интернет.

В настоящее время большой популярностью пользуется научная библиотека «КиберЛенинка», она при поддержке Российской Государственной библиотеки предлагает свободный доступ к широкому спектру научных статей.

Справка состоит из трех разделов, в которых материала сгруппирован по алфавиту.

В ней отражены вопросы:

- основы сетевой безопасности

-криптографические методы, управление ключами

- аутентификация

Рассчитана справка на преподавателей, аспирантов и студентов для использования в научной и учебной работе.

Литература, имеющаяся в фонде библиотеки ДонНУ, отмечена шифром и инвентарными номерами, а отсутствующая – звездочкой (*). Литература из библиотеки «КиберЛенинка» отмечена словами «КиберЛенинка».

В список включено 172 названий.

Составитель:
рав. сектором б-ки Фесенко Н.А.

Консультант:
доктор техн. наук Данилов В.В.

Редактор:
зав. сектором б-ки Кротова В.А.

ОСНОВЫ СЕТЕВОЙ БЕЗОПАСНОСТИ.

1. Бабак В.П. Інформаційна безпека та сучасні мережеві технології: англо-укр.-рос. Словник термінів: 3500 термінів / В.П. Бабак, О.Г. Корченко. – Київ: НАУ, 2003. – 667 с.

З97я2
Б12 436320

2. *Бабак В.П. Теоретичні основи захисту інформації: підручник / В.П. Бабак. – Київ: НАУ, 2008. – 752 с.

3. *Бабаш А.В. Криптография: методический материал / А.В. Бабаш, Г.П. Шанкин. – Москва: СОЛОН-Р, 2002. – 511 с.

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

З97
Б124 839120

5. *Баричев С.Г. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – Москва: Горячая линия – Телеком, 2002. – 175 с.

6. *Белоус Л.Ф. Информационные сети: учеб. пособие / Л.Ф. Белоус. – Москва: Логос, 2005. – 140 с.

7. *Бернет С. Криптография: официальное руководство RSA Security / С. Бернет, С. Пэйн. – М.: БИНОМ, 2002. – 381 с.

8. *Бєгун А.В. Інформаційна безпека: навч. посібник / А.В. Бєгун. – Київ, 2008. – 278 с.

9. *Болотов А.А. Криптографические протоколы на эллиптических кривых: учеб. пособие по курсу «Криптографические методы защиты информации» для студентов по всем направлениям подготовки АВТИ и слушателей ФПКП и СМЭИ(ТУ) / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – Москва: Изд. Дом МЭИ; Красноармейск, 2007. – 84 с.

10. Бурак Р. Unix для Internet: энциклопедия пользователя / Р. Бурак, Д.Б. Хорват. – Киев: ДиаСофт, 1999. – 496 с.

З97я20
Б914 825588

11. Быстро и легко осваиваем работу в сети Интернет: учеб. пособие / под. Ред.: Ф.А. Резникова. – Москва: Лучшие кН., 2004. – 378 с.

З98я73
Б955 833526

12. Введение в защиту информации: учеб. пособие для вузов по специальностям, не входящим в группу специальностей 075000, изучающих федерал. Компонент по основам информационной безопасности и защиты гос. тайны / В.Б. Байбурин, М.Б. Бровкова, И.Л. Пластун и др. – Москва: Форум: ИНФРА-М, 2004. – 128 с.

З973я73
В24 833252

13. *Введение в криптографию: монография / В.В. Ященко, Н.П. Варнавский, Ю.В. Нестеренко и др. – Москва: МЦНМО; ЧеРо, 1999. – 271 с.

14. *Введение в криптографию: монография / В.В. Ященко, Н.П. Варнавский, Ю.В. Нестеренко и др. – Москва: МЦНМО; ЧеРо, 2000. – 287 с.

15. *Введение в криптографию: новые математические дисциплины: учеб. пособие / В.В. Ященко, Н.П. Варнавский, Ю.В. Нестеренко и др. – Санкт-Петербург: Питер, 2001. – 287 с.

16. Вельшенбах М. Криптография на Си и С++ в действии: учеб. пособие: математическая теория криптографических алгоритмов / М. Вельшенбах. – Москва: Триумф, 2004. – 461 с.

З973я73

В286 833528

17. *Вишняков В.М. Захист даних в інформаційних системах: навч. посібник для студ. Спец. 7.05010101 «Інформаційні управляючі системи та технології» та 7.05010102 «Інформаційні технології проектування» / В.М. Вишняков. – Київ: КНУБА, 2010. – 127 с.

18. Галатенко В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. – Москва: ИНТУИТ, 2004. – 264 с.

З973я73

Г151 833256

19. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – Москва: ДМК Пресс, 2004. – 616 с.

