УДК 683.15

***Б. В. Дурняк, В. З. Пашкевич***

# ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІДЕНТИФІКАЦІЇ ПОЛІГРАФІЧНИХ ДОКУМЕНТІВ

*Досліджуються методи захисту документів, що грунтуються на використанні графічних засобів. Запропоновано проводити ідентифікацію документів на основі вимірювання окремих параметрів, зокрема, міри насиченості фрагмента графічного образу, міри роздільності двох суміжних ліній узору,зміни роздільності двох суміжних ліній, локальної густини засобу захисту.*

*The methods of defence of documents, that are based on the use of graphic facilities are explored. It is offered to conduct authentication of documents on the basis of measuring of separate parameters, in particular, measures of saturation of fragment of graphic appearance, measures of divisible of two contiguous lines of pattern, changes of divisible of two contiguous lines, local density of mean of defence.*

Сьогодні поліграфічні документи широко застосовуються як у соціальній сфері, так і в сфері управління. Велика кількість їх фальсифікацій може призвести до критичної ситуації в системі управління. У зв'язку з тим завдання захисту документів від підробки є надзвичайно актуальними.

У рамках цієї роботи досліджуються методи захисту документів, що ґрунтуються на використанні графічних засобів, на противагу тим, які базуються на порівнянні з еталонними зразками, що потребує значних ресурсів часу і пам'яті. У результаті проведених нами досліджень існує можливість проводити ідентифікацію документів на основі вимірювання окремих параметрів графічних засобів захисту, зокрема, міри насиченості фрагмента графічного образу, міри роздільності двох суміжних ліній узору, зміни роздільності двох суміжних ліній, локальної густини засобу захисту. Для перевірки передбачуваної ефективності використання запропонованих вище параметрів графічних засобів захисту документів при їх ідентифікації на комп'ютерних моделях проводили ряд експериментів з визначення:

кількості точок, застосовуваних у межах одного фрагмента графічного образу для встановлення комплектів базових параметрів;

кількості фрагментів для необхідного проведення вимірювань параметрів;

величини ризику використання захищених документів.

У процесі двох перших експериментів потрібно було імітувати атаки на документ, який ідентифікується, вибрати базовий тип графічного засобу захисту, визначити величини загроз для різних варіантів досліджень.

Атаки на документ являють собою підробку засобів захисту, яка відповідно до заданої величини загрози полягає в точності відтворення елементів графічного засобу захисту. Оскільки графічний засіб захисту аналізується в дискретному просторі (у даному випадку в дискретно визначеній площині), то для спрощення процесів елементом дискретної площини було вибрано одиничний квадрат. Таким чином, усі вимірювання, що проводилися в рамках експериментів відповідно до базових одиничних квадратів, і точки, які вибиралися для реалізації досліджень щодо встановлення величин параметрів, визначалися згідно з масштабом за введеною сіткою квадратів.

Базовим засобом захисту був графічний образ — узор типу віньєтки. Для формування графічних образів використовувалися стандартні графічні пакети, що забезпечують широкі можливості для їх створення та модифікації [4].

Процеси ініціації атак полягали в наступному і включали вибір:

точок модифікації елементів графічного образу стосовно одного документа;

фрагмента графічного образу, у рамках якого передбачалося проводити модифікацію елементів образу;

величини відхилень параметрів або елементів графічних засобів захисту, що ідентифікують атаку як таку.

Перераховані вище процеси ґрунтуються на використанні генераторів псевдовипадкових послідовностей, які досить широко досліджуються у зв'язку з їх використанням в інших задачах, наприклад у галузі криптографії [2]. Для реалізації необхідних процедур вибрано одну із схем реалізації стохастичного параметра псевдовипадкової послідовності, що ґрунтується на використанні R-блока, який описується співвідношенням

$$R_H(A,B) = H((m_A + B) \bmod 2^n), \qquad (1)$$

де $m_A$ — адреса елемента таблиці $H$, що вміщає код $A$, або $H(m_A)=A$.

Суть роботи блока R полягає в зчитуванні вмісту комірки таблиці $H$, що циклічно зміщається на $B$ позицій у бік старших адрес, відносно комірки, яка вміщає код $A$. Величина такого зміщення може ґрунтуватися на використанні алгоритмів створення таблиць заміни.

