Б. В. Дурняк, Д. В. Музика, В. І. Сабат

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ДОКУМЕНТІВ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Б. В. Дурняк, Д. В. Музика, В. І. Сабат

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ДОКУМЕНТІВ

Львів — 2014

ББК Ф+73
Д-843
УДК 004:002.1

Дурняк Б. В. Стеганографічні методи захисту документів / Б. В. Дурняк, Д. В. Музика, В. І. Сабат. – Львів : Укр. акад. друкарства, 2014. – 160 с.

У монографії висвітлено основи інформаційної технології проектування систем стеганографічного захисту інформації. Розглянуто особливості формування графічних засобів захисту документів, побудови моделей захисту інформації з використанням методів стеганографії та реалізації засобів контролю документів із стеганографічними методами захисту. Значну увагу приділено розробленню основних компонент системи захисту на основі стеганографічних методів укриття даних у графічному середовищі.

Для студентів-магістрів та фахівців у галузі захисту інформації в системах документообігу, документів суворої звітності та цінних паперів.

ISBN 978-966-322-401-5

Затверджено до друку
вченою радою Української академії друкарства
(протокол № 8/651 від 13.05.2014 р.)

Рецензенти:
Машков О. А. – д-р техн. наук, професор
(Державна екологічна академія післядипломної освіти
та управління Мінприроди України, м. Київ)
Коростіль Ю. М. – д-р техн. наук, професор
(Інститут проблем моделювання в енергетиці НАН України, м. Київ)
Сікора Л. С. – д-р техн. наук, професор
(Національний університет «Львівська політехніка», м. Львів)

ЗМІСТ

ВСТУП

Необхідність захисту документів та цінних паперів постає на всіх етапах їх використання. Оскільки документи містять інформацію про управління різними технологічними процесами, то здійснення такого управління можливе лише в тому випадку, якщо документ або цінний папір не може бути сфальсифікованим із спотвореною чи зміненою інформацією про управляючу дію. Більшість документів, призначених для обслуговування технологічних процесів, паперові, тому їх захист особливо актуальний.

Асортимент документів, що використовуються в сучасному суспільстві для управління технологічними процесами, доволі широкий. Тому документи, орієнтовані на обслуговування певних технологічних процесів, потребують різних рівнів захисту. Це зумовлює необхідність створення таких засобів безпеки документів, які б забезпечували різні рівні їх захисту.

Для документів, виготовлених поліграфічним способом, здебільшого застосовуються графічні засоби захисту, тому в монографії розглядається стеганографічний метод захисту паперових документів, з якими більшість користувачів постійно стикається у повсякденному житті при реалізації тих чи інших технологічних процесів. До таких документів належать персональні документи: паспорти громадян, дипломи про освіту, посвідчення особи або документи,

що визначають вартість об'єкта чи підприємства: акцизні марки, акції, доручення на матеріальні цінності тощо. Документи можуть поділятися за часом існування на довготривалі, короткотривалі та постійного типу. До довготривалих документів можна віднести паспорт із визначеним терміном дії, до короткотривалих — квитки на проїзд чи в театри, акцизні марки тощо. До документів постійного типу належать дипломи про освіту, дипломи про нагороди тощо.

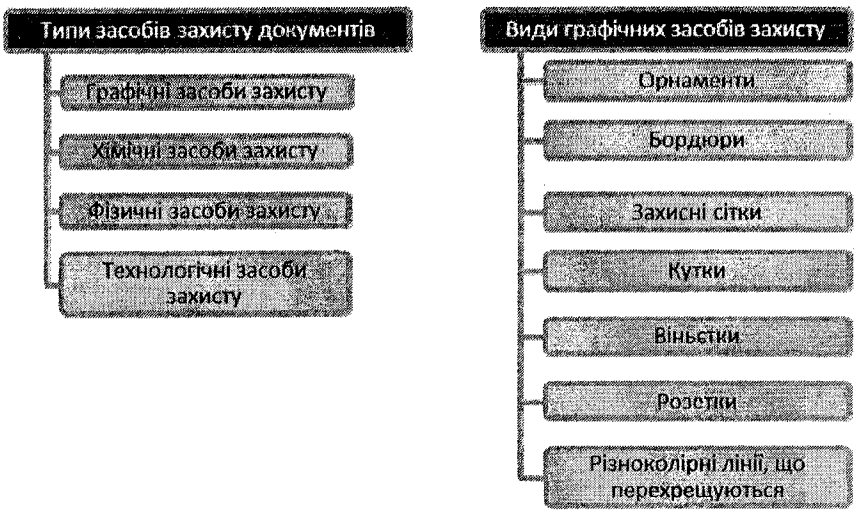
Документи, залежно від свого призначення, параметрів, що їх характеризують, та цілого ряду інших факторів, потребують різних засобів захисту, які забезпечують певний рівень безпеки та мають відповідну вартість. Отже, створення інформаційної технології формування графічних засобів захисту, які відповідають у кожному випадку певним вимогам, є актуальною проблемою в галузі захисту документів та цінних паперів.

Автори висловлюють щиру подяку рецензентам книги: д-ру техн. наук, професору Машкову О. А., д-ру техн. наук, професору Коростілю Ю. М., д-ру техн. наук, професору Сікорі Л. С. за поради та цінні вказівки при підготовці видання.

ЗАХИСТ ДОКУМЕНТІВ ТА ЦІННИХ ПАПЕРІВ У ПОЛІГРАФІЇ

Аналіз засобів захисту документів та цінних паперів

У сучасних документах, що виготовляються поліграфічним способом, поширені різноманітні засоби захисту, зокрема: графічні, фізичні, хімічні та технологічні (рис. 1, а).



а *б*

Рис. 1. Засоби захисту паперових документів:
а) типи засобів захисту документів, б) види графічних засобів захисту

Графічні засоби захисту — це спеціальні фігури, що наносяться на поверхню паперу друкарським способом. Оскільки кожний документ на одному з етапів проходить стадію проектування, то графічні засоби захисту, що наносяться на поверхню документа друкарським способом, також проектуються разом з іншими зображеннями та текстом, які передбачається розмістити на документі. Сучасні графічні засоби захисту складаються з різних графічних елементів, які можна поділити на окремі види (рис. 1, б).

До найпоширеніших елементів цього типу належать гільйоширні елементи — геометричні образи у вигляді тонкої графіки [1], до яких належать: різноколірні лінії, що перехрещуються; захисні сітки; орнаменти; розетки; бордюри; віньєтки; кутки тощо.

Здебільшого застосовується типовий орнамент, який складається з різних елементів, що перебувають у встановленій комбінаційній залежності. Типові орнаменти насамперед відрізняються такими параметрами, як розміщення кольорових ліній, способи підбору кольорів та формування різної змістової частини. В поліграфічній практиці виготовлення графічних засобів захисту вибір того чи іншого виду елементів захисту здійснює замовник. Це призводить до перекладання відповідальності за вибір певних графічних засобів захисту документів від виконавця до замовника, відповідно і вибирається рівень безпеки документів з тими чи іншими засобами захисту. Якщо звернути увагу на те, що замовник за характером своєї діяльності, може не мати відношення до проблем захисту документів і, тим паче, до проблем, пов'язаних з аналізом рівня захисту, то така практика призводить до неоптимального використання засобів захисту і загалом — до дискредитації всієї системи захисту документів [2].

Тангірні сітки, що також застосовуються для захисту документів, — це складні геометричні перетини лінійної тонкої графіки, що заповнюють весь фон поля поліграфічного продукту.

Інший клас графічних засобів захисту становлять спеціальні растри. Зображення, що створюються за допомогою лінійних растрів, — це сітки з концентричних кіл прямих чи кривих ліній. За допомогою таких растрів можна створювати півтонові зображення, які формуються на основі стандартних форм растрової крапки у вигляді кола, ромба, квадрата чи іншої геометричної фігури. Стохастичне растрування полягає у випадковому виборі розміщення точок на площині документа. Зображення будується з точок, які зумовлюють відповідний характер візерунка. Концентрація стохастичного розміщення точок на різних ділянках аркуша відповідає кольоровій щільності зображення. Зображення, що створю-

ється при використанні лінійних растрів формуються за рахунок зміни товщини ліній, що утворюють відповідні растри.

Для захисту цінних документів часто застосовується мікрографіка, — у межах ліній, що сприймаються людським оком у звичайних умовах як тонкі суцільні лінії, відтворено символи різних шрифтів, окремі знаки та інші зображення, які можна розрізнити лише за допомогою мікроскопа чи лупи. Для забезпечення відповідної скритості інформації висота мікрошрифту становить не більше 200–300 мкм у випадку позитивного зображення мікрографіки і 300–400 мкм — при негативному зображенні. Такі розміри унеможливлюють відтворення мікрографіки при ксерокопіюванні відповідних документів [3].

Один із графічних засобів захисту забезпечується введенням у графічний образ спеціальних дефектів, а саме: нестандартних шрифтів, нерівних за шириною чи висотою літер, а також літер, що хаотично змінюють свою товщину. Якщо в документі розміщується значна кількість тексту, то такі зміни можуть бути непомітними.

До графічних засобів захисту належать засоби, що містять об'ємний ефект. При побудові відповідного графічного засобу ця властивість досягається за рахунок врахування особливостей людського сприйняття графічних образів [4]. Можливість побудови об'ємних графічних засобів існує завдяки єдиним психовізуальним закономірностям сприйняття візуальної інформації системою зору людини. Для побудови таких образів формуються досить складні моделі створення об'ємних зображень, на основі яких формуються об'ємні фігури на поверхні документа [5,6]. Психофізіологічні можливості людського зору досить різноманітні, тому при побудові образів можна досягати різних психовізуальних ефектів сприйняття. В цьому випадку захисні властивості об'ємних образів ґрунтуються на складності алгоритмів їх створення. Як приклад, можна навести такі образи та їх ефекти, що сприймаються людиною:

— прихований рисунок;

— прихований текст;

— насичений образ на захисній сітці тощо.

Для створення графічних засобів захисту також використовується призматичний друк, який становить окремий випадок застосування тангірних сіток, зазвичай, із двох кольорів. У таких сітках кольори змінюються плавно у межах площі виробу. Використання багатоколірного пантографічного фону в багатьох випадках робить неможливим кольорове ксерокопіювання чи сканування захищеного документа [7].

Відомими засобами графічного захисту документів є графічні пастки "ЫРТ", які можуть мати різні варіанти застосування.

При використанні графічних засобів захисту різних типів існують нормативи, що забезпечують досягнення захисних функцій для відповідних засобів захисту. Наприклад, гільйоширні елементи згідно з такими нормативами повинні займати не менше 70% площі цінних паперів, при цьому багатоколірні композиції з гільйоширних елементів мають розміщуватися в більшій частині документа. Такі композиції мають створюватись на основі сполучення позитивних та негативних ліній товщиною 50–90 і 40–70 мкм, відповідно [8]. Очевидно, що формування таких ліній довільної складності та накладання растрових зображень може бути реалізоване на основі використання складних математичних моделей, які описують процеси побудови відповідних графічних образів.

