Криптографія на захисті інформації

Книжкова виставка читального залу обслуговування літературою природничого та технічного профілю (травень 2007 р.)

Криптографія — тайнопис — спеціальна система видозміни звичайного письма, розрахована на те, що зміст написаного зрозуміє лише обізнаний з цією системою.

	Enigma (40-і роки XX ст.), німецька електромеханічна шифрувальна машина
	M-209 (40-і роки XX ст.), американська шифрувальна машина

"Фиалка" (40-і роки XX ст.), радянська шифрувальна машина

1. **10 років на захисті інформаційного простору України** : Департамент спеціальних телекомунікаційних систем та захисту інформації / Служба безпеки України; Департамент спеціальних телекомунікаційних систем та захисту інформації / Валерій Володимирович Барлабанов (голов.ред.). - Ювіл. вид. - К. : Служба Безпеки України, 2002. - 82с. : фотоіл.
   Шифр зберігання книги в НБУВ: **ВС39689**

2. Алешников Сергей Иванович, Болтнев Юрий Федорович. **Математические методы защиты информации** : Учеб. пособие / Калининградский гос. ун-т. - Калининград, 2000. - Библиогр.: с. 113. **Ч. 1 : Алгебраические методы**. - 114с. - ISBN 5-88874-206-6.

   Введение в математические методы защиты информации - криптографию и теорию кодов, исправляющих ошибки. Излагается весь необходимый математический аппарат, включая основы теории коммутативных колец, полей и конечных полей. Представлено краткое описание пакета компьютерной алгебры Maple V и некоторые алгоритмы вычислений в конечных полях.
   Шифр зберігання книги в НБУВ: **В345319**

3. Аліпов Ілля Миколайович. **Методи захисту інформації при її передаванні** : Автореф. дис... канд. техн. наук: 05.13.08 / Харківський держ. технічний ун-т радіоелектроніки. - Х., 1997. - 22с.

   Метою дисертаційної роботи є розробка і дослідження методів захисту інформації в ЕОМ при її передачі і зберіганні на основі завадостійких до віртуальних завад алгоритмів пошуку точки екстремуму унімодальної функції.
   Шифр зберігання книги в НБУВ: **РА297297**

4. Алферов Александр Павлович, Зубов Анатолий Юрьевич, Кузьмин Алексей Сергеевич, Черемушкин Александр Васильевич. **Основы криптографии** : Учеб. пособие для студ. вузов, обучающихся по группе спец. в области информ. безопасности. - М. : Гелиос АРВ, 2001. - 480с. - Библиогр.: с. 469-474. - ISBN 5-85438-019-6.

   Излагаются основные понятия и разделы, позволяющие получить представление о задачах и проблемах современной криптографии. В пособие вошли как

традиционные вопросы классификации и оценки надежности шифров, так и системные вопросы использования криптографических методов защиты информации.
Шифр зберігання книги в НБУВ: **ВА627155**

5. Бабаш Александр Владимирович, Шанкин Генрих Петрович. **Криптография** / В.П. Шерстюк (ред.), Э.А. Применко (ред.). - М. : ООО Издательство "Солон-Р", 2002. - 511с. - (Серия книг "Аспекты защиты"). - ISBN 5-93455-135-3.

   Рассмотрены вопросы дешифрования простейших шифров, методы криптоанализа и синтеза криптосхем, вопросы криптографической стойкости, помехоустойчивости и имитостойкости шифросистем.
   Шифр зберігання книги в НБУВ: **ВА649356**

6. Бардіс Ніколас. **Розробка підходу і застосування апарату булевих функцій для аналізу і синтезу ефективних криптографічних алгоритмів захисту інформації** : Автореф. дис... канд. техн. наук: 05.13.13 / Національний технічний ун-т України "Київський політехнічний ін-т". - К., 1998. - 16с.

   Мета роботи полягає в розробці засобу оцінки рівня захищеності криптографічних алгоритмів захисту інформації на основі їх аналізу на рівні булевих функцій, а також в створенні ефективних засобів формального синтезу булевих функцій, як функціональної основи цього класу алгоритмів та генераторів псевдовипадкових послідовностей.
   Шифр зберігання книги в НБУВ: **РА306340**

7. Блінцов Володимир Степанович, Гальчевський Юрій Леонідович. **Математичні основи криптології + CD** : Навчальний посібник для студ. вищих навч. закл. / Національний ун-т кораблебудування ім. адмірала Макарова. - Миколаїв : НУК, 2006. - 232с. : рис., табл; - ISBN 966-321-056-7.

   Приведений математичний апарат, який використовується в криптографії і криптоаналізі. Особлива увага приділена питанням "Теорії інформації", "Теорії складності", "Теорії чисел", "Кінцевим полям", "Генераторам псевдовипадкових послідовностей". На компакт-диску містяться критерії оцінки захищеності інформації в комп"ютерних системах від несанкціонованого доступу і термінологія в галузі захисту інформації в комп"ютерних системах від несанкціонованого доступу.
   Шифр зберігання книги в НБУВ: **ВА673978**

8. Богуш Володимир Михайлович, Мухачов Владислав Андрійович. **Криптографічні застосування елементарної теорії чисел** : Навч. посібник / Державний ун-т інформаційно-комунікаційних технологій. - К. : ДУІКТ, 2006. - 126с. - Бібліогр.: с. 25. - ISBN 966-2970-06-1.

   Приведена структурована сукупність відомостей щодо застосування методів елементарної теорії чисел для побудови та тестування параметрів криптосистем.
   Шифр зберігання книги в НБУВ: **ВА676987**

9. Варецький Ярема Юрійович. **Математична модель та метод біометричного захисту в криптографічних системах** : Автореф. дис... канд. техн. наук: 01.05.02 / Національний ун-т "Львівська політехніка". - Л., 2006. - 19с.

   Метою дослідження є розробка математичної моделі та методу біометричного захисту ключів криптографічних алгоритмів. Вирішено задачі дослідження існуючих класичних систем криптографічного захисту та біометричної ідентифікації, дослідження методів генерації та захисту ключової інформації, створення

математичної моделі, яка описує процес ключів сучасних криптографічних алгоритмів за допомогою біометричних даних, розробки методу зв"язування криптографічних ключів із біометричними даними людини, апробації результатів досліджень шляхом створення прикладної інформаційної системи.
Шифр зберігання книги в НБУВ: **РА343060**

10. **Введение в алгебру (с приложением к криптографии)** : Учеб. пособие для студ. и асп. по спец. 08.02.02 - прикл. математика / В.А. Фильштинский, Л.А. Фильштинский, С.В. Фильштинский; Ин-т содерж. и методов обучения {Сумы}, Сум. гос. ун-т. - Суми: ИПП "Мрія-1" ЛТД, 1999. - 206 с. - Библиогр.: 9 назв. - рус.

    Викладено традиційні теми загальної алгебри: групи, кільця, поля та їх найпростіші властивості, початкові відомості про поля Галуа та кільця багаточленів. Наведено найпростіші додатки до криптографії. Сформульовано задачі, які можна використовувати для проведення практичних занять.
    Шифр зберігання книги в НБУВ: **ВА592549**

11. Вербіцький Олег Васильович. **Вступ до криптології**. - Львів : Вид-во Наук.-техн. літ., 1998. - 247с. - (Університетська математика). - ISBN 966-7148-03-3. - ISBN 966-7148-23-8.