В експериментах реалізація атаки полягала в модифікації графічного засобу захисту, що досліджувався в рамках вищезазначених процесів. Це означає, що еталонний образ графічного засобу захисту змінювався наступним чином. На підставі використання псевдовипадкового генератора вибиралися координати точок для модифікації відповідних елементів графічного образу. Випадковим чином визначалися величини відхилень, що вимірювалися в абсолютних одиницях. Модифікація точок здійснювалася в межах, окреслених дискретами, що задаються елементарними квадратами, які визначають топологію відповідної площини. Діапазон величини відхилень у графічному образі вибирався виходячи з величини значень параметрів загроз, що

характеризують засіб захисту. Оскільки величина значень параметрів загрози визначає допустимі відхилення в оригінальних документах ($\pm\delta_z$), то діапазон відхилень в атакованого документа вибирали за співвідношенням

$$D_{Ai}(P_i) = [d_z \pm D_M], \quad (2)$$

де $\Delta_A(P_i)$ — величина відхилення значень параметра $P_i$ при реалізації атаки $A_i$; $\Delta_м$ — залежно від знака максимальне і мінімальне відхилення параметра $P_i$ при модифікації, що відбувається при реалізації атаки $A_i$ у кожному окремому випадку (величина відхилень $\Delta_{мi}$ вибиралася в межах заданого діапазону $\Delta_{Ai}$ випадковим чином).

У процесі даного експерименту потрібно було встановити, чи виявлення відхилень у засобі захисту на основі вимірювання запропонованих параметрів і порівняння їх з еталонними значеннями є ефективним для викривання підробок. Одним з важливих аргументів впровадження відповідних параметрів є те, що завдяки їх використанню з'являється можливість перевіряти оригінальність документа не порівнянням всього графічного образу засобу захисту з еталонним зразком, а зіставленням величин запропонованих параметрів з їх еталонними значеннями. Більше того, такі еталонні значення є різними для рівнів захисту, що визначається величинами параметрів загроз відповідних засобів захисту. Тому виникає задача вибору точок і фрагментів, де проводиться вимірювання величин параметрів, що перевіряються при ідентифікації документів. Один із способів розв'язку цієї задачі полягає у виборі на графічному образі координат для визначення величин параметрів, що контролюються, на основі використання генераторів псевдовипадкових послідовностей. Очевидно, що такі генератори не повинні бути схожими з генераторами, використовуваними для моделювання атак. При проведенні експериментів для вибору точок, в яких параметри контролювалися, застосовували генератор Галуа, що реалізується на регістрах зсуву з лінійними оберненими зв'язками (LFSR) [3] й описується примітивним многочленом

$$\Phi(x) = x^8 + x^7 + x^5 + x^3 + 1. \quad (3)$$

Серед параметрів, запропонованих у роботі, є геометричні та графові. У нашому експерименті використовувалися геометричні параметри. Це зумовлюється тим, що графові, в основному, застосовуються для аналізу документів у випадку чергового тиражу із санкціоновано модифікованими параметрами графічного образу. Крім того, графові параметри потребують аналізу, що подається у вигляді графового наближення. Очевидно, що оперативне використання цих параметрів для ідентифікації документів доцільне тоді, коли рівень безпеки документів, який повинні гарантувати графічні засоби захисту, є вищим від рівня, забезпечуваного лише геометричними параметами захисту. Тому потреба використання графових параметрів при ідентифікації визначається методикою, яка ґрунтується на певних вимогах щодо гарантії необхідного рівня безпеки документа.

Методика проведення експериментів щодо визначення ефективності ідентифікації документів полягає в наступному. У графічний образ вводяться модифікації його елементів згідно з вищенаведеними умовами використання псевдовипадкових генераторів. Після введення певної кількості модифікацій реалізується процес ідентифікації документа шляхом перевірки значень геометричних параметрів, точки вимірювання яких вибираються випадковим чином. Ідентифікування полягає у виборі саме тих точок, в яких передбачається проводити контрольне вимірювання з використанням власного псевдовипадкового генератора, завдяки чому координати точок для вимірювання значень параметрів є випадковими. На цьому етапі ідентифікації здійснюється кілька вимірювань усіх геометричних параметрів. Оскільки всі параметри важко звести до єдиної одиниці вимірювань, то вибирається деякий діапазон значень для кожного з параметрів, а виміряна величина переводиться в проценти. Відповідно, переводиться в проценти різниця між виміряними величинами параметрів та еталонними значеннями. Остання порівнюється з певними параметрами загроз, які відповідають документам, що перевіряються. Якщо величина параметрів загроз більша за обраховану вище різницю, то документ визначається як оригінальний. Якщо ця різниця більша від величини відповідного параметра загрози, то документ вважається підробленим, або атакованим певною небезпекою. Описані вище дії називатимемо одним циклом експериментальних досліджень ефективності використання параметрів ідентифікації. У межах одного циклу проводиться $m$ модифікацій і, відповідно, $m$ ідентифікацій графічного образу. В наступному циклі експерименту кількість елементарних кроків, що виконуються в одному циклі, збільшується на величину $\Delta\kappa_i$. Тоді $m_{i+1}=m_i+\Delta k_i$, при цьому $\Delta\kappa_i$ може дорівнювати одиниці. Якщо в межах одного циклу число кроків, на яких документ визнаний атакованим, не перевищує заданої величини в процентному відношенні до загальної кількості кроків циклів, наприклад, рівної $\varepsilon$, то документ приймається як оригінальний, і навпаки. У кожному наступному циклі експерименту значення збільшується на величину $\sigma_i$. Отримані результати відображено графічно на рис. 1.

