РОЗДІЛ 5
СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056

В. Ю. Корольов,
кандидат технічних наук,
старший науковий співробітник

СТАН ПРОБЛЕМИ КОМП'ЮТЕРНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ USB-ФЛЕШ НАКОПИЧУВАЧІВ У ДЕРЖАВНИХ УСТАНОВАХ І КОРПОРАЦІЯХ

Подано огляд флеш-накопичувачів корпоративного призначення. Наведено класифікацію функцій флеш-накопичувачів для захисту інформації в корпоративних пристроях зберігання. Обґрунтовано необхідність апаратно-програмної реалізації криптографічного захисту процесу обміну даними між таким накопичувачем і хост-комп'ютером.

Ключові слова: флеш-накопичувачі, їх функції і класифікація, захист інформації.

Із масовим використанням флеш-накопичувачів для зберігання приватної і ділової інформації постала необхідність у розробці апаратно-програмних засобів з розширеними функціями захисту інформації (апаратним шифруванням) і керуванням доступу до конфіденційної інформації. Сьогодні на ринку представлені як розробки для корпорацій, державних установ і військових, так і накопичувачі, що орієнтовані на пересічного покупця.

Аутентифікація користувача найчастіше будується на основі введення пароля з клавіатури, рідше — за допомогою зчитування відбитка пальця (дублюється введенням паролю), трапляються варіанти й введення PIN-коду з кнопок, розташованих на корпусі флеш-накопичувача. Пристрої зберігання даних в США і Канаді, призначені для корпоративного і державного використання, проходять процедуру сертифікації функцій інформаційної безпеки від Національного інституту стандартів (НИС) США.

Стандарт FIPS-140-2 було затверджено американським і канадським урядами. Тестування пристроїв НИС на відповідність цьому стандарту полягає у повірці криптографічних модулів на предмет їх відповідності заявленим специфікаціям. Це досить коштовна процедура, під час якої перевіряють якість засобів, включених у продукт підсистеми безпеки від сторонніх виробників, а також виконують тестування на наявність чорних ходів, недоліків та інших слабких місць. Виконання стандарту FIPS 140-2 стає обов'язковою вимогою для багатьох державних і комерційних установ, яким призначено виконувати захист інформації з обмеженим доступом від несанкціонованого доступу.

Актуальність розробки флеш-накопичувачів з реалізацією функцій захисту інформації і аутентифікації на базі низькорівневих мікропрограм контролера пристрою зберігання

На споживчому ринку представлено багато різновидів мобільних пристроїв із біометричною аутентифікацію користувача, але якість розпізнавання ідентифікатора є недосконалою. Здебільшого це пристрої зчитування відбитка пальця на базі скануючої лінійки протяжного типу з роздільною здатністю близько 500 dpi. Для того щоб забезпечити зручність використання пристрою і надійність розпізнавання зчитаного відбитка пальця, виробники пропонують ввести у флеш-накопичувач відбитки кількох пальців лівої і правої рук, а також до трьох варіантів відбитка кожного пальця. Кількість спроб аутентифікації користувача за скануванням відбитка пальця не обмежується. При цьому тестування показало, що можливе помилкове

розпізнавання відбитка пальця іншої людини як вірного після 30–40 спроб аутентифікації флеш-накопичувачем при недосить якісному введенні своїх відбитків власником у систему.

Іншою, більш серйозною, загрозою для інформаційної безпеки даних є використання технології віртуального CD-ROM як бази для керування перемиканням закритим і відкритим розділами пам'яті для дешевих флеш-накопичувача зі скануючою лінійкою. В интернет-публікації [1] наведено приклад зламу такої системи для флеш-накопичувача фірми A-Data за допомогою утиліти plscsi. Аналогічну систему керування доступом мають флеш-накопичувачі фірм Transcend і TakeMS, і тому вони також є потенційно вразливими до такого типу хакерських атак. Таким чином, актуальною проблемою є поліпшення якості аутентифікації користувача носіїв конфіденційної інформації у корпоративних системах.

Огляд флеш-накопичувачів корпоративного класу

Із перелічених вище причин переважна більшість світових виробників флеш-накопичувачів корпоративного класу використовують систему аутентифікації користувачів за допомогою паролів, а керування закритим і відкритим розділами пам'яті реалізують без звернення до системних програм операційної системи Windows. Варто зазначити, що сертифікація HIC США не є абсолютною гарантією правильності технічної реалізації рішення і у пристроях корпоративного класу трапляються помилки у проектуванні [2].