    Кожен розділ, присвячений певному класові криптосистем, починається обговоренням основних концепцій і містить опис конкретних алгоритмів та їх детальний математичний аналіз. Виклад математичного апарату максимально замкнений.
    Шифр зберігання книги в НБУВ: **ВА583566**

12. Гарбарчук В., Зинович З., Свиц А. **Кибернетический подход к проектированию систем защиты информации** / Украинская академия информатики ; Волынский гос. ун-т им. Леси Украинки ; Люблинский политехнический ун-т. - К. ; Луцк ; Люблин, 2003. - 658с. : рис. - Библиогр.: с. 648-653. - ISBN 966-8064-84-4.

    Книга является одной из первых работ по вопросам теории и практики проектирования систем защиты информации и включает четко систематизированнный материал по методологии защиты информации и методологии проектирования соответствующих систем, прикладной теории информации, кибернетической теории моделирования систем защиты информации.
    Шифр зберігання книги в НБУВ: **ВА655211**

13. Горбенко Іван Дмитрович, Гріненко Тетяна Олексіївна. **Захист інформації в інформаційно-телекомунікаційних системах** : Навч. посіб. для студ. спец. "Комп'ютерні науки", "Комп'ютена інженерія", "Прикладна математика", "Інформаційна безпека" вищ. навч. закл. / Харківський національний ун-т радіоелектроніки. - Х. : ХНУРЕ, 2004. - Бібліогр.: с. 364-368. **Ч. 1 : Криптографічний захист інформації**. - 368с. : рис. - ISBN 966-659-081-6.

    Викладено основи криптології, криптографічні системи та протоколи, мережні протоколи та розглянуто комплекс задач практичного значення.
    Шифр зберігання книги в НБУВ: **В348247**

14. Грездов Глеб Геннадьевич. **Современные методы криптографической защиты информации: (обзор по материалам открытой печати)** . - К., 2002. - 31с. : рис. - (Препр. / 2002; 01). - Библиогр.: с. 28-30.

    Изложены законодательные аспекты защиты информации, требования к криптографическим системам, этапы развития методов криптографической защиты

информации. Приведена классификация современных методов криптографической защиты информации, рассмотрены проблемы и перспективы развития криптографических систем.
Шифр зберігання книги в НБУВ: **Р93788**

15. Ерош Игорь Львович. **Дискретная математика. Математические вопросы криптографии** : Учеб. пособие / Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - СПб., 2001. - 55с. - Библиогр.: с.54.

    Кратко изложены основные положения криптографии, которая по используемому математическому аппарату может рассматриваться как раздел дискретной математики.
    Шифр зберігання книги в НБУВ: **ВА625738**

16. Ємець Володимир, Мельник Анатолій, Попович Роман. **Сучасна криптографія: Основні поняття** . - Л. : БаК, 2003. - 144с. : рис., табл. - (Захист інформації в комп'ютерних та телекомунікаційних мережах). - Бібліогр.: с. 128. - ISBN 966-7065-44-8.

    Розглянуто основні теоретичні положення сучасної криптографії. Описано сучасні симетричні шифрувальні алгоритми. Наведено теоретичні основи для асиметричних шифрувальних алгоритмів та практично всі відомі сьогодні класи цих алгоритмів. Висвітлено генерування псевдовипадкових послідовностей та використання хешувальних функцій. Пояснено побудову цифрових підписів на підставі асиметричних алгоритмів. Викладено одне з ключових питань у разі застосування криптографії на практиці - адміністрування ключами. Розглянуто можливі сучасні підходи до зламування криптосистем.
    Шифр зберігання книги в НБУВ: **ВА653345**

17. Жельников Владимир. **Криптография от папируса до компьютера**. - М. : ABF, 1996. - 336с. - ISBN 5-87484-054-0.

    В увлекательной живой форме автор рассказывает о науке криптологии и сферах ее применения человеком с древнейших времен и до сегодняшнего дня. Книга поможет написать шифрованное письмо другу и защитить данные в компьютере от любопытных глаз хакеров. Особое внимание уделено безопасности персональных ЭВМ.
    Шифр зберігання книги в НБУВ: **ВА574020**

18. Задірака Валерій Костянтинович, Олексюк Олександр Степанович. **Комп'ютерна криптологія** : Підручник / Тернопільська академія народного господарства; НАН України; Інститут кібернетики ім. В.М.Глушкова. - К., 2002. - 504с. : іл. - Бібліогр.: с. 491-502. - ISBN 5-7763-0485-7.
    Шифр зберігання книги в НБУВ: **ВА633216**

19. **Захист інформації в інформаційно-телекомунікаційних системах** : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації / І.Д. Горбенко, Т.О. Гріненко; Харк. нац. ун-т радіоелектрон. - Х., 2004. - 368 с. - Бібліогр.: 73 назв. - укр.

    Викладено основи криптології, описано криптографічні системи та протоколи, зокрема мережеві. Розглянуто математичну модель захищеної інформаційно-телекомунікаційної системи, умови стійких криптосистем, а також систем з відкритими ключами та їх відкритим розподілом. Висвітлено питання криптоперетворення в групі точок еліптичних кривих, теорію автентичності, властивості електронного цифрового підпису, алгоритмів формування

псевдовипадкових та випадкових послідовностей. Наведено оцінку автентичності захисту інформації з використанням симетричних алгоритмів. Розкрито основи побудови та застосування захищених віртуальних мереж.
Шифр зберігання книги в НБУВ: **В348247**

20. **Захист інформації. Криптографічні методи** : Підруч. для вищ. навч. закл. / І.І. Маракова, А.І. Рибак, Ю.С. Ямпольський; Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с. - Бібліогр.: 46 назв. - укр.

    Розглянуто основні проблеми захисту інформації та криптографічних методів. Викладено основи інформативної бази, концепцію комплексного підходу до питань захисту інформації. Описано класичні та сучасні методи шифрування, сучасні засоби захисту, що є основою інформації та електронного цифрового підпису.
    Шифр зберігання книги в НБУВ: **ВА620329**

21. **Защита информации: Компьютерная криптография. Защита от компьютерных вирусов** / Б.Ю. Ключевский (сост.). - М. : Гротек, 1998. - 62с. - (Профессиональное досье).

    Рассмотрены основы компьютерной криптографии, криптографические ключи и робота с ними, криптографические протоколы, синтез систем обработки информации с защитой от компьютерных вирусов.
    Шифр зберігання книги в НБУВ: **СО23944**

22. **ДСТУ 4145-2002. Інформаційні технології ; Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння** / О. Шаталов (розроб.)Кочубінський А. (розроб.). - Офіц. вид. - К. : Державний комітет України з питань технічного регулювання та споживчої політики, 2003. - V, 31 с. - (Національний стандарт України). - Бібліогр.: с. 30.
    Шифр зберігання книги в НБУВ: **СТ1005**

23. **Информационная безопасность в каналах телекоммуникаций** : Учеб. пособие / А.А. Замула, Л.А. Клименко, В.П. Филиппович, Г.З. Халимов; Ред.: А.В. Королев. - 2-е изд. - Х.: Регион-информ: ХФИ "Транспорт Украины", 2000. - 215 с. - (Новые информ. технологии; Вып. 2). - Библиогр.: 21 назв. - рус.

