Я.П. Кісь *(Національний університет «Львівська політехніка», Україна)*
В.М. Теслюк *(Національний університет «Львівська політехніка», Україна)*

МЕТОДИ І ЗАСОБИ АВТЕНТИФІКАЦІЇ БІОМЕТРИЧНИХ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ*

У статті розглянуто й описано сучасний стан розвитку методів автентифікації біометричних даних в інформаційних системах. Проведено порівняльний аналіз біометричних методів автентифікації даних, доведено надійність їх використання та пріоритетність застосувань цих методів в інформаційних системах.
Ключові слова: *інформаційні системи, інтелектуальні системи прийняття рішень, автентифікація даних, ідентифікація даних, цифровий підпис.*
Табл. 2. Літ. 15.

Я.П. Кись *(Национальный университет «Львовская политехника», Украина)*
В.Н. Теслюк *(Национальный университет «Львовская политехника», Украина)*

МЕТОДИ И СРЕДСТВА АУТЕНТИФИКАЦИИ БИОМЕТРИЧЕСКИХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В статье рассмотрено и описано современное состояние развития методов аутентификации биометрических данных в информационных системах. Проведен сравнительний анализ биометрических методов аутентификации данных, доказана надежность их использования и приоритетность применения этих методов в информационных системах.
Ключевые слова: *информационные системы, интеллектуальные системы принятия решений, аутентификация данных, идентификация данных, цифровая подпись.*

Y.P. Kis *(National University "Lviv Polytechnics", Ukraine)*
V.M. Teslyuk *(National University "Lviv Polytechnics", Ukraine)*

METHODS AND TOOLS FOR BIOMETRIC DATA AUTHENTICATION WITHIN INFORMATION SYSTEMS

The article considers and describes the current stage in the development of authentication methods for biometric data within information systems. The comparative analysis of biometric methods for data authentication is carried out; the reliability of their usage is grounded as well as the priority of application of these methods within information systems.
Keywords: *information systems; intellectual systems of decision-making; data authentication; data identification; digital signature.*

Постановка проблеми. В сучасних умовах проблема автентифікації та ідентифікації біометричних даних є актуальною в обчислювальних мережах, електронних системах управління, електронній комерції і взагалі там, де є необхідність переконатись у справжності отриманого каналами зв'язку або на машинних носіях повідомлення чи документа. Завдання автентифікації можна поділити на такі типи: автентифікація абонента; автентифікація належності абонента до групи; автентифікація документів, що зберігаються на машинних носіях. Безпаперова обробка інформації має низку переваг при обміні документами, наказами, розпорядженнями, листами, постановами з мережею зв'язку або машинними носіями. У таких випадках витрати часу на роздруку-

* статтю підготовлено на основі доповіді на XI-му міжнародному науковому семінарі «Сучасні проблеми інформатики в управлінні, економіці, освіті та екології» (2–7 липня 2012 р., Київ – оз. Світязь).

вання, пересилання, введення отриманого документа з клавіатури суттєво знижуються, прискорюється пошук документів, скорочуються витрати на їх зберігання тощо. Однак при цьому виникає проблема автентифікації автора документа і самого документа, тобто встановлення справжності підпису і відсутності змін в отриманому документі. Ці проблеми у звичайній обробці даних вирішуються за рахунок того, що інформація в документі тісно пов'язана з фізичним носієм, папером, а на машинних носіях такого зв'язку немає.

Аналіз останніх публікацій і досліджень. Дослідженню проблем аутентифікації та ідентифікації біометричних даних, оцінюванню надійності використання алгоритмів і методів захисту інформації значну увагу приділяли такі провідні вітчизняні та зарубіжні науковці, як Л. Адлеман [14], А.І. Березовський [2; 3], Л.Ю. Боков [6], А.М. Боровиков [7], Л.А. Завадська [10], В.К. Задирака [2; 3], Р.Є. Сміт [12], А.М. Фаль [10], Л.Б. Шевчук [2; 3] та інші. Однак у працях цих дослідників недостатньо проаналізовано методи й засоби автентифікації біометричних даних, а також недостатньо уваги приділено їх вибору для конкретної інформаційної системи.