Друкуючи документи та цінні папери, широко застосовують фізичні методи створення засобів захисту. Такі методи і, відповідно, засоби захисту, орієнтовані насамперед на зорове сприйняття образів людини [9]. До особливо надійних фізичних засобів захисту в паперових документах належить використання водяного знаку. Водяний знак — це графічний образ у паперовій масі, який є видимим на просвіт. Такі засоби захисту належать до фізичних методів їх створення, оскільки реалізуються в рамках фізичних процесів, що ініціюються при виконанні технологічного процесу формування паперового полотна. За розміщенням водяного знаку на поверхні документа вони поділяються такі типи (рис. 2):

— фоновий водяний знак;

— локальний водяний знак;

— одноразовий водяний знак.

За кількістю параметрів, якими характеризується водяний знак, їх можна розділити на:

— дворівневий водяний знак;

— півтоновий водяний знак.

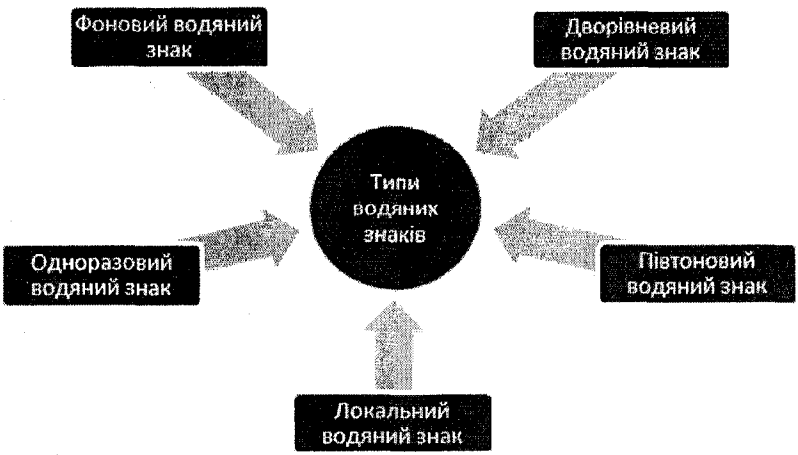


Рис. 2. Типи водяних знаків

Фоновий водяний знак регулярно розташований на поверхні паперу і багаторазово повторюється по всій поверхні документа. На відміну від нього локальний водяний знак розташовується у чітко визначеному місці документа, яке синхронізоване з іншими зображеннями, що використовуються в документі. Одноразовий водяний знак являє собою монохроматичне зображення у вигляді фігур чи малюнків, причому їх інтенсивність відрізняється від інтенсивності тону паперового полотна. Дворівневий водяний знак являє собою двотонове зображення, що вирізняється кольором або тоном від паперового полотна. Півтоновий водяний знак — це півтонове зображення оригіналу, сформоване у паперовій масі, що використовується для виготовлення документів [10].

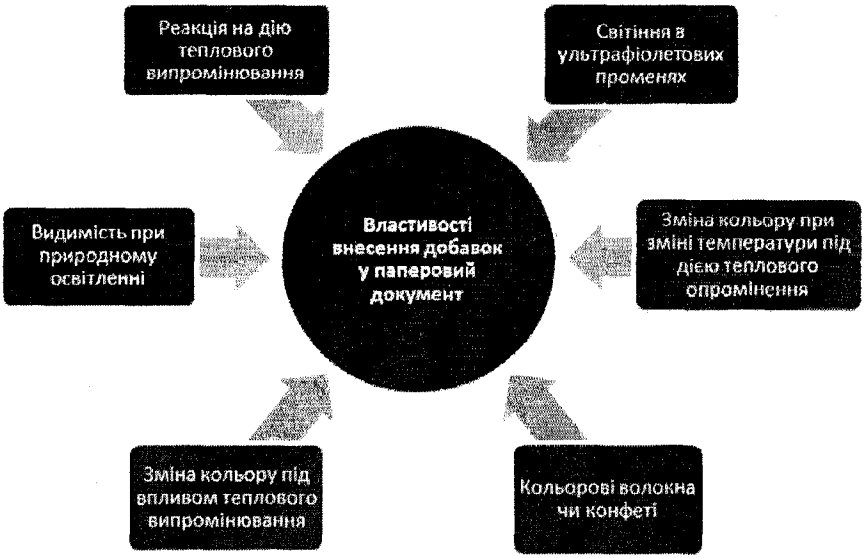


Рис. 3. Властивості внесення добавок у паперовий документ

До фізичних методів створення засобів захисту документів належать різноманітні внесення добавок у паперову масу, що, як і у водяних знаках, реалізуються в технологічному процесі виготовлення паперу (рис. 3). В паперову масу вносяться волокна, нитки чи конфеті з різними функціональними властивостями, які, як і внесені добавки, можна спостерігати візуально. До таких властивостей добавок у паперову масу можна віднести:

— колір волокон чи конфеті;
— свічення в ультрафіолетових променях;
— елементи, видимі в природному освітленні;
— зміна кольору під впливом теплового випромінювання, при цьому елементи можуть стати видимими чи невидимими у природному освітленні;
— добавки можуть змінювати колір під впливом теплового випромінювання та відновлювати попередній колір з припиненням дії теплового опромінювання;

— добавки можуть реагувати певним чином на дію теплового випромінювання при зміні температури їх нігрівання, і ця реакція може повторюватися безліч разів;
— деякі добавки можуть бути розрахованими на певну кількість разів змін кольору під дією зміни температури теплового опромінювання.

Окремо розглядаються внесення у паперову масу металізованих волокон, що дає змогу контролювати електричні характеристики відповідних добавок та паперу загалом. Найочевиднішою електричною характеристикою є провідність фрагментів паперу або окремих його добавок. Перевагою використання такого типу добавок є можливість досить простого контролю провідності паперу.

До іншого типу добавок, що використовуються як елементи засобів захисту паперових документів, належить внесення в паперове полотно псевдоголографічних плівок, з яких нарізується конфеті, що в процесі формування паперового полотна вноситься у паперову масу. Це призводить до створення візуального ефекту появи металізованого зображення.

Для реалізації засобів захисту паперових документів використовуються також внесення в паперове полотно полімерної нитки, що дає змогу реалізувати такі різновиди добавок, які відповідають різним варіантам реалізації на цій основі засобів захисту, а саме:
— нитка може повністю вводитися в паперову масу таким чином, що буде видимою тільки на просвіт;
— нитка може вводитись частково в паперову масу, що призводить до того, що частина нитки є видимою на поверхні паперу, а частина нитки, що занурена в паперову масу, може бути видимою тільки на просвіт;
— для занурення в полотно паперу може використовуватися полімерна нитка, на якій нанесено мікрошрифт, або машиносчитувальні коди, які стають видимими тільки при їх значному збільшенні;

— полімерна нитка може застосовуватися з нанесеними на неї голографічними вкрапленнями, які викликають псевдоголографічні ефекти;
— полімерні нитки, як і інші добавки, можуть мати нанесені елементи, які змінюють колір під впливом ультрафіолетового або інфрачервоного випромінювання.

До фізичних методів створення засобів захисту паперових документів також належать внесення в паперову масу планшеток — матеріалів діаметром 1–2 мм, які можуть бути кольоровими, райдужними, безколірними, видимими тільки в ультрафіолетовому випромінюванні.

Планшетки виготовляються з тонких термопластикових плівок, наприклад, райдужні — з тонких плівок, спресованих між собою [11].

Для побудови засобів захисту документів фізичними методами є характерним те, що при їх створенні досить важко забезпечити ту чи іншу величину значень параметрів, що характеризують появу необхідних ефектів. Наприклад, при включенні конфеті в паперову масу досить важко забезпечити потрібну точність їх розміщення в цій масі щодо базових координат документа. Ефект видимості при певному типі випромінювання досить важко пов'язати з величиною інтенсивності випромінювання, при якій такий ефект проявляється. Вимірювати величину зміни температури, що необхідна для виявлення того чи іншого ефекту, досить складно у разі потреби оперативного контролю документа з використанням відповідного засобу захисту. Аналогічна ситуація спостерігається і з водяними знаками, захисна функція яких полягає у їх існуванні, при цьому параметри водяного знака, що могли б бути ознаками міри захищеності, не змінюються для всієї партії документів. Це пов'язано з технологічними процесом виготовлення захищеного паперу, що розрахований на досить великий об'єм паперового полотна і, відповідно, велику кількість документів чи цінних паперів, що на ньому друкуються [12].

Розглянемо основні хімічні методи створення засобів захисту паперових документів. Такі методи ґрунтуються на використанні

різних хімічних речовин, якими обробляється папір. До хімічних методів захисту можна віднести:

— нанесення на паперове полотно мікрокапсули фарби для аутентифікації паперового полотна;

— нанесення на паперове полотно грубодисперсної суміші капсульного шару.

Хімічні засоби захисту використовуються проти підробок паперового полотна і полягають у нанесенні на полотно мікрокапсул фарби, які в процесі аутентифікації документа розчиняються відповідним реагентом. Фарба з мікрокапсул попадає на поверхню паперу і формує на ньому відповідні плями, які ідентифікують паперове полотно як непідроблене. Очевидно, що цей хімічний засіб є разовим, і після його застосування відповідний документ не використовується у технологічних процесах, які він обслуговує.

Нанесення на паперове полотно грубодисперсної суміші капсульного шару створює засіб захисту, аналогічний вищевказаному, але дозволяє використовувати інші процедури аутентифікації документа, що як і в першому випадку є одноразовими.

Вищенаведені методи створення засобів захисту документів, по суті, є технологічними, оскільки реалізуються на різних етапах технологічних процесів виготовлення документів — від виготовлення паперу до друкування графічних образів. Проте існують методи створення засобів захисту, орієнтовані тільки на їх формування, які не призводять до певних фізичних ефектів, і виникнення яких є підтвердженням оригінальності документів. До таких методів належать:

— перфорація певних даних;

— видруковування визначеної інформації, що є спільною для всього класу документів;

— спеціальна механічна обробка торців документа;

— визначені способи механічного скріплення документа, якщо він складається з окремих аркушів паперу;

— спеціальне механічне скріплення паперового полотна документа з конструктивними додатками, запроектованими як окремі деталі документа.

Перфорація певних даних досить поширена як засіб захисту документів, оскільки може реалізуватися на останньому етапі технологічного процесу формування документа, що, зазвичай, реалізується на основі даних, які надаються користувачем бланків документів для їх виготовлення поліграфічним методом. Тому міра захисту документа такими засобами, порівняно з засобами захисту, які виготовляються на основних етапах технологічного процесу, є невелика.

Більшість бланків документів та цінних паперів містять інформацію у вигляді текстових фрагментів, що є спільними для всього класу документів. Як мінімум, така інформація містить назву відповідного класу документів. Вибрані і вдруковані фрагменти текстів проектуються таким чином, щоб їх відтворення при спробах підробки документів було досить складним.