З97

Г158 830514

20. *Гамаюнов Д.Ю. Обеспечение сетевой безопасности с помощью программно-конфигурируемых сетей / Д.Ю. Гамаюнов, И.С. Платонов, Р.Л. Смелянский // Системы высокой доступности. – Москва, 2013. – Т.9, №3. – С. 85-87.

21. *Голышев Д.Н. Криптографическая защита информации: учеб. пособие / Д.Н. Голышев, С.В. Моторин. – Новосибирск: НГАВТ, 2008. – 85 с.

22. *Грунтович М.М. Основы криптографии с открытыми ключами: учеб. пособие / М.М. Грунтович. – Пенза: [б.и.], 2000. – 57 с.

23. *Гулак Г.Н. Основы криптографической защиты информации: учеб. пособие / Г.Н. Гулак; Гос. ун-т информ.-коммуникац. технологий. – Киев: ГУИКТ, 2009. – 228 с.

24. *Гулак Г.М. Основи криптографічного захисту інформації: підручник / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко. – Вінниця, 2011. – 199 с.

25. Дейтел Х. Операционные системы: в 2 т. Т.2: Распределительные системы, сети, безопасность / Х. Дейтел, П. Дейтел, Д. Чофнес. – Москва: БИНОМ, 2007. – 704 с.

З973.2

Д274 850805

26. *Емец В. Современная криптография: основные понятия / В. Емец. – Львов: Бак, 2003. – 144 с.

27. *Ерош И.Л. Криптография. Первое знакомство: учеб. пособие / И.Л. Ерош. – Санкт-Петербург: ГУАП, 2008. – 83 с.

28. *Защита информации: науч. серия / ред. Е.М. Сухарев. – Москва: Радиотехника, 2007. – Кн.4: Криптографические методы защиты информации В.М. Амербаев. – 304 с.

29. Защита от хакеров Web-приложений / Д. Форристал, К. Брумс, Д. Симонис и др. – Москва: АйТи; ДМК Пресс, 2004. – 492 с.

З97
З402 836013

30. Защита программного обеспечения / Д. Гроувер, Р. Сатер, Дж. Фипс и др. – Москва: Мир, 1992. – 286 с.

З97
З402 786570

31. *Захист інформації: навч. посібник / уклад.: Б.В. Кузьменко; КМ України. – Київ, 2009. – 190 с.

32. *Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – Москва: КУДИЦ-ОБРАЗ, 2001. – 363 с.

33. Карпов В.Е. Основы операционных систем: курс лекций: учеб. пособие для вузов по специальности «Прикладная информатика» / В.Е. Карпов, К.А. Коньков. – Москва: Интернет ун-т информ. Технологий, 2004. – 628 с.

З973я73
К265 831597

34. Карпов В.Е. Основы операционных систем: курс лекций: учеб. пособие для вузов по специальности «Прикладная информатика» / В.Е. Карпов, К.А. Коньков. – Москва: Интернет ун-т информ. Технологий, 2005. – 628 с.

З973я73
К265 850794

35. Компьютеры. Криптография [Электронный ресурс]. – Киев, 2005. – 1 электронный опт. диск (CD-ROM).

З07я2
К637 СКИ: ми374

36. *Коржик В.И. Основы криптографии: учеб. пособие по специальности 210403 «Защищенные телекоммуникационные системы связи» / В.И. Коржик, В.П. Просихин. – Санкт-Петербург: Линк, 2008. – 250 с.

37. *Кормич Б.А. Информационная безопасность: организационно правовые основы : учеб. пособие для студентов вузов / Б.А. Кормич. – Киев: Кондор, 2004. – 384 с.

38. Корт С.С. Теоретические основы защиты информации: учеб. пособие для студентов вузов, обучающихся по специальности в области информационной безопасности / С.С. Корт. – Москва: Гелиос АРВ, 2004. – 233 с.

З973я73

39. *Котенко И.В. Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей / И.В. Котенко, Е.С. Новикова // Вопросы защиты информации. – Москва, 2013. - №3(102). – С. 33-42.

40. *Криптографическая защита информации: учеб. пособие / А.В. Яковлев и др. – Тамбов: Изд-во ТГТУ, 2006. – 139 с.

41. Кудрявцева С.П. Міжнародна інформація: навч. посібник для студ. ВНЗ / С.П. Кудрявцева, В.В. Колос. – Київ: Слово, 2005. – 395 с.

Ч23я73
К889 838859

42. *Кузнецов О.О. Захист інформації в інформаційних системах. Методи традиційної криптографії: навч. посібник / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. – Харків, 2010. – 314 с.

43. *Куценко И.О. Методы и принципы криптографической защиты информации / И.О. Куценко, Д.А. Жайворонок // Вестн. Воронежского ин-та МВД России. – Воронеж, 2007. - №4. – С. 145-155.

44. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учеб. пособие для студентов вузов по специальности 510200 «Прикладная математика и информатика» / О.Р. Лапонина. – Москва: Интернет ун-т информ. технологий, 2005. – 605 с.

