«Розроблення та впровадження програмних засобів захисту інформації від несанкціонованого доступу в електронних системах документообігу у вищих навчальних закладах України»

Основні наукові результати

- створена нова теорія симетричного блокового криптографічного захисту інформації з обмеженим доступом в комп'ютерних мережах з параметрами шифрування, що динамічно керуються. Відмінна риса теорії симетричного блокового шифрування (СБШ) даних, що пропонується, полягає у наступному. В розробленому алгоритмі СБШ, позначеному як RSB-32, використано оригінальний примітив «ковзного кодування», якій забезпечує криптографічні властивості шифратору, що перевищують кращі світові показники. Завдяки використанню позначеного примітиву асимптотичне «відбілювання» вхідного відкритого тексту відбувається за два раунди шифрування, коли в той же час відомий американський шифратор AES, якій вважається стандартом XXI-го сторіччя, забезпечує відповідне відбілювання за чотири раунди шифрування;

- запропоновано новий матричний метод передавання таємних ключів шифрування по відкритих каналах зв'язку. Позначений метод заснований на використанні сучасних розділів алгебраїчної теорії незвідних і примітивних поліномів, а також розширених полів Галуа. В порівнянні з відомими матричними методами передавання ключів шифрування метод, що пропонується, забезпечує значне підвищення криптостійкості алгоритму;

- розроблені нові технології криптографічного захисту інформації та оцінки криптографічної стійкості алгоритмів шифрування, на які отримані чотири Свідоцтва Державного департаменту інтелектуальної власності МОНУ (наведені у списку публікацій);

- створено апаратно-програмний комплекс криптографічного захисту інформації, до складу якого надходять комп'ютер, інтерфейс зв'язку з комп'ютерною мережею, безпосередньо комп'ютерна мережа НАУ та пакети прикладних програм;

- при виконанні НДР були використані 14 патентів України, авторами яких є виконавці роботи;

- створені узагальнені математичні моделі основних примітивів криптографічного захисту інформації (КЗІ) в системах ЕДО;

- розроблено алгоритмічне й програмне забезпечення КЗІ та генерування і розподілу секретних ключів шифрування даних між легалізованими абонентами комп'ютерних мереж по відкритим каналам зв'язку;

- проведено експериментальне дослідження пакетів прикладних програм щодо забезпечення КЗІ та генерування й розподілу ключів шифрування даних в системах ЕДО на базі локальної комп'ютерної мережі НАУ;

- розроблені рекомендації зі створення програмних засобів криптографічного захисту інформації в системах ЕДО в комп'ютерних мережах ВНЗ України;

- наукова новизна алгоритмів та програмних засобів КЗІ, що використані в проекті, підтверджена багатьма патентами України, які отримані виконавцями НДДКР у попередні роки безпосередньо до початку роботи над проектом. Свідченням цього є також те, що розроблений у проекті RSB-32 алгоритм КЗІ забезпечує більш високі показники з криптостійкості у порівнянні з кращими світовими зразками;

- практична значимість отриманих результатах полягає в тому, що використання виконаних розробок надає можливість позбутися зарубіжних засобів КЗІ, які ще досі застосовуються в системах ЕДО України. Позитивним наслідком такого переходу до вітчизняного продукту може бути не лише економія коштів на придбання закордонних засобів КЗІ, але й підвищення Національної безпеки держави в цілому.

Практична цінність

Значимість проекту для розв'язання економічних проблем полягає у наступному. Як відомо, Україна досі ще немає національних стандартів симетричних алгоритмів криптографічного захисту інформації. Тому різні організації використовують, як правило, системи шифрування, що розроблені за кордоном (в основному – це російська система ГОСТ 28147-89, яка вже

застаріла і не відповідає сучаснім вимогам щодо швидкодії тощо). До цього слід додати, що використання закордонних криптосистем пов'язано зі значними фінансовими витратами. Тому розробка власних систем криптографічного захисту інформації має не лише позбавити державу від зайвих матеріальних витрат, а й відповідає основним положенням національної безпеки України в інформаційній сфері.