    Рассмотрены потенциальные нарушения безопасности информации и принципы защиты, которыми нужно руководствоваться при проектировании механизмов защиты, в нескольких взаимосвязанных областях - криптографии, защите объектов, средствах коммуникаций. Приведены методы и механизмы защиты, различные криптоалгоритмы. Описаны возможные воздействия нарушителя на систему, обсужден ряд возможных контрмер против этих воздействий. Подробно освещены теоретические основы и практические методы аутентификации, применяемые в современных вычислительных системах и сетях. Приведено описание принципов и механизмов контроля доступа, в частности, различных реализаций матриц доступа. Изложены механизмы защиты, поддерживающие функции обеспечения целостности данных и управления доступом в сетях, а также определения подлинности объекта сети. Описаны различные модели паролей, используемых для вхождения в вычислительную систему или выполнения пакетного задания. Модели паролей представлены в виде алгоритмов формализованной последовательности некоторых шагов.
    Шифр зберігання книги в НБУВ: **ВА599968**

24. **Інформаційна безпека: організаційно-правові основи** : Навч. посіб. для студ. вищ. навч. закл. / Б.А. Кормич. - К.: Кондор, 2004. - 384 с. - (Юрид. кн.). - Бібліогр.: с. 373-382. - укр.

    Розглянуто історію формування суті поняття національної безпеки (НБ), а також особливості правового регулювання її питань. Показано роль інформації в житті держави та суспільства, запропоновано її класифікацію в українському законодавстві. Розкрито суть поняття державно-правового механізму інформаційної безпеки, а також правові аспекти реалізації її політики. Проаналізовано особливості технічного та криптографічного захисту інформації в інформаційних системах.
    Шифр зберігання книги в НБУВ: **ВА647837**

25. **Інформаційні системи і технології в юридичній діяльності** : Навч.-метод. посіб. / О.О. Денісова; Київ. нац. екон. ун-т. - К., 2005. - 254 с. - Бібліогр.: 19 назв. - укр.

    Викладено основи криптографічного захисту інформації за допомогою системи PGP, управління документами на основі програмно-технологічного комплексу "DIS:class", використання правових інформаційно-пошукових систем, пошуку правових документів у Глобальній мережі правової інформації (GLIN) та в системі "Закони та підзаконні акти України в Інтернет", а також пошуку інформації в реєстрах Міністерства юстиції України.
    Шифр зберігання книги в НБУВ: **ВА667441**

26. **Інформаційні технології; Методи захисту. Геш-функції** / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2004. - (Національний стандарт України). - Бібліогр.: с. 5. **Ч. 1 : ДСТУ ISO/IEC** . - IV, 6с.
    Шифр зберігання книги в НБУВ: **СТ1755**

27. **Інформаційні технології; Методи захисту. Геш-функції** / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2004. - (Національний стандарт України). - Бібліогр.: с. 17. **Ч. 2 : ДСТУ ISO/IEC** . - V, 17с. : р и с .
    Шифр зберігання книги в НБУВ: **СТ1755**

28. **Інформаційні технології; Методи захисту. Геш-функції** / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2004. - (Національний стандарт України). - Бібліогр.: с. 84. **Ч. 3 : ДСТУ ISO/IEC** . - VI, 84с.
    Шифр зберігання книги в НБУВ: **СТ1755**

29. **Інформаційні технології; Методи захисту. Неспростовність** / М. Карнаух (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2006. - (Національний стандарт України). **Ч. 1 : ДСТУ ISO/ IEC 13888-1:2002; Загальні положення (ISO/IEC 13888-1:1997, IDT)** . - IV, 17с.
    Шифр зберігання книги в НБУВ: **СТ2584**

30. **Інформаційні технології; Методи захисту. Неспростовність** / М. Карнаух (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2006. - (Національний стандарт України). **Ч. 3 : ДСТУ ISO/ IEC 13888-3:2002; Механізми з використанням асиметричних методів (ISO/IEC 13888- 3:1997, IDT)** . - IV, 10с.
    Шифр зберігання книги в НБУВ: **СТ2584**

31. **Інформаційні технології; Методи захисту; Цифрові підписи з доповненнями** / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид. - К. : Держспоживстандарт України,

2006. - (Національний стандарт України). **Ч. 1 : ДСТУ ISO/IEC 14888-1:2002; Загальні положення (ISO/IEC 14888- 1:1998, IDT)** . - IV, 14с. : рис.
Шифр зберігання книги в НБУВ: **СТ2738**

32. **Інформаційні технології; Методи захисту; Цифрові підписи з доповненнями** / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид. - К. : Держспоживстандарт України, 2006. - (Національний стандарт України). - Бібліогр.: с. 29. **Ч. 3 : ДСТУ ISO/IEC 14888-3:2002; Механізми на основі сертифікатів (ISO/IEC 14888-3:1998, IDT)** . - IV, 30с.
Шифр зберігання книги в НБУВ: **СТ2738**

33. **Інформаційні технології; Методи захисту; Цифрові підписи з доповненням** / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид. - К. : Держспоживстандарт України, 2006. - (Національний стандарт України). - Бібліогр.: с. 17. **Ч. 2 : ДСТУ ISO/IEC 14888-2:2002; Механізми на основі ідентифікаторів (ISO/IEC 14888- 2:1999, IDT)** . - IV, 18с. : рис.
Шифр зберігання книги в НБУВ: **СТ2738**

34. Исагулиев Карэн Паруйрович. **Справочник по криптологии** . - Минск : ООО "Новое знание", 2004. - 236с. - ISBN 985-475-079-5.

    Собраны основные сведения об основах криптографии и криптоанализа, о современной нормативной базе в сфере защиты информации, а также об используемых алгоритмах и ключах. При подготовке учтены последние достижения криптологии, а также особенности ее применения в странах СНГ.
    Шифр зберігання книги в НБУВ: **ВА670453**

35. **Кибернетический подход к проектированию систем защиты информации** / В. Гарбарчук, З. Зинович, А. Свиц; Укр. акад. Инф-ки, Волын. гос. ун-т им. Л.Украинки, Любл. политехн. ун-т. - К.; Луцк; Люблин, 2003. - 658 с.: рис. - Библиогр.: с. 648-653. - рус.

    Рассмотрены история развития криптологии, а также методы криптоанализа, принятия проектных решений, определения криптостойкости. Приведены общие требования к разработке шифров. Изложены криптологические средства проектировщика систем. Охарактеризованы основоположные принципы квантовой криптографии. Проанализированы особенности методологической защиты информации. Раскрыта сущность понятий теории живучести систем.
    Шифр зберігання книги в НБУВ: **ВА655211**

36. **Комп'ютерна криптологія** : Підруч. / В.К. Задірака, О.С. Олексюк; Терноп. акад. нар. госп-ва, НАН України. Ін-т кібернетики ім. В.М.Глушкова. - К., 2002. - 504 с.: іл. - Бібліогр.: с. 491-502. - укр.