З973я73
Л244 835670

45. *Лапонина О.Р. Основы сетевых безопасности: криптографические алгоритмы и протоколы взаимодействия: учеб. пособие для студентов вузов обучающихся по специальности «Прикладная математика и информатика» / О.Р. Лапонина. – Москва: Интернет ун-т информ. технологий, 2007. – 531 с.

46. Ларин Д.А. Пакет инструментов для электронного задачника по основам криптографии / Д.А. Ларин, О.В. Тимонина // Дистанционное образование. – 2000. - №3. – С. 28-34. 4 ч/з

47. Лебедева Т.Ф. Инновационные подходы при изучении проблем безопасности информации / Т.Ф. Лебедева, А.Н. Солопов // Информатика и образование. – 2005. - №7. – С. 111-114. 4 ч/з

48. *Левин Криптография без секретов: руководство пользователя / М. Левин. – Москва: Новый изд. Дом, 2005. – 315 с.

49. *Левин М. Криптография: руководство пользователя / М. Левин. – Москва: Познават. кн. плюс, 2001. – 319 с.

50. Ленков С.В. Методы и средства защиты информации: в 2 т. Т.1: Несанкционированное получение информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Киев: Арий, 2008. – 464 с.

З97
Л458 861386

51. Ленков С.В. Методы и средства защиты информации: в 2 т. Т.2: Информационная безопасность / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Киев: Арий, 2008. – 342 с.

З97
Л458 861387

52. Локхарт Э. Антихакинг в сети. Трюки / Э. Локхарт. – Москва и др.: Питер, 2005. – 296 с.

З97

Л734 834971

52. Лукацкий А.В. Звериный оскал информационной безопасности / А.В. Лукацкий // Информатика и образование. – Москва, 2007. - №12. – С. 90-93.

53. *Лукьянов Г.В. Основы кодирования и криптографического преобразования информации: учеб. пособие / Г.В. Лукьянов. – Москва: Моск. гос. лингвист. Ун-т, 2005. – 128 с.

54. Мао Венбо. Современная криптография: теория и практика / Венбо Мао. – Москва: Вильямс, 2005. – 763 с.

З97

М248 847556

55. *Маркова И. Защита информации. Криптограф ичес методы: учебник для вузов / И. Маркова, А.И. Рыбак, Ю.С. Ямпольский. – Одесса, 2001. – 174 с.

56. *Математичні методи захисту інформації: курс лекцій / ред..: Т.В. Литвинова. – Київ., 2008. – Ч.1. – 128 с.

57. *Методи та засоби кодування, захисту й ущільнення інформації: тези доп. II Міжнар. наук.-практ. конф.: (22-24 квіт. 2009 р.) / ред..: В.А. Лужецький; Вінниц. Нац.. техн.. ун-т. – Вінниця: Універсум, 2009. – 201 с.

58. *Моделирование безопасной обработки информации в компьютерных системах / А.М. Богданов, А.В. Корейко, Г.С. Корхмазов и др. – Киев: Наук. мнение, 2000. – 160 с.

59. *Молдован А.А. Криптография: учебник для вузов / А.А. Молдован, Н.А. Молдован, Б.Я. Советов. – Санкт-Петербург: Лань, 2000. – 218 с.

60. *Мухопад А.Ю. Системы криптографической защиты информации с микропрограммным управлением / А.Ю. Мухопад // Сборник научных трудов НГТУ / Новосиб. гос. техн. ун-т. – Новосибирск, 2013. - №3(73). – С. 75-84.

61. Мышкин Л. Меры безопасности для защиты информации IT-службы: существует огромное количество статей, книг и других публикаций о защите важной бизнес-информации. Но ситуация сильно осложняется, когда речь идет о защите информации самой IT-структуры / Л. Мышкин // Системный администратор. – 2008. - №12. – С. 56-59. 4 ч/з

62. *Нечаев В.И. Элементы криптографии. Основы теории защиты информации: учеб. пособие для студентов пед. вузов с углубленным изучением математики / В.И. Нечаев. – Москва: Высш. шк., 1999. – 110 с.

63. Олифер В.Г. Компьютерные сети: принципы, технологии, протоколы: учеб. пособие для студентов вузов по направлению «Информатика и вычислительная техника» / В.Г. Олифер, Н.А. Олифер. – Москва и др.: Питер, 2010. – 943 с.

З973я73

О546 871493

64. Осипян В.О. Криптография в задачах и упражнениях / В.О. Осипян, К.В. Осипян. – Москва: Гелиос АРВ, 2004. – 144 с.

З973я73

О743 831882

65. *Основы криптографии: учеб. пособие для студентов вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – Москва: Гелиос АРВ, 2001. – [б.с.].