Невирішені проблеми. На даний час невирішеною проблемою є вибір ефективних методів і засобів автентифікації та ідентифікації біометричних даних для конкретних інтелектуальних інформаційних систем.

Мета дослідження: аналіз методів і засобів автентифікації та ідентифікації біометричних даних в інформаційних системах та їх використання для конкретних інтелектуальних інформаційних систем.

Основні результати досліджень. Засоби автентифікації та ідентифікації біометричних даних є важливими компонентами сучасних інтелектуальних інформаційних систем. Вони забезпечують перевірку справжності суб'єкта відповідно до заявленого ним ідентифікатора і дозволяють впевнитись у тому, що суб'єкт є дійсно тим, за кого він себе видає. Розглядаючи випадок обміну секретними документами (військовий або дипломатичний зв'язок), з великим ступенем впевненості можна припустити, що обмін здійснюють гідні довіри сторони. Однак можливо, що обмін перебуває під наглядом і управлінням зловмисника, який здатний виконувати складні обчислення і потім або створювати свої власні документи, або перехоплювати й змінювати документи законного джерела, тоді захищатись потрібно лише від зловмисника. У комерційному світі справедливим є майже зворотнє твердження, тобто передавач і одержувач можуть обманювати один одного навіть більшою мірою, ніж сторонні. У першому випадку схему автентифікації побудувати не важко. Слід забезпечити абонентів надійним шифром і комплектом унікальних ключів для кожного документа, що пересилається. Це забезпечить захист каналу зв'язку. Це завдання висуває суворі вимоги до системи шифрування. Так, метод гамірування у цьому разі не підходить, оскільки зловмисник, аналізуючи відкритий і шифрований текст, отримає гаму і зможе нав'язати будь-який потрібний йому текст. У другому випадку будь-який з абонентів може дезорієнтувати один одного. Аналогічний підхід, що ґрунтується на класичній криптографії, неприйнятний, оскільки існує принципова можливість зловмисних дій однієї зі сторін, що володіють секретним ключем. Наприклад, приймаюча сторона може згенерувати будь-який документ, зашифрувати його на наявному ключі,

спільному для одержувача й передавача, а потім заявити, що він отримав його від законного передавача. Тут слід використовувати схеми, засновані на асиметричній криптографії. У таких випадках у передавача мережі є свій секретний ключ підпису, а в одержувача – несекретний відкритий ключ підпису передавача. Цей відкритий ключ можна розглядати як набір перевірочних співвідношень, що дають змогу перевірити справжність підпису передаючого абонента, але не дозволяють відновити секретний ключ підпису. Передавач несе одноособову відповідальність за свій секретний ключ. Ніхто, крім нього, не в змозі згенерувати коректний підпис. Секретний ключ передавача можна розглядати як особисту печатку і він повинен обмежувати доступ до нього сторонніх осіб. Загальноприйнятою є модель автентифікації, у якій функціонують 4 учасники: передавач, одержувач, зловмисник, арбітр. У цьому випадку передавач посилає повідомлення, одержувач приймає, зловмисник намагається скоїти зловмисні дії, а арбітр приймає рішення у конфліктних випадках, тобто визначає, твердження якої сторони з найбільшою ймовірністю є неприйнятними. Звичайно, у ролі зловмисника можуть виступати передавач і одержувач. Метою автентифікації є захист від можливих видів зловмисних дій, серед яких можуть бути такі: активне перехоплення – зловмисник, що підключився до мережі, перехоплює документи чи файли і змінює їх; маскарад – абонент-зловмисник надсилає документ від імені абонента передавача; ренегатство – абонент-передавач заявляє, що не надсилав повідомлення абоненту отримувачу, хоча насправді надсилав; переробка – абонент отримувач змінює документ і стверджує, що цей змінений документ отримав від абонента передавача; підміна – абонент-отримувач формує новий документ і заявляє, що отримав його від абонента передавача; повтор – абонент-зловмисник повторює раніше переданий документ, який абонент-передавач надіслав абоненту-отримувачу.