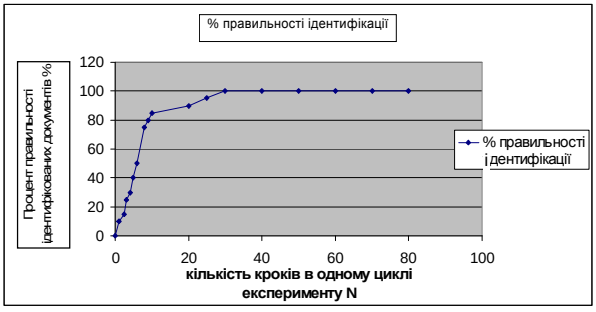


**Рис. 1. Залежність між кількістю правильно ідентифікованих документів (у процентах) і числом кроків ідентифікації** в межах одного циклу перевірки $N$

Дані кожного кроку, реалізованого в межах одного циклу, повторювалися шляхом порівняння графічного образу з еталонним. Суть такої перевірки полягала в зіставленні модифікованого образу з еталонним в цілому, по всіх точках, якими описується відповідний графічний образ. Очевидно, що міра реальної збіжності залежала від параметрів загроз. Згідно з методикою експерименту, вважали, що цей спосіб забезпечує 100%-ний контроль оригінальності документа. Тому на рис. 1 зображено криву, яка відображає процент правильно ідентифікованих документів, тобто таких, що є оригінальними, при використанні опрацьованого підходу.

Запропонований підхід при використанні 20 кроків ідентифікації документа забезпечує 93,75% достовірності результатів ідентифікації, а 30 кроків — майже 100%. При цьому максимальне число точок, які описують відповідний фрагмент графічного образу в даному експерименті, на порядок більше за максимальну кількість кроків, що реалізувалися в експерименті, або $M_{max}$=80x10=800 точок.

Методика проведення експериментів з визначення кількості точок, що використовуються в межах одного фрагмента графічного образу, для встановлення комплектів нормативних параметрів, полягає в наступному. У даному випадку під комплектом нормативних параметрів розуміється кількість точок, для яких визначаються ці параметри. Оскільки базова процедура визначення параметра — це вимірювання відстані між вибраними точками образу й інші геометричні параметри, крім насиченості, є похідними, то знаходження одного параметра здійснюється шляхом усереднення значень параметрів, визначених у різних точках. Модифікація фрагментів графічного образу проводиться на основі використання псевдовипадкових генераторів. Відповідний експеримент щодо вибору точок, за якими проводяться вимірювання, повторюється. Кількість таких експериментів залежить від величини змін у вимірюваних параметрах при проведенні окремих досліджень. Якщо величини цих параметрів перестають змінюватися, то серія експериментів закінчується, а точками, де повинен проводитися контроль, вибираються ті, в яких значення параметра ідентифікації є найбільшим. На рис. 2 крива відображає величину зміни вимірюваного параметра. Останній приводиться до значення параметра в еталонному зразку. Для цього зміна вимірюваної величини береться як абсолютне число і визначається за формулою

$$D\mathrm{x}_i^* = \frac{\left|D x_i\right|}{\left|D x_i^e\right|}, \qquad (4)$$

де $\Delta x_i$ — виміряна величина; $\Delta x_i^e$ — еталонне значення відповідної величини.

Експеримент з визначення необхідної кількості фрагментів, в яких проводяться вимірювання, грунтується на повторенні вищеописаного. При цьому на основі використання генератора псевдовипадкових послідовностей

вибирали різні фрагменти графічного образу, що вважався еталонним, та формували різні величини загроз. Фізична інтерпретація величини загрози являє собою допустиму величину відхилень значень параметрів, що контролюються. Ці величини відхилення приймалися для різних експериментів у межах окремих фрагментів різними. Відповідні фрагменти, як і величини загроз, вибирали випадковим чином. Після того для кожного експерименту формували фальсифіковані зображення зі зміненими величинами параметрів, які визначаються на основі вимірювання відстаней між точками ліній. Оскільки кількість фальсифікованих фрагментів у кожному випадку була відома, то при порівнянні випадково вибраних фрагментів для контрольних перевірок виявилося, що із збільшенням величини загрози зростало число невиявлених фальшивих документів. Але через недертермінованість між вибором фрагментів для фальсифікації та їх вибором для зміни величини загрози кількість успішно атакованих документів збільшувалася (рис. 3).