Перейдемо до огляду наявних технічних рішень, що запропоновані виробниками для підвищення рівня захисту інформації у комерційних і державних організаціях.

USB-флеш накопичувачі фірми Kingstone

Флеш-накопичувачі з USB-інтерфейсом фірми Kingstone з апаратним шифруванням (AES-256) потоку даних між пристроєм і хост ПК представлені сімейством продуктів DataTravel: Vault (Two Partions), Vault Privacy, Secure, Privacy, Secure Privacy, Black Box. Серія Vault (Two Partions), що підтримує закритий і відкритий розділи флеш-пам'яті, решта продуктів — лише закритий. Доступ до закритої частини пам'яті накопичувача виконується за допомогою консолі MyDataZone введенням сильного паролю [4] з клавіатури. Фабрична прошивка надає 10 спроб на введення паролю, після чого пристрій блокується і його подальше використання можливе лише після форматування накопичувача. Продукти Two Partions орієнтовані на індивідуального власника, всі інші серії призначені для корпоративного використання. Пристрої сімейства Black Box сертифіковані за рівнем FIPS-140-2.

Для підвищення продуктивності роботи флеш-накопичувачів сімейства DataTravel у пристроях зберігання використовується два незалежні процесори: контролер флеш-пам'яті і USB-інтерфейса та криптографічний співпроцесор. Ключі для криптографічних алгоритмів забезпечує генератор істинно випадкових чисел. Вироби мають стальний водонепроникний корпус.

USB-флеш накопичувачі фірми SanDisk

Лінійка USB-флеш накопичувачів SanDisk із посиленою системою захисту інформації представлена трьома продуктами під торговою маркою SanDisk Cruzer: Professional, Enterprise, FIPS. Всі пристрої цієї лінійки забезпечують апаратне шифрування потоку даних алгоритмом AES-256 між накопичувачем і хост-ПК. Флеш-накопичувачі серії Professional мають відкриту і закриту частини пам'яті, серії Enterprise і FIPS — тільки закриту. Доступ користувача до закритої частини пам'яті здійснюється введенням сильного паролю з клавіатури. Використання накопичувачів серії Professional передбачає, що пристрій перебуває у приватній власності фізичної особи. Продукти серії Enterprise і FIPS повинні бути власністю організації, яка видаватиме накопичувачі працівникам. Для керування життєвим циклом флеш-накопичувачів, які підключаються до обчислювальної мережі організації (створення/видалення запису про користувача флеш, контроль даних, що копіюються на носій) пристроїв серій Enterprise і FIPS, компанія SanDisk пропонує програмний комплекс CMC (Central Management and Control).

Накопичувачі серії FIPS відрізняються від Enterprise повною відповідністю нормам FIPS-140-2, що надає можливість використовувати їх не тільки у комерційних, але й у державних установах. Крім

того, у накопичувачах серії FIPS для виключення доступу до ключів шифрування мікросхему запресовано в епоксидний компаунд.

USB-флеш накопичувачі фірми IronKey

Флеш-накопичувачі компанії IronKey забезпечують апаратне шифрування потоку даних між ПК і пристроєм зберігання за алгоритмом AES-128 у режимі CBC. На думку розробників, шифрування 128 бітним ключем є прийнятним захистом конфіденційної інформації для комерційних структур. У сімействі продуктів фірми IronKey є три серії: Basic, Personal, Enterprise.

У маркетингових матеріалах компанія IronKey підкреслює, що в її продуктах використовується досвід військових розробок. Усі серії пристроїв зберігання сертифіковані НІС США за стандартами FIPS: 140-2, 186-2, 197.

Аутентифікація користувачів флеш-накопичувачів забезпечується введенням символів з клавіатури у панель керування паролями. У випадку 10 послідовних невдалих спроб ввести пароль пам'ять флеш-накопичувача гарантовано стирається за запатентованим фірмою IronKey алгоритмом. Хеш-функції (SHA-256) паролів зберігаються у спеціалізованому чіпі, що виконує криптографічні операції. Цифрові ключі для криптографічних алгоритмів: 128 біт DRND, PKI 2048-біт RSA забезпечує вбудований генератор істино випадкових чисел. У всіх серіях накопичувачів є тільки закрита частина пам'яті.

