підвищення кваліфікації працівників. Коли фотоекспонуючий пристрій на світлочутливий матеріал буде замінено пристроєм експонування офсетних пластин, оператори повинні вільно володіти комп'ютером і повністю розуміти всі найдрібніші деталі нового технологічного процесу.

Таким чином, виявлено основні технологічні особливості застосування технології К–ДФ і запропоновано методику оптимального впровадження її в умовах реального виробництва. Невирішеним залишається завдання оптимального підбору технології К–ДФ для різноманітних друкарень.

1. Бауфельд У., Дорра М., Рознер Х. Передача информации и печать. М., 1998. 2. Допечатное оборудование / Ю.Н.Самарин, Н.П.Сапошников, М.А.Синяк. М., 2000. 3. Запоточний В.Й. Новітні друкарські технології. Львів. 1996. 4. Мельничук С.І., Ярема С.М. Офсетний друк: Навч. посіб.: У 2 кн.: Кн. 1. Технологія та обладнання додрукарських процесів. К., 2000. 5. Практика фальцювання: від спуску шпальт до готової продукції. К., 2001. 6. Ющик О.В. Моделирование формирования монтажных спусков полос на формы // Труды ВНИИ полиграфии. Т. 36. Вып. 2. М., 1986. 7. Ющик О.В. Моделирование процессов формирования монтажных спусков полос при автоматизированном изготовлении печатных форм книжно-журнальных изданий // Тезисы докладов Всесоюзн. совещ. по методам расчета полиграф. машин-автоматов. Львов, 1987. 8. Ющик.О.В. Особенности формирования монтажных спусков сверстанных книжно-журнальных полос на печатные формы с использованием ЭВМ // Тезисы докладов Третьей научно-практ. конф. молодых ученых и специалистов печати «Печать. Молодежь. Рынок». М., 1992.

УДК 655.027

М.В. Якимець, І.З. Миклушка

ЗАХИСТ ЕЛЕКТРОННИХ ДОКУМЕНТІВ МЕТОДОМ ЦИФРОВОГО ПІДПИСУ

Пропонується метод створення електронного підпису на основі криптографії. Рекомендуються алгоритм криптуваня та блок-схема програмного продукту.

Предлагается метод создания электроннной подписи на основе криптографии. Рекомендуются алгоритм криптирования и блок-схема программного продукта.

У кінці звичайного листа чи документа автор, звісно, ставить свій підпис. Це зазвичай має дві цілі. По-перше, отримувач листа, порівнюючи підписи, має можливість переконатися, що лист не є фальшивкою. По-друге, особистий підпис є для документа юридичним гарантом авторства. Якщо підробити підпис на папері досить складно, тому що існують ефективні криміналістичні методи його ідентифікації, то електронний цифровий підпис можна отримати значно простіше. Повторити послідовність бітів, просто скопіювавши її, або непомітно ввести в документ нелегальні виправлення може навіть програміст невисокої кваліфікації. З поширенням електронних документів і засобів їх опрацювання постала проблема істинності й авторства документа. Існує безліч алгоритмів створення цифрового підпису, зокрема, найбільш простий і розповсюджений з них RCA [2].

Для доведення авторства того чи іншого електронного документа потрібно, щоб він був захищений електронним підписом [3]. Метод, що пропонується, полягає в дописуванні до графічного файла певних кодів, які отримують на базі шифрувальних алгоритмів. Відомості про автора кодуються згідно з алгоритмом (рис.1).

Для захисту криптографічних кодів використовується їх контрольна сума. Тобто, якщо змінити хоча б один біт інформації, то контрольна сума, що записана у файлі, не буде збігатися з контрольною сумою, порахованою при читанні відомості про автора. При цьому одержуємо повідомлення, що відомості про автора були змінені.

