

УДК 346.5:351.862.6

АНАЛІЗ МОДЕЛЕЙ ЗАХИСТУ ПОЛІГРАФІЧНОЇ ПРОДУКЦІЇ

З. М. Сельменська, Ю. В. Грик, І. В. Огірко

*Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна*

Розглянуто вплив інформаційних технологій на поліграфічну продукцію, особливості захисту у сучасних видавничих структурах з огляду на інформаційно-комунікаційні технології.

Ключові слова: *інформаційні технології, інформація, засоби захисту електронних видань, захист поліграфічної продукції.*

Постановка проблеми. Захист інформації сьогодні набуває вагомого значення на державному рівні [1–4]. Інформація в електронному чи друкованому вигляді потребує новітніх способів захисту від фальсифікації. На сучасному етапі розвитку інформаційних технологій стає дедалі легше сфальсифікувати будь-яку документацію. Щоб підвищити рівень захисту, потрібно розробляти нові методи, відтворення яких потребує багато часу та зусиль. Ефективний захист має задовольняти критерії надійності та економічності. Чим вищий ступінь захисту, тим важче здійснити підробку. Сучасні технології дають змогу підробити буквально все, але тоді виникає питання чи вартує підробка затрачених зусиль та коштів. Основна мета захисту — зробити підробку нерентабельною. Зрозуміло, що зростання якості захищеності документів веде до підвищення вартості фальсифікації. Розглянувши різні випадки захисту документів, можна стверджувати, що розробляти захищений документ необхідно з урахуванням максимального захисту та рентабельності.

Аналіз останніх досліджень та публікацій. Відомо, що захищений документ має володіти властивостями: конфіденційності — бути захищеним від несанкціонованого ознайомлення; цілісності — бути захищеним від несанкціонованого спотворення, руйнування або знищення; доступності — бути захищеним від несанкціонованого блокування [2, 3].

Електронний або друкований документ може піддаватися таким наступним загрозам: фальсифікація документа; втрата деякої інформації; заміна деякої інформації; копіювання паперового носія; оцифрування даних; заміна документа. Отже, можна ідентифікувати такі загрози: часткова підробка; повна підробка; фальсифікація документу; фальсифікація персоналізованих атрибутів і реквізитів документа; крадіжка.

Мета статті — розглянути структуру системи захисту даних, яка містить засоби захисту, загрози, небезпеки від фальсифікаторів у поліграфічній продукції, вміння захистити свою продукцію яка знаходиться в електронному вигляді від атаки несанкціонованого доступу до ресурсів.

Виклад основного матеріалу дослідження. Поняття інформаційних технологій включають в себе різноманіття методів і способів управління концепцією її формування, сукупність всіх видів апаратно-програмних інформаційних засобів [1–3]. Інформаційні технології пов'язують з процесами збору, обробки, зберігання та цілеспрямованої передачі різноманітних даних, організованими на базі сучасних обчислювальних машин і систем, мережевих технологій, банків і баз даних і знань, різноманітного системного, прикладного та проблемно-орієнтованого програмного забезпечення.

У видавничій діяльності та поліграфії інформаційні технології використовуються в інформаційних процесах, а також стають виробничими технологіями через те, що на їх основі створюється кінцевий поліграфічний продукт (книги, журнали, газети, і інші поліграфічні продукти).

Для нових інформаційних технологій характерне наступне [2–6]:

1. Робота користувача здійснюється в режимі взаємодії із сучасними професійними програмними продуктами, максимально адаптованими до конкретних інтегрованих технологічних операцій.

2. Здійснюється інформаційна підтримка на всіх етапах підготовки і обробки інформації на основі інтегрованих баз або баз даних, які передбачають єдину уніфіковану структуру представлення даних, організацію їх зберігання, пошуку, відновлення та захисту.

3. Безпаперовий процес обробки інформації, за якого на папері фіксується лише остаточний варіант інформації. Всі інші верстки документів або матеріалів представлені в машинних кодах на спеціальних носіях.

4. Інтерактивний режим роботи користувача з використанням інтерактивної підтримки.