Спеціальна механічна обробка торців документа як засіб його захисту полягає у виборі певним чином сформованої геометрії формування торця. Це означає, що геометрія торця може змінюватися від одного накладу до другого візуально непомітним способом. Типовим прикладом використання такого засобу захисту є поштові марки, в яких по контуру формується певна геометрія торця марки.

Скріплення окремих аркушів документа є досить ефективним засобом захисту, оскільки механіка скріплення окремих частин може передбачати достатньо багато прихованих елементів у вузлі скріплення, які при несанкціонованій розшивці документа руйнуються, або повторення яких при спробі його фальсифікації є не можливим з технічних причин, що зумовлюються технологією зшивання документа. Наприклад, зшиваючи документ спеціальними нитками, на них може наноситись мікротекст, який синхронізується з розміщенням зшиваючої нитки в конструкції відповідного з'єднання.

Останнім часом широко використовують конструктивні додатки до документів із застосуванням голограм [13,14]. Голограми являють собою окремі фрагменти, зазвичай, металевої фольги, на які голографічним способом нанесено додаткову інформацію, що може надаватись у вигляді графічних образів чи текстів. Завдяки застосуванню голографічних способів нанесення інформації на голограми вона не може бути безпосередньо зчитаною, для цього необхідне спеціальне устаткування, призначене для відтворення голограм.

Поліграфічні методи формування графічних засобів захисту документів

Наявність функцій захисту у графічних засобах захисту суттєво залежить від технології їх виготовлення. Оскільки в нашому випадку розглядається захист паперових документів, то базовим елементом технології створення засобів захисту є процес їх друкування. Функція захисту полягає у тому, що поліграфічні технології друку, які використовуються для створення графічних засобів захисту, повинні бути недоступними для неуповноважених виробників документів. Це досягається різними методами технічного та соціального характеру. Детальніше розглянемо технічні методи забезпечення функцій захисту.

До функцій захисту можна віднести:

— застосування технічно складних методів у друкуванні відповідних засобів захисту, реалізація яких потребує додаткових даних, що можуть бути відомими тільки визначеному колу осіб;

— реалізація технологічно складних процесів друкування потребує використання досить дорогого обладнання, яке має перебувати на обліку в соціальних системах, що належать до засобів забезпечення захисту документів;

— у технологічних процесах друкування документів і, відповідно, графічних засобах захисту повинні використовуватися нові досягнення в конструкторських чи технологічних рішеннях, які становлять таємницю легальних виробників документів.

Розглянемо деякі методи друкування та їх особливості, які відображаються в друкованих образах [15,16]. Образи, які містять елементи захисту, набувають захисних функцій. Однак вибір способу друку визначається не тільки необхідністю створення графічних образів з певними особливостями, але насамперед параметрами паперу, на якому запроектовано друкувати документи, величиною тиражу друку документів, характером документа чи цінного паперу та іншими параметрами.

Розглянемо деякі види друку, особливо поширені для друкування поліграфічної продукції і, в тому числі, для друкування документів та цінних паперів (рис. 4).

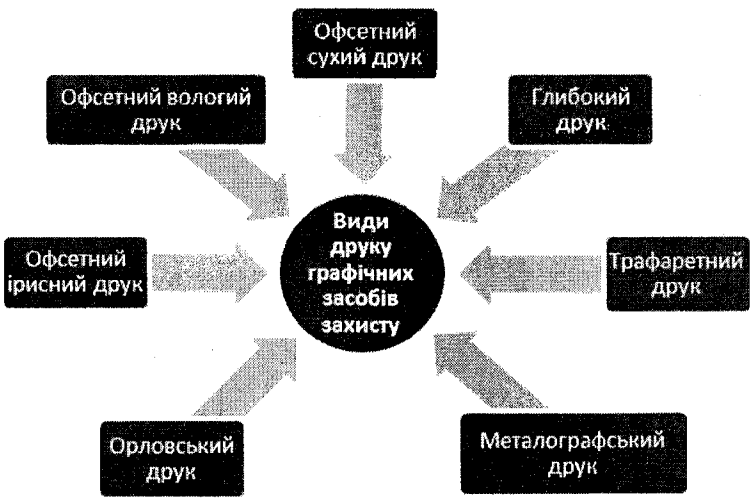


Рис. 4. Види друку графічних засобів захисту документів

Офсетний друк — один із широко застосовуваних методів друку цінних паперів та документів. Для офсетного друку використовуються високолінеатурні форми плоского друку, які забезпечують повноколірне друкування через проміжний офсетний циліндр густими фарбами. Швидкість такого друкування становить 15–18 тисяч аркушів на годину. В цьому методі вибірний ефект

забезпечується змочуванням водою пробільних елементів форм. Такий спосіб друкування дозволяє досягнути високої точності кольоропередачі та високої роздільної здатності рисунка. Для друкування цінних паперів поширений флексографський друк, що полягає у використанні рідких фарб для друкування з еластичних фотополімерних форм високого друку і забезпечує високу швидкість друкування бланків, конвертів тощо. Офсетна форма глибокого друку полягає у передачі зображення з форм глибокого друку через офсетний циліндр. Такий спосіб друку застосовують при друкуванні на готових виробах чи інших твердих матеріалах [17].

Різновидом офсетного друку є сухий друк, що здійснюється з форм плоского друку високоякісних, багатоколірних зображень з високими лініатурами растра через офсетний циліндр без зволоження. Цей спосіб друку використовується у випадку, коли не можна допускати зволоження матеріалу, на якому здійснюється друкування [18].

Іншим різновидом друку є ірисний друк, за допомогою якого на однофарбових машинах офсетного та високого друку можна отримати багатоколірне зображення з плавним переходом фарби перпендикулярно до руху аркуша в друкарській машині. Це забезпечується завантаженням в один фарбовий апарат фарб декількох кольорів, за рахунок їх проникнення та перемішування утворюються перехідні, з плавно змінними кольорами, зображення [19].

До високошвидкісної технології друку можна віднести глибокий друк, що являє собою технологію повноколірного друкування рідкими фарбами, що швидко висихають. Друкування здійснюється з високолініатурних друкарських форм, в яких друкувальними елементами є растрові комірки, що мають різну глибину заповнення. При цьому за рахунок різної товщини фарбового шару досягається градація півтонів, а завдяки м'якому розтіканню фарби на ділянках, що відповідають окремій растровій крапці, досягається дискретність зображення надрукованого матеріалу.

Ще один із способів друку — орловський друк — забезпечує створення багатоколірних зображень завдяки перенесенню

друкарських фарб з кольороподілених друкарських форм високого друку на збірну форму, на якій синтезується кольорове зображення. На подальшому етапі технологічного процесу друкування синтезоване зображення передається на матеріал, на якому виконується друкування, а формування образу здійснюється одним відбитком. Завдяки такій технології формування відбитку образу підробити надрукований образ іншим способом друку на інших друкарських пристроях чи за допомогою іншої технології друку неможливо [20].

При друкуванні графічних засобів захисту важливо надати друкованому образу таких властивостей, які можна було б використати для ідентифікації документа, на котрому відповідний образ надруковано. Металографський друк є одним з таких способів друкування, при якому надрукований образ характеризується такими ознаками:

— образ може мати високу роздільну здатність, що особливо важливо при друкуванні гільйоширних елементів;
— для друкованого образу можна забезпечити відтворення широкої гами півтонів, що є важливим при створенні спеціальних лінійних растрів, які формуються на основі стандартних форм растрової крапки;
— у надрукованому таким способом зображенні можна сенсорно контролювати його рельєф;
— фарби, що використовуються в цьому способі друку, змінюють свій колір при зміні кута зору щодо джерела світла.

Металографський друк здійснюється із заглиблюючих друкувальних елементів гравірованих друкуючих форм. Друкування з таких форм реалізується на поверхні матеріалу з використанням густих фарб під великим тиском.

Додаткова функція захисту, яку містить зображення, надруковане таким способом, полягає у тому, що завдяки певній фіксації індивідуальних особливостей різальних інструментів, що використовуються для гравірування друкуючих форм, можна виявити підробки, які створюються з інших гравірованих друкуючих форм. Очевидно, що всі особливості гравірування окремої гравірувальної

друкуючої форми можна відстежити з надрукованого графічного образу при його детальному аналізі.

Важливим, з точки зору друкування графічних засобів захисту, є трафаретний друк. У цьому способі друку зображення передається з друкарської форми, що являє собою високолініатурну сітку, через відкриті комірки, які відповідають друкувальним елементам [21]. Друкування здійснюється шляхом протиснення за допомогою ракеля друкуючої фарби крізь відкриті комірки високолініатурної сітки. Порівняно з іншими видами друку, трафаретний друк дозволяє отримувати максимальний за товщиною шар фарби на відбитку. Це, зокрема, дає змогу створювати на відбитку надруковані образи, для яких використовувались інші способи друку.

З вищенаведених способів друку видно, що однією з ключових компонент довільної технології друкування є фарба, яка наноситься на папір і створює відповідний графічний образ [22]. Оскільки фарба — складний і багатогранний продукт хімічних перетворень, то слід очікувати, що вона може мати цілу низку своїх властивостей. Властивості друкарської фарби можуть проявлятися при дії на неї зовнішніх чинників, які можна використати для задач захисту документів за допомогою надрукованих графічних образів. Очевидно, що в цьому випадку не йдеться про такі властивості фарби, як колір. Додаткові властивості, які мають різні фарби, — це ті властивості, що призводять до спеціальних ефектів, характерних для тих чи інших фарб. Функції захисту в цьому випадку полягають у тому, що хімічні реакції, завдяки яким можна отримати фарби з необхідними властивостями, досить складні. З точки зору фахівців, для їх проведення необхідне складне хімічне обладнання та унікальні хімічні складники, що входять до складу відповідних фарб і надають їм тих чи інших властивостей. Як і у випадку друкарських технологій, захисні властивості графічних засобів захисту, що виникають завдяки застосуванню спеціальних фарб, зумовлюються тим, що вони є матеріалами обмеженого і цільового використання, їхні хімічні структури і формули є промисловою таємницею, що дозволяє унеможливити їх використання неуповноваженим особам. Крім того, в галузі створення

друкарських фарб з оригінальними властивостями постійно проводяться дослідження, а позитивні результати таких досліджень визначаються як технологічні таємниці, що є суттєвим фактором для забезпечення графічних засобів захисту додатковими захисними функціональними можливостями [23,24].

Розглянемо основні фарби та їх властивості, що безпосередньо використовуються для створення графічних засобів захисту, з точки зору їх функціональних можливостей, а не хімічного складу чи структури фарби.