66. * Основы криптографии: учеб. пособие для студентов вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – Москва: Гелиос АРВ, 2002. – 480 с.

67. *Основы криптографической защиты информации: учебник / Г.М. Гулак и др. – Винница: ВНТУ, 2011. – 199 с.

68. *Остапов С.Э. Основы криптографии: учеб. пособие для студентов вузов / С.Е. Остапов, Л.А. Валь. – Черновцы: Книги ХХ1, 2008. – 188 с.

69. Паркер Т. TCP/IP /Т. Паркер, К. Сиян. – Москва и др.: Питер, 2004. – 859 с.

З97
П182 832675

70. *Петров А.А. Компьютерная безопасность. Криптографические методы защиты : монография / А.А. Петров. – Москва: ДМК, 2000. – 445 с.

71. *Поповский В.В. Основы криптографической защиты информации в телекоммуникационных системах / В.В. Поповский, А.В. Персиков. – Харьков, 2010. – Ч.1. – 350 с.

72. Программно-аппаратные средства обеспечения информационной безопасности: защита программ и данных: учеб. пособие для студентов вузов, обучающихся по специальности «Защищающие телекоммуникационные системы» и др. / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – Москва: Радио и связь, 2000. – 169 с.

З973я73
П784 814820

73. *Прокушев Я.Е. Криптографическая защита информации: учеб. пособие / Я.Е. Прокушев. – Белгород: Кооп. образование, 2005. – 145 с.

74. *Романьков В.А. Введение в криптографию: курс лекций / В.А. Романьков. – Омск: Изд-во ОМГУ, 2006. – 168 с.

75. Рублинецкий В.И. Введение в компьютерную криптографию / В.И. Рублинецкий; Харьковский гуманит. ин-т «Нар. Укр. Акад.». – Харьков: ОКО, 1997. – 128 с.

З98
Р824 806023

76. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: Коло, 2007. – 296 с.

Е
Р885 853198

77. Рябко Б.Я. Криптографические методы защиты информации: учеб. пособие для студентов вузов, обучающихся по специальностям «Многоканальные коммуникационные системы», «Радиосвязь, радиовещание и телевидение», «Защитные системы связи» / Б.Я. Рябко, А.Н. Фионов. – Москва: Горячая линия-Телеком, 2005. – 229 с.

З973я73
Р981 856318

78. Семенов Ю.А. Алгоритмы телекоммуникационных сетей: в 3 ч.: учеб. пособие / Ю.А. Семенов. – Москва: Интернет ун-т информ. технологий, 2007. – Ч.3: Процедуры, диагностика, безопасность. – 511 с.
З973я73
С302 854209
79. *Семин М.Ю. Пути развития современной симметричной криптографии / М.Ю. Семин // вестн. Волжского ун-та. – 2006. – Вып. 9. – С. 51-63. – (Сер.: Информатика).
80. *Смарт Н. Криптография: монография / Н. Смарт. – Москва: Техносфера, 2005. – 525 с.
81. *Старовойтов А.В. Вопросы криптографии / А.В. Старовойтов // Интеллектуальные информационные системы. – Москва, 2008. – Т.1, №1. – С. 63-69.
82. *Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс. – Москва и др.: Вильямс, 2001. – 669 с.
83. Таненбаум Э.С. Компьютерные сети / Э.С. Таненбаум, Д. Уэзеролл. – Санкт-Петербург и др.: Питер, 2012. – 955 с.
З97
Т181 876055
84. *Тарасов А.М. Криптография и электронная подпись: правовые и организационные вопросы / А.М. Тарасов // Вестн. Акад. права и управления. – Москва, 2011. - №22. – С. 9-19.
85. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по специальности «Компьютерная безопасность» / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. – Москва: Радио и связь, 2000. – 192 с.
З973я73
Т338 812752
86. Тилборг ванн Хенк К.А. Основы криптологии: проф. руководство и интерактивный учебник / Х.К.А. Тилборг. – Москва: Мир, 2006. – 471 с.
З973я73
Т405 850136
87. *Феликсов Н.Н. К вопросу о методах защиты информации в системах управления на основе криптографических преобразований / Н.Н. Феликсов // Вестн. Акад. эконом. Безопасности МВД России. – Москва, 2009. - №7. – С. 101-103.
88. *Червяков Н.Н. Новые технологии криптографической защиты информации с использованием эллиптических кривых / Н.И. Червяков, А.Н. Гловко // Инфокоммуникационные технологии. – Самара, 2009. - №2. – С. 8-12.
89. Чмора А.Л. Современная прикладная криптография: учеб. пособие / А.Л. Чмора. – Москва: Гелиос АРВ, 2001. – 256 с.
З973я73
Ч746 816841
90. * Чмора А.Л. Современная прикладная криптография: монография / А.Л. Чмора. – Москва: Гелиос АРВ, 2002. – 244 с.