Ці види зловмисних дій завдають значної шкоди функціонуванню банківських, комерційних структур, державних підприємств і організацій, приватним особам, які застосовують у своїй діяльності комп'ютерні інформаційні технології. Крім того, можливість зловмисних дій підриває довіру до комп'ютерної технології. У зв'язку з цим автентифікація є дуже важливою. При виборі алгоритму автентифікації повідомлень у мережі слід передбачити надійний захист від усіх перелічених раніше видів зловмисних дій. Поряд з такими характеристиками системи автентифікації, як швидкодія й об'єм пам'яті, ступінь захищеності та стійкості від загроз є дуже важливим параметром.

Серед біометричних методів автентифікації суб'єкта найбільш практичними вважаються ті, що використовують ознаки: відбитки пальців, райдужну оболонку ока, риси обличчя. Розглянемо питання, пов'язані з їх використанням. Візерунки відбитка пальців мають такі властивості: індивідуальність, неповторність, стійкість, відновлюваність. Ці властивості дають можливість абсолютно надійно ідентифікувати особу. На світовому ринку біометричних систем ідентифікації найбільшою популярністю користуються автоматичні системи розпізнавання відбитків пальців – AFIS. У примусовому порядку AFIS використовується для збирання відбитків пальців у криміналістиці, частіше в поліції для дактилоскопії. Частка AFIS складає половину обсягу

продажу біометричної продукції, а з урахуванням криміналістичних систем – 80%. Сканування відбитка пальця – один із найбільш перспективних методів. Пристрої для сканування пальців прості і зручні в користуванні. Розробка фірми "Biolink Technologies" дає можливість за 0,1 с зчитати відбиток пальця, а за 0,2 с – розпізнати його і дозволити доступ до інформації. На відміну, наприклад, від систем сканування сітківки ока, AFIS не створює дискомфорт користувачам. Відбиток пальців індивідуальний і не змінюється з часом. Системи розпізнавання за відбитками пальців демонструють високі показники точності: ймовірність того, що доступ до секретних даних одержить неавторизований користувач, практично дорівнює нулю. В даний час активно розробляються алгоритми, стійкі до шуму в зображеннях – образах відбитку пальця, що дозволяє досягти збільшення точності й швидкості розпізнавання в реальному часі. "Biolink Technologies" повідомляє про ймовірність помилкового доступу на рівні 10^{-9}, а ймовірність помилкової відмови – від 0,1 до 3,1% (залежно від налаштування системи) [11].

Завдяки ергономічності та малим розмірам сканувальні пристрої можуть бути інтегровані в комп'ютерну мишу, клавіатуру чи ноутбук. Серед біометричних систем автентифікації сканери відбитків пальців найбільш дешеві, тому найбільш вразливі. Технологічними вадами AFIS є також те, що деякі відбитки пальців непридатні для аналізу, потрібен контакт – безконтактне використання виключається. Слід зауважити, що українські вчені виготовили пристрій, який разом із відбитком пальця заміряє показники біоенергетичного поля користувача, що також унікальне, як і відбиток пальця. Отже, згадані підробки стануть у недалекому майбутньому неможливими при використанні такого пристрою. За технологічною структурою і рівнем надійності з методом ідентифікації особи за відбитком пальця можна порівняти метод ідентифікації за геометрією руки, але він використовується значно рідше. Серед систем, які можуть сканувати й інші параметри руки, популярна система Handkey, що сканує внутрішню й зовнішню сторони долоні, використовуючи для цього вбудовану відеокамеру й алгоритми стиснення інформації.