До широкого класу фарб із специфічними властивостями належать фарби, які реагують на ультрафіолетове випромінювання. До їх складу входять пігменти, що світяться під дією ультрафіолетових променів. Оскільки папір поглинає ультрафіолетове випромінювання, то світиться тільки образ, надрукований із застосуванням відповідних фарб. Папір, що поглинає світіння пігменту, при ультрафіолетовому опроміненні образу не слід використовувати для друкування такими фарбами. До таких типів паперу належить крейдяний папір та інші. Окрім того, такі фарби не рекомендовано застосовувати для друкування на синтетичних матеріалах. Основою для фарб, що можуть світитися при ультрафіолетовому опроміненні, може бути весь колірний спектр Panton, за винятком темних кольорів. Такі фарби візуально нічим не відрізняються від звичайних. Для досягнення ефекту світіння при ультрафіолетовому опроміненні образів можна використовувати безбарвні або невидимі фарби. Для створення графічних засобів захисту можуть використовуватися барвники, що, крім специфічного світіння, при опроміненні образів ультрафіолетовим промінням змінюють колір основи фарби.

Наступним класом фарб, що здатні проявляти певні фізичні ефекти, є фарби та лаки, чутливі до інфрачервоного опромінення. Такий ефект полягає у тому, що при інфрачервоному опроміненні рисунка надрукованого такими фарбами він може зникати або проявлятися. Такі ефекти досягаються за допомогою додавання до фарб інфрачервоних барвників. Якщо використовувати фарби, що стають невидимими в інфрачервоному опроміненні, то можна

досягнути ефекту маскування. При цьому образ, що маскується, покривається образами, надрукованими фарбами, які стають невидимими в інфрачервоному опроміненні. Тоді образ, надрукований під образом чутливою до інфрачервоного опромінення фарбою, стає видимим.

При друкуванні документів та цінних паперів використовуються фарби, що можуть створювати ефект люмінесценції. Це також ефективно застосовується для створення графічних засобів захисту. Завдяки широкому асортименту відомих люмінесцентних матеріалів [23,24] виготовляють фарби, що дають можливість отримувати найрізноманітніші ефекти, а саме:

— барвники, що мають власну люмінесценцію, яка проявляється при їх використанні;
— флюоресценція фарби може проявлятися при денному чи штучному освітленні;
— барвники, що накопичують ефект люмінесценції тощо.

При використанні барвників, що накопичують ефект люмінесценції, вони при звичайному освітленні не світяться, а в темряві через деякий час починають світитися. Для посилення ефекту люмінесценції необхідно застосовувати методи друку, за яких забезпечується накладання товстих шарів фарби. До таких методів належить трафаретний друк.

Ще одним класом фарб, що проявляють додаткові ефекти, є фарби з барвниками, які дають можливість змінювати колір при дії зовнішніх чинників. Для таких фарб ключовим зовнішнім фактором є зміна теплового випромінювання, що може діяти на відповідні кольорозмінні барвники. При цьому може змінюватися інтенсивність кольору чи сам колір. Зміна інтенсивності теплового випромінювання може здійснюватися під дією джерела світла при регулюванні відстані від джерела світла до зображення тощо. Зміна кольору чи насиченості фарб є зворотною.

Рис. 5. Форми прояву ефектів термочутливих барвників

За способами прояву додаткових ефектів термочутливих барвників виділяють такі їх типи (рис. 5):

— барвники з незворотною кольоровою реакцією, які застосовують для документів разового використання;

— барвники із зворотною кольоровою реакцією, в яких пігменти реагують на тепло від дотику руки людини до фарб, при цьому чутливість фарб вибирається в межах 35–38 °С. В цьому випадку колірні характеристики можуть змінюватися залежно від величини температури;

— барвники з дворівневою колірною реакцією, для яких рівні реакції визначаються величиною температури, наприклад, перший рівень колірної реакції відповідає 35–38 °С, і на цьому рівні зберігаються зворотні властивості зміни кольору, на другому рівні температурного впливу при 50–60 °С колірні зміни мають незворотний характер;

— термочутливі фарби, що втрачають колір, в цьому випадку барвники переходять у невидимий стан;

— двошарові термочутливі барвники, наприклад, безбарвний барвник, частково видимий, наноситься на поверхню паперу першим, а знебарвлена фарба наноситься другим шаром. При тепловому впливі на зображення верхній забарвлений шар знебарвлюється, а нижній шар барвника, навпаки, стає видимим.

Сьогодні поширені фарби, які забезпечують сенсорну контрольованість засобів захисту. Такий ефект досягається за рахунок додавання пігменту, що реагує на заданий хімічний реагент. Використовуються також фарби, що реагують на окислюючу дію, яка досягається тертям відповідного місця документа, в результаті чого з'являється невидиме раніше зображення.

Фарби, що містять світлочутливі ефекти, використовуються для формування засобів захисту. Для цього до фарби додаються металізовані барвники, які надають їй характерного металевого відблиску. Такий відблиск не відтворюється копіювальними апаратами і це є одним з аспектів функції захисту.

Використовується внесення у фарбу великодисперсійної суміші, що наносяться поверх графічних зображень. В результаті цього барвник набуває металевого блиску у вигляді крапель. До фарб також додаються пігменти, які забезпечують спучування лаку при ультрафіолетовому опроміненні. Тоді можна зазначити наявність цілого комплексу захисних ефектів, а саме:

— спучування лаку при ультрафіолетовому опромінюванні графічного образу;
— завдяки ефекту спучення можна створювати рельєфність для окремого образу;
— можна забезпечити переливчастий, металізований відблиск фарб;
— можна досягти ефектів світіння образів в ультрафіолетовому випромінюванні.

Функцій захисту можна досягати, використовуючи фарби, що мають струмопровідні властивості. Для того щоб надати фарбі таких властивостей, додається пігмент з металізованими добавками. Завдяки цьому ефекту можна контролювати різницю потенціалів на поверхні паперу і таким чином виявляти наявність у фарбі металізованого пігменту.

Для створення рельєфних поверхонь на друкованих захисних образах використовують фарби та лаки, що спучуються, відомі як «Puff-Jnk». Вони створюють стійкий рельєф після дії на них ультрафіолетового випромінювання. Таке випромінювання може

застосовуватися при сушінні фарб у процесі друку. Якщо використовувати лак, що спучується, то його можна наносити поверх звичайних поліграфічних фарб.

У деяких випадках використовуються ароматизовані фарби, до яких додаються пігменти-ароматизатори. Наявність запаху встановлюється без застосування спеціальних приладів, але цей процес є досить суб'єктивним. Суттєвим недоліком використання таких ефектів для захисту є те, що інтенсивність запаху змінюється, і з часом він може зникнути.

Крім вищенаведених фарб, для захисту документів використовуються фарби:

— товстим шар;

— з тесторним ефектом;

— з магнітними включеннями;

— фарби, що не сохнуть, та інші.

Використання спеціальних фарб для створення графічних засобів захисту не дає можливості оцінювати значення величини міри захищеності, яку забезпечує відповідний графічний засіб. Таким чином, функції захисту, які отримує певний засіб, завдяки застосуванню спеціальних фарб, носять якісний характер. Це означає, що захист забезпечується фактором наявності того чи іншого ефекту, прояв якого забезпечує відповідна фарба. Отже, якщо є необхідний ефект графічного образу, то це зумовлює наявність захисту та збільшує ймовірність того, що відповідний документ не підроблений. Розглядати міру захищеності можна лише тоді, якщо б існували оцінки складності використання необхідних фарб або у випадку, коли можна досягти різних значень величини ефекту в межах одного типу засобу захисту. В цьому випадку необхідно пов'язати процедури використання спеціальної фарби з мірою забезпечення заданого рівня прояву певного ефекту. Сьогодні такі завдання не розглядаються, оскільки процедури застосування спеціальної фарби при друкуванні зводяться до однієї технічної процедури формування відбитку графічного образу для захисту на документі. Значною мірою цей фактор зумовлюється специфікою роботи друкарських машин.

Методи стеганографічного захисту інформації

Стеганографія — це метод укриття інформації в певному інформаційному середовищі [25]. Стеганографія, як метод вирішення задачі захисту, характеризується та визначається такими ознаками та параметрами (рис. 6):

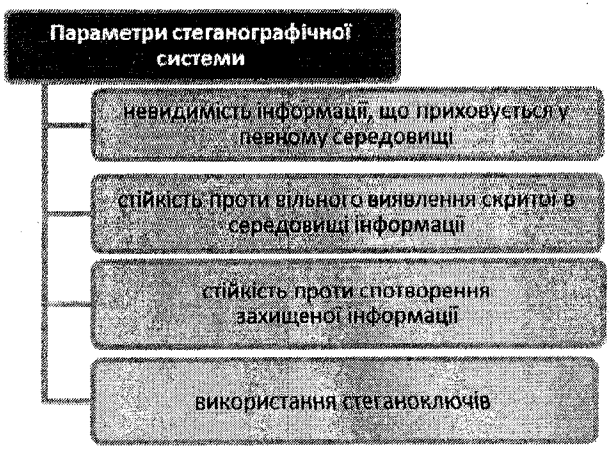


Рис. 6. Параметри стеганографічної системи

— невидимість інформації, що приховується у певному середовищі (η);

— стійкість проти вільного виявлення скритої в середовищі інформації (μ);

— стійкість проти спотворення захищеної інформації технологічними чинниками, що можуть діяти на відповідне середовище незалежно від того, чи розміщена у ньому скрита інформація (λ);

— необхідність використання стеганоключів для забезпечення легального виявлення скритої інформації у відповідному середовищі ($\aleph$).

У багатьох випадках [26] приймається, що можливе застосування стеганографічних методів, якщо повідомлення W_i

розміщується в деякому середовищі S таким чином, щоб при звичайному перегляді такого середовища W_i не можна було виявити. Таке спрощення уявлень про стеганографію призводить до суперечливих ситуацій. Наприклад, якість стеганографічного укриття інформації вимірюється мірою невидимості відповідних спотворень середовища, до якого впроваджено повідомлення. З іншого боку, уявлення про видимість чи невидимість повідомлення в середовищі є поняттям суб'єктивним. Те, що для однієї особи може бути невидимим, для іншої може виявитись видимим. Окрім того, використання тільки однієї ознаки невидимості для визначення стеганографічного методу захисту даних потребує уточнення, оскільки існує ряд традиційних засобів, якими можуть послуговуватися потенційні користувачі інформаційного середовища, які не передбачають виявляти додаткові дані, скриті в цьому середовищі. Наприклад, при перегляді графічного образу користувач може використовувати збільшуване скло у вигляді лупи чи більш потужного засобу. В такому випадку, якщо невидимість забезпечується певними розмірами, які не перевищує скрита інформація, то вона буде виявлена навіть тоді, коли користувач відповідної цілі не ставив. Тому другий критерій, у якому визначається стійкість скритого повідомлення до вільного його виявлення, якраз і передбачає врахування тих чинників, які можуть використовуватися при перегляді образу незалежно від того, чи користувач хоче розглядіти скрите повідомлення, чи ні.

Очевидно, що параметр μ, який характеризує стеганосистему, тісно пов'язаний з середовищем, з котрим працює відповідна стеганосистема, та доступними традиційними засобами його аналізу. В цьому випадку під традиційним аналізом середовища S розглядається такий його аналіз, який не призначений для виявлення W в S.

