



Рисунок 4 - Алгоритм биномиального вычитающего счета

#### Выводы.

В данной работе решена задача нумерации равновесных кодовых комбинаций на основе биномиальных чисел, позволяющая производить декодирование равновесных кодов и их сжатие, что имеет значение для задач эффективной передачи и хранения информации. Использование биномиальных чисел для выполнения указанных задач позволяет упростить алгоритм нумерации равновесных кодов, сделать его адаптивным и помехоустойчивым. Предлагаемые алгоритмы перспективны для адаптивного кодирования равновесных кодов и для криптографической защиты сообщений.

#### ЛИТЕРАТУРА

1. Андерсон Джеймс А. Дискретная математика и комбинаторика. –М.: Изд. Дом «Вильямс», 2003. –960 с.
2. Амелькин В.А. Методы нумерационного кодирования. –Новосибирск: Наука, 1986. –155 с.
3. Борисенко А.А. Введение в теорию биномиального счета: Монография. –Сумы: ИТД «Университетская книга», 2004. –85 с.
4. Борисенко А.А. Биномиальный счет. Теория и практика: Монография. –Сумы: ИТД «Университетская книга», 2004. –170 с.

Поступила в редколлегию 03.09.2004

БОРИСЕНКО О.А., ЧЕРЕДНИЧЕНКО В.Б. НУМЕРАЦІЯ РІВНОВАЖНИХ КОДІВ НА ОСНОВІ БІНОМІАЛЬНИХ ЧИСЕЛ

Викладаються алгоритми нумерації рівноважних кодів з використанням двійкових біноміальних систем числення, що дозволяють підвищити надійність перетворення й спростити його реалізацію.

\*\*\*

BORISENKO A.A., CHEREDNICHENKO V.B. NUMBERING OF EQUILIBRIUM CODES ON THE BASIS OF BINOMIAL NUMBERS

Algorithms of numbering of equilibrium codes with use of the binary binomial notations are stated, allowing to raise reliability of numbering and to simplify its realization.

УДК 65.012.8(0:044)

**А.В. ШЕВЧУК**, канд. техн. наук, ст. наук. співр.

Поліграфічний комбінат "Україна"

## НОВЕ ПОКОЛІННЯ ВИСОКОЗАХИЩЕНИХ ДОКУМЕНТІВ СУВОРОГО ОБЛІКУ, ЩО ЗАСВІДЧУЮТЬ ОСОБУ

Розглянуті питання створення персоналізованих документів ідентифікації особи; наведені біометричні методи їх захисту від підроблення та фальсифікації; розглянуті нові види паспортів й принципові вимоги до їх конструкції та дизайну. Описана процедура внесення персоналізованих даних, система автоматизованої перевірки та встановлення невідомості паспортних документів.

За багатовікову історію людська спільнота накопичила багатий досвід створення документів, які є засобами ідентифікації для встановлення особи. Такі документи практично стали невід'ємними супутниками кожної людини на усіх ступенях її життєдіяльності, тому в кожній країні виготовляються та випускаються в обіг різноманітні персоналізовані документи, які поєднують наявність визна-

ченої інформації про особу власника. Найбільш поширеними персоналізованими документами є паспорти. Вони, як правило, представляють інтерес для кримінальних структур і потребують захисту від підроблення та фальсифікації. Відсутність захищеності паспортів може нанести значну шкоду та збитки державі та її громадянам. Тому основна вимога до паспортів – це максимально високий

ступінь захисту, викликаний небезпекою загроз фальсифікацій та зловживань [1, 2]. Необхідність захисту регламентована в кожній країні чинним законодавством.

Захист документів з розвитком високих технологій зберігання інформації та її захисту поступово перетворюється в високотехнологічну галузь. В передових країнах світу в останні роки з'явилися нові прогресивні наукоємні комп'ютерні та інформаційні технології, які значно підняли рівень виготовлення і захисту від підробки паспортів. Новітні технології у сфері виготовлення документів дали змогу реалізувати новий напрямок захисту – внесення до документів, що засвідчують особу, біометричної інформації про особу-власника документа [3, 4].