Загальноприйняті методи управління загрозами: стратегічне управління; тактичне управління. Документ, залежно від ступеня захищеності, може перебувати у: контрольованому оточенні; неконтрольованому оточенні; професійному оточенні. Внаслідок цього пропонуються рекомендації щодо управління, тобто формується методика протидії визначеній множині загроз та формуємо політику безпеки документа. На рис. 1 наведено формування комплексу засобів захисту у системі захисту інформації для друкованих та електронних документів, які перебувають у зовнішньому середовищі. Щоб захистити інформацію, розробляється програмне забезпечення, яке здійснювало б захист електронних та документів на етапі додрукарської підготовки.

Високий ступінь захисту поліграфічної продукції визначається трьома складовими: складністю технологічних процесів; обмеженням доступу до матеріалів та обладнання; новизною і закритістю методів, що застосовуються. Інформаційно-комунікаційні технології безпечного поліграфічного виробництва — сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів [1–7]. Технології, що забезпечують та підтримують інформаційні процеси, тобто процеси пошуку, збору, передачі, збереження,

накопичення, тиражування інформації та процедури доступу до неї. Інформаційна технологія безпечного поліграфічного виробництва — цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування. Інформаційна технологія безпечного поліграфічного виробництва — це сукупність методів, виробничих процесів та програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує виконання інформаційних процесів з метою підвищення їхньої надійності та оперативності і зниження трудомісткості ходу використання інформаційного ресурсу.

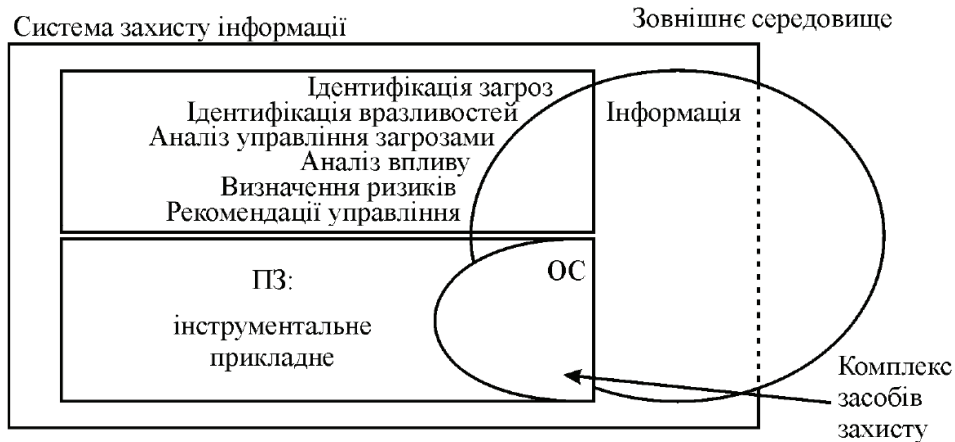


Рис. 1. Аналіз формування загроз

Розробляти і застосовувати складні технології, наприклад, металографічного, глибокого друку, використовувати спеціальні фарби і покриття, захисні ламінати, голограми не завжди доцільно з точки зору економічної ефективності. Застосування матеріалів зі спеціальними хімічними, фізичними властивостями створює необхідність застосування спеціального обладнання для визначення автентичності продукції.

Найпростішими, зручними і економічно доцільними є засоби захисту, що реалізуються на додрукарському етапі. Їх застосування не вимагає спеціального устаткування і матеріалів. При цьому залишається можливість їх використання для створення комбінованих засобів захисту.

Розроблення нових та вдосконалення існуючих методів захисту друкованих документів має велике значення для безпеки та захисту друкованих документів.

Безпечний друк включає в себе такі відомі технології, як водяні знаки, спеціальний папір, голограми, глибокий друк, мікро-друк, магнітні фарби, захисні нитки, антикопіювальні знаки, серійні номери, призматичне фарбування та інші. Ці методи повинні забезпечити промислові продукти та їх помилкові зміни. Основна роль охорони безпеки полягає в тому, щоб уникнути незаконних дій, таких як підроблення, фальсифікація, шахрайство, імітація та інші неправомірні дії.