Будь-який документ, що виробляється, орієнтований на обслуговування одного чи декількох технологічних процесів. Більшість технологічних процесів, в яких використовуються документи, стосується соціальних процесів чи процесів, у реалізації яких бере

участь людина. Не викликає сумнівів той факт, що в процесі використання документів на них діятимуть різні зовнішні чинники, наприклад, якась частина документа може піддаватися постійному тертю в руках людини, наприклад, документ книжкового типу має перегортатись при його використанні. В результаті такого тертя може пошкодитися скрите повідомлення, якщо воно розміщується у відповідному місці. Технологічні перетворення, що відбуваються з документами можуть мати й інший характер, передбачений технологією їх застосування у тому чи іншому технологічному процесі. Необхідність використання ключа зумовлюється тим, що при дослідженні інформаційного середовища може виникнути ситуація, коли дослідник виявить спотворення в середовищі, що зумовлюються введеним повідомленням. Для того щоб можна було ідентифікувати такі збурення, як повідомлення треба, щоб існував відповідний таємний засіб, який дозволить з виявленого збурення перейти до повідомлення. Таким засобом є стеганографічний ключ. Описана ситуація характерна для випадку, коли інформаційним середовищем виявляється графічний образ.

В галузі захисту документів ознаки стеганографічних методів наявні в ряді засобів захисту (рис. 7). Термін «ознаки» вжито тому, що стеганографічні методи, які уже використовуються в захисті документів характеризуються лише параметром невидимості.

Найбільш очевидним засобом захисту документів є мікрографіка або мікротекст. У цьому випадку не виконується друга умова, яка визначає метод як стеганографічний, що визначає параметр μ (стійкість проти вільного виявлення інформації в середовищі). Мікрографіка створюється за рахунок ефекту отримання скритого зображення за допомогою використання високої роздільної здатності графічних ліній. Завдяки цьому лінії, що сприймаються людським оком у звичайних умовах, у вигляді тонкої суцільної лінії, складаються із знаків, символів шрифту, що читаються тільки за допомогою лупи чи мікроскопа, які в необхідній мірі збільшують зображення [27].

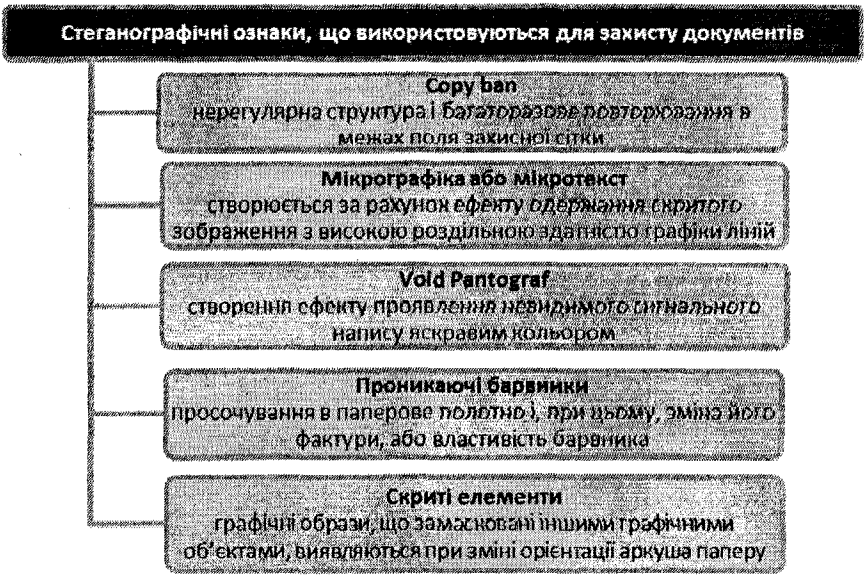


Рис. 7. Стеганографічні ознаки, що використовуються для захисту документів та цінних паперів

У поліграфії для захисту поліграфічної продукції досить поширені скриті елементи. Під скритими елементами розуміють складну геометричну сукупність елементів тонкої графіки. Скриті зображення у поліграфії називають латентними, примарними, або фантомами. Ці зображення становлять графічні образи, що замасковані іншими графічними об'єктами. Латентні зображення створюються на основі рельєфу, який формується певним способом друку. Ефект невидимості зображення полягає у тому, що при зміні орієнтації аркуша паперу під визначеним кутом, на якому надруковане відповідне зображення, з'являються нові елементи. Прикладом побудови такого типу образу може бути образ, який створено з рівнобіжних та однакових за шириною ліній переднього і заднього планів. У цьому випадку лінії переднього плану будуть більш рельєфними щодо ліній заднього плану. При звичайному освітленні обидва плани нічим не відрізняються і тільки, коли лист паперу повернути на певний кут зору, то стане видимою відмін-

ність між лініями заднього і переднього планів. Латентні зображення при звичайному огляді виглядають як елементи дизайну [28]. При певному освітленні аркуша паперу стає помітною прихована інформація у вигляді графічного образу.

Відомим у поліграфії є метод під назвою «Void Pantograf» [29], за допомогою якого створюється ефект проявлення сигнального напису яскравим кольором. Цей напис приховано у фоновій сітці, а при копії поліграфічного продукту він проявляється. Зображення, що проявляється, має регулярний, систематичний характер. Растрове зображення тангірної сітки, що задається рівновеликими растровими крапками на першому етапі друкування, робить видимим прихований напис. При розтискуванні растрової крапки на другому етапі друкування приховане зображення зливається з растровим фоном тангіра і стає візуально невидимим.

Поліграфічний засіб захисту під назвою «Copy ban» має нерегулярну структуру і багаторазово повторюється в межах поля захисної сітки. Розмір шрифту, що використовується при цьому, – необмежений, тому цей засіб захисту може застосовуватися для поліграфічних виробів довільного формату.

До засобів захисту, що при звичайному огляді є невидимі, належать суміщені зображення. Суміщене зображення — це таке зображення, у якому одна частина малюнка наноситься на одну сторону поля документа, а друга — розміщується синхронізовано з першою частиною на зворотному боці аркуша паперу документа. При розгляданні малюнка на просвіт усі елементи зображення, що сполучаються між собою, повинні збігатися та утворювати суцільний рисунок [30]. Крім того, незабарвлені деталі малюнка стають кольоровими за рахунок забарвлених частин малюнка з протилежного боку.

Інший метод створення невидимого зображення, яке можна віднести до зображень типу водяних знаків, полягає у використанні спеціальних проникаючих барвників та хімічних реагентів. Є хімічні реагенти, що здатні просочуватися в паперове полотно і при цьому змінювати його фактуру або властивість барвника. Одним з таких різновидів хімічного реагенту є жиромістка безбарвна фарба,

якою здійснюється друкування. Така фарба має підвищену абсорбцію в паперову масу, завдяки чому відповідні місця стають прозорими. Особливістю такого типу барвників є їх світіння під дією ультрафіолетового випромінювання. В рамках цього методу є можливим використовувати двокомпонентні фарби, що проникають у масу паперу. Всі методи створення скритих образів чи їхніх фрагментів, що не відповідають вищенаведеним ознакам стеганографічних методів, називатимемо псевдостеганографічними методами. Таким чином, описані приклади методів формування невидимих образів як графічних засобів захисту можна віднести до псевдостеганографічних. Фактором захисту в таких методах є невидимість образу або його фрагментів при звичайному спостереженні образу та складність технології створення невидимого образу у випадку, коли атакою на документ є його підробка чи підміна. Перший фактор захисту в таких засобах, як правило, є досить слабким чинником, оскільки в більшості випадків необхідні зовнішні засоби для викриття прихованого засобу є простими і доступними. Ця обставина зумовлюється, з одного боку, необхідністю максимально спростити процедури контролю документів, а з іншого, — фізичними можливостями відповідних компонент, що беруть участь у створенні відповідних ефектів невидимості. В цьому випадку такими фізичними можливостями є закони оптики системи зору людини, а у іншому випадку такі можливості визначаються законами флоуресценсії тощо. Тому вищенаведені способи укриття даних доцільно віднести до фізичних та хімічних методів укриття інформації.

До розвитку та поширення комп'ютерних мереж стеганографія розвивалась лише на основі використання різноманітних фізичних, хімічних та інших природних чинників, що створюють ефекти, які можна застосовувати для укриття окремих фрагментів інформації в різних формах, з яких найбільш поширена форма графічних образів. Інтенсивний розвиток стеганографічних методів, зумовлений розвитком цифрових систем передусім сприяв розвитку цифрової стеганографії, яка ґрунтується на використанні значної надмірності в цифрових середовищах [31,32]. В рамках цього

напрямку розвитку стеганографії сформувався інформаційний підхід до розробки методів стеганографічного укриття даних, що дало змогу суттєво розширити можливі підходи до методів розв'язання відповідних задач. В рамках інформаційного підходу, на відміну від фізичного підходу, суттєво розширюється кількість факторів, що зумовлюють виникнення властивостей захисту у відповідних засобах. До таких факторів можна віднести (рис. 8):

— алгоритмічні методи формування графічних засобів захисту;
— комбінаційні перетворення графічних образів, що використовуються як засоби захисту;
— інформаційні властивості засобів захисту;
— семантичні характеристики інформаційної складової графічних засобів захисту;
— компоненти методів формування засобів захисту, які можуть складати таємну частину визначених алгоритмів побудови відповідних засобів захисту.

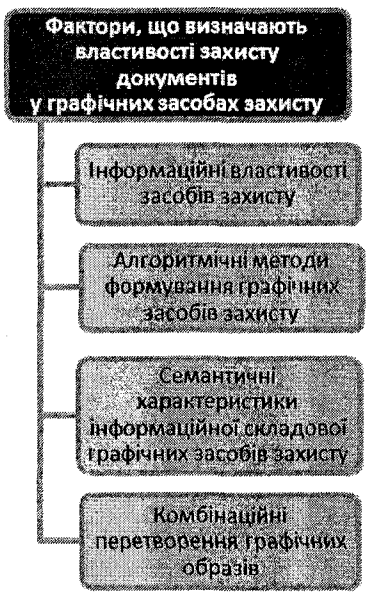


Рис. 8. Фактори, що визначають властивості захисту документів у графічних засобах захисту

Таке розширення методів стеганографічного укриття інформації в різних середовищах, і насамперед в інформаційних середовищах, дозволяє значно ширше використовувати стеганографію для захисту документів, а особливо тих форм документів, які сьогодні вважаються перспективними. Для сучасних документів характерним є включення в їх склад різних функціонально орієнтованих конструктивних елементів, що суттєво розширює можливі способи реалізації засобів захисту документів, включаючи можливість ширшого застосування стеганографічних способів створення засобів захисту. Для того щоб продемонструвати можливості використання стеганографії для створення засобів захисту документів, розглянемо основні їх типи, які сьогодні вже застосовуються і прогнозують новий напрям розвитку документів.