У березні 2003 р. робоча група ІКАО (Міжнародна організація громадянської авіації в сфері нових технологій (РГНТ) підготувала Новоорлеанську Резолюцію. В ній йдеться про те, що спільна група технічних консультантів по машиннозчитувальним прозорим документам (МЗПД) та РГНТ визнає, що країни-учасниці застосовують в даний час та будуть використовувати надалі зображення обличчя в якості ідентифікатора МЗПД, і рекомендує застосування в цій якості стандартизованих зображень обличчя, котрі зберігаються в цифрових запам'ятовуючих пристроях як міжнародний біометричний показник, що має допоміжне значення для технології розпізнавання осіб за допомогою машинної верифікації особи з використанням МЗПД, а, також додається зображення рогової ока. Країнам-учасницям на початковій стадії впровадження МЗПД із біометричними показниками рекомендується використати безконтактні носії достатньої ємності для забезпечення переносного зберігання додаткових даних МЗПД та біометричних показників.

#### 1. Поширення можливостей захищених документів за допомогою біометрики

Під біометрикою розуміють психологічні, фізичні чи поведінкові особливості, які можна автоматично виміряти, внести в базу даних та згодом порівняти з живим зразком (ідентифікувати). Основним принципом є фіксація обраної біометричної характеристики, створення контрольних зразків та їх зберігання. Популярні біометричні методи включають ідентифікацію по обличчю, верифікацію підпису, розпізнавання відбитків пальців, визначення геометрії руки, сканування сітчатки та розпізнавання райдужної оболонки ока, верифікацію голосу. Крім того, існують менш розповсюджені процедури: розпізнавання візерунків вен, запаху, ходи, манери набору на клавіатурі та ін.

Переваги біометричних методів:

- особа, яка підлягає ідентифікації, повинна бути присутня особисто;
- ідентифікація на основі біометричних даних усуває необхідність в запам'ятовуванні пароля чи носінні посвідчення;
- біометричні методи можуть перешкоджати несанкціонованому доступу чи використанню банкоматів, мобільних телефонів, смарт-карт, комп'ютерів та їх мереж.

**Фотографія.** Широко, більше ніж 100 років, як засіб автентифікації та ідентифікації особи застосовується фотографія обличчя. В новітніх технологіях виготовлення документів використовується цифрове фото обличчя, що дозволяє одразу після зйомки виконувати його комп'ютерну обробку. При цьому в комп'ютерному пошуку аналога використовуються окремі характеристики

обличчя, його геометрія.

**Підпис.** Як засіб біометричної ідентифікації підпис особи використовується протягом кількох століть, але він легко підроблюється, а сучасні навчальні комп'ютерні системи, взагалі, дозволяють швидко навчитися "підписуватися" за іншу особу. Крім того, підпис людини досить часто залежить від її психічного та фізичного стану. Технології та обладнання для забезпечення процедури ідентифікації за підписом порівняно прості та дешеві, але вони мають високий процент помилок. Використання динамічних характеристик дозволяє мати значно більше "прихованих" особливостей підпису особи. Автентифікація за таким "живим" підписом дає 0,01 % помилок - при відносно невисокій вартості такої технології. Як правило, підпис особи використовується в комплексі з іншими біометричними характеристиками.

**Відбитки пальця.** Лінії папілярного візерунка пальця, як засіб біометричної ідентифікації особи в документах, набув широкого застосування після розробки методів автоматизованої обробки інформації. Візерунок знімається шляхом прикладання пальця до віконця спеціального пристрою. На основі візерунка формується спеціальний код, що враховує його особливості, який може бути розміщений в документі або в комп'ютерній базі даних для подальшого використання в процедурах автентифікації та ідентифікації. Об'єм такого коду - близько 1 кілобайта. Сам візерунок може зберігатися у спеціальній базі даних для проведення експертиз. При цьому величина помилки хибної відмови, як правило, становить близько 2 % з першої спроби і може бути зменшена шляхом виконання 2-3 спроб, величина помилки хибного допуску становить 0,00001 % або одна помилка на 100 000 пред'явлень.