91. Чусавитина Г.Н. Элективный курс «Основы информационной безопасности» / Г.Н. Чусавитина // Информатика и образование. – 2007. - №4. – С. 43-56. 4 ч/з

92. *Шаньгин В.Ф. Защита информации и информационная безопасность: учеб. пособие в 2-х кН. / В.Ф. Шаньгин. – Москва: [б.и.]. – Ч.1: Основы информационной безопасности. Симметричные криптосистемы. – 1999. – 139 с.

93. *Широчин В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / В.П. Широчин, В.Е. Мухин, А.В. Кулик. – Киев: ВЕК+, 2000. – 112 с.

94. *Delfs H. Introduction to cryptography [Электронный ресурс]: principles and applications / H. Delfe, H. Knebl. – Berlin; Heidelberg: Springer-Verlag, 2007.

95. *Encyclopedia of cryptography and security [Электронный ресурс]: /ed.: H. Tilborg. – Electronic text data. – Boston, Ma: International federation for information processing, 2005.

96. Koops Bert-Jaap. The Crypto Controversy: A Key Conflict in Information Society / Bert-Jaap Koops. - The Hague a.o.: Kluwer Law Intern., 1999. – 285 p.

Х301
К73 821080

97. *Theory of cryptography [Электронный ресурс]: 4th Theory of cryptography conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007: proceedings / ed. S.P. Vadhan. – Electronic text data. – Berlin; H Heidelberg: Springer-Verlag, 2007.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ.

98. *Авдошин С.М. Криптографические методы защиты информационных систем / С.М. Авдошин, А.А. Савельев // Изв. Акад. инж. наук. – 2006. – Т.17: Бизнес-информатика. – С. 84-91.

99. Бабенко Л.К. Анализ симметричных криптосистем / Л.К. Бабенко, Е.А. Ищукова // Изв. Южного федерального ун-та. – 2012. - №12(137). – С. 136-147. – (Сер.: Технические науки). КиберЛенинка

100. Бабенко Л.К. Развитие криптографических методов и средств защиты информации / Л.К. Бабенко, Е.А. Ищукова, Е.А. Маро // Изв. Южного федерального ун-та. – 2012. - №4, Т.129. – С. 40-50. – (Сер.: Технические науки). КиберЛенинка

101. *Болелов Э.А. Криптографические методы защиты информации: учеб. пособие / Э.А. Болелов. – Москва: МГТУ ГА, 2011. – Ч.2: Асимметричные криптосистемы. – 2013. – 81 с.

102. *Будников А.Н. Сравнительный анализ защищенности криптографических протоколов электронного голосования с массовым удаленным участием и DRE-систем / А.Н. Будников // Электротехнические и информационные комплексы и системы. – Уфа, 2013. – Т.9, №3. – С. 73-75.

103. Варецький Я.Ю. Математична модель та метод біометричного захисту в криптографічних системах: автореф. дис…канд.. техн.. наук: (01.05.02) / Нац. ун-т «Львівська політехніка». – Львів, 2006. – 19 с. ав52026

104. Вертузаєв М.С. Захист інформації в комп'ютерних системах від несанкціонованого доступу: навч. посібник / М.С. Вертузаєв, О.М. Юрченко. – Київ: Вид-во Європ. ун-ту, 2001. – 321 с.

З973я73

В358 818961

106. Главчев М.И. К вопросу генерации ключей для асимметричных криптосистем / М.И. Главчев, Ю.Ю. Дроздов // Вестн. Харьковского нац. техн. ун-та . – 2004. - №46. – С. 74-77. – (Сер.: Информатика и моделирование).

КиберЛенинка

107. Головашич С.О. Методи побудови високостійких блокових симетричних шифрів та схем їх використання: дис…канд.. техн.. наук: (05.13.21) / Харк. Нац.. ун-т радіоелектроніки. – Харків, 2001. – 23 с.

З98

Г61 щдис2017

108. *Довгаль В.М. Криптографическая защита электронных документов на основе сети Фейстеля с применением детерминированных хаотических отображений / В.М. Довгаль, А.А. Тарасов // Изв. Курского гос. техн. ун-та. – Курск, 2010. - №1(30). – С. 44-48.

109. *Еремченко А.В. Исследование алгоритма генерации криптографических ключей из биометрической информации пользователей компьютерных систем / А.В. Еремченко, А.Е. Сулавко // Информационные технологии. – Москва, 2013. - №11(207). – С. 47-51.

110. *Зубов А.Ю. Криптографические методы защиты информации: совершенные шифры: учеб. пособие / А.Ю. Зубов. – Москва: Гелиос АРВ, 2005. – 191 с.