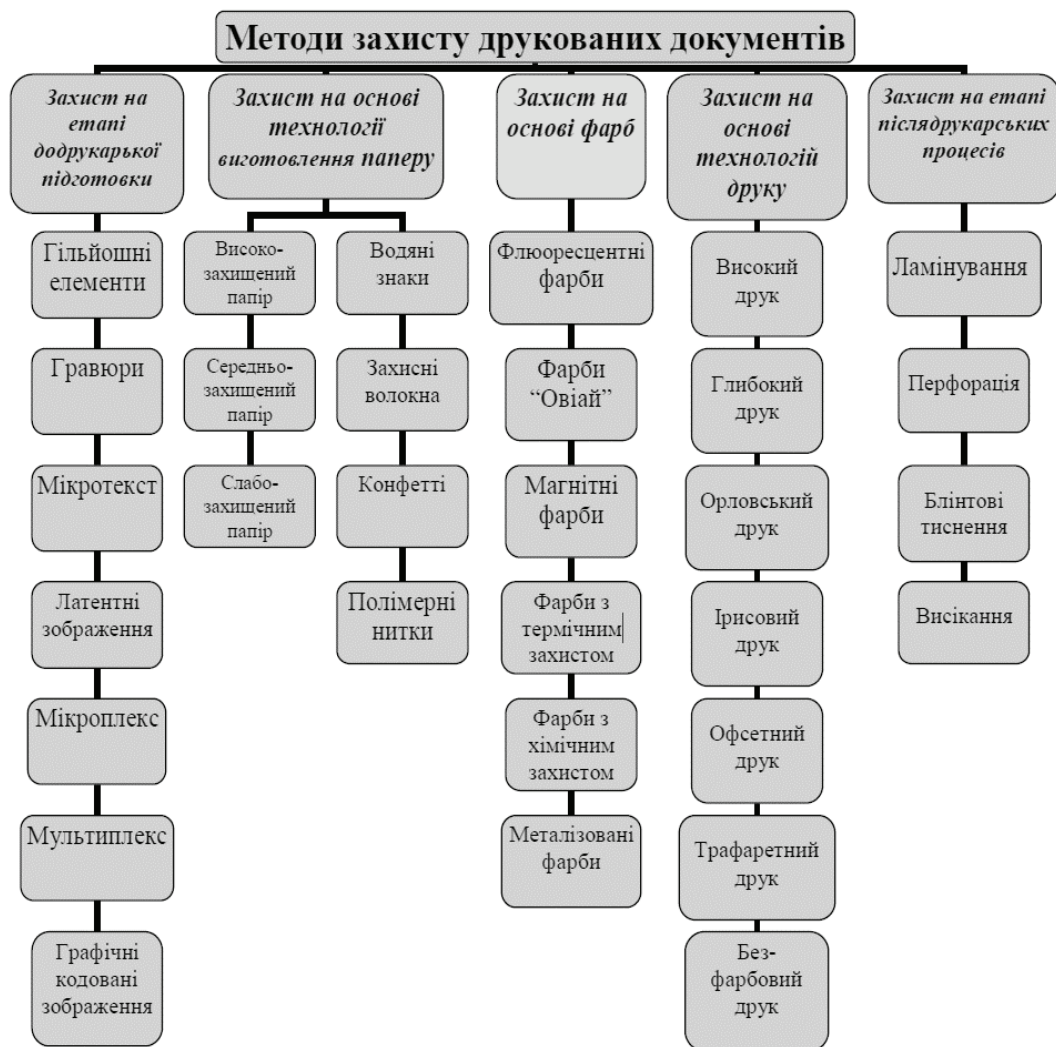


Рис. 2. Аналіз методів захисту друкованих документів

Глобальний друк на ринку безпеки сегментований на основі технології DOVID та голограми, міцні підкладки, захисні фарби, маркери, водяні знаки, нитки, біометрії, RFID та кодування. Ці технології далі розподіляються, оскільки DOVID та голограми включають кінєграм, альфаграм, ідентиграм, holoID, OVMesh, дифракційні ідентифікаційні пристрої (DID), trustseal, христаграм і секундот; захисні фарби включають глибокі чорнила, оптично змінні фарби OVI, оптично змінні магнітні чорнила OVMI, машино читані OVI, метамерні OVI, машино читані фарби, магнітні фарби та фотонні чорнила; нитки включають оптикс, прокатну зірку і рух; RFID та кодування включають чіп, чорнило та коди [8].