Сенсорні технології для ідентифікації ліній папілярного візерунка підпадають під три основні категорії сигналів: оптичні (оптичні сенсори), електричні (на електрооптичних та смісних сенсорах), термічні. Інші технології, такі як ультразвукові та технології вимірювання тиску, виявилися неефективними або їх можливості до кінця не вивчені.

Вартість біометричних систем ідентифікації на базі ліній папілярного візерунка постійно знижується – відбувається перехід від оптичних сканерів на кремнієві та полімерні мікросхеми. Вдосконалюється також алгоритм автентифікації, що дозволяє знаходити для них все ширше застосування, особливо в документах у вигляді пластикових карток. Щоб знайти підроблені відбитки пальців було розроблено концепцію автентифікації володаря. Використовуючи в сенсорі термінал вводу та інші можливості, користувач може ввести код (літерно-цифровий). Як правило, сформований код папілярного візерунка пальця записується в інтегральну схему (останнім часом — безконтактну), а сам візерунок додатково може бути внесений у документ поліграфічним способом. Код доповнює відбитки пальців та автентифікує користувача. Такий спосіб ідентифікації особливо ефективний при використанні активного термічного сенсора, але може застосовуватися і з іншими сенсорами відбитків пальців.

**Кисть руки.** Геометрія кисті руки, як засіб автоматичної біометричної ідентифікації, зараз використовується на підприємствах та установах в системах обмеження доступу. З огляду на економію, спосіб ідентифікації за геометрією кисті руки – один з найдешевших і компактних. Так,

інформація щодо геометрії кисті руки займає лише близько 10 байт пам'яті. Система не висуває вимог до температури, чистоти, вологості руки. Ймовірність хибного допуску і хибної відмови у допуску мають значення від 0,1 до 0,2 %. Але геометрія кисті руки як засіб автентифікації особи в документах, що засвідчують особу, як правило, в даний час не використовується.

**Райдужна оболонка ока** Використовується для біометричної ідентифікації особи тільки в останні 10-15 років у зв'язку з налагодженням масового виробництва високоякісних відеокамер із високою роздільною здатністю. При цьому відеозображення ока фіксується камерою на відстані 20-30 см, автоматично виділяється зніщя, райдужна оболонка та її візерунок. Помилкова ідентифікація особи складає близько 0,0001 %, а рівень помилки хибної відмови – не більше 2 %. Технологія розпізнавання райдужної оболонки ідентифікує людину на основі її фактичних біологічних характеристик та даних документа. Найчастіше візерунок райдужної оболонки ока використовувався в системах обмеження доступу.

Розпізнавання райдужної оболонки – це найскладніша форма біометрики. У процесі сканування перевіряється 244 унікальних біологічних показника, де скануючий пристрій послідовно розраховує алгоритмічний код. Вірогідність генерування двох ідентичних кодів для двох різних людей складає 1:1048. Технологія Irisbox зводить процес верифікації до єдиної перевірки, біологічні показники володаря карти не зберігаються та не зіставляються. В результаті цього, особиста інформація володаря карти не може бути розголошеною, і виключається можливість використання вкраденої чи загубленої карти. При реалізації фінансових операцій відпадає необхідність в ПІН-кодах, а відповідним організаціям більше не потрібно видавати ці коди чи допомагати володарям карт, що забули свої коди.

**Генетичний код.** Генетичний код – засіб практично безпомилкової ідентифікації особи. Однак така ідентифікація складна технологічно і з високою вартістю процедури, до того ж, поки що не дозволяє одержати результат в прийнятні строки. Тому масового застосування в документах ця технологія сьогодні не має і використовується при визначенні родинних зв'язків, експертизі злочинів тощо.