111. Коренева А.М. Об одном обобщении блочных шифров Фейстеля / А.М. Коренева, В.М. Фомичев // Прикладная дискретная математика. – 2012. - №3. – С. 34-40. КиберЛенинка

112. *Лагун А.Е. Криптографічні системи та протоколи: навч. посібник / А.Е. Лагун. – Львів: Вид-во «Львів. політехніка», 2013. – 95 с.

113. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учеб. пособие / О.Р. Лапонина. – Москва: Интернет ун-т информационных технологий, 2005. – 605 с.

З973я73

Л244 835670

114. *Леонтьев К.Б. Комментарий к Федеральному закону «Об электронной цифровой подписи»: постатейный / К.Б. Леонтьев. – Москва: Проспект, 2003. – 56 с.

115. Леонтьев Б.К. Крэкинг без секретов / Б.К. Леоньтев. – М.: Познават. КН. Плюс, 2001. – 575 с.

З97я2

Л478 821605

116. Лепеха О.М. Методи побудування схем розгортання ключів в сучасних блоках симетричних шифрах: автореф. дис…канд.. техн.. наук: (05.13.21) / Харк. нац.. ун-т радіоелектроніки. – Харків, 2005. – 23 с. дсп2087

117. Лисицька І.В. Методологія оцінки стійкості блокових симетричних крипто перетворень на основі зменшених моделей: автореф. дис…д-ра техн.. наук: (05.13.05) / Харків. нац.. ун-т. радіоелектроніки . – Харків, 2012. – 40 с.
ав76136

118. Мельничук Є.Д. Методи оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів: автореф. дис…канд.. техн.. наук: (05.13.21) / Харків. нац.. ун-т. радіоелектроніки. – Харків, 2013. – 24 с. ав84862

119. Михайленко М.С. Методи та засоби блокового симетричного шифрування з підвищеною стійкістю: автореф. дис…канд.. техн.. наук / Харків. нац.. ун-т радіоелектроніки. – Харків, 2008. – [б.с.]. дсп2160

120. *Молдовян Н.А. Введение в криптосистемы с открытым ключом: учеб. Пособие / Н.А. Молдовян, А.А. Молдовян. – Санкт-Петербург: БХВ-Петербург, 2005. – 286 с.

121. Олейников Р.В. Новый подход к построению схем разворачивания ключей для симметричных блочных шифров / Р.В. Олейников, В.И. Руженцев // Изв. Южного федерального ун-та. – 2010. - №11, т.112. – С. 156-162. – (Технические науки). КиберЛенинка

122. *Основы криптографии: учеб. пособие / А.П. Алферов и др. – Москва: Гелиос АРВ; Калуга, 2005. – 480 с.

123. *Панасенко С.П. Криптографические методы защиты информации / С.П. Панасенко // Вопросы защиты информации. – 2006. - №2. – С. 6-12.

124. Панкратов И.В. О поточных и автоматных шифрсистемах с симметричным ключом / И.В. Панкратов // Прикладная дискретная математика. – 2009. - №3. – С. 59-68. КиберЛенинка

125. Поляков А.О. Лабораторний практикум з навчальної дисципліни «Захист інформації в інформаційних системах»: навч.-практ. посібник / А.О. Поляков, С.П. Євсєєв, В.В. Огурцов. – Харків: Вид-во ХНЕУ, 2012. – 208 с.
З973я73
П542 876904

126. *Развитие криптографических методов и средств защиты информации / Л.К. Бабенко, Е.А. Ищукова, Е.А. Маро и др.// Изв. ЮФУ. – Таганрог, 2012. - №4(129). – С. 40-50.

127. *Рожков М.И. Криптографические методы защиты информации на основе несимметричных криптосистем: учеб. пособие / М.И. Рожков. – Москва: [б.и.], 2000. – 137 с.

128. Руженцев В.І. Методи оцінки стійкості блокових симетричних шифрів до диференційних атак: автореф. дис…канд.. техн.. наук: (05.13.21) / Харк. нац.. ун-т радіоелектроніки. – Харків, 2003. – 20 с. дсп2050

129. Рябко Б.Я. Криптографические методы защиты информации: учеб. пособие / Б.Я. Рябко, А.Н. Фионов. – Москва: Горячая линия – Телеком, 2005. – 229 с.
З973я73
Р981 865318

130. Суханов М.Б. Изучение принципов шифрования информации с открытым ключом / М.Б. Суханов, А.Г. Суханова // Информатика и образование. – 2009. - №10. – С. 100-103. 4 ч/з

131. *Терентьев А.И. Построение асимметричных криптографических систем на основе числовых линейных блоковых корректирующих кодов / А.И. Терентьев // Науч. вестн. МГТУ ГА / Моск. гос. техн. ун-т граждан. авиации. – Москва, 2009. - №145(8). – С. 82-88.