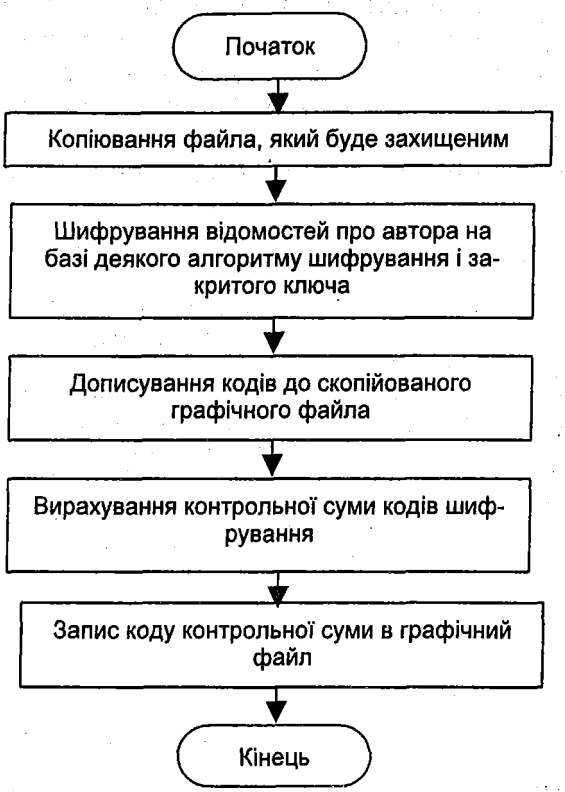

Рис. 1. Блок-схема алгоритму криптування файла

Дана програма реалізована для графічного формату JPEG, оскільки він є найпоширенішим в Інтернеті [1]. Блок-схема програми зображена на рис.2.

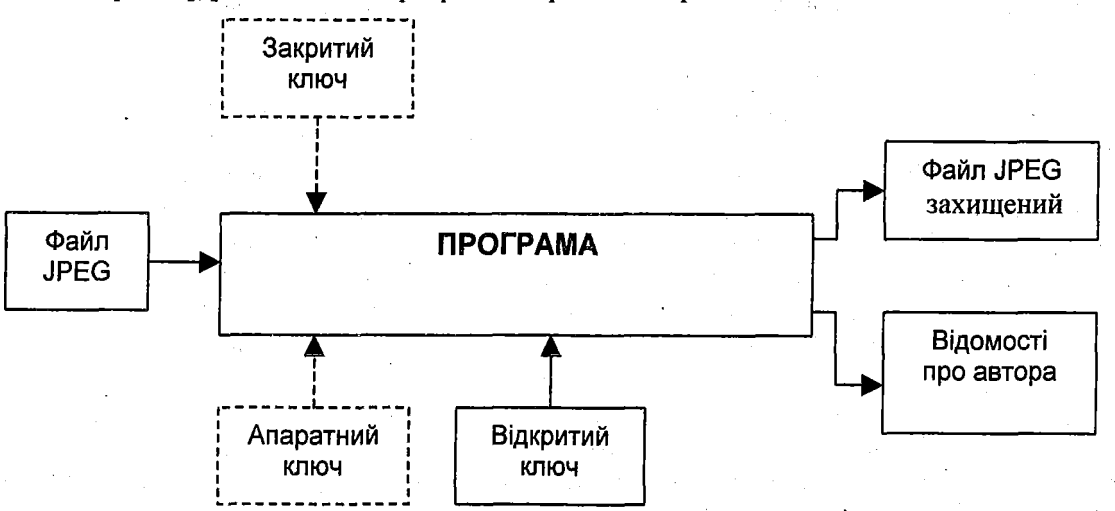

Рис.2. Блок-схема програми

Електронний ключ, яким захищається сама програма, планується зробити апаратним. Влаштовується він в один з портів комп'ютера (наприклад, в USB) і містить в собі логічну схему. При відсутності апаратного ключа неможливо запустити виконуючий файл програми криптування.

Закритий ключ, на базі якого здійснюється шифрування, генерується самою програмою і записується на гнучкий диск.