    Розглянуто методи сучасної криптографії та особливості їх застосування до проектування безпечних комп'ютерних систем. Наведено організаційні, правові, технічні та криптографічні методи захисту інформації, а також методи цифрового підпису. Висвітлено методологію захисту автоматизованих систем обробки інформації. Охарактеризовано ресурси криптографії в мережі Internet.
    Шифр зберігання книги в НБУВ: **ВА633216**

37. **Комп'ютерні мережі військового призначення** / В.М. Антонов, О.Ю. Пермяков. - К.: "МК-Прес", 2005. - 320 с. - Бібліогр.: с. 260-266. - укр.

Розглянуто питання побудови, використання та реалізації сучасних комп'ютерних мереж цивільного та військового призначення на підставі нових інформаційних технологій. Висвітлено проблему побудови мереж військового призначення з використанням нового підходу АРМ-технології, що дозволяє проектувати та використовувати спеціальні мережі у форматі ефективного керування військами на сучасному етапі. Проаналізовано особливості використання криптології та криптографії для побудови криптосистем у військових і спеціальних мережах.
Шифр зберігання книги в НБУВ: **ВА664426**

38. Конахович Георгий Филимонович, Климчук Владимир Павлович, Паук Сергей Михайлович, Потапов Вячеслав Геннадиевич. **Защита информации в телекоммуникационных системах** . - К. : МК-Пресс, 2005. - 279с. : рис., табл. - На обл. указ. только 1-й автор. - Библиогр.: с. 279. - ISBN 966-8806-03-4.

    В книге рассмотрены основные проблемы защиты информации, возникающие в ведомственных системах связи и передачи данных, радиотехнических системах и системах связи общего пользования. Отдельные главы посвящены криптографии и шифрованию.
    Шифр зберігання книги в НБУВ: **ВС41056**

39. **Криптографічні застосування елементарної теорії чисел** : Навч. посіб. / В.М. Богуш, В.А. Мухачов; Держ. ун-т інформ.-комунікац. технологій. - К., 2006. - 125 с. - Бібліогр.: 12 назв. - укр.

    Розглянуто питання застосування методів елементарної теорії чисел для побудови та тестування параметрів криптосистем. Описано методи сучасної криптології, модульні операції в симетричній криптографії, арифметичні алгоритми в асиметричній криптографії.
    Шифр зберігання книги в НБУВ: **ВА676987**

40. **Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей** : Моногр. / Ю.Є. Яремчук. - Вінниця: Кн.-Вега, 2002. - 135 с. - Бібліогр.: 88 назв. - укр.

    Наведено результати дослідження теоретико-числових властивостей рекурентних послідовностей. Розглянуто питання розробки модифікованих методів, програмних та апаратних засобів реалізації шифрування інформації, оцінено складність алгоритмів її шифрування. Проаналізовано криптостійкість модифікованих методів. Запропоновано пакет програм шифрування інформації. Описано пристрої для виконання операцій модулярної арифметики багаторазової точності, спеціальні процесори шифрування інформації.
    Шифр зберігання книги в НБУВ: **ВА634716**

41. Кузнецов Георгій Віталійович, Фомичов Вадим Володимирович, Сушко Світлана Олександрівна, Фомичова Людмила Яківна. **Математичні основи криптографії** : Навч. посіб. / Національний гірничий ун- т. - Д. : НГУ, 2004. - 392с. - Бібліогр.: с. 389-391. **Ч. 1** - 392с. - ISBN 966-8271-79-3.
    Шифр зберігання книги в НБУВ: **В348154**

42. Левин Максим. **Криптография: Руководство пользователя**. - М. : Издательство "Познавательная книга плюс", 2001. - 319с. - (Ваш персональный компьютер). - Библиогр.: с. 303-305. - ISBN 5-8321-0181-1.

Дается общее введение в криптографию, рассматриваются вопросы сетевой и комплексной системы безопасности, основные виды и источники атак на информацию, криптографическая система PGP, защита телефонных разговоров, почтовые серверы открытых ключей, использование PGP в Linux, шифрование электронной почты и файлов.
Шифр зберігання книги в НБУВ: **ВА649416**

43. Левин Максим. **Криптография без секретов: Руководство пользователя** - М. : ЗАО "Новый издательский дом", 2005. - 315с. - Библиогр.: 307-308. - ISBN 5-9643-0063-1.

    Издание посвящено тем, кто интересуется теоретическими аспектами криптологии и желает практически реализовать алгоритмы криптографии на персональном компьютере.
    Шифр зберігання книги в НБУВ: **ВА680066**

44. Лук'янов Дмитро Олександрович. **Управління ключовою інформацією в системах захисту групових комунікацій** : Автореф. дис... канд. фіз.-мат. наук: 01.05.03 / Київський національний ун-т ім. Т.Г.Шевченка - К., 2004. - 16с.

    Метою дослідження є створення, теоретичне обгрантування та програмна реалізація концептуального підходу, конкретних методів і алгоритмів управління ключовою інформацією в системі криптографічного захисту групової комунікації, адекватних сучасним науково-теоретичним та технологічним досягненням в цій сфері.
    Шифр зберігання книги в НБУВ: **РА330674**

45. Мао Венбо. **Современная криптография: Теория и практика** / Д.А. Клюшин (пер.с англ.и ред.). - М.; СПб.; К. : Издательский дом "Вильямс", 2005. - 763с. - Библиогр.: с. 731-754. - ISBN 5-8459-0847-7 (рус.). - ISBN 0-13-066943-1 (англ.).

    Автор критикует "учебные" криптографические алгоритмы и описывает принципы разработки криптосистем и протоколов повышенной стойкости. Изложены математические основы криптографии, описаны промышленные стандарты криптографических протоколов, включая IPSec, IKE, SSH, TLS (SSL) и Kerberos, приведены формальные доказательства сильной стойкости практичных схем шифрования, цифровой подписи, зашифрованной подписи и аутентификации, а также проанализированы протоколы с нулевым разглашением.
    Шифр зберігання книги в НБУВ: **ВС42276**

46. Маракова Ірина Іллівна, Рибак Анатолій Іванович, Ямпольський Юрій Степановмч. **Захист інформації. Криптографічні методи** : Підруч. для вищ. навч. закл. / Одеський держ. політехнічний ун-т; Інститут радіоелектроніки і телекомунікацій. - О., 2001. - 164с. - Бібліогр.: с. 158-160. - ISBN 966-7813-04-9*.

    Розглядаються основні проблеми захисту інформації взагалі і криптографічних методів зокрема. Викладені основи нормативної бази, концепція комплексного підходу до питань захисту інформації. Описані класичні і сучасні методи шифрування, сучасних засобів захисту, що є основою інформації і електронного цифрового підпису.
    Шифр зберігання книги в НБУВ: **ВА620329**

47. Масленников Михаил. **Практическая криптография: Некоторые идеи метра криптографии Клода Шеннона; Основные криптологические процедуры; Построение качественного генератора гаммы; Хэш-функция и электронная**

подпись . - СПб. : БХВ-Петербург, 2003. - 458 с. : рис.+ 1 CDR - (Мастер решений). - ISBN 5-94157-201-8.

Наряду с основными теоретическими положениями рассматривается создание криптографического ядра, встраивание криптографических алгоритмов в Microsoft Outlook и Lotus Notes, создание автоматизированной системы документооборота, технология отпечатков пальцев. Все программное обеспечение, описываемое в книге, создано в Borland C++ Builder. На компакт-диске находятся демонстрационные версии некоторых программ и документация.
Шифр зберігання книги в НБУВ: **ВА643552/CDR206**

48. **Математичні основи криптографії** : Навч. посіб. Ч. 1 / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова; Нац. гірн. ун-т. - Д., 2004. - 391 с. - Бібліогр.: 42 назв. - укр.