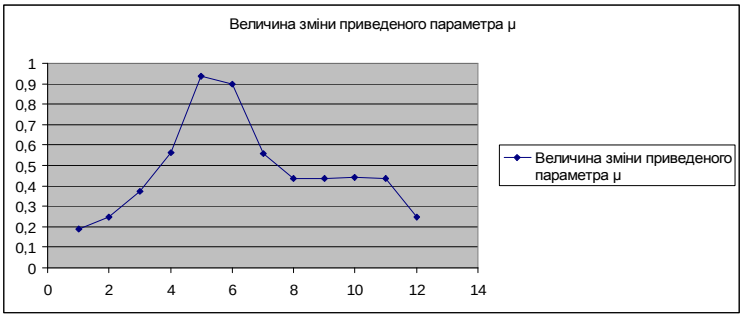


**Рис. 2. Залежність величини зміни приведеного параметра *m* від кількості кроків в одному експерименті**

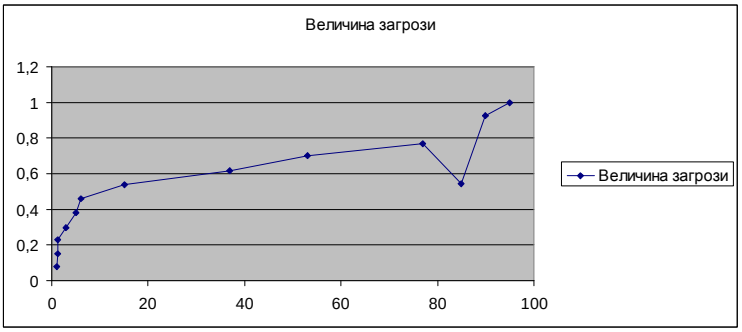


**Рис. 3. Залежність величини загроз від кількості успішних атак на документи**

Кількість успішних атак визначається в процентах від їх загального числа. Величина загроз встановлюється як відношення допустимого відхилення, що визначається величиною загрози, до відстані, заданої в еталонному зразку.

З отриманих даних випливає, що існує деяке критичне значення допустимої величини загроз, після якого кількість успішних атак різко зростає.

Результати проведених нами експериментів показали, що за допомогою запропонованих параметрів графічних засобів можна забезпечити необхідний рівень захисту документа.

1. Зенин О. С., Иванов М. А. Стандарт криптографической защиты XXI века — AES. Теория конечных полей. М., 2002. 2. Іванов М. А., Чугункою И. В. Теория применения и оценка качества генераторов псевдослучайных последовательностей. М., 2003. 3. Осмоловский С. А. Стохастические методы передачи данных. М., 1991. 4. Пономаренко С. Corell DRAW 9.Спб., 2000.

УДК 655.3.026.32

***П. Б. Петрик, З. В. Чоп, Д. А. Вакуліч***

## ВИГОТОВЛЕННЯ ЛИСТІВОК У ЗРАЗКОВІЙ ДРУКАРНІ «БЛІЦ-ПРИНТ»: ТЕХНОЛОГІЯ, УСТАТКУВАННЯ, МАТЕРІАЛИ

*Проведено аналіз листівок, виготовлених у зразковії друкарні «Бліц-Принт». Описано найпоширеніші види листівок, матеріали, устаткування й технології, що використовуються для їх виготовлення та оздоблення.*

*The analysis of postcards which were produsedat the model printing-house «Blits-Print» has been realized. And it has been revealed the most common types of postcards, materials, equipment and technologies that are used in manufacturing and finishing.*

Листівка як об'єкт, за допомогою якого здійснюється спілкування, має певне соціальне, економічне, політичне та культурне значення, свою історію, філософію, естетику й етику, особливості дизайну. Найчастіше виготовляється поліграфічними способами, займає досить важливе місце в загальному обсязі видавничо-поліграфічного виробництва.

З огляду на значимість листівок виникла потреба у вивченні досвіду виготовлення й оздоблення їх на одному з відомих в Україні поліграфічних підприємств — у зразковій друкарні «Бліц-Принт».

Аналіз 90 листівок «Бліц-Принту» за 2006 рік показав (рис. 1 — 8), що найпоширенішими є такі види:

*за змістом* — «Вітаємо» (32,2 %);
*за стилем* — з текстовим написом без побажань (56,7 %);
*за розміщенням ілюстрацій* — книжкові (94,4 %);
*за форматом* — 268 х 190 мм (67,8 %);
*за фарбовістю* — 4+0 (55 %);
*за способом тиснення* — комбіноване (35 %);
*за використанням фольги* — золота (51,1 %);
*за кольором блістера* — золотий (54,4 %).