Розпізнавання за райдужною оболонкою і сітківкою ока. У сканерів райдужної оболонки є значні переваги, що можуть бути основою для використання їх у багатьох сферах. Зокрема, здатність сканерів сканувати райдужну оболонку на певній відстані дає можливість використовувати їх, наприклад, у банкоматах. Ця технологія вже кілька років працює в держустановах США, а також у в'язницях і організаціях з високим рівнем секретності, зокрема на заводах з виробництва ядерного озброєння. Метод має і принципові вади: з віком розміщення плям на райдужній оболонці може досить значно змінюватися. Наприклад, райдужна оболонка дитини за кілька років модифікується так, що біометрична система не може її розпізнати. Труднощі демонструє цей метод у роботі з людьми, у яких ослаблений зір чи косоокість, і зовсім не працює, якщо людина користується окулярами або кольоровими контактними лінзами. Помилка в ідентифікації може виникнути при кон'юнктивіті, невеликій травмі ока і навіть після безсонної ночі або через підвищене навантаження на очі. Зміни райдужної оболонки в таких випадках незначні, але система ідентифікації може її помітити. Крім того, правозахисники небезпідставно

побоюються, що інформація, знята з райдужної оболонки, буде використана з іншою метою – око чітко відображає стан здоров'я людини. При ідентифікації можна визначити хворобу і зловживання деякими речовинами.

Стосовно сітківки ока ідентифікація проводиться з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю ока до кровоносних судин на задній стінці ока. У сканерів сітківки ока один із найнижчих відсотків відмови в доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу. Але зображення має бути чітким, тому катаракта може негативно вплинути на якість ідентифікації особи.

Рівень розвитку технологій розпізнавання облич ще недосконалий – вони дають приблизно від 30% до 70% ідентифікації при 10% помилкових дозволів. Замасковані за допомогою перук, накладних вусів, великих капелюхів, окулярів і гриму службовці одного аеропорту розпізнавалися системою тільки в одному випадку із трьох. У той же час здатність людей розпізнавати представників інших рас недостатня, і в цьому разі допомога систем розпізнавання за рисами обличчя може бути значною. Технології розпізнавання обличчя орієнтовані на пошук в режимі «один до багатьох» і порівняння конкретного обличчя з тисячами інших із бази даних. Технології сканування обличчя працюють з відеозображенням (320x240 пікселів на дюйм) у потоці 3–5 кадрів у секунду. При ідентифікації з великої відстані результат значною мірою залежить від якості відеокамери.

Існує кілька методів розпізнавання обличчя. Вони включають аналіз зображення в градаціях сірого для виявлення унікальних характеристик обличчя, аналіз розпізнавальних рис (використовується більш всього метод розпізнавання, адаптований до зміни міміки), аналіз на основі нейронних мереж (порівняння за «особливими точками», метод застосовують для ідентифікації облич у важких умовах) й автоматична обробка зображення обличчя (визначення відстаней і співвідношення відстаней між особливостями обличчя людини, що легко визначаються), яку можна ефективно використати в слабоосвітлених приміщеннях.

У системах статистичного розпізнавання на основі набору біометричних даних та їх обробки формується електронний взірець як унікальне число, що стосується конкретної особи. Основні етапи використання методу: сканування об'єкта, вибір індивідуальних характеристик, формування шаблона і його порівняння з базою даних. Сканування обличчя триває 20–30 с. Далі відбувається процес ідентифікації, створення шаблона в реальному часі і порівняння його з файлом шаблона. Необхідний для перевірки рівень подібності – це обчислювальний поріг, який регулюється залежно від різних чинників (потужності ПК, освітлення тощо).

На відміну від паролів та інших базових секретів, біометричні дані рідко збігаються повністю. Механізм автентифікації вимірює, наскільки ці дані збігаються з показниками із запису користувача. Припускається, що показники однієї й тієї ж людини близькі, тоді як показники різних людей відрізняються суттєво. Точність біометричної системи вимірюється шляхом оцінки відсоткової частки помилкових підтверджень і помилкових відмов, що в середньому дає система. Оцінка точності звичайно базується на експериментах, в яких пе-

ревіряється велика кількість біометричних «підписів» і близькість їх з набором біометричних зразків. При цьому збирається велика кількість даних у множини випадково вибраних людей, віддаючи перевагу тим, що належать до групи, яка, можливо, користуватиметься біометричною системою.