132. *Трифонов С.Е. Методы и средства защиты информации: учеб. пособие по специальности «Вычислительные машины, системы и сети» / С.Е. Трифонов, Л.И. Трифонова. – Пенза: [б.и.], 2002. - Ч.2: Криптографические методы защиты информации: введение в теорию секретных систем и теорию аутентификации. – 94 с.

133. Уфимцева В.Б. Метод та засоби перетворення інформації в АСУ на основі узагальнених чисел Фібоначчі: автореф. дис…канд.. техн.. наук: (05.13.21) / Харк. нац.. ун-т радіоелектроніки. – Харків, 2005. – 20 с. дсп2091

134. Филенко Е. Проблемы использования электронной цифровой подписи / Е. Филенко // Делопроизводство. – 2007. - №4. – С. 35-40. 4 ч/з

135. Фомина И.А. Управление ключами в криптографических системах / И.А. Фомина // Вестн. Нижегородского ун-та. – 2010. - №4. – С. 165-169.
КиберЛенинка

136. Хорев П.Ю. Криптографические интерфейсы и их использование / П.Б. Хорев. – Москва: Горячая линия – Телеком, 2007. – 277 с.
97
Х792 856309

137. Черемушкин А.В. Криптографические протоколы: основные свойства и уязвимости / А.В. Черемушкин // Прикладная дискретная математика: приложение. – 2009. - №2. – С. 115-150. КиберЛенинка

138. *Шаньгин В.Ф. Защита информации и информационная безопасность: учеб. пособие: в 2-х кН. / В.Ф. Шаньгин. – Москва, 2000. – Ч.2: Асимметричные криптосистемы. Идентификация, аутентификация, цифровая подпись и управление ключами. – 131 с.

139. Koops Bert-Jaap. The Crypto Controversy: A Key Confict in the Information Society / Koops Bert-Jaap. – The Hague a.o.: Kluwer Law Intern., 1999. – 285 p.
Х301
К73 821080

140. *Public key cryptography – PKC 2005 [Electronic resource]: 8th Intern. W0rkshop on theory and practice in public key cryptography, (Les Diablerets, Switzerland, Jan. 23-26, 2005). – Electronic text data. – Berlin; Heidelberg: Springer-Verlag, 2005. On-line

141. *Public key cryptography – PKC 2005 [Electronic resource]: 10th Intern. Conference on practice in public key cryptography Beijing, (China, April 16-20: proceedings) / T. Okamoto, X. Wang. - Electronic text data. – Berlin; Heidelberg: Springer-Verlag, 2007. On-line

АУТЕНТИФИКАЦИЯ.

142. *Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: монография / А.А. Афанасьев и др. – Москва: Горячая линия – Телеком; Вологда 2009. – 552 с.

143. Бирюков А. Средства однократной аутентификации: необходимость ввода паролей при входе в различные приложения может доставлять пользователю серьезные неудобства. Для автоматизации ввода пароля используются системы однократной аутентификации / А. Бирюков // Системный администратор. – 2011. - №7/8. – С. 58-62. 4 ч/з

144. Вишневский А.В. Windows Server 2003: для профессионалов / А.В. Вишневский . – Москва и др.: Питер, 2005. – 767 с.

З973.2
В555 834975

145. Гаряка А.А. Основы ASP. NET 2.0: учеб. пособие / А.А. Гаряка. – Москва: Интернет-ун-т информ. Технологий, 2007. – 296 с.

З973я73
Г219 850791

146. Гузик В.Ф. Биометрический метод аутентификации пользователя / В.Ф. Гузик, М.Н. Десятерик // Изв. Южного федерального ун-та. – 2000. - №2, т.16. – С. 129-133. – (Технические науки). КиберЛенинка

147. Дарвіш Л. Методи та засоби підвищення ефективності передачі в захищених комунікаційних середовищах: автореф. дис…канд.. техн.. наук: (01.05.03) / Нац. техн.. ун-т України «Київ. політехн. ін.-т». – Київ, 2006. – 20 с.
ав52778

148. *Зубов А.Ю. Математика кодов аутентификации / А.Ю. Зубов. – Москва: Гелиос АРВ, 2007. – 480 с.

149. Зубов А.Ю. Почти совершенные шифры и коды аутентификации / А.Ю. Зубов // Прикладная дискретная математика. – 20111. - №4. – С. 28-33.
КиберЛенинка

150. Измайлов Т. Пароли в интернет / Т. Измайлов // Компьютерная практика: пособие для профессионалов. – 2007. - №6. – С. 47-48. 4 ч/з

151. Иртегов Д.В. Введение в сетевые технологии: учеб. пособие для студентов вузов по направлении. «Информатика и вычислительная техника» / Д.В. Иртегов. – Санкт-Петербург: БХВ-Петербург, 2004. – 559 с.

З973я73
И845 833257

152. *Исхаков А.Ю. Двухфакторная аутентификация на основе программного токена / А.Ю. Исхаков, Р.В. Мещеряков, И.А. Ходашинский // Вопросы защиты информации. – Москва, 2013. - №3(102). – С. 23-28.