До класів документів з новою конструкцією можна віднести документи, що посвідчують їхнього власника. Типовим зразком такого документа є пластикова картка для посвідчення особи [33], якою в майбутньому передбачається замінити класичні посвідчення книжкового типу, якими є паспорти громадян. Карткові документи виготовляються у вигляді картки двох типорозмірів. На картках розміщується зона візуальної перевірки та машинозчитувальна зона, для зчитування якої застосовуються технології з оптичним розпізнаванням знаків [34]. Крім того, на картці є зона співіснуючих технологій. У картках використовується уніфікація розміщення інформаційних відомостей за допомогою поділу картки на інформаційні зони. В окремих зонах розміщуються такі елементи:

— заголовок документа;

— особливі дані;

— підпис власника документа;

— ідентифікатор системи тощо.

У зоні візуальної перевірки розміщується зображення особи. Зчитування даних з машинною перевіркою здійснюється пристроями, орієнтованими на відповідні типи носіїв інформації, з яких такі зони компонуються. Такими носіями можуть бути:

— контактні елементи;

— безконтактні чіпи;
— магнітна стрічка;
— оптична пам'ять;
— двомірний штрих-код та інші.

У таких карткових документах переважно використовують чіпи, на яких розміщується оперативна пам'ять розміром не менше 128 байтів та постійна пам'ять розміром не менше 2048 байтів. Термін експлуатації таких карточок понад десять років. Протягом цього часу карткові документи повинні зберігати свої фізичні властивості у діапазоні температур від 35 до 90 °С при відносній вологості 5÷95%, а також витримувати тести з дотриманням вимог міжнародних стандартів ISO 10373. Картки виготовляються з використанням попередньо задрукованого матеріалу основи. Повноколірний друк на матеріалі основи здійснюється з роздільною здатністю не меншою ніж 600 точок на дюйм, допуски на розміри становлять ±0,754 мм, товщина ламінаційного шару — 0,25–1,25 мм. Вимоги до захисту документів карткового типу визначаються вимогами міжнародної організації ICAO «Машинозчитувальні проїзні документи». Матеріал, з якого виготовляються карткові документи, контролюється державними установами.

Розглянемо інші типи документів спеціального призначення, з точки зору забезпечення їх захисту від підробки, фальсифікації та несанкціонованого використання, які є основними видами атак на документи. До документів спеціального призначення, окрім посвідчень особи (паспорта, прав водія, перепусток тощо), належать: акцизні марки; дипломи, атестати; поштові марки.

Акцизні марки мають досить багато засобів захисту, оскільки їх функціональна орієнтація найбільш схильна до різного типу атак. Для нанесення зображення на акцизну марку застосовується офсетний або металографський друк. Гільйоширні, гравюрні елементи, лінійні сітки та різні растри друкуються ірисним друком. В акцизній марці застосовується мікротекст. Для друкування захисних елементів використовуються захисні фарби різного призначення. Важливими засобами захисту інформації на акцизній марці є голографічні елементи, захист за допомогою перфорації та нуме-

рації. Голограми, що застосовуються для захисту, можуть мати різну структуру, це можуть бути 3D-голограми чи стереограми. Нумерація, що наноситься на марку, може бути надрукована різними способами, наприклад, традиційним високим друком, з використанням захисних фарб, ударними принтерами чи лазерними нумераторами. Для здійснення нумерації може застосовуватися фігурна висічка та перфорування, що дозволяє розпізнавати повторне використання одного і того ж документа.

До окремої групи документів належать дипломи, атестати, посвідчення та цінні папери. Для документів цієї групи характерним є їх порівняно малий тираж та висока вартість кожного окремого документа. Цю групу документів характеризують такі технологічні особливості.

Оригінали документів проектуються із застосуванням сучасних технологій. Конструкція документів проектується на основі технічних вимог замовника. Для виготовлення вищевказаних документів використовуються такі засоби захисту:

— текстові елементи;
— штрихові елементи;
— фонові елементи;
— півтонові елементи в різних комбінаціях з плавним або дискретним органічним об'єднанням з іншими елементами та ін.

Висока якість виготовлення таких документів забезпечується використанням великої кількості гарнітур і зміною кегля шрифтів, різноманіттям готових рисунків, слайдових елементів, тангірних сіток тощо. Проте основною особливістю застосування вищевказаних засобів є те, що їх створення та нанесення визначається художником-дизайнером. Ця обставина забезпечує або може забезпечити високий естетичний вигляд відповідного документа, хоча однією із основних вимог до документів є досягнення необхідного рівня його безпеки, для чого і створюються при його проектуванні описані вище компоненти та технологічні прийоми. В цьому полягає одна із суперечностей, яка має місце в галузі виготовлення документів. Друга суперечність полягає у тому, що вимоги до документів, включаючи вимоги до використання різних засобів захисту,

формулює замовник, який може не бути фахівцем в поліграфічних технологіях і в сфері захисту документів. У свою чергу виробники документів, які є фахівцями в поліграфії та в методах захисту поліграфічних продуктів, належать до виконавчої сторони в замовленні до друку, з дорадчими функціями для замовника. Поштові марки та блоки марок належать до категорії документів, які займають проміжну ланку між звичайним документом та грошовою асигнацією, оскільки на них в процесі друку встановлюється ціна відповідного документа. Проте, з точки зору захисту, поштова марка має значно менше засобів захисту і, відповідно, нижчий рівень захисту порівняно з асигнаціями [35].

Основною, принциповою вадою існуючих засобів захисту є те, що більшість з них не піддається досить точній оцінці, яка б визначала міру захисту, котру цей засіб у кожному окремому варіанті його використання може забезпечити. Це зокрема призводить до неоптимального використання досить дорогих технологій створення засобів захисту документів, і тому часто виникає ситуація, коли дорогі засоби захисту не відповідають реальним вимогам до рівня скритості документів. Існування такого стану справ зумовлено наступними факторами:

— проблемами захисту документів повинні займатися фахівці, які їх проектують і виробляють;
— необхідні такі засоби захисту, які дозволили б достатньо адекватно оцінювати величину рівня захисту;
— потрібна інформаційна система, яка б на основі різних методів забезпечувала визначення необхідного рівня захисту кожного документа на основі даних про атаки на них у процесі їх експлуатації.

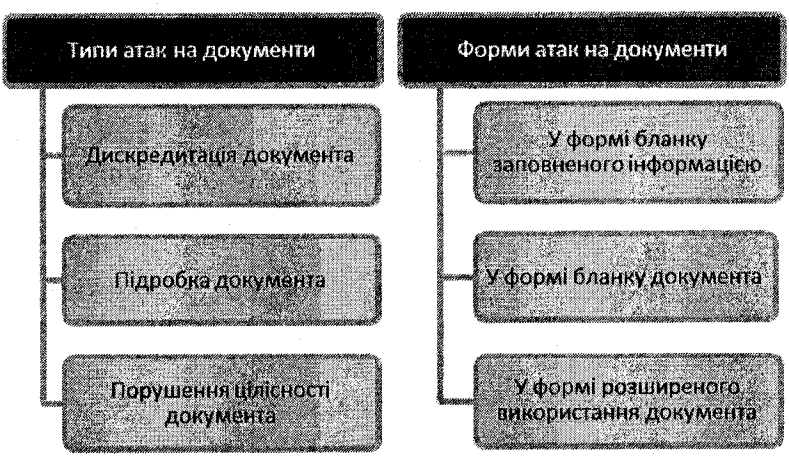
Одним із напрямів розв'язку другої з вищевказаних проблем є створення таких графічних засобів захисту, які дозволили б оцінювати рівень безпеки, який вони гарантують, із достатньою точністю.

ОСОБЛИВОСТІ ПОБУДОВИ МОДЕЛЕЙ ЗАСОБІВ ЗАХИСТУ ДОКУМЕНТІВ

Логічні засоби опису моделей графічних засобів захисту документів та цінних паперів

Використання засобів захисту документів має сенс лише за умови, якщо існують небезпеки та ініційовані ними атаки на документи (рис. 9, а). Що стосується поліграфічних документів, то більшість атак на них зводиться до:

— підробки документів;
— порушення цілісності документів;
— дискредитації документів.



а *б*

Рис. 9. Типи та форми атак на документи

Поліграфічний документ може бути поданий у таких формах (рис. 9, б):

— бланк документа;
— бланк, заповнений інформацією з повністю завершеною системою захисту документа;
— розширеного використання.

Коли документ є у формі бланка, то на ньому розміщуються тільки засоби захисту, які використовуються для цілого класу певного типу документів. Це не означає, що система захисту бланка документа не може бути повною або завершеною. Атаки на бланки документів переважно зводяться до атак типу підробок. У цьому випадку небезпека підробки засобів захисту полягає у тому, щоб відповідну підробку було не можливо виявити. Процедури виявлення підробки бланків документів, які здійснюються в рамках інформаційної технології гарантування безпеки документів, значно ширші від процедур, що ґрунтуються на основі використання графічних засобів захисту. Насамперед таке розширення пов'язане з тим, що виробник бланків документів та виробники документів, які використовують відповідні бланки, розподілені в просторі і часі. В цьому випадку можна застосовувати лише процедури контролю бланків документів та документів у цілому, які ґрунтуються на використанні тільки засобів захисту, а саме — графічних засобів захисту. Окрім того, бланк як елемент матеріального продукту в процесі виробництва отримує цілий ряд параметрів та ознак, які безпосередньо не відображаються на ньому або можуть відображатися частково в межах бланка документа. До таких параметрів належать:

— тираж друкування даної партії бланків;
— ідентифікатор чи номер партії;
— дані про кількість і типи графічних засобів захисту, що використовуються для бланків даного типу;
— параметри засобів захисту;
— характеристики процедур контролю;
— параметри, що характеризують взаємозв'язок між окремими засобами захисту, які використовуються в рамках бланка;
— способи застосування бланка;
— функціональне призначення бланка;
— дані про технологічні особливості виготовлення бланка.

Тираж певної партії бланків, ідентифікатори номера тиражу або партії документів, як правило, вказуються на допоміжних

технічних полях бланка. В рамках ідеології використання інформаційних технологій захисту документа, таку інформацію надавати у відкритому вигляді, як це робиться сьогодні, не доцільно. Річ у тому, що така інформація може використовуватися для захисту відповідних бланків, а її передача може здійснюватися на основі використання інформаційних зв'язків, що в рамках інформаційної технології існують між усіма учасниками процесу легального виробництва, використання та контролю документів. В цьому випадку ідентифікатори, якими, по суті, є дані про тираж, номер замовлення, номер тиражу та координати виробника, можуть бути замінені ідентифікаторами, наприклад, виробника документа, які реалізуються на бланку у скритій формі. Одним із таких методів укриття може бути метод, що ґрунтується на застосуванні стеганографії.

Іншою особливістю застосування інформаційної технології, що також ґрунтується на існуванні інформаційних зв'язків між учасниками технологічного процесу використання документів, є можливість формування інформаційних доповнень до засобів захисту, що використовуються у документах, завдяки чому з'являється можливість суттєвого розширення функцій захисту відповідних засобів [36].

Наступною особливістю є формування додаткових функціональних можливостей захисту за рахунок створення системи захисту документа, яка складається з окремих засобів захисту і об'єднує їх таким чином, що система захисту в цілому здобуває додаткових функцій [37].