Компанія "Sandia" провела дослідження ефективності деяких комерційних пристроїв для біометричної автентифікації. Дані про надійність різних методів розпізнавання наведено в табл. 1.

Таблиця 1. **Надійність біометричних методів автентифікації** [11]

Техніка	Відсоток похибок
Розпізнавання голосу (метод Alpha)	3%
Розпізнавання голосу (метод ECCO)	2%
Динаміка факсимільного підпису	2%
Сканування сітківки	0,4%
Геометрія руки	0,1%
Відбитки пальців	9% помилкових відмов, помилковий доступ відсутній

Інші характеристики існуючих методів наведено в табл. 2. Виділимо низку пріоритетних застосувань автоматизованих систем на основі алгоритмів ідентифікації за рисами обличчя. *Прикордонний паспортний контроль*, коли фото на документ порівнюється з обличчям його власника.

Таблиця 2. **Порівняльний аналіз методів автентифікації** [11]

Характеристика	Найкращий	Найгірший
Ергономічність	Рука	Голос
Помилкова відмова	Рука	Пальці
Помилковий доступ	Рука, сітківка, пальці	Голос
Продуктивність	Рука, сітківка, пальці	Голос, підпис
Обсяг пам'яті для збереження взірця	Сітківка	Голос
Складність імітації	Сітківка	Голос, підпис
Вартість пристрою	Голос	Сітківка

Реєстрація пасажирів. Системи розпізнавання облич суттєво підвищують рівень безпеки при реєстрації й оформленні авіабілетів і виявленні злочинців, що перебувають у розшуку. *Зовнішній відеоконтроль*. Система розпізнавання облич у реальному часі видає дані про присутність розшукуваних осіб або тих, чия поведінка привертає увагу. *Контроль доступу*. Системи розпізнавання облич можуть запобігти несанкціонованому доступу за периметр безпеки сторонніх осіб, автоматично засвідчуючи повноваження особи (наприклад, при огляді екіпажу). *Слідчі відділи* карного розшуку використовують бази даних, за допомогою яких фото автоматично порівнюється з електронними зображеннями. Використання пристроїв розпізнавання облич прискорить роботу правоохоронних органів. *Імміграційні служби* зможуть виявити суб'єктів, що імітують інших осіб.

Важливим механізмом підтвердження ідентифікаційних характеристик цінних паперів та електронних грошей є електронний цифровий підпис. Традиційно для захисту ідентифікаційних ознак використовується один з варіантів електронного цифрового підпису – сліпий підпис (blind signature). Скориставшись сліпим методом, можна запропонувати на підпис будь-яку інформа-

цію, яка гарантовано не буде розкрита стороною, що підписує документ. Доцільно розрізняти методи ідентифікації цінних паперів та електронних грошей і методи ідентифікації їхніх носіїв. Залежно від методів, що використовуються для ідентифікації та захисту носіїв, наприклад, електронних грошей, доцільно визначити два типи систем:

1. Системи, що зберігають «електронні гроші» на інтелектуальних картках (наприклад, Mondex);

2. Системи, що зберігають «електронні гроші» на традиційних носіях, таких як накопичувач на жорстких магнітних дисках, дискети тощо (наприклад: PayCash, Digicash, Netcash, CyberCoin). Слід відзначити, що системи першого типу принципово є більш захищеними. У таких системах інтелектуальна картка може розглядатися як аналог традиційного гаманця.

Алгоритми автентифікації з використанням засобів асиметричної криптографії. Практичну реалізацію можна розглянути на таких прикладах. Одна ситуація, коли передавач і одержувач повністю довіряють один одному. Складніший випадок полягає в припущенні, що вони не довіряють один одному або навіть здатні на шахрайство. Звичайна кредитна операція є класичним прикладом інформаційного обміну між учасниками угод, які не довіряють один одному. Оскільки для прийняття рішення щодо суперечки про дійсність угоди неминуче залучається третя сторона, тобто банк, суд або арбітр, прийняте рішення має відповідати інтересам усіх учасників угоди і на основі цього рішення має бути логічно визначена сторона, яка повинна нести відповідальність за недостовірну інформацію.