Викладено математичні основи криптографії, розглянуто питання множин та відношень, багаточленів та їх коренів, полів Галуа. Описано теорію чисел, висвітлено основи класичної криптографії та криптографічні алгоритми теорії чисел.
Шифр зберігання книги в НБУВ: **В348154**

49. **Математичні основи криптології + CD** : Навч. посіб. для студ. вищ. навч. закл. / В.С. Блінцов, Ю.Л. Гальчевський; Нац. ун-т кораблебудування ім. Адмірала Макарова. - Миколаїв, 2006. - 232 с. - укр.

Висвітлено математичні підходи та методи, які використовуються криптографами та криптоаналітиками. Описано основні властивості інформації як предмета захисту, розкрито суть понять складності алгоритму, арифметики та повної системи відрахувань, кінцевих полів, векторного простору над полем, мультиплікаційного звертання, генераторів псевдовипадкових послідовностей, кореляційної незалежності, рекурентних бінарних послідовностей, великих чисел і операцій з ними, лінійного поділу секрету для довільних структур доступу. Наведено критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
Шифр зберігання книги в НБУВ: **ВА673978**

50. **Материалы международной научно-технической конференции "Повышение эффективности систем защиты информации" "Защита-97"** / Киевский международный ун-т гражданской авиации. - К., 1997. - 230с.

Приводятся доклады по дифференциальному криптоанализу, применению полей Галуа в криптографии, криптографической защите данных в сетях связи и др.
Шифр зберігання книги в НБУВ: **ВА583226**

51. Мельников Виталий Викторович. **Защита информации в компьютерных системах**. - М. : Финансы и статистика, 1997. - 368с. : ил. - ISBN 5-279-01631-4.

Наряду с другими методами защиты информации в компьютерных системах в книге представлен метод криптографического преобразования информации.
Шифр зберігання книги в НБУВ: **ВА575594**

52. Мельникова Оксана Анатоліївна. **Розробка методів та засобів криптографічного захисту інформації в комп'ютерних системах та мережах** : Автореф. дис... канд. техн. наук: 05.13.06 / Харківський держ. технічний ун-т радіоелектроніки. - Х., 1998. - 18 с. : мал.

Метою роботи є розробка комп"ютерних технологій забезпечення автентичності , причетності, конфіденційності та захисту від НСД банківської та іншої цінної інформації на всіх етапах її життєвого циклу, а також захист інформаційних та обчислювальних ресурсів для моделі взаємної недовіри та взаємного захисту, з урахуванням реальних погроз в умовах обмежених матеріальних та технічних ресурсів, а також важко прогнозуємого розвитку теорії та практики криптоаналізу.
Шифр зберігання книги в НБУВ: **РА301793**

53. **Моделирование безопасной обработки информации в компьютерных системах** / А.М. Богданов, А.В. Корнейко, Г.С. Корхмазов, В.В. Мохор, С.С. Ярманов; НАН Украины. Ин-т пробл. моделирования в энергетике. - К.: Наук. думка, 2000. - 160 с. - Библиогр.: 55 назв. - рус.

    Освещены проблемы моделирования безопасной обработки информации в компьютерных системах (КС). Изложены подходы к построению моделей функционирования систем защиты информации в КС, а также процессов их создания. Проанализированы основные методы моделирования криптографической защиты информации в КС на основе отечественного алгоритма симметричного цифрования по ГОСТ 28147-89.
    Шифр зберігання книги в НБУВ: **ВА603967**

54. **Моделі і системи оцінювання, обробки та захисту фінансової інформації** : Моногр. / Г.М. Азаренкова, С.В. Гадецька, І.Д. Горбенко, Ю.В. Дубницький, О.О. Єгоршин; Ред.: О.В. Васюренко. - Х.: Константа, 2005. - 380 с. - Бібліогр.: с. 368-380. - укр.

    Розглянуто математичні методи аналізу фінансової інформації - моделювання конкурсу за умов корупції та суперництва сторін під час їх активної взаємодії, а також статистичного оцінювання параметра кривої Лоренца. Охарактеризовано інформаційне та програмне забезпечення, необхідне для реалізації економічного аналізу та прийняття рішень у банківських установах. Розроблено експертну систему для реалізації багатокритеріального вибору у сфері банківського кредитування та методику виконання фінансових розрахунків за умов нестохастичної невизначеності. Наведено приклади використання засобів моделювання під час розв'язання фінансово-економічних задач. Визначено пріоритетні завдання аналізу та прогнозування часових рядів, наведено методику вилучення трендів. Розглянуто моделі Бокса - Дженкінса та їх програмне забезпечення. Запропоновано перспективні методи криптографічного захисту банківської інформації на основі перетворень у групі точок еліптичних кривих.
    Шифр зберігання книги в НБУВ: **ВА664188**

55. Молдовян Николай Андреевич, Молдовян Александр Андреевич. **Введение в криптосистемы с открытым ключом**.- СПб.: БХВ-Петербург, 2005.- 288 с.: ил.- ISBN 5-94157-563-7.

    Отражена проблематика современной криптографии, рассмотрена краткая характеристика современных криптосистем с секретным ключом и специфика задач, решаемых с использованием шифров с открытым ключом. Приведены сведения из теории чисел, необходимые для понимания всех рассмотреннных алгоритмов и протоколов двухключевой криптографии. Детально представлены системы открытого шифрования, открытого распределения ключей и электронной цифровой подписи. Обсуждаются особенности схем слепой подписи, протоколы с нулевым разглашение и пороговые схемы разделения секрета. Раскрывается

понятие хэш-функций, требования к ним и их использование в системах ЭЦП. Рассматриваются вопросы управления секретными ключами, инфраструктура открытых ключей и формирование цифровых сертификатов.
Шифр зберігання книги в НБУВ: **ВС41397**

56. Мустафа Акрам Ареф Найеф. **Розробка засобів ефективного вибору та реалізації алгоритмів захисту інформації в комп'ютерних системах** : Автореф. дис... канд. техн. наук: 05.13.13 / Національний технічний ун-т України "Київський політехнічний ін- т". - К., 2003. - 21с.

    Метою роботи є підвищення оперативності комплексного оцінювання рівня захищенності інформації в комп"ютерних системах та мережах за рахунок ефективної організації обчислювальних процедур комплексного тестування алгоритмів захисту інформації, а також підвищення оперативності захисту інформації в комп"ютерних системах за рахунок розпаралелювання реалізації алгоритмів захисту шляхом їх модифікації без зменшення рівня захищеності даних.
    Шифр зберігання книги в НБУВ: **РА322985**

57. Мухачев Владислав Андреевич, Хорошко Владимир Алексеевич. **Методы практической криптографии**. - К. : ПолиграфКонсалтинг, 2005. - 214с. - Библиогр.: с. 209-214. - ISBN 966-8440-48-X.