Відкритий ключ додається користувачеві разом з програмою. Програма для зчитування відомостей про автора не захищається апаратним ключем. За допомогою відкритого ключа і

програми можна переглянути відомості про автора, але не можна їх змінити. Змінити цю інформацію можна лише при наявності як апаратного, так і закритого ключа шифрування тексту.

Дана програма проста в реалізації і має два рівні захисту – апаратний і програмний. Такий метод захисту є новим і досить ефективним.

1. Климов А.С. Форматы графических файлов. К., 1995. 2. http://edocs.al.ru. 3.http://www.citforum.ru/internet/securities/cryptobook07.shtml.

УДК 655.28:681

І.В. Піх

СИСТЕМОТЕХНІЧНА КОНЦЕПЦІЯ В АНАЛІЗІ ІНГРАДІЄНТІВ ФОРМАТІВ ДАНИХ КНИЖКОВИХ ВИДАНЬ

Описується один з можливих підходів до аналізу інградієнтів форматів даних книжкових видань з метою подальшої їх оптимізації та поліпшення якості друкованої продукції. Розглядаються особливості прийняття рішень у складній ієрархічній системі.

Описывается один из возможных подходов к анализу инградиентов форматов данных книжных изданий с целью последующей их оптимизации и улучшения качества печатной продукции. Рассматриваются особенности принятия решений в сложной иерархической системе.

При дослідженні задач, пов'язаних з проектуванням даних і їх складових для комп'ютерних видавничих систем (КВС), будемо користуватися поняттями й засобами, що стосуються загальної теорії систем [2], зокрема одного з її напрямів – теорії ієрархічних багаторівневих систем [3]. Незважаючи на зростаючий обсяг публікацій з цих питань, теорія систем у конкретному її застосуванні вимагає додаткових досліджень, що стосуються задач синтезу та аналізу систем і даних, які опрацьовуються ними, визначення їх функцій і структури, вибору апарату моделювання для загального проектування й створення алгоритмів реалізації функцій. Одним з визначальних при цьому є поняття системи, яке і сьогодні не має єдиного й строгого визначення. Причина полягає, очевидно, у тому, що для кожного класу або типу систем характерна певна просторова або функціональна замкнутість [4]; їх різнорідність також накладає свій відбиток на поняття системи.

Визначимо систему як сукупність елементів різної природи, які взаємодіють між собою, є єдиним цілим і призначені для досягнення певної мети. Елементами системи вважаються її частини, зв'язки між якими визначаються структурою системи. Поділ на елементи залежить від глибини та рівня структурування системи. Зв'язки між елементами системи повинні бути міцнішими від їх зв'язків із зовнішнім середовищем, що спричиняє входження елементів у рамки системи. Порушення зв'язків, звичайно, призводить до зміни функцій системи або до її руйнування чи припинення функціонування.

Життєдіяльність будь-якої системи передбачає наявність входу в систему і виходу з неї. У "правильно" зреалізованій системі повинен бути головний елемент (диспетчер), що визначає задачі і функції інших елементів і керує їхньою роботою.

Ми розглядатимемо тільки такі системи, які для свого функціонування потребують керуючих дій. Подібні системи називаються кібернетичними або керованими. Параметри та вихідні дані в них можуть набувати різних значень, що викликає зміну стану або значень елементів, зв'язків між ними, а отже, і загального стану системи. Межі зміни параметрів і вихідних даних заздалегідь обумовлюються.

Кардинальним моментом створення та ефективного застосування систем, основним робочим інструментом яких вважаються програми, є наявність комп'ютерів. Принципово нові моменти їх використання свого часу відзначав академік В.М. Глушков [1]. Вони полягають у: різкому збільшенні числа регульованих параметрів (від 2–5 у звичайних регуляторах до багатьох сотень і навіть тисяч); можливості реалізації складних алгоритмів управління; універсаль-