«Розробка та впровадження новітніх технологій стиску та захисту сигналів і зображень в радіоелектронних системах і комплексах»

Основні наукові результати

– методи стиснення даних із застосуванням ортогональних розкладень дискретних сигналів та на їх основі запропоновані алгоритми та структурні схеми пристроїв, що реалізують методи стиснення даних у різних системах базисних функцій;

– методи та алгоритми стиснення мовних сигналів, що базуються на використанні сучасного математичного апарату вейвлет-перетворення;

– алгоритмічне та програмне забезпечення криптографічного захисту інформації в корпоративних комп'ютерних мережах на основі оригінальних методів симетричної блокової та потокової криптографії.

Запропоновані в проекті методи стиснення даних та криптографічного захисту інформації є новими фундаментальними дослідженнями. Їх реалізація в алгоритмах та структурних схемах радіоелектронних системах і комплексах відповідає світовому рівню в галузі сучасних методів та засобів обробки сигналів та зображень.

Практична цінність

Впровадження результатів виконання роботи надає можливість позбутися використання закордонних технологій стиснення та криптографічного захисту інформації і тим самим отримати значну перевагу при обґрунтуванні захищеності конфіденційної інформації з обмеженим доступом у вітчизняних комп'ютерних мережах.

Перелік основних наукових публікацій, доповідей на конференціях, семінарах

Монографіі:

1. Білецький А.Я., Білецький О.А., Білецький Є.А. «Преобразования Грея». – К.: Изд-во НАУ, 2007. – Том 1 «Основы теории». – 440 с.
2. Білецький А.Я., Білецький О.А., Білецький Є.А. «Преобразования Грея». – К.: Изд-во НАУ, 2007. – Том 2 «Прикладные аспекты». – 612 с.
3. Белецкий А.Я., Белецкий Е.А. Квазиэквидистантные коды. – К.: Вид-во «НАУ-друк», 2008. – 460 с.

Отримано 10 патентів України щодо способу криптографічного захисту інформації у комп'ютерних мережах.

1. Патент на корисну модель № 20653 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 15 лютого 2007 р., Бюл. № 2. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., ЮкальчукА.А.
2. Патент на корисну модель № 20654 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 15 лютого 2007 р., Бюл. № 2. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., ЮкальчукА.А.
3. Патент на корисну модель № 22215. Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 25 квітня 2007 р., Бюл. № 5. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Московченко І.В.
4. Патент на корисну модель № 27582 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 12 листопада 2007 р., Бюл. № 18. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Сергієнко Р.В.
5. Патент на корисну модель № 27583 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 12 листопада 2007 р., Бюл. № 18. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Сергієнко Р.В.
6. Патент на корисну модель № 27584 «Спосіб криптографічного перетворення інфор-

мації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 12 листопада 2007 р., Бюл. № 18. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Сергієнко Р.В.

7. Патент на корисну модель № 29663 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.01.2008, Бюл. №2. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Сергієнко Р.В.

8. Патент на корисну модель № 29664 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.01.2008, Бюл. №2. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Сергієнко Р.В.

9. Патент на корисну модель № 30503 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.02.2008, Бюл. №4. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Московченко І.В.

10. Патент на корисну модель № 30504 «Спосіб криптографічного перетворення інформації» видано відповідно до Закону України «Про охорону прав на винаходи і корисні моделі». Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.02.2008, Бюл. №4. Автори Білецький А.Я., Білецький О.А., Кузнецов О.О., Московченко І.В.

Публікації в наукових виданнях:

1. Белецкий А.Я., Корчинский А.П. Алгоритмы построения деревьев разбиений и синтез двоичных счетчиков Грея // Електроніка та системи управління, №1(11), 2007. – С. 17 – 29.
2. Белецкий А.Я., Белецкий А.А., Кузнецов А.А. Семейство симметричных блочных RSB криптографических алгоритмов с динамически управляемыми параметрами шифрования // Електроніка та системи управління, № 1(11), 2007. – С. 5 – 16.
3. Белецкий А.Я., Белецкий А.А., Кузнецов А.А. Семейство Уолша генераторов поточного блочно-сбалансированного шифрования // Захист інформації, № 2(33), 2007. – С. 42–55.
4. Бойко І.Ф., Мурка І.М. Генератор реалізацій ортогональних лінійних стохастичних послідовностей на базі функцій Уолта // Електроніка та системи управління. – К.: НАУ, 2007, № 2(12). – С. 5–10.
5. Белецкий А.Я. Преобразования Грея в полях Галуа по модулю неприводимого многочлена // Вісник Сумського державного університету. – Суми: Вид-во СумДУ, 2007. – С. 113–120.
6. Бойко І.Ф. Безмежно подільні випадкові процеси як моделі випадкових сигналів і завад в системах обробки інформації // Матеріали VIII Міжнародної науково-технічної конференції „АВІА-2007” (25 – 27 квітня), том 2. – С. 22.182 – 22.185.
7. Миронов Н.А. О размерности импульсной переходной характеристики // Електроніка та системи управління, № 2(12), 2007. – С. 47–50.
8. Белецкий А.Я., Белецкий А.А. RSB блочный криптографический алгоритм // Искусственный интеллект. – 2008. – № 3. – С. 132-136.
9. Бойко І.Ф. Стохастичні ортогональні розкладення в теорії нелінійних систем // Електроніка та системи управління, № 1 (15), 2008. - С. 5 – 11.
10. Бойко І.Ф., Мурка І.М. Принципи застосування стохастичних ортогональних розкладань для аналізу та синтезу нелінійних систем // Електроніка та системи управління, № 2 (16), 2008. - С. 9 – 16.
11. Бойко І.Ф. Ортогональні скалярні стохастичні двовимірні лінійні поля // Електроніка та системи управління, № 3 (17), 2008. - С. 8 – 16.
12. Белецкий А.Я., Белецкий А.А. Блочный криптоалгоритм с динамическим управлением параметрами шифрования // Системи обробки інформації. – 2009. –Вип. 7(79). – С. 125-126.
13. Белецкий А.Я., Белецкий А.А. Синхронный алгоритм поточного шифрования цифровой информации // Системи обробки інформації. – 2009. –Вип. 7(79). – С. 127-128.
14. Белецкий А.Я. Симметричный блочный RSB-32 криптографический алгоритм // Ме-

тоди та засоби кодування, захисту й ущільнення інформації: Друга МНПК. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – С. 64-65.

15. Белецкий А.Я. Поточный SPB криптографический алгоритм защиты цифровой информации // Методи та засоби кодування, захисту й ущільнення інформації: Друга МНПК. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – С. 66-67.

16. Білецький А.Я., Стеценко Д.А., Ткаченко П.Л., Бабич В.В. Система розповсюдження ключів шифрування // Захист в інфрмаційно-комунікаційних системах: НПК.- К.: НАУ. – 2009. – С. 39-40.

17. Белецкий А.Я., Белецкий Е.А. Преобразования Грея. Основы теории и приложения // Обробка сигналів негауссівських процесів: II МНПК. – Черкаси: ЧДТУ. – 2009. – С. 38-40.

18. Бойко И.Ф., Турчак В.В. Идентификация систем // Електроніка та системи управління, № 1 (19), 2009. – С. 11-19.

19. Миронов Н.А. Тестирование цифровых 1/n-октавных анализаторов сигналов // Електроніка та системи управління, № 1 (19), 2009. – С. 53-59.

20. Бойко И.Ф., Турчак В.В. Приближение функциональных зависимостей и проблема многомерной аппроксимации // Електроніка та системи управління, № 3 (21), 2009. – С. 5-11.

21. Белецкий А.Я. Симметричный блочный RSB криптоалгоритм / Матеріали IX МНТК «АВІА-2009». Том 2. К.: НАУ, 2009. – С. 11.35-11.38.

22. Белецкий А.Я. Поточный SPB криптоалгоритм / Матеріали IX МНТК «АВІА-2009». Том 2. К.: НАУ, 2009. – С. 11.39-11.40.

23. Белецкий А.А. Гибкое управление базовыми раундовыми ключами в симметричном блочном RSB криптоалгоритме / Матеріали IX МНТК «АВІА-2009». Том 2. К.: НАУ, 2009. – С. 11.41-11.44.

24. Белецкий Е.А. Обобщенные преобразования Грея в системы функций Уолша / Матеріали IX МНТК «АВІА-2009». Том 2. К.: НАУ, 2009. – С. 11.45-11.48.

25. Бойко І.Ф. Стохасичні ортогональні розкладання випадкових сингалів та полів / Матеріали IX МНТК «АВІА-2009». Том 2. К.: НАУ, 2009. – С. 11.56-11.59.

26. Миронов Н.А. Модификация преобразования Фурье / Матеріали IX МНТК «АВІА-2009». Том 2. К.: НАУ, 2009. – С. 10.62-10.65.