Висновки. В умовах розвитку інформаційного суспільства книги, журнали, газети і інші поліграфічні продукти залишаються засобом обміну соціальної

інформації. Нові інформаційно-комунікаційні прийоми не витісняють форми комунікації, що вже склалися, а інтегруються, що дає можливість редакторів ефективно працювати в інформаційному просторі, яке постійно ускладнюється. Яскравим прикладом тут може слугувати дедалі глибше проникнення комп'ютерних технологій у редакційно-видавничий процес, а також у сферу книгорозповсюдження. Тому майбутнім видавцям обов'язково необхідні знання, що поєднують у собі різні функції, пов'язані із виготовленням і друком видань, підготовки медійних продуктів тощо. Вміння захистити свій продукт від фальсифікації і розповсюдження несанкціонованих копій як поліграфічного продукту, так і в електронному вигляді. У такому випадку потрібні доволі ґрунтовні знання поліграфічних процесів та новітніх інформаційних технологій. Разом з основними правилами макетування та верстання треба ознайомитися з методами захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Огірко І. В. Цифрова безпека інформації як складова економічної безпеки. Всеукраїнська науково-практичної конференція «Економічна безпека України: стан, проблеми та перспективи». 22 квітня 2016 р. Львів, 2016. С. 4.
2. Ткаченко В. П., Огірко І. В., Огірко О. І. Математична модель оцінювання захисту WEB-сайтів. Сб. Полиграфические, мультимедийные и web-технологии. Т. 1. Харьков: ХНУРЕ, 2016. С. 98–101.
3. Ткаченко В. П., Огірко І. В., Пілат О. Ю., Огірко О. І. Метод оцінювання якості сайтів. 1-й Международ. науч.-техн. конф. (16–20 мая 2016). Полиграфические, мультимедийные и web-технологии. Харьков: ХНУРЕ, 2016. С. 96–97.
4. Огірко І. В., Огірко О. І. Математична модель оцінювання якості та захисту WEB-сайтів. науково-технічна конференція професорсько-викладацького складу, наукових працівників і аспірантів (16–19 лютого 2016 р.): тези доповідей. Українська академія друкарства. Львів, 2016. С. 133.
5. Огірко І., Огірко О. Інформаційні технології та моделі. Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення: Матеріали IV Всеукраїн. наук.-практ. конф. (18–20 травня 2017 р., м. Львів): Укр. акад. друкарства, 2017. С. 125–128.
6. Огірко І. В., Огірко О. І. Математичні моделі та методи безпеки. Актуальні проблеми економічної безпеки держави, регіону, підприємства. Всеукраїнська науково-практична конференція. 26 06 2017 р. Львів, 2017. С. 173–175.
7. Огірко І. В., Романюк О. П., Огірко О. І. Інформаційні технології книгодрукування та експертизи якості. Научное издание Белорусского государственного технологического университета. К 500-летию белорусского книгопечатания. Материалы III Международного форума. С. 254–258.
8. Google. Аналітика / Ринок захищеного друку. URL: <http://www.decisiondatabases.com/ip/257-security-printing-market-report>.

ANALYSIS OF MODELS FOR PROTECTION OF PRINTING PRODUCTS

Selmenska Z. M., Hryk Yu. V., Ohirko I. V.

*Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine*

The influence of information technologies on printing products, peculiarities of protection in modern publishing structures have been considered in view of the information and communication technologies.

Keywords: *information technologies, information, means of electronic publications protection, protection of printing products.*

Стаття надійшла до редакції 00.00.2018.

Наукове видання

Квалілогія книги

Book Qualilogy

Випуск № 2 (32) 2017 р.

Дизайн обкладинки: О. М. Борисенко

Макетування: А. І. Шустикевич

Редактори: Н. М. Калинів, О. В. Музичка, М. А. Маринович, О. С. Чорна

Коректори: М. А. Маринович, О. В. Музичка

Верстання: А. І. Шустикевич

Свідоцтво про внесення до державного реєстру

ДК № 3050 від 11.12.2007 р.

Підписано до друку 29.09.2016 р.

Формат 70×100/16. Папір офсетний. Друк офсетний.

Тираж 100. Зам. № _____.

Віддруковано в НВЛПТ

Української академії друкарства

79008, м. Львів, пл. Митна, 1