Серії продуктів фірми IronKey: Basic, Personal, Enterprise нарощують кількість сервісів інформаційної безпеки в порядку переліку. Пристрої зберігання серій Basic і Personal призначені для особистого використання та мають однакову вартість. Basic серія забезпечує мінімальний сервіс за допомогою оболонки Control Panel: керування файлами та оновленнями ПЗ, резервне копіювання та зміна паролів. Власники накопичувачів серії Personal, крім сервісів Basic, отримують можливості безпечної роботи в Internet за допомогою спеціально конфігурованої версії браузера Mozila FireFox: проміжні дані web-сесій, паролі до інтернет-ресурсів зберігаються на флеш, виконується перевірка безпеки сайтів.

Пристрої зберігання даних серії Enterprise призначені для корпоративного застосування і супроводяться ПЗ для підтримки політики керування життєвим циклом накопичувачів, резервним збереженням даних для кількох пристроїв, системою разової ідентифікації користувачів за допомогою разових паролів (на одну сесію) фірми RSASecureID, а також он-лайн підтримкою продуктів фірми IronKey.

Усі вироби фірми IronKey мають стальний корпус, водонепроникні за військовим стандартом, мікросхеми, запресовані в епоксидний компаунд. У разі зламу корпуса накопичувача, що реєструється вбудованим детектором, конфіденційна інформація фізично знищується.

USB-флеш накопичувачі фірми MxiSecurity

Фірма MxiSecurity розробляє флеш-накопичувачі, призначені для державних і комерційних організацій, яким потрібен високий рівень захисту конфіденційної інформації від несанкціонованого доступу. У флеш-накопичувачах підтримується два розділи пам'яті: закритий, доступ до якого надається після процедури аутентифікації, і відкритий, з якого дозволено тільки читання.

Шифрування потоку даних між пристроєм зберігання і ПК виконується за алгоритмом AES-256 у режимі CBC, який реалізовано на базі ПЛІС [2]. У раніше розроблених моделях використовується виключна парольна аутентифікація операторів, а в нових моделях парольна аутентифікація доповнюється скануванням відбитка пальця з обмеженою кількістю спроб. Таким чином, нові пристрої мають двофакторну аутентифікацію користувача і трьохфакторну для запуску програм з накопичувача (пароль, відбиток пальця і унікальний цифровий номер-ідентифікатор накопичувача).

Випускається чотири серії продуктів: StealthMini(ClipDrive і Secure ClipDrive), StealthMXP, StealthMXP Passport, OutBarkerMXP. Зіставлення характеристик продуктів наведено у табл. 1. Продукти StealthMXP і OutBarkerMXP підтримують аутентифікацію декількох (до п'яти облікових записів) користувачів. Керування життєвим циклом реалізовано за допомогою ПЗ Access Enterprise фірми MxiSecurity.

Таблиця 1 — **Порівняння характеристик серій накопичувачів фірми MxiSecurity**

№ з/п	Назва продукту	Парольна аутентифікація	Біометрична аутентифікація	Апаратне шифрування	Цифрові ідентичності і криптосервіси	Керування життєвим циклом	Відповідність FIPS 140-2
1	Stealth Mini	+		+		+	
2	StealthMXP Passport	+		+	+	+	+
3	StealthMXP	+	+	+	+	+	+
4	OutBarkerMXP	+	+	+	+	+	+

Флеш-накопичувачі серії OutBarker передбачають, що їх покупець бажає носити з собою весь вміст робочого місця. Тому накопичувачі цієї серії мають об'єм пам'яті як у тонкого клієнта або ноутбука. Габарити накопичувачів серії OutBarker відповідають портмоне. Для компенсації пониженої потужності USB-порту, яка характерна для ноутбуків, які працюють від акумулятора, накопичувачі серії OutBarker комплектуються внутрішнім джерелом живлення.

З усіх сучасних флеш-накопичувачів з апаратним захистом інформації продукти StealthMXP і OutBarkerMXP мають найповніший набір криптосервісів: спецконтейнери для симетричних, асиметричних ключів і разових хешованих ключів (HOTP), разова генерація паролів (OATH), розрахунки хеш-функцій SHA-1 і SHA-256, HMAC з перемиканням, RSA шифруванням, цифровий підпис, генератор випадковий чисел і ключів (1024/2048/3072 біт), генератор токенів для SAML WS-trust, підтримка сумісності з системами RSASecure ID і Entrust. Тому фірма MxiSecurity стверджує, що її продукти можуть задовольнити найвибагливіших користувачів.