Однією з найважливіших властивостей засобів захисту, яких набуває система захисту та окремі її захисні засоби, є її здатність кількісно оцінювати величину рівня захищеності на основі даних про реальні значення параметрів системи захисту та параметрів окремих засобів захисту.

Використання системи захисту документів дозволяє не обмежуватися в процесі контролю документа лише визначенням величини тих чи інших параметрів, що характеризують засоби захисту, а формувати методи контролю, які полягають у встановленні параметрів та особливостей зв'язків між окремими засобами

захисту. Такі зв'язки можуть мати функціональний характер, завдяки чому є можливість обчислювати значення відповідної функції на основі значень виміряних параметрів окремих засобів захисту [38]. Крім того, зв'язки між окремими параметрами різних засобів захисту та параметрами, що характеризують зв'язки між окремими засобами захисту в межах всієї системи захисту, можуть описуватися логічними функціями. Для таких логічних функцій є можливою така інтерпретація її значення, що полягає у твердженні, чи документ атакований, чи ні.

Специфіка проблеми захисту документів за допомогою графічних засобів захисту полягає у наступному. Для документів, як певного типу об'єктів захисту, поняття успішної чи неуспішної атаки та поняття про те, що документ є атакованим, суттєво відрізняється від понять для інших технічних об'єктів, для яких задачі захисту зводяться до захисту інформаційних систем, що функціонують на основі комп'ютерних засобів [39, 40]. Ця відмінність полягає у тому, що стосовно документів можна говорити про те, чи вони атаковані, чи ні, при цьому в першому випадку атака виявлена або не успішна. Це означає, що система захисту або окремі засоби захисту дозволили виявити атаку і так захистили документ. Таким чином, фізично захищений документ не придатний до подальшого використання і має бути замінений аналогічним не атакованим або, наприклад, не підробленим екземпляром документа. Тоді як захищена інформаційна комп'ютерна система після виявлення атаки і, відповідно, її ліквідації, може безпечно продовжувати свою роботу.

З вищенаведеного випливає що, більш коректно можна аналізувати не захист окремого документа, а технологічного процесу, на обслуговування якого він орієнтований. Здебільшого у технологічних процесах, що містять системи документообігу, використовується деяка система різних за своїм функціональним призначенням документів. Тому при виявленні одного атакованого документа з такої множини різнотипних документів технологічний процес не перестає функціонувати, а лише виключає атакований документ із системи обслуговування, що допускає у більшості

випадків можливість продовжувати безпечне функціонування процесу при відповідній його модифікації.

Таким чином, завдяки інформаційній технології захисту проблеми захисту певних документів можна розглядати в контексті захисту технологічного процесу, який використовує відповідні документи. При цьому основні аспекти інформаційної технології захисту повинні зосереджуватися на засобах та системах захисту, що розміщуються на документах. При такому підході дається додаткова можливість управління рівнем захисту згідно з вимогами до технологічного процесу виготовлення відповідних документів. Отже, стає можливим враховувати цілий ряд об'єктивних факторів, що можуть визначати або впливати на визначення рівня захисту для кожного окремого документа для обслуговування певного технологічного процесу. До таких факторів слід віднести:

— загрозу, яка може визначатися певним рівнем захисту окремого документа відносно величини його впливу на безпеку технологічного процесу, який цей документ використовує;
— методологію контролю документа, яка є можливою або яку зумовлює технологічний процес (ТР) у відповідному фрагменті свого функціонування, в якому він використовує даний документ;
— дані про порушення безпеки технологічного процесу, що зумовлюються певним рівнем захисту окремого документа;
— модифікації ТР, що зумовлені цілями задач, що розв'язуються ТР, які зокрема зумовлюють необхідність модифікації засобів захисту і системи захисту документа в цілому;
— зміну змісту документа, який формується шляхом заповнення відповідного бланка тією чи іншою інформацією, що стосується ТР.

Вищенаведене розширення вихідних вимог до визначення необхідної міри захисту, яку повинен мати певний документ, дає змогу застосовувати для розв'язання цих задач нові підходи та модифіковані методи побудови засобів захисту. Новий підхід в даному випадку полягає у можливості використання математичної логіки [41] для опису взаємозв'язків між окремими засобами

захисту в рамках системи захисту документа, для опису залежностей між засобами захисту та зовнішніми щодо окремого документа факторами, які діють в рамках технологічного процесу, що використовує документи. Крім того, в цьому підході існує можливість апроксимації опису окремих засобів захисту, що мають складну структуру, з різною мірою точності їх відображення.

Можливість модифікації методів побудови графічних засобів захисту розглядатимемо стосовно латентних образів. При цьому модифікація їх побудови може ґрунтуватися на більш широкому застосуванні методів, що відомі в стеганографії [42].

Перш ніж розглядати окремі випадки використання математичної логіки розглянемо можливості, які можуть виникнути завдяки цьому (рис. 10).

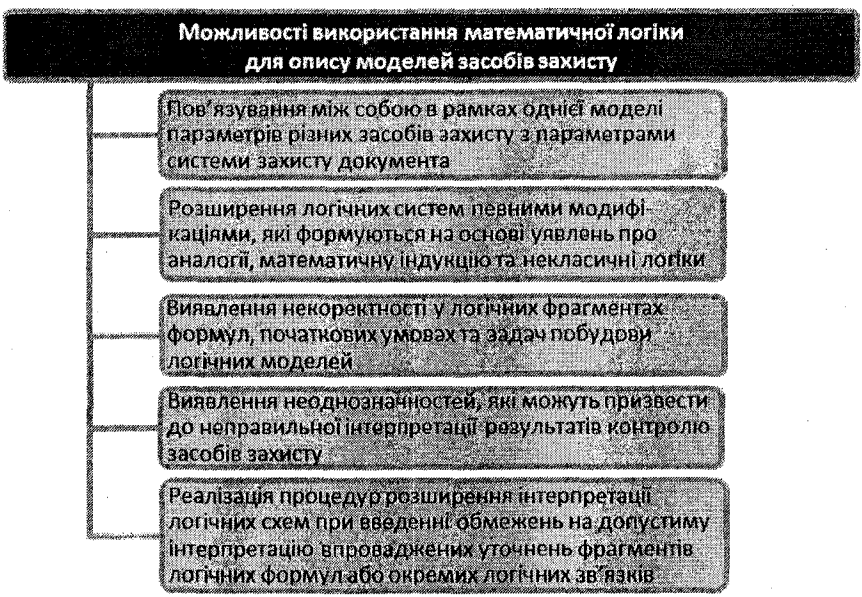


Рис. 10. Можливості використання математичної логіки в моделях засобів захисту документів

До таких можливостей слід віднести:

— математична логіка дозволяє формувати опис залежностей на найбільш загальному рівні, завдяки чому виникає можливість пов'язувати між собою в рамках однієї моделі: параметри різних засобів захисту; параметри, що характеризують зовнішні відносно документів чинники з параметрами системи захисту документа та описувати всі ті зв'язки між параметрами засобів захисту документів, які можуть призводити до зміни рівня захищеності в рамках системи захисту документа;

— завдяки уявленням про суперечності в логічних співвідношеннях та розширеннях інтерпретації поняття логічної суперечності з'являється можливість виявляти некоректність у логічних фрагментах формул та у початкових умовах задач побудови логічних моделей;

— з уявлення про повноту логічної системи, що складається з правил перетворення логічних формул та базових визначень, які прийнято називати аксіомами, стає можливим виявляти неоднозначності, які можуть призвести до неправильної інтерпретації результатів контролю засобів захисту;

— в рамках математичної логіки є можливість розширити логічні системи певними модифікаціями, які формуються на основі уявлень про аналогії, математичну індукцію, некласичні логіки тощо;

— логічні співвідношення та формули допускають реалізацію процедур розширення інтерпретації логічних схем введенням обмежень на допустиму інтерпретацію впроваджених уточнень фрагментів логічних формул або окремих логічних зв'язків.

Розглянемо теоретичні та інтерпретаційні аспекти вищевказаних можливостей. Одним з найпоширеніших способів контролю параметрів графічних засобів захисту є порівняння ідентичності образу на документі з образом зразка або з еталоном. Ця обставина призводить до того, що захисні властивості відповідних засобів полягають у точності повторення відповідного образу на документі згідно з еталонним образом. Суттєвим недоліком такого стану

справ є потреба використовувати велику кількість точок еталонного образу для порівняння з образом документа. Застосування логічних моделей систем захисту документа дозволить спростити методику контролю документів таким чином, щоб достовірність такого контролю порівняно з традиційними методами контролю не зменшилась. Методи контролю в рамках ідеології використання інформаційної технології стають одним із ключових моментів у задачах захисту документів і, відповідно, технологічних процесах. Це можна здійснити лише в рамках моделей, що пов'язують опис системи захисту окремого документа з описом методології контролю документа в ТР, а це можна реалізувати лише на основі застосування логічних методів.

Розглянемо, як уявлення про суперечність у системі логічних формул може бути використане для підвищення достовірності контролю. Для цього введемо наступні уявлення. Нехай в результаті порівнянь певних фрагментів засобів захисту з відповідними фрагментами еталонних образів деякі фрагменти не збігаються з еталоном з певною розбіжністю в значеннях параметрів, відносно яких контролюється збіжність. Це означає, що існує можливість записати деяке логічне співвідношення, в якому логічним змінним, що ідентифікують параметри, приписується значення, наприклад, «1», якщо відповідні параметри збіглися з необхідною точністю, і значення «0», якщо не збіглися [43]. Якщо в такій сукупності параметрів вони використовуються незалежно один від одного, і умовою ідентифікації документів є задана міра збіжності образів, що порівнюються за всіма параметрами, то відповідна формула запишеться у вигляді:

$$L_i = x_1 \& , \ldots , \& x_n ,$$

де x_i — параметри, за якими порівнюються образи. Така формула відображає найпростіший спосіб контролю окремого документа. В цьому випадку дискредитується геометрична структура графічних засобів захисту. Геометричну складність образу можна відобразити у вигляді логічних формул. Очевидно, що таке відображення можливе за умови, що прийняті певні домовленості стосовно інтерпретації

логічних функцій, які використовуються для побудови логічної формули, правила стосовно інтерпретації змінних та значень логічної формули в цілому. В найпростішому випадку приймемо, що формула $L_i = \varphi(x_1,...,x_n)$ рівна «1», якщо документ виявляється оригінальним і $L_i = \varphi(x_1,...,x_n) = 0$, — у протилежному випадку, а інтерпретація змінних x_i буде така, як наведена вище. Слід зазначити, що структура графічного образу може залежати від особливостей технології їх створення, що значно розширює захисні властивості відповідних графічних засобів.