Відсутність експрес-методів одержання результатів стримує використання в технологіях ідентифікації таких біометричних характеристик як запах тіла, будова вуха тощо, хоча наукові розробки за цими напрямками вже проводяться.

## 2. Виготовлення паспортів

Паспорт - це найбільш масовий вид документа в світі. Потреба використовувати нові види паспортів із безконтактними чіповими технологіями виникла для забезпечення оптимального захисту від підроблення та для оперативної ідентифікації володаря документа. Чіп та антена поміщені між декількома шарами полікарбонату, в результаті чого носій забезпечує не тільки механічний захист, але й стійкість до зовнішніх впливів.

В багатьох країнах вироблені такі принципові вимоги до паспортів:

- відповідність нормативам ІКАО;
- ступенева захищеність від несанкціонованого копіювання. Окрім поліграфічних видів захисту повинні використовуватись й альтернативні підвищені ступені захисту;

- перевірка дійсності паспорта повинна бути простою та надійною без постійного звернення до центральної бази даних;

- паспорт повинен мати надійні біометричні показники, що дозволяють встановити зв'язок між документом та його законним власником;

- кожна країна вважає, що в паспорті повинна максимально використовуватися вітчизняна технологія.

Є також загальні вимоги до дизайну (конструкції). Окрім того, мають бути використані такі технології:

- найновіша чіпова технологія;
- передові методи стиснення інформації;
- методи симетричного кодування підвищеної захищеності;

- включення "активного елемента" – "чіпової антени-вставки" (INSERT) товщиною в декілька міліметрів, який, як правило, ламінований в задню сторінку паспорта.

За пропозицією IRIS по рішенню завдань біометричної ідентифікації біометричні дані складаються з кольорової фотографії власника паспорта, що ідентична фотографії на сторінці з біографічними даними. Біометрична фотографія перетворюється в цифрову форму та стискається за сучасною технологією стискання. Стиснені дані кодується та надійно зберігаються в чіпі. Коли паспорт розміщується поблизу зчитувального приладу, файл із фотографією зчитується з чіпа, декодується, розгортається та відображається на моніторі ПК.

При виготовленні та випуску в обіг паспортів елементи INSERT виготовляються на спеціалізованій фабриці підвищеної безпеки. На державній друкарні, що виготовляє захищені документи, вони вставляються між форзацом та задньою сторінкою паспорта з використанням клеєвого ламінування. Далі паспорт персоналізується та кодується.

Процедура видання паспортів складається з таких етапів: заявник подає потрібну інформацію, встановлюється дійсність усіх відповідних первинних документів, комплект документів спрямовується в організацію по виробництву паспортів.

Далі здійснюється персоналізація документа:

- виготовляється спеціальний ламінат, на якому друкуються особисті дані та фотографія;

- ламінат приклеюється до титульної сторінки паспорта;

- відбувається перетворення в цифрову форму та стиснення фотографії, а також кодування фотографії та інформації про власника. Завершальним етапом є детальна перевірка якості.

В результаті виготовлення паспортів владні органи одержують:

- можливість виявляти підроблені паспорти та паспорти, в яких зроблені підміни (інша фотографія);
- автоматизацію процесу контролю (в'їзду/виїзду);
- скорочення до 10 секунд процесу обробки документів, при їх перевірці.

Є також можливість виготовляти паспорти з додатковими біометричними даними: крім стисненого та закодованого фотографічного зображення в паспорт на перших етапах вміщуються відбитки двох великих пальців (500 байт на відбиток).

## 3. Система видачі проїзних документів

У світі діють 3 типові системи, які видають документи:

- системи паспортних столів (СПС);
- системи поліцейської служби (СПОЛ);
- комунально-адміністративні системи (КАС).