Перелік основних наукових публікацій, доповідей на конференціях, семінарах

1. Белецкий А.Я., Стеценко Д.А. Порядок абелевых циклических групп, порождаемых обобщенными преобразованиями Грея // Електроніка та системи управління. - №1(23), 2010. - С.5-11.
2. Белецкий А.Я., Ткаченко П.Л. Неформальный синтез кодов Хэмминга // Електроніка та системи управління. - №1(23), 2010. – С.12-19.
3. Белецкий А.Я., Аксентий Е.А. Программній комплекс для исследования криптографических примитивов типа перестановки єлементов шифруемого блока // Сучасний захист ірформації. НТ журнал. К: Держ. у-т ІКТ, вип. 1, 2010. – С. 43-53.
4. Белецкий А.Я., Аксентий Е.А. Программный комплекс для исследования статистических характеристик криптографических примитивов типа нелинейной подстановки // Сучасний захист інформації. НТ журнал. К: Держ. у-т ІКТ, вип. 2, 2010. – С. 30-41.
5. Белецкий А.Я. Матричный алгоритм Диффи-Хэллмана // Системи обробки інформації. – 2010. – Вип. 8. – С. 87-90.
6. Белецкий А.Я. Матричные циклические группы, порождаемые составными кодами Грея // Матеріали МК Теорія та прикладні аспекти побудови програмних систем – TAAPSD-2010 – К.: Нац.у-т Т.Г Шевченко. - С. 67-75.
7. Белецкий А.Я., Белецкий Е.А. Модифицированный Пэли-алгоритм синтеза симметрических нормализованных матриц Адамара // Вісник СумДУ, серія Технічні науки, № 1, 2010. С. 51-56.
8. Белецкий А.Я., Белецкий А.А., Стеценко Д.А. Модифицированный матричный ассиметричный криптографический алгоритм Диффи-Хэллмана // Искусственный интеллект, № 3, 2010. - С. 697-705.
9. Демьяник Д.С. Программная реализация быстрых преобразований Фурье в базисе Виленкина-Крестенсона функций // Електроніка та системи управління.-№1(23), 2010.–С.20-25.
10. Белецкий А.Я. Матричные циклические группы максимального порядка, порождаемые обобщенными преобразованиями Грея / Белецкий А.Я. // Сучасний захист інформації. – К.: ДУІКТ. – 2011. – № 1. – С. 65-71.
11. Белецкий А.Я. Дифференциальные характеристики мини версий симметричного RSB шифратора / Белецкий А.Я., Белецкий А.А., Аксентий Е.А. // Сучасний захист інформації. – К.: ДУІКТ. – 2011. – № 2. – С. 71-81.
12. Белецкий А.Я. Матричные алгоритмы криптографической защиты информации и обмена ключами шифрования / Белецкий А.Я., Белецкий А.А., Стеценко Д.А. // Інформаційни технології в освіті: Збірник наукових праць, Вип. 1. – Херсон: ХДУ, 2011. – С. 65-76.
13. Білецький А.Я. Асимптотичні оцінки логарифмічної щільності розрядних полів систем числення із двійковим алфавітом / Білецький А.Я. // Наукоємні технології. – К.: НАУ. – 2011. – № 1. – С. 47-52.
14. Белецкий А.Я. Матричные циклические группы максимального порядка, порождаемые обобщенными преобразованиями Грея / Белецкий А.Я. // Journal of Qafqaz University. An Internetional Journal. – Баку. Университет Кавказа. – 2011. – № 1. – С. 37-46.
15. Белецкий А.Я. Оценка дисперсии гармоник спектра односвязного марковского гауссовского процесса в дискретных базисах Виленкина-Крестенсона функций / Белецкий А.Я., Демьяник Д.С. // Системи обробки інформації. – Х. ХУПС. – 2011. - № 3. – С. 107-111.
16. Белецкий А.Я. Синтез обобщеных примитивных полиномов / Белецкий А.Я. // Вісник СумДУ. – Суми. – 2011. - № 4. С. – 56-63.
17. Белецкий А.Я. Обобщенные примитивные полиномы / Белецкий А.Я. // Актульные проблемы современной математики, механики и информатики. – Х. ХНПУ. – 2011. – С. 93-101.

Свідоцтва Департаменту Інтелектуальна власність на програмні продукти

1. Білецький А.Я. Синтез невироджених двійкових матриць, які утворюють циклічні групи максимального порядку (комп'ютерна програма) / Білецький А.Я., Стеценко Д.А. // Свідоцтво про реєстрацію авторського права на твір. № 38773 від 23.06.2011. – К.: МОНУ, Державний департамент інтелектуальної власності.
2. Білецький А.Я. Порівняльна оцінка виявлення доплеровських сигналів на фоні гаусівського білого шуму в базисах систем Віленкіна-Крестенсона функцій (комп'ютерна програма) / Білецький А.Я., Дем'яник Д.С. // Свідоцтво про реєстрацію авторського права на твір. № 38774 від 23.06.2011. – К.: МОНУ, Державний департамент інтелектуальної власності.
3. Білецький А.Я. Диференціальний аналіз міні-версій алгоритму шифрування RSB (комп'ютерна програма) / Білецький А.Я., Аксетній Е.О. // Свідоцтво про реєстрацію авторського права на твір. № 38776 від 23.06.2011.–К.: МОНУ, Державний департамент інтелектуальної власності.
4. Білецький А.Я. Криптографічний захист даних на основі RSB алгоритму (комп'ютерна програма) / Білецький А.Я., Аксетній Е.О. // Свідоцтво про реєстрацію авторського права на твір. № 38777 від 23.06.2011. – К.: МОНУ, Державний департамент інтелектуальної власності.
5. Білецький А.Я. Матричні алгоритми шифрування (комп'ютерна програма) / Білецький А.Я., Стеценко Д.А. // Свідоцтво про реєстрацію авторського права на твір. № 38835 від 24.06.2011. – К.: МОНУ, Державний департамент інтелектуальної власності.