153. *Казарин О.В. Разработка инкрементальных схем для аутентификации и обеспечения целостности программ / О.В. Казарин // Вопросы защиты информации . – Москва, 2012. - №4(99). – С. 21-26.

154. *Ковалев Д.А. Защита протоколов ультралегкой аутентификации от атак на LSD / Д.А. Ковалев, С.В. Беззатеев // Изв. ВУЗов. – 2013. – Т.56, №8. – С. 58-61. – (Приборостроение).

155. *Константинов И.С. Подсистема многофакторной аутентификации пользователей в сети корпоративных порталов с применением универсального цифрового ключа доступа / И.С. Константинов, С.А. Лазарев, П.П. Силаев // Вестн. компьютерных и информационных технологий. – Москва, 2013. - №11(113). – С. 55-60.

156. Лапонина О.Р. Межсетевое экранирование: учеб. пособие / О.Р. Лапонина. – Москва: Интернет-ун-т информ. Технологий, 2007. – 343 с.

З973я73

Л244 850128

157. Луцків А.М. Математичне моделювання і обробка динамічно введеного підпису для задачі аутентифікації особи у інформаційних системах: автореф. дис…канд.. техн.. наук: (01.02.02) / Тернопільський держ. техн.. ун-т. – Тернопіль, 2008. – 20 с. ав58975

158. Маркелов А. Настраиваем TLS/SASL-шифрование и аутентификацию в MTA Sendmail: подробное руководство / А. Маркелов // Системный администратор. – 2008. - №8. – С. 64-66. 4 ч/з

159. Милославская Н.Г. Интрасети: доступ в Internet, защита: учеб. пособие для студентов вузов, обучающихся по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» / Н.Г. Милославская, А.И. Толстой. – Москва: ЮНИТИ, 2000. – 527 с.

З97я73

М606 811161

160. *Нашуан А.К. Аль-Маджарм. Методы аутентификации информации и обеспечения защищенности документов от подделки: автореф. дис…канд. техн. наук: (05.13.19). – Санкт-Петербург, 2009. – 17 с.

161. *Петров В.И. Новый подход к множественной аутентификации пользователя в современных разнородных информационных системах / В.И. Петров, М.С. Комар, Е.А. Кучерявый // Моделирование и анализ информационных систем. – Ярославль, 2013. – Т.20, №4. – С. 91-103.

162. Полянская О.Ю. Инфраструктуры открытых ключей: учеб. пособие / О.Ю. Полянская, В.С. Горбатов. – Москва: Интернет-ун-т информ. технологий, 2007. – 367 с.

З973я73

П545 854192

163. Проскурин В.Г. Программно-аппаратные средства обеспечения информационной безопасности: защита в операционных системах: учеб. пособие для студентов вузов, обучающихся по специальности «Защищающие телекоммуникационные системы», «Организация и технология защиты информации», «Комплексное обеспечение информационной безопасности автоматизированных систем» / В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич. – Москва: Радио и связь, 2000. – 168 с.

З973я73

П824 814879

164. Прохода А.Н. Обеспечение интернет-безопасности: практикум: учеб. пособие для студентов вузов, обучающихся по специальности «Средства связи с

подвижными объектами» / А.Н. Прохода. – Москва: Горячая линия – Телеком, 2007. – 180 с.
З98я73
П844 856315
165. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: Коло, 2007. – 286 с.
Е
Р885 853198
166. *Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации / А.Г. Сабанов // Вопросы защиты информации. – Москва, 2014. - №1(104). – С. 13-22.
167. *Смит Р.Э. Аутентификация: от паролей до открытых ключей / Р.Э. Смит. – Москва: Вильямс, 2002. – 432 с.
168. Соколов А.В. Защита в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – Москва: ДМК Пресс, 2002. – 656 с.
З97
С594 822346
169. Хенриксон Х. IIS 6: полное руководство: справочник профессионала / Х. Хенриксон, С. Хоффман. – Москва: ЭКОМ, 2004. – 672 с.
З98я2
Х385 850837
170. Юркин Д.В. Анализ временных и сложностных характеристик парольной аутентификации в защищенных операционных системах семейства Unix / Д.В. Юркин, А.В. Винель, В.В. Таранин // Информационно-управляющие системы. – Санкт-Петербург, 2013. - №3(64). – С. 62-66.
171. Яворски Д. Система безопасности Java: руководство разработчика / Д. Яворски, П.Дж. Перроун. – Москва и др.: Вильямс, 2001. – 524 с.
З97
Я227 822364
172. Яремчук С. Система аутентификации веб-пользователей WebAuth / С. Яремчук // Системный администратор. – 2007. - №6. – С. 68-72. 4 ч/з

СОДЕРЖАНИЕ