Процес подання заявок змінюється в залежності від системи, що використовується. Форма подання заявок особисто – СПОЛ, КАС – заповнюється за допомогою посадової особи. При СПС форма заповнюється вдома чи на пошті. В цьому випадку форма повинна бути підписана адвокатом, нотаріусом, священником чи місцевим лікарем, де підтверджується, що особисті дані вірні і особа йому відома. Потім заявка надсилається в паспортний стіл.

При централізованому виготовленні/персоналізації процес займає декілька днів. Документ надійде замовним листом або його потрібно буде забрати особисто. Якщо виготовлення/персоналізація відбувається децентралізовано, то документ готується в присутності заявника.

Загальною тенденцією є те, що все більше країн ЄС відмовляється від децентралізованої обробки документів і переходить до централізованої. Всього 8 із 15 країн-членів ЄС використовують централізований процес персоналізації (а з 2004 р. – 9).

Причини переходу до централізованої системи такі:

- збільшується якість та надійність процесу персоналізації;
- для розподілу бланків паспортів не потребується спеціальна система забезпечення (логістика);
- немає необхідності зберігати бланки паспортів в децентралізованих пунктах (при цьому зменшується можливість їх крадіжки);
- витрати на введення нових паспортів чи нових ступенів захисту скорочуються і спрощуються.

#### 4. Встановлення справжності документів та їх авторизація.

Автоматична безконтактна чіпова технологія з застосуванням полікарбонатних носіїв дає можливість зчитувати дані безконтактно [5]. Процес автоматичної перевірки можна поділити на три етапи.

При автоматичній перевірці контроль першого та другого рівнів не здійснюється – перевіряючий не бере участі в перевірці захисту, невідомість якого встановлюється за допомогою криптопроцесора, який на відміну від чіпу пам'яті може виконувати криптографічні розрахунки. В чіпі зберігаються три основних види інформації:

- біометричні характеристики володаря, які записані у відповідності до логічної структури даних (ЛСД – рекомендований ІКАО стандарт для зберігання даних про володаря документа, включаючи біометричні дані. Стандарт визначає застосування технологій зберігання даних в проїзних документах);

- ключ документа. Асиметрична криптографія використовує парні ключі для шифрування та обміну інформацією. Пара ключів складається з таємного (особистого) ключа та відкритого ключа. Якщо інформація була закодована з використанням відкритого ключа, її можна декодувати за допомогою відповідного закритого ключа. В результаті зашифрованої інформації може прочитати тільки володар таємного ключа. Цей процес дає можливість кодувати інформацію та використовувати відкритий ключ для засвідчення справжності;

- біосертифікат – цифровий сертифікат, що містить низку біометричних показників в електронному форматі.

Біосертифікат містить такі види інформації:

- хешований номер – розраховується відносно визначеного обсягу даних за допомогою стандартного алгоритму. Незважаючи на унікальність номера, фактичні дані не можуть бути із нього витягнуті, це забезпечує цілісність даних, що перевіряються без їх розголошення;

- хешовані дані МЗЗ (машинозчитувальна зона) – застосування безконтактно чіпової технології обумовлює введення спеціальних заходів, що спрямовані на захист особистої інформації володаря документа. Чіп зберігає не особисті дані, а хешований номер, розрахований на основі особистих даних;

- хешовані дані ББД (блок біометричних даних) – біометричні показники володаря – отримують з ЛСД та заносяться в сертифікат як хешований номер;

- відкритий ключ;

- підпис органа, що видав документ (в сертифікаті вміщується електронний підпис, що підтверджує інформацію про повноважний орган влади, який видав сертифікат та про відсутність підроблення сертифіката).