Як приклад структурної інтерпретації таких логічних функцій, як диз'юнкція, імплікація та заперечення можуть бути наступні інтерпретації. Диз'юнкція означає надмірність з'єднаних між собою параметрів при визначенні оригінальності документа [44]. Нехай в L_i існує фрагмент $\{x_i \vee x_{i+1} \vee x_{i+2} \vee ...\}$, тоді згідно з інтерпретацією L_i, якщо цей фрагмент рівний «1», то в його межах існування заперечень $\neg x_{i+j}$ не впливає на загальне значення формули L_i. З традиційної точки зору, невідповідність одного з параметрів еталонному значенню повинна розглядатися як невідповідність документа його оригінальному походженню. Однак, якщо взяти до уваги, що рівень безпеки документів є величиною змінною, яка змінюється від одного типу документа до іншого, а графічні засоби захисту у різних документах можуть мати однаковий сюжет, то можливість існування параметрів з різною мірою відповідності еталонному образу є достатньо обґрунтованим. Іншим аспектом, який обумовлює можливість існування описаної вище ситуації, є те, що безпека документа і, відповідно, ТР однаковою мірою залежить як від засобів захисту, так і від методики контролю документів. У цьому випадку в рамках методології контролю документів не розглядається методика абсолютного контролю документа, яка характерна для процесів експертизи документів, а лише ті методи контролю, які здійснюються в процесі реалізації ТР. Це обумовлюється тим, що експертиза документів здійснюється лише тоді, коли успішно атаковано ТР в

цілому, і результати такої атаки є підставою для проведення експертизи. Через об'єктивні причини рівень контролю документів у різних фрагментах ТР є різним, а формула L_i в загальному випадку має повною мірою описувати достовірність документа, що контролюється, в процесі його експертизи. Тому використання диз'юнкції окремих параметрів захисту відображає можливі варіанти реалізації контролю документів у різних фрагментах ТР [45]. Це означає, що у випадку, коли з технологічних причин у деякому фрагменті ТР можна контролювати разом з іншими параметрами параметр x_i, то в інших фрагментах ТР повинні контролюватися параметри x_j, x_{j+1} тощо, а параметр x_i може бути упущеним, що для відповідної змінної означає інтерпретацію $x_i = 0$. Припустимо, що для кожного випадку контролю документа можна скласти окрему логічну функцію L_i^k, тоді буде втрачене загальне уявлення про стан контрольованого документа на кожному кроці контролю, який відповідає його окремому фрагменту. Оскільки йдеться про використання інформаційної технології захисту, то можна прийняти, що всі фрагмент ТР, в яких здійснюється контроль документів, пов'язані між собою як мінімум в частині інформування про результати контролю у кожному фрагменті ТР.

Імплікація як логічна функція має одну суттєву особливість відносно & чи V — вона не є комутативною. Це означає, що $(x_i \to x_j) \neq (x_j \to x_i)$. Загалом це означає, що вона встановлює певний порядок на множині змінних, на якій вона визначена. Оскільки такими змінними є параметри засобів захисту, то така функція визначає порядок контролю параметрів, що характеризують засоби захисту на підмножині параметрів, які пов'язані цією функцією. Наявність такого порядку на множині параметрів $\{x_1,...,x_n\}$ зумовлюється мірою величини захищеності, яку визначає окремий параметр відносно іншого параметра, а різна міра захищеності, що забезпечується різними параметрами, є наслідком існування структурних факторів у засобах захисту, які також мають свою міру захищеності. Функція імплікації в даному випадку може

інтерпретуватися таким чином для окремого процесу контролю документа, якщо параметр x_i в $x_i \to x_j$ перевірено, і він підтверджує достовірність документа, то результат перевірки x_j в рамках даного фрагмента процесу контролю не впливає на результат інтерпретації фрагмента контролю $x_i \to x_j$. Таким чином, окремі фрагменти L_i можна використовувати для формування окремих методів контролю документів.

Особливо важливою логічною функцією є функція заперечення «$\neg$», оскільки її наявність забезпечує повноту функціональної системи [46]. Ця функція одномісна і означає заперечення значення змінної або предиката, перед яким вона використовується. В рамках предметної області засобів захисту документів, яка об'єднується з областю контролю документів, якщо x_i=1 відповідає ознаці оригінальності документа, то $\neg x_i$ може означати відсутність необхідного контролю даного параметра при реалізації процедури контролю, що відповідає даному фрагменту L_i. Така інтерпретація $\neg x_i$ не є суперечною, оскільки можна вважати, що коли x_i=0, то це означає негативний результат контролю параметра x_i або відсутність в процедурі контролю перевірки x_i. Негативний результат контролю x_i в рамках системи захисту не мусить означати наявності атаки на документ [47], оскільки в ряді документів може використовуватися один і той самий засіб захисту, для яких він забезпечує різні рівні захисту. Прикладом такого засобу захисту може бути голограма.

Використання формальних граматик і теорії автоматів для опису та дослідження моделей графічних засобів захисту

Графічні образи, що використовуються як засоби захисту незалежно від способу їх відображення, мають певну інтерпретацію, наявність якої означає можливість побудови детермінованого алгоритму, за допомогою якого можна побудувати ключові

фрагменти образу. До неключових фрагментів образу належать допоміжні частини типу тіней, кольорових заливок, фонів тощо. Основною ознакою базових фрагментів образу є наявність у них контурів окремих фрагментів образу, що пов'язані між собою, або контуру всього образу, який можна однозначно виділити в графічному образі. Довільний контур або ряд контурів можна апроксимувати за допомогою певної кількості, переважно скінченої, графічних примітивів або за допомогою одного примітиву. Вибір масштабів таких примітивів та їх типу дозволяє забезпечити необхідну точність апроксимації контуру графічного образу. Лінії, що апроксимують відповідні контури, являють собою геометричні примітиви і їх можна інтерпретувати, як деяку мову $L(M_i)$, яка породжується певною граматикою G. Тут апроксимація може реалізовуватися не тільки при масштабуванні графічних примітивів, а й за допомогою вибору дискретної множини допустимих орієнтацій окремих примітивів щодо примітиву попередника. Загальноприйнятий спосіб визначення допустимих орієнтацій полягає у визначенні та виборі певної структури площини, якщо розглядаються образи на площині, з заданою метрикою, яка, по суті, і визначає масштабування апроксимуючих геометричних примітивів [48]. Структура простору при її виборі визначає можливу кількість дискретних орієнтацій, які у відповідній структурі є допустимими. Наприклад, при виборі структури площини, що задається прямокутною сіткою, кількість можливих орієнтацій для поточного примітиву дорівнює 7. Загалом кількість таких орієнтацій дорівнює $m = n - 1$, де m — кількість допустимих дискретних орієнтацій для поточного примітиву, n — кількість вершин найближчого оточення точки, з якої виходить черговий геометричний примітив. При побудові апроксимуючої кривої один напрямок або одна орієнтація віднімається, оскільки вона зайнята попереднім геометричним примітивом.

На рис. 11 наведено опис графічних засобів захисту за допомогою методу формальних граматик із задачами, які необхідно розв'язувати для побудови графічних засобів захисту.

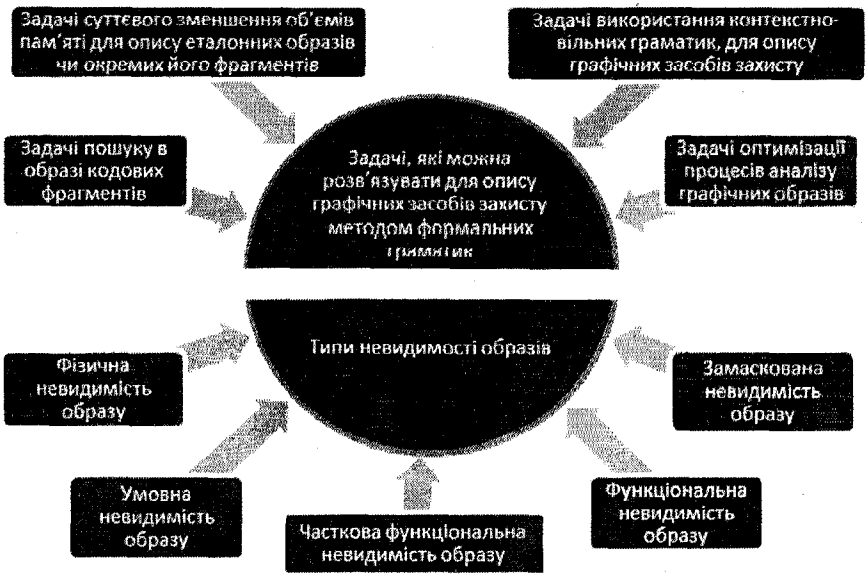


Рис. 11. Задачі, які розв'язуються для опису графічних засобів захисту методом формальних граматик та типи невидимості образів

Використання мови $L_t(M)$ для опису контурів графічних образів дозволяє формувати та розв'язувати цілий ряд задач, безпосередньо пов'язаних з побудовою, аналізом та контролем відповідних графічних засобів захисту. До таких задач можна віднести побудови латентних образів, що мають різну міру невидимості:

- задачі суттєвого зменшення об'ємів пам'яті для опису еталонних образів чи окремих його фрагментів;
- задачі оптимізації процесів аналізу графічних образів;
- задачі пошуку в образі кодових фрагментів;
- методи збереження однозначності побудови латентних частин графічного образу;
- розв'язність регулярних мов, що використовуються для опису графічних образів;
- проблеми застосування контекстно вільних граматик для опису графічних засобів захисту.

Перш ніж детально досліджувати кожну з вищенаведених задач коротко проаналізуємо та розглянемо їх інтерпретацію у галузі використання графічних засобів захисту.

Латентність передбачає невидимість цілого образу або його фрагмента. Невидимість може бути:

— фізичною невидимістю образу;

— умовною невидимістю образу;

— функціональною невидимістю;

— частковою функціональною невидимістю;

— замаскованою невидимістю.

Фізична невидимість образу використовується в поліграфії для створення графічних засобів захисту і полягає в тому, що невидимий образ стає видимим чи проявляється в результаті дії на поверхню, на якій він розміщений, певних фізичних чинників, теплового або ультрафіолетового випромінювання тощо.

Умовною невидимістю латентного образу називається такий спосіб забезпечення невидимості графічного образу, який тим чи іншим способом нанесено на папір, що забезпечує його невидимість при звичайному спостереженні образу [49]. Однак при використанні стандартних, загальнодоступних засобів або при зміні умов його огляду, що не потребують додаткових засобів, відповідний образ стає видимим. Наприклад, спостереження водяного знака на просвіт або використання побутової лупи для зчитування мікротексту і т. д.

Функціональна невидимість образу полягає у наступному. Нехай маємо деякий образ з визначеною інтерпретацію і деяким сюжетом. Коли образ має сюжет, то це означає, що він має додаткову загальноприйняту інтерпретацію в предметній області об'єктивної реальності, наприклад, образ зображує портрет деякої особи, краєвид, будинок тощо. Тоді функціональна невидимість полягає у тому, що в рамках відповідного образу існує деякий додатковий фрагмент або додатковий образ, який суміщено з сюжетом, якщо загальне зображення не змінює такий сюжет, відображає, або суміщене з інтерпретацією загального образу, то при перегляді образу відповідний фрагмент або додатковий образ є

невидимий. При цьому він не