    Рассматривается круг вопросов, связанных с надежностью действующих систем криптографической защиты информации. Обосновываются требования к параметрам ряда распространенных криптоалгаритмов и криптографическим свойствам некоторых преобразований. Приводятся методы их генерации и тестирования.
    Шифр зберігання книги в НБУВ: **ВА668256**

58. Мухачев Сергей Валентинович, Богданчиков Вадим Борисович. **Компьютерные преступления и защита информации**: Учеб.-практ. пособие / Уральский юридический ин-т МВД России - Екатеринбург : Издательство Уральского юридического ин-та МВД России, 2000. - 147с. - Библиогр.: с. 138-146.

    Пособие содержит теоретические и практические сведения о преступлениях в сфере компьютерной информации, проблемах информационных нападений, а также методах и средствах защиты информации, среди которых и криптографическое преобразование информации.
    Шифр зберігання книги в НБУВ: **ВА621132**

59. Нечаев Василий Ильич. **Элементы криптографии. Основы теории защиты информации** : Учеб. пособие для студ. ун-тов, пед. вузов и вузов с углубленным изуч. математики. - М. : Высшая школа, 1999. - 110с. : ил. - (Высшая математика). - ISBN 5-06-003644-8.

    Книга является первым учебным пособием по теории защиты информации, фундаментом которой является прикладная теория чисел. Рассматриваются современные методы шифрования по открытому ключу и электронная подпись. Также содержится интересный исторический очерк развития криптографии.
    Шифр зберігання книги в НБУВ: **ВА593777**

60. Новиков Валерий Евгеньевич, Ридель Валерий Вольдемарович. **Введение в криптологию** : Учеб. пособие для студ., специализирующихся в обл. защиты информации / Саратовский гос. ун-т им. Н.Г.Чернышевского. - Саратов :

Издательство Саратовского ун-та, 2000. - 104с. : рис. - Библиогр.: с. 103. - ISBN 5-292-02503-8.

Раскрывается место криптографических методов в общей системе защиты информации, содержатся примеры наиболее известных методов шифрования, излагаются основные вопросы теоретической криптографии, а также некоторые идеи по реализации криптографических систем и организации общей системы защиты информации.

Шифр зберігання книги в НБУВ: **ВА631826**

61. Нысанбаев Рустэм Камильевич. **Разработка нетрадиционных методов и средств криптографической защиты информации** : Автореф. дис... канд. техн. наук: 05.13.06 . - Алматы, 2000. - 25с.

    В роботе решаются задачи исследования современных криптографических методов и алгоритмов защиты информации, разработки криптографического метода и алгоритма на основе арифметики непозиционной системы счисления с полиномиальными основаниями, разработки нетрадиционного криптографического метода и алгоритма , базирующегося на использовании непозиционной мультипликативной композиции векторов и их представлении в виде интерполяционных многочленов Лагранжа, создания программных средств шифрования и дешифрования информации с обнаружением ошибок.

    Шифр зберігання книги в НБУВ: **РА310009**

62. Пономарьов Аскольд Анатолійович. **Математичні методи і технічні засоби захисту інформації зовнішніх запам'ятовуючих пристроїв**: Автореф. дис... канд. фіз.-мат. наук : 01.05.03 / НАН України; Інститут кібернетики ім. В.М.Глушкова - К., 1997. - 17с.

    Метою роботи є розробка криптографічно якісних алгоритмів вироблення псевдовипадкових чисел (ПВЧ), розробка програмних і апаратних засобів потокового шифрування інформації зовнішніх запам"ятовуючих пристроїв (ЗЗП), створення методів побудови високоефективних кодів з обмеженими довжинами серій та ін.

    Шифр зберігання книги в НБУВ: **РА296421**

63. **Поточные шифры** / А.В. Асосков, М.А. Иванов, А.А. Мирский и др.- М.: КУДИЦ-ОБРАЗ, 2003. - 336 с. - (СКБ - специалисту по компьютерной безопасности).

    Рассматриваются основы криптографии с секретным ключом, дается классификация симметричных шифров, проводится сравнительный анализ блочных и поточных шифров, описываются строительные блоки, использующиеся при создании современных поточных шифров и хеш-генераторов. Дается обзор современных синхронных поточных шифров, современных самосинхронизирующихся шифров. Описывается новое направление - стохастические поточные криптоалгоритмы , основанные на использовании стохастических сумматоров (R-блоков).

    Шифр зберігання книги в НБУВ: **ВА644908**

64. **Практическая криптография [Электронный ресурс]: Демо-версии программ. Документация**. - СПб. : БХВ-Петербург, 2003. - 1 электрон. опт. диск (CDR) - (Мастер решений). - Приложение к книге ВА643552.

    Шифр зберігання книги в НБУВ: **CDR206/ВА643552**

65. Рамзі Анвар Саліба Сунна. **Високопродуктивна реалізація протоколів захисту інформації на базі операцій модулярної арифметики** : Автореф. дис... канд. техн. наук: 05.13.13 / Національний технічний ун-т України "Київський політехнічний ін-т". - К., 2006. - 19с.

    Виконано теоретичне обґрунтування і одержано нове вирішення наукової задачі підвищення продуктивності реалізації протоколів захисту інформації в комп'ютерних мережах, обчислювальною основою яких є мультиплікативні операції модулярної арифметики.
    Шифр зберігання книги в НБУВ: **РА346262**

66. **Розробка підходу і застосування апарату булевих функцій для аналізу і синтезу ефективних криптографічних алгоритмів захисту інформації** : Автореф. дис... канд. техн. наук: 05.13.13 / Бардіс Ніколас; Нац. Техн. Ун-т України "Київ. політехн. ін-т". - К., 1998. - 16 с. - укр.

    Дисертацію присвячено розробці підходу до аналізу рівня захищеності та синтезу алгоритмів криптографічного захисту інформації на основі використання апарату булевих функцій. Показано тотожність проблем розкриття криптографічних алгоритмів та розв'язання системи булевих рівнянь, які визначаються булевими функціями бітових перетворень, що реалізуються алгоритмом. Встановлено критерії оцінки складності розв'язання систем булевих рівнянь, та засоби їх практичного визначення. Запропоновано методи синтезу булевих функцій, які забезпечують високий рівень криптостійкості алгоритмів, побудованих на їх основі. З використанням запропонованого підходу проведено дослідження криптостійкості найпоширеніших алгоритмів захисту інформації.
    Шифр зберігання книги в НБУВ: **РА306340**

67. Расторгуев Сергей Павлович. **Программные методы защиты информации** : Учеб. пособие / Пензенский гос. ун-т. - Пенза : Издательство Пензенского гос. ун-та, 2000. - 95с. : рис. - Библиогр.: 93-94.

    Пособие посвящено организации компьютерной безопасности программными методами. Представлены математические модели, на базе которых можно осуществлять расчеты надежности защитных механизмов. Изложены принципы построения программной системы защиты и принципы зашиты данных на основе экспертных и самообучающихся систем, некоторые методы защиты от несанкционированного доступа.
    Шифр зберігання книги в НБУВ: **ВА613068**

68. Рублинецкий В. И. **Введение в компьютерную криптологию** / Харьковский гуманитарный ин-т "Народная украинская академия". - Х. : ОКО, 1997. - 125с. - ISBN 966-526-039-1.