Після видачі володарю документа, перевірою обладнання використовується для зчитування як МЗЗ, так і біосертифіката. В перевірою обладнанні використовується відкритий ключ для перевірки справжності електронного підпису на біосертифікаті. Щоб пересвідчитися, що в МЗЗ не були зроблені підміни, обладнання перетворює дані МЗЗ, використовуючи стандартний алгоритм розрахунку хешованого номера МЗЗ, що занесений в біосертифікат. Результат перетворення порівнюється з хешованим номером МЗЗ, який занесений в біосертифікат.

#### 5. Вітчизняні паспорти.

На основі тенденцій розвитку документів в світовій практиці у нас було зроблено висновок про доцільність в даний час застосування в паспортних документах України таких біометричних характеристик особи, як лінії папілярного візерунка в комплексі з експертною оцінкою фотографії обличчя та підпису особи. Ці характеристики можна зберігати як в комп'ютерній базі даних, так і в документах, що посвідчують особу, виготовлених за сучасними технологіями, які дозволяють записувати цифрову інформацію в документах. Ці параметри до нинішнього року відповідали сучасним міжнародним вимогам.

Постановою Кабінету Міністрів України від 2.08.1996 р. № 898 започатковано роботи, пов'язані з створенням Єдиної державної автоматизованої паспортної системи, яка забезпечуватиме облік громадян за місцем проживання з застосуванням комп'ютерної мережі на єдиних принципах їх ідентифікації (із використанням особистих (ідентифікаційних) номерів громадян, від цифрового образу особи і біометричної ідентифікації) і взаємодії з базами даних інших інформаційних систем (як вітчизняних, так і іноземних), а також видачу громадянам паспортів, що оформлюватимуться за єдиною технологією.

Функціонально система складатиметься з підсистем: ідентифікації особи, обліку громадян, документування громадян, запиту та аналізу даних, взаємодії з зовнішнім середовищем, контролю доступу і захисту інформації. Система створюється як найважливіша складова частина Державного реєстру фізичних осіб. До організаційної структури такої системи входять Центр виготовлення документів із цільовим банком даних, 27 регіональних центрів та 850 паспортних відділів на місцевому рівні.

До структури інтегрованої бази даних ЄДАПС нале-

жать:

- ідентифікаційна інформація – цифрове фото обличчя, особистий підпис, облікова інформація – особистий номер, прізвище, ім'я, по-батькові, стать, дата і місце народження, батьки, сімейний стан, діти, місце проживання, військовий обов'язок, освіта, місце роботи, громадянство;

- документи – типи документів, номер документа, причина видачі, орган, що оформив документ, вилучені документи, дублікати документів, обмежене використання, знищені документи;

- події – перелік облікових даних, перелік ідентифікаційних даних, переміна даних щодо документів, міграція, перетин кордону, смерть, судові рішення;

- нормативно-довідкова інформація – державні та відомчі класифікатори, ДСТУ, службові класифікатори.

В даний час йде інтенсивна підготовка до переходу на нові паспорти [6, 7]. Документами, що посвідчують особу громадянина України, є паспорт громадянина України, паспорт громадянина України для виїзду за кордон, проїзний документ дитини для виїзду за кордон, дипломатичний паспорт України, посвідчення особи на повернення в Україну та інші, всього 8 найменувань. Загальна чисельність населення, якому треба буде обміняти/видати паспорти громадянина України, складає близько 40 млн. осіб.

В Україні запроваджено сім машинозчитувальних документів, що призначені для візуального і машинного читування (шість типів паспортів та машинозчитувальна візова етикетка). На картках розміщені зона візуальної перевірки, машинозчитувальна зона з використанням технології оптичного розпізнавання знаків, зона співіснуючих технологій. Можливість динамічного запису (перезапису) інформації складає не менше як 128 байт. Можливість статичного зберігання машинозчитувальної інформації складає не менше 2048 байт.