USB-флеш накопичувачі фірми Verbatim

Фірма Verbatim випустила накопичувачі сімейства Store 'n' Go з апаратним шифруванням потоку даних комп'ютером і пристроєм зберігання за алгоритмом AES. У Європі продають серії Bisness Secure (AES-256) і Executive (AES-128). У США пропонують три серії: PRO (AES-256), Corporate Secure (AES-256) та Corporate Secure FIPS Edition (AES-256 режим EBC), яку сертифіковано за стандартом FIPS-140-2. Аутентифікація користувача виконується за допомогою введення паролю з клавіатури, кількість спроб дорівнює десяти. Серія PRO підтримує відкриту і закриту зони флеш-пам'яті за допомогою програми V-Safe Security, а у серії Corporate Security дозволено лише закриту частину флеш пам'яті. Серія накопичувачів Store 'n' Go Corporate Secure є сумісною з ПЗ mTrust, призначеного для централізованого управління і контролю корпоративних мобільних накопичувачів даних. У накопичувачах серії Corporate Secure FIPS Edition для запобігання доступу до ключів шифрування мікросхеми запресовані в епоксидний компаунд.

USB-флеш накопичувачі фірми Kanguru

Фірма Kanguru пропонує дві серії накопичувачів з апаратним шифруванням потоку даних між ПК і пристроєм зберігання за алгоритмом AES-256: Defender і Defender PRO. Характеристики інших своїх продуктів виробник не подав на сайті. Аутентифікація користувачів здійснюється за допомогою введення паролю з клавіатури. Кількість спроб введення пароля дорівнює десяти. Принципова різниця між серіями полягає у типі використаної NAND флеш-пам'яті. Для накопичувачів серії Defender — це MLC-технологія, а для Defender PRO — SLC. Відповідно до швидкості читання/запису для накопичувачів серії Defender PRO вдвічі вищі за пристрої серії Defender. Станом на сьогодні тільки серія MicroDriveAES пройшла сертифікацію рівня FIPS-140-2.

USB-флеш накопичувачі Pivot plus фірми Imation

Серія Pivot plus фірми Imation забезпечує апаратне шифрування потоку даних між ПК і пристроєм зберігання за алгоритмом AES-256. Аутентифікація користувача забезпечується введенням пароля з клавіатури, який має складатися мінімум із

семи букв і цифр. У разі семи послідовних невдалих спроб введення пароля пристрій блокується. У серії Pivot plus всі дані зберігаються у закритій частині пам'яті флеш-накопичувача. Передбачено також підтримка майстер-пароля для накопичувачів при корпоративному застосуванні.

Наведемо дані для флеш-накопичувачів корпоративного призначення для середнього об'єму пам'яті — 4ГБ (табл. 2).

Таблиця 2 — **Характеристики USB-флеш накопичувачів корпоративного класу з об'ємом пам'яті 4 ГБ і апаратним захистом інформації**

№ з/п	Фірма-виробник	Вартість, дол. США	Швидкість читання|запису, МБ/с	Серверне ПЗ для КЖЦ накопичувача
1	Kingstone	191	24|10	—
2	SanDisk	144	24|20	CMC
3	IronKey	149	30|20	My.IronKey.com
4	MxiSecurity	189	н/д	ACCESS EnterPrise
5	Verbatim	130	30|12	mTrust
6	Kanguru	130	30|15	—
7	Imation	133	н/д	—

КЖЦ — керування життєвим циклом.

Класифікація характеристик флеш-накопичувачів, представлених на ринку

Наведемо класифікацію характеристик функцій сучасних флеш-накопичувачів, яка може бути використана для проектування найбільш функціонально-повного пристрою зберігання з апаратним шифруванням потоку даних між накопичувачем і хост-ПК.