    Популярно описується , як зашифровують інформацію , що передається від комп"ютера до комп"ютера, а також способи дешифрації. Бажано, щоб читач вмів програмувати на Паскалі.
    Шифр зберігання книги в НБУВ: **ВА581592**

69. Салех Ібрагім Ахмад Аль-Омар. **Розробка засобів застосування булевих функцій спеціальних класів для підвищення ефективності хеш-адресації, контролю та захисту інформації** : Автореф. дис... канд. техн. наук: 05.13.13 / Національний технічний ун-т України "Київський політехнічний ін-т". - К., 2004. - 20с.

Метою роботи є підвищення ефективності хеш-адресації , алгоритмів захисту інформації та надійності виявлення помилок в комп'ютерних системах за рахунок організації процесів обробки даних з застосуванням булевих функціональних перетворень, що мають максимальне значення повної і диференційної ентропії, а також розробки методів синтезу таких перетворень, способів та засобів їх реалізації.
Шифр зберігання книги в НБУВ: **РА329042**

70. Свинарьов Андрій Володимирович. **Методи та засоби комбінованих несиметричних криптографічних перетворень інформації із зменшеною обчислювальною складністю** : Автореф. дис... канд. техн. наук: 05.13.06 / Харківський держ. технічний ун-т радіоелектроніки. - Х., 1998. - 17 с.

    Метою роботи є дослідження та розробка комбінованих алгоритмів шифрування та автентифікації інформації, розробка програмних та програмно-апаратних засобів захисту інформації для моделі взаємної недовіри і взаємного захисту, які реалізують функції цілісності, справжності, конфіденційності, причетності, управління доступом з мінімальною обчислювальною складністю і потрібною криптостійкістю.
    Шифр зберігання книги в НБУВ: **РА301838**

71. Смарт Н. **Криптография** / С.А. Кулешова (пер.с англ.). - М. : Техносфера, 2006. - 519с. - (Мир программирования; 8-05). - Библиогр.: в конце ст.. - ISBN 1-5-94836-043-1. - ISBN 0077099877 (англ.).

    Чрезвычайно подробно изложены симметричные шифры, криптосистемы с открытым ключом, стандарты цифровых подписей, отражение атак на криптосистемы. Даны примеры на языке Java, многочисленные оригинальные задачи, отражающие новейшее развитие теории и практики криптографии.
    Шифр зберігання книги в НБУВ: **ВС43083**

72. **Современные методы криптографической защиты информации: (обзор по материалам открытой печати)** / Г.Г. Грездов. - К., 2002. - 31 с.: рис. - (Препр. / 2002; 01). - Библиогр.: с. 28-30. - рус.

    С использованием положений правовых актов относительно ответственности пользователя за правонарушения с конфиденциальной информацией, компьютерами и компьютерной информацией в развитых странах рассмотрено современное состояние и перспективы развития методов криптографической защиты информации, проанализированы этапы их развития, предложена классификация данных методов. Рассмотрены особенности хеш-функций, криптографические систем с секретными и открытыми ключами, их параметры алгоритмов. Определены требования, предъявляемые к криптографическим системам.
    Шифр зберігання книги в НБУВ: **Р93788**

73. Столлингс Вильям. **Криптография и защита сетей. Принципы и практика** / А.Г. Сивак (пер.с англ.), А.А. Шпак (пер.с англ.). - 2-е изд. - М. ; СПб. ; К. : Издательский дом "Вильямс", 2001. - 669с. : рис. - ISBN 5-8459-0185-5 (рус.). - ISBN 0-13-869017-0 (англ.).

    Обзор основ криптографии и практики ее использования для защиты сетей. Включены вопросы безопасности на системном уровне, в частности принципы разработки блочных шифров, алгоритмов шифрования с использованием открытых ключей, описание основных средств сетевой защиты и защиты данных в Internet, вопросы защиты от вирусов и несанкционированного доступа к данным, защиты от

сетевых атак, использования брандмауэров и высоконадежных систем. Книга удостоена награды TEXTY как лучшая из книг по компьютерным наукам и программированию в 1999 году.
Шифр зберігання книги в НБУВ: **ВС42266**

74. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. - Л.: БаК, 2003. - 144 с. - (Захист інформації в комп'ют. та телекомунікац. мережах). - Бібліогр.: 14 назв. - укр.

Висвітлено основні теоретичні положення сучасної криптографії, описано симетричні шифрувальні алгоритми. Розкрито засади асиметричних шифрувальних алгоритмів, розглянуто питання генерування псевдовипадкових послідовностей та використання хешувальних функцій, побудови цифрових підписів на підставі асиметричних алгоритмів, адміністрування ключами, зламування криптосистем.
Шифр зберігання книги в НБУВ: **ВА653345**

75. Теория и техника передачи, приема и обработки информации : Сб. науч. тр. по материалам 7-й Междунар. конф., 1 - 4 окт. 2001 г. / Харьк. гос. техн. ун-т радиоэлектрон. - Х., 2001. - 483 с.: рис. - рус.

Освещены вопросы телекоммуникационных сетей и систем, устройств радиотехники и средств телекоммуникаций, информационно-аналитических систем поддержки принятия решений, перспективного развития вакуумных приборов СВЧ. Рассмотрены проблемы реализации безусловно стойких криптографических систем. Раскрыта сущность политики безопасности информации в электронных платежных системах, приведены комплексные измерения параметров тонких неферромагнитных пленок. Проанализировано влияние внешнего стационарного электрического поля на энергетические состояния частиц и квазичастиц в полупроводниковых наноструктурах. Описан процесс разработки алгоритма аппаратно-ориентированного преобразования изображений.
Шифр зберігання книги в НБУВ: **ВА619875**

76. Томашевський Олег Михайлович. **Методи та алгоритми системи захисту інформації на основі нейромережевих технологій**: Автореф. дис. канд... техн. наук: 05.13.23 / НАН України; Державний НДІ інформаційної інфраструктури. - Львів, 2002. - 20с. : рис.

Метою роботи є розробка математичних моделей, методів та алгоритмів для підвищення рівня захищеності інформаційних характеристик при передачі і обробці даних в інформаційних системах на основі нейромережевих технологій.
Шифр зберігання книги в НБУВ: **РА321747**

77. Третя міжнародна алгебрична конференція в Україні, Суми, 2 - 8 лип. 2001 р. / Ред.: Ю.А. Дрозд; Укр. мат. Конгрес, Ін-т математики НАН України. - Суми: СумДПУ ім. А.С.Макаренка, 2001. - 292 с. - Текст. укр., рос. та англ. мовами. - укр.

Рассмотрена избыточная числовая система в кольце Z[i], ее применение в криптографии. Освещены вопросы конгруэнции на групповых системах Менгера. Представлен материал о мультифакторизуемых конечных разрешимых группах, новых классах формаций и классах Фиттинга, а также разрешимо насыщенных произведениях формаций конечных групп. Приведены критерии сверхразрешимости и нильпотентности конечных групп, а также идемпотенты факторстепеней IS (N) і S(N), инварианты изотопии конечных квазигрупп.

Рассмотрена система компьютерной алгебры GAP. Изучены вопросы о подгруппах Шмидта ранга 2 в конечных группах, разрешимых группах ограниченного порядка, контроле частичных графов с использованием определяющих соотношений. Исследованы конечные рі-разрешимые группы с формационными подгруппами примарного индекса.
Шифр зберігання книги в НБУВ: **ВС35219**

78. Усенко Владислав Костянтинович. **Застосування двомодових когерентно-корельованих променів в квантовій криптографії** : Автореф. дис... канд. фіз.-мат. наук: 01.04.02 / НАН України; Інститут теоретичної фізики ім. М.М.Боголюбова - К., 2006. - 18с.