Уніфікація інформаційних відомостей здійснюється застосуванням 7 спеціальних зон, де розміщуються обов'язковий заголовок, обов'язкові та необов'язкові елементи особових даних та даних документів, підпис власника, ідентифікатор системи та ін. Структура машинозчитувальної інформації паспорта громадянина України: верхній машинозчитувальний рядок – тип документа; держава, що видала документ; прізвище, ім'я та по-батькові; нижній машинозчитувальний рядок – персональний номер; громадянство; дата народження (рік, місяць, день); стать; термін дії документа (рік, місяць, день); персональний номер; необов'язкові елементи даних; контрольні цифри; загальна контрольна цифра.

Компонування зони машинного читування прово-

диться із застосуванням таких співіснуючих технологій: контактні або безконтактні чіпи, магнітна стрічка, оптична пам'ять, двомірний штрих-код. Прикладне програмне забезпечення функціонує в середовищі операційних систем WINDOWS NT, WINDOWS 95 та OS2. Підтримується алфавіт державної та інших мов, що передбачені ЄДАПС, забезпечується інтерфейс в СКБД ORACLE та DB2 та можливість внесення інформації до паспортних документів за визначеними координатами.

Паспорти розроблено на рівні аналогічних документів провідних країн світу, а за деякими параметрами вони перевищують його. В даний час йде робота з створення регіональної інфраструктури по підготовці до видачі нових паспортів, оснащення їх відповідною технікою, підготовкою спеціалістів. На поліграфічному комбінаті "Україна" проводиться реалізація відповідного пілотного проекту по виготовленню паспортів для виїзду за кордон, створюються та відпрацьовуються канали зв'язку, системи підготовки інформації, передачі її по створеним каналам у відповідні банки даних, відпрацьовується координація такої роботи. В даний час технічні можливості комбінату вже дозволяють виготовляти 1000 паспортів на день.

#### ЛІТЕРАТУРА

1. Шевчук А.В., Музика В. Система захисту цінних паперів та документів суворого обліку – наукоємна проблема державного масштабу // Друкарство. -2002. -№ 4. – Липень-серпень. -С.72-74.
2. Валиев С., Эльтазаров Б. Защита ценных бумаг. -М.: ЧеРо, 1997.
3. Бувько М.М. Ідентифікаційні картки: минуле, сучасне, майбутнє. -К.: УкрІНТЕІ, 2000.
4. Григор'єв С.Ф., Глива В.А., Давидюк А.Д., Яценко В.В. Методи захисту пластикових карток –К.: УкрІНТЕІ, 2000.
5. Григор'єв С.Ф., Глива В.А., Давидюк А.Д., Яценко В.В. Тестування пластикових карток –К.: УкрІНТЕІ, 2000.
6. Шевчук А.В., Музика В.П. Технологічні проблеми виготовлення вітчизняних високозахисних паспортів // 36. наук. пр. Видав.-поліграф. фак. НТУУ КПІ. -2003. -№ 1. -С.46-50.
7. Шевчук А.В., Музика В. Виготовлення та захист вітчизняних паспортних документів // Друкарство. -2003. -№ 5. Вересень-жовтень. -С.12-16.

Надійшла до редколегії 09.09.2004

#### ШЕВЧУК А.В. НОВОЕ ПОКОЛЕНИЕ ВЫСОКОЗАЩИЩЕННЫХ ДОКУМЕНТОВ СТРОГОГО УЧЕТА ДЛЯ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ

Рассмотрены вопросы создания персонифицированных документов идентификации личности; приведены биометрические методы их защиты от подделки и фальсификации; рассмотрены новые виды паспортов и принципиальные требования к их конструкции и дизайну. Описана процедура внесения персонифицированных данных, система автоматизированной проверки и установления неподдельности паспортных документов.

\*\*\*

#### SHEVCHUK A.V. NEW GENERATION OF HIGH SECURE IDENTITY DOCUMENTS

Questions of creation person documents of identification of the person are considered; biometric methods of their protection against a fake and falsification are given; new kinds of passports and basic requirements to their design and design are considered. Procedure of entering person the data, system of the automated check and an establishment of genuineness of passport documents is described.