1. *Характеристики систем захисту інформації накопичувачів.*
1.1. Аутентифікація користувачів.
1.1.1. Однофакторна (ім'я користувача і пароль, що вводиться з клавіатури).
1.1.2. Двофакторна (сканування відбитка пальця, ім'я користувача і пароль, що вводиться з клавіатури).
1.2. Апаратний алгоритм шифрування.
1.2.1. AES з 256-битними ключами шифрування.
1.2.1.1. CBC-режим шифрування блоків.
1.2.1.2. EBC-режим шифрування блоків.
1.2.2. AES з 128-бітними ключами шифрування.
1.2.2.1. CBC-режим шифрування блоків.
1.2.2.2. EBC-режим шифрування блоків.
1.3. Спосіб розмежування і захисту доступу до пам'яті флеш-накопичувача.
1.3.1. Використання тільки закритого розділу пам'яті з зашифрованими даними користувача.
1.3.2. Використання відкритого розділу пам'яті (для читання і запису або тільки для читання) і закритого розділу пам'яті з зашифрованими даними користувача.
1.4. Сертифікація.
1.4.1. Сертифіковані за стандартом FIPS-140-2.
1.4.2. Не сертифіковані.
1.5. Спосіб реалізації алгоритму генерування випадкових чисел.
1.5.1. Алгоритм генерування випадкових чисел у відповідності до криптографічних стандартів якості.
1.5.2. Алгоритм перетворення даних стохастичного фізичного процесу у випадкову послідовність у відповідності до криптографічних критеріїв якості.
1.6. Повнота реалізації криптосервісів.
1.6.1. Базовий набір сервісів (хеш-функції, асиметричні алгоритми обміну ключів і т.п.).
1.6.2. Розширений набір сервісів (базові сервіси, разові ключі, підтримка захищеного запуску додатків тощо).
1.7. Захист від фізичного доступу до секретних даних.
1.7.1. Відсутній (міцний корпус).
1.7.2. Запресування мікросхем у епоксидний компаунд.
1.7.3. Датчик злому корпусу, що подає сигнал на знищення мікросхеми з секретними даними.
2. Експлуатаційні характеристики.

2.1. Можливість запису унікального ідентифікатора у пам'ять флеш-накопичувача (для роботи систем керування життєвим циклом пристрою зберігання).
2.2. Кількість користувачів флеш-накопичувача.
  2.2.1. Один користувач.
  2.2.2. Кілька користувачів.
2.3. Портабельне програмне забезпечення [5] і ПЗ для керування життєвим циклом накопичувача.
  2.3.1. Власне ПЗ.
  2.3.2. ПЗ від партнерів або сторонніх виробників.
2.4. Об'єм пам'яті пристрою зберігання.
2.5. Швидкість читання/запису флеш-накопичувача.
  2.5.1. Низька (6/5).
  2.5.2. Середня (15-12/10).
  2.5.3. Висока (30/25).
2.5. Захист від впливу оточуючого середовища.
  2.6.1. Базовий захист (пластиковий корпус).
  2.6.2. Високий ступінь захисту (вологостійкий і ударозахищений корпус).

Повний набір наведених характеристик не реалізовано у жодному із сучасних накопичувачів, пристрої зберігання фірм Kingston, SanDisk, IronKey та MxiSecurity задовольняють більшість показників. Накопичувачі інших фірм задовольняють тільки мінімально необхідний набір характеристик для того, щоб їх виріб можна було використовувати для захисту корпоративної інформації з обмеженим доступом.

Розглянуті флеш-накопичувачі з USB-інтерфейсом використовують аутентифікацію користувача за допомогою введення надійного паролю з клавіатури ПК з обмеженою кількістю спроб, пакети даних між пристроєм зберігання і ПК шифруються за алгоритмом AES-256, інформація з обмеженим доступом зберігається у закритій частині флеш-пам'яті. Пристрої зберігання, які позиціонуються виробниками як професіональні (є приватною власністю фізичної особи), підтримують відкриту і закриту зони пам'яті, розміри яких визначаються користувачем. Таким чином, у разі крадіжки, підміни або втрати накопичувача конфіденційна інформація лишається недоступною для зловмисників. Апаратне шифрування потоку даних між хост-ПК і флеш-накопичувачем забезпечує суттєве збільшення захищеності інформації з обмеженим доступом при роботі за межами безпечної корпоративної мережі, в якій спеціалізовані програми контролюють потоки даних і порти. Тому немає виключно програмних рішень, які пройшли сертифікацію у НИС рівня FIPS-140-2.