    Метою роботи є розробка теорії побудови квантово-криптографічних каналів на основі випромінення та їх криптографічне застосування. Результати можуть бути використані для побудови принципово нових високоефективних багатофотонних квантово-криптографічних каналів.
    Шифр зберігання книги в НБУВ: **РА344282**

79. Управління ключовою інформацією в системах захисту групових комунікацій : Автореф. дис... канд. фіз.-мат. наук: 01.05.03 / Д.О. Лук'янов; Київ. нац. ун-т ім. Т.Г.Шевченка. - К., 2004. - 16 с. - укр.

Розроблено та обгрунтовано ефективні методи криптографічного захисту інформації динамічної багаточисленної групової комунікації, що має просторово розподілену структуру. На підставі результатів аналізу досліджень захисту інформації групової комунікації, сформульовано концептуальний підхід щодо керування ключовою інформацією, для реалізації якого розроблено нові та модифіковано існуючі схеми та алгоритми, створено відповідне програмне забезпечення. Запропоновано проект комплексу практичних засобів криптографічного захисту інформації розподіленого багаточисленного групового утворення (установи) з високим рівнем оптимізації та автоматизації управлінських процесів.
Шифр зберігання книги в НБУВ: **РА330674**

80. Фергюсон Нильс, Шнайер Брюс. **Практическая криптография** / Н.Н. Селина (пер.с англ.). - М.; СПб.; К. : Диалектика, 2005. - 421с. - Библиогр.: с. 410-417. - ISBN 5-8459-0733-0 (рус.). - ISBN 0-4712-2357-3 (англ.).

    Книга представляет собой уникальное в своем роде руководство по практической разработке криптографической системы, устраняя тем самым досадный пробел между теоретическими основами криптографии и реальными криптографическими приложениями.
    Шифр зберігання книги в НБУВ: **ВА673989**

81. Фильштинский Вадим Аншелович, Фильштинский Леонид Аншелович, Фильштинский Станислав Вадимович. **Введение в алгебру (с приложением к криптографии)** : Учеб. пособие для студ. и асп. по спец. 08.02.02- прикладная математика / Институт содержания и методов обучения {Сумы}; Сумский гос. ун-т. - Суми : ИПП "Мрія-1" ЛТД, 1999. - 206с. - ISBN 966-566-111-6.

    Викладені традиційні теми загальної алгебри: групи, кільця, поля та їх найпростіші властивості, початкові відомості про поля Галуа та кільця багаточленів. Наведено найпростіші додатки до криптографії. Сформульовано достатньо багато задач, які можна використовувати для проведення практичних занять.
    Шифр зберігання книги в НБУВ: **ВА592549**

82. Харин Юрий Семенович, Берник Василий Иванович, Матвеев Геннадий Васильевич, Агиевич Сергей Валерьевич. **Математические и компьютерные основы криптологии** : Учеб. пособие для студ. мат. и инж.-техн. спец. вузов - Минск : ООО "Новое знание", 2003. - 382с. : рис. - Библиогр.: с. 371-378. - ISBN 9 8 5 - 4 7 5 - 0 1 6 - 7 .
Шифр зберігання книги в НБУВ: **ВС38607**

83. Хорев Павел Борисович. **Методы и средства защиты информации в компьютерных системах** : Учеб. пособие для студ. вузов, обучающихся по направлению 230100 (654600) "Информатика и вычислительная техника". - М. : Издательский центр "Академия", 2005. - 255с. : рис., табл. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 5-7695-1839-1.
Шифр зберігання книги в НБУВ: **ВА680312**

84. Чижухин Геннадий Николаевич. **Основы защиты информации в вычислительных системах с сетях ЭВМ** : Учеб. пособие для студ. спец. 220100 - Вычислительные машины, комплексы и сети / Пензенский гос. ун-т. - Пенза : Издательство Пензенского гос. ун-та, 2001. - 164 с. : ил.

    Изложены как основные положения теории защиты информации, так и современные методы и средства защиты информации в вычислительных системах, локальных и корпоративных сетях Internet, в том числе и защиты от удаленных атак через сеть Internet. Отдельно рассмотрены основы построения криптографических средств защиты и вопросы безопасности электронных платежных систем.
    Шифр зберігання книги в НБУВ: **ВА617775**

85. Шаньгин Владимир Федорович, Тимофеев Петр Александрович. **Защита информации и информационная безопасность** : Учеб. пособие / Московский гос. ин-т электронной техники (Технический ун-т). - М. : МИЭТ, 2000. - Библиогр.: с. 1 2 8 - 1 2 9 .
    Ч. 2 : Асимметричные криптосистемы. Идентификация, аутентификация, цифровая подпись и управление ключами. - 132с. : рис. - ISBN 5-7256-0243-5.

    Рассмотрены асимметричные криптосистемы с открытыми ключами , алгоритмы и процедуры идентификации, аутентификации и электронной цифровой подписи , а также методы и средства управления криптографическими ключами. Описаны методы и средства защиты информации в современных электронных платежных системах.
    Шифр зберігання книги в НБУВ: **В346282**

86. Широчин Валерий Павлович, Мухин Вадим Евгеньевич, Кулик Анатолий Владимирович. **Вопросы проектирования средств защиты информации в компьютерных системах и сетях** . - К. : ВЕК+, 2000. - 112с. - (Компьютерная инженерия). - ISBN 966-7140-13-X.

    Рассмотрены основные проблемы защиты информации в компьютерных системах и сетях, а также вопросы проектирования современных средств защиты информации от несанкционированного доступа к информации. Приведены примеры программирования выбранных функций идентификации и аутентификации пользователей, а также криптографической защиты информации по курсу "Основы защиты информации".
    Шифр зберігання книги в НБУВ: **ВА598195**

87. Щербаков Андрей Юрьевич, Подуфалов Николай Дмитриевич. **Методы программирования криптографических алгоритмов. Особенности программной реализации** : Учеб. пособие / Московский гос. инженерно-физический ин-т (технический ун-т). - М. : Издательство МИФИ, 2000. - 201с. - ISBN 5-7262-0329-1.

    Рассмотрены основные прблемы компьютерной безопасности, связанные с реализацией криптографических механизмов в компьютерных системах (КС). Рассмотрены методы защиты конфиденциальности информации в КС (шифрование), методы поддержания целостности (имитовставка, электронная цифровая подпись - ЭЦП), методы реализации ключевой системы для шифрования и ЭЦП и методы использования реализованных в КС криптографических механизмов (криптографические интерфейсы).

    Шифр зберігання книги в НБУВ: **ВА616417**

88. Яремчук Юрій Євгенович. **Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей** . - Вінниця : Книга-Вега, 2002. - 135с. : рис. - Бібліогр.: с.128-135.. - ISBN 966-621-117-3.

    Запропонований новий клас рекурентних послідовностей, під час обчислення елементів яких використовуються рекурентні співвідношення з коефіцієнтами, що пов"язані з початковими елементами послідовностей. Розроблені пакет програм та структури спеціалізованих процесорів для шифрування інформації за модифікованими методами.

    Шифр зберігання книги в НБУВ: **ВА634716**