Автентифікація може використовуватися для виконання зазначених вимог на кількох стадіях. Покупець може бути ідентифікований так, щоб надалі це можна було перевірити третіми сторонами, які в реальному часі не є учасниками угоди. Для цього можуть бути застосовані два способи, вибір яких залежить від того, яка ідентифікаційна інформація використовується – внутрішня чи зовнішня. Внутрішня інформація є сукупністю фізичних ознак індивіда: відбитки пальців, сітківка ока, підпис і динаміка підпису, геометрія руки, зовнішність, зріст, маса, характерні ознаки тощо. Зовнішня інформація – це інформація, яка має бути відомою законному індивіду: наприклад, паролі доступу до ЕОМ, телефонні номери кредитних карток, номери рахунків відповідних банків, персональні ідентифікаційні номери, паролі для постів охорони тощо. Для того, щоб мати достатньо стійку схему ідентифікації, що ґрунтується на зовнішніх ознаках, потрібно створити протокол, який би дав змогу індивіду довести, що він знає секретну частину деякої інформації, не розкриваючи всю інформацію, яка могла б допомогти ймовірному зловмиснику видати себе за нього. Схеми ідентифікації залежать від інтерактивних схем, які можна довести і які часто називаються доведеннями з нульовими знаннями. У таких випадках індивід відповідає на серію запитань, складених так, що законний користувач може на них відповісти, а зловмиснику зробити це практично неможливо.

Після цього використовується добре відомий канал автентифікації, який ґрунтується на алгоритмі RSA як для відкритого каналу, так і для закритого каналу автентифікації. Джерело буде у такий самий спосіб, що й при обчисленні

прийнятного модуля алгоритму RSA, вибирати пару простих чисел, обчислювати відповідні показники ступеня шифрування-розшифрування і потім використовувати їх як відкритий ключ. Центральний пункт і джерело мандатів мають спочатку встановити справжність і точність відповідної інформації для кожного потенційного покупця, потім виробити автентифікаційний запис, який буде віддаватися покупцеві як його ідентифікаційний мандат. Він міститиме в собі внутрішню інформацію, зашифровану з використанням ключа двоключової криптосистеми, а також зовнішні ознаки. Ключі розшифрування мають доставлятися всім продавцям тощо як автентифіковані, але не обов'язково секретні повідомлення, а ті, у свою чергу, забезпечують цілісність ключа, але не його секретність. Покупець повинен пред'явити зашифрований запис, який у нього є, і надати можливість обладнанню у пункті продажу перевірити його атрибути. Використовуючи ключ розшифрування, продавець спочатку має розшифрувати шифр і перевірити справжність шифру за надлишковою інформацією. Далі він повинен визначити, чи відповідають тільки що перевірені індивідуальні атрибути розшифрованої інформації внутрішнім атрибутам. Ця інформація міститься в автентифікованому повідомленні. Якщо отримано прийнятну відповідність, особистість покупця буде підтверджена, оскільки шифр міг бути отриманий тільки при використанні секретного ключа шифрування. Зокрема, припускається, що зловмисник не може достатньо точно імітувати внутрішні атрибути інших осіб.

У системах з високими вимогами до рівня безпеки вся інформація, з якою працює система, звичайно зберігається зашифрованою. Безпечний обмін даними між комп'ютером користувача або об'єктом (смарт-карткою, брелоком, кишеньковим комп'ютером), який перевіряється і є носієм інформації, і головним комп'ютером (сервером) завжди передбачає застосування шифрування даних, що передаються, а також здійснення автентифікації цих даних. Безпечний обмін даними передбачає: забезпечення конфіденційності, секретності даних або повідомлень, що досягається шифруванням даних; забезпечення справжності і цілісності даних, що досягається відповідною автентифікацією даних. Для забезпечення більш високої криптостійкості щодо атак для розшифрування інформації, яка використовується для ідентифікації й автентифікації на спеціальних цифрових носіях, розглянемо можливості використання алгоритмів, що реалізують методи асиметричної криптографії [8; 9]. Серед найбільш відомих є алгоритм RSA [13] асиметричного шифрування та алгоритм Ель-Гамала [15]. Алгоритм RSA можна використовувати як для шифрування та розшифрування, так і для генерації й перевірки електронного цифрового підпису. Стійкість криптосистем RSA базується на складності факторизації багаторозрядних цілих чисел. При застосуванні криптосистем і RSA розмір модуля повинен перебувати в діапазоні [1024,5000] бітів. Асиметричну криптосистему Ель-Гамала можна використовувати для електронного цифрового підпису. Криптостійкість цієї системи визначається трудомісткістю обчислення дискретного логарифму.

Висновки:

1. Аналіз показав, що підвищення захисту інформації в інтелектуальних інформаційних системах досягається за рахунок сертифікації, ліцензування та

впровадженням необхідних засобів технічного й програмного захисту; створення спеціалізованих організаційних структур, які забезпечують постійне функціонування захисту та засобів генерації ключів і паролів.

2. Підвищення ефективності захисту інформації в інтелектуальних інформаційних системах досягається сумісним використанням декількох методів захисту інформації.

3. Використання спеціальних цифрових носіїв підвищує захист інформації в інтелектуальних інформаційних системах.

1. *Бабенко Л.К., Ищуков С.С. Макаревич О.Б.* Защита информации с использованием смарт-карт и электронных брелоков. – М.: Гелиос АРВ, 2003. – 352 с.

2. *Березовский А.И., Задирака В.К., Шевчук Л.Б.* О тестировании быстродействия алгоритмов и программ выполнения основных операций для ассиметричной криптографии // Кибернетика и системный анализ.– 1999.– №5. – С. 56–66.

3. *Березовський А.І., Задірака В.К., Мельникова С.С., Шевчук Л.Б.* Деякі резерви оптимізації обчислень для множення багаторозрядних чисел // Теорія обчислень: Збірник. – К., 1999. – С. 325–329.

4. *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: Політехніка, 2004. – 224 с.

5. *Богуш В.М., Кривуца В.Г., Кудін А.М.* Інформаційна безпека: Термінологічний навч. довідник. – К., 2004. – 508 с.

6. *Боков А.Ю., Рахманов О.В.* Обзор технологии пластиковых карт // Безопасность информационных технологий.– 1999.– №2. – С. 47–53.

7. *Боровиков А.М., Тимошенко А.А.* Системы защиты информационного обмена «Клиент – Банк» // Безопасность информации.– 1995.– №1. – С. 53–60.

8. *Вербіцький О.В.* Вступ до криптології. – Львів: Вид-во науково-технічної літератури, 1998. – 247 с.

9. *Гайкович В., Першин А.* Безопасность электронных банковских систем. – М.: Единая Европа, 1994. – 364 с.

10. *Завадская Л.А., Фаль А.М.* Криптографически сильные генераторы псевдослучайных последовательностей // Безопасность информации.– 1997.– №1. – С. 7–11.

11. Компьютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навч. посібник / В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк. – К.; Тернопіль, 2007. – 272 с.

12. *Смит Р.Э.* Аутентификация: от паролей до открытых ключей / Пер. с англ. – М.: Вильямс, 2002. – 432 с.

13. *Ян С.Й.* Криптоанализ RSA. – М.; Ижевск: Регулярная и хаотическая динамика, Ижевский інститут комп'ютерних исследований, 2011. – 312 с.

14. *Adelman, L.M., Huang, M.A.* (1992). Primality testing and Abelian varieties over finite fields. Lecture Notes in Mathematics, 1512: 142.

15. *El-Gamal, T.* (1985). A Public Key Cryptosystem and a Signature Schema Based Discrete Logarithms. IEEE Transactions on Information Theory, 31: 469–472.

Стаття надійшла до редакції 31.07.2012.