Висновки. Розробники корпоративних флеш-накопичувачів заявляють, що гарантують безпеку роботи службовців із мобільними пристроями зберігання поза офісом на будь-яких ПК, які не є власністю організації, за допомогою підсистеми виявлення хакерських атак контролером накопичувача, об'єктом яких є процес обміну даними і командами між з комп'ютером. За стандартами комп'ютерної безпеки паролі мають змінюватись не частіше одного разу на місяць і не слугувати довше півроку. Якщо в середині мережі організації проводиться аудит ПЗ і перевірка файлів, які приносять службовці, то поза корпорацією гарантувати безпеку процесу введення паролю практично неможливо. Слід зазначити, що сьогодні існує багато безкоштовних програм-шпигунів, які дають можливість зафіксувати пароль, введений з клавіатури та записувати дані, з якими працює оператор. Отже, при використанні флеш-накопичувачів поза організацією аутентифікація користувачів за допомогою введення складних паролів не може гарантувати інформацію з обмеженим доступом від несанкціонованого використання.

Аутентифікація користувачів на базі BIK-технології [3], не змінюючи по суті технологію аутентифікації за допомогою введення паролів, дає змогу суттєво підвищити захищеність даних у накопичувачі, оскільки хеші введених BIK-ключів не залишають пристрій зберігання. Перший етап аутентифікації використовує комп'ютер тільки для живлення накопичувача від USB-порта. Процедура перевірки ключа використовується і виконується контролером у середині пристрою. На другому етапі у пристрій надходять дані, введені з клавіатури, а на виході з пристрою у високорівневу програму надходить складний пароль. Таким чином, використання BIK-ключа для аутентифікації користувачів флеш-накопичувача дає змогу захистити процес формування паролю від зчитування шпигунськими програмами при роботі на комп'ютері, що не контролюється корпоративною системою безпеки.

Подан обзор флеш-накопителей корпоративного назначения. Приведена классификация функций флеш-накопителей для защиты информации в корпоративных устройствах хранения. Обоснована необходимость аппаратно-программной реализации криптографической защиты процесса обмена данными между таким накопителем и хост-компьютером.

Ключевые слова: флеш-накопители, их функции и классификация, защита информации.

The survey of corporate flash drives is presented. The information security function classification of flash drives for corporate storage devises is discussed. Hardware cryptographic security realization of data exchange between host-computer and flash drive support is given.

Key words: flash drives, their functions, classification, information protection.

Література

1. http://www.h-online.com/security/Secure-USB-sticks-cracked--/features/110280/0

2. http://www.h-online.com/security/USB-stick-with-hardware-AES-encryption-has-been-cracked--/features/111194

3. *Корольов В. Ю., Поліновський В. В., Малікова О. В.* Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора // Вісник Хмельницького національного університету. — 2008. — № 3. — С. 175–181.

4. http://www.microsoft.com/protect/yourself/password/create.mspx

5. *Королёв В. Ю., Полиновский В. В.* Синтез портабельных информационных сервисов для флеш-накопителей // Управляющие системы и машины. — 2008. — № 6. — С. 28–33.

СЕРІЯ:

«ІНФОРМАТИКА, ОБЧИСЛЮВАЛЬНА ТЕХНІКА ТА КІБЕРНЕТИКА»

КИЇВ 2010

УДК 004+007](06)
ББК 32.973я43+32.81я43
І-74

Рекомендовано до друку Вченою радою
Відкритого міжнародного університету розвитку людини «Україна»
(Протокол № 5 від 25 жовтня 2010 р.)
Свідоцтво про державну реєстрацію
серія Кі № 470 від 01.03.2000 р.

ВІСНИК УНІВЕРСИТЕТУ «Україна» № 8, 2010

Серія «Інформатика, обчислювальна техніка та кібернетика»

Засновник: Відкритий міжнародний університет розвитку людини «Україна»

Інформатика, обчислювальна техніка та кібернетика : Вісник Університету «Україна», — № 8. — К. : Університет «Україна», 2010. — 227 с.
ISBN 978-966-388-252-9.

УДК 004+007](06)
ББК 32.973я43+32.81я43

ISBN 978-966-388-252-9

ВІСНИК УНІВЕРСИТЕТУ «УКРАЇНА»

Серія «Інформатика, обчислювальна техніка та кібернетика»

№ 8, 2010

Свідоцтво про державну реєстрацію Кі №470
від 01.03.2000 року
Засновано у 2000 році
Засновник: Відкритий міжнародний університет
розвитку людини «Україна»

Київ 2010

університет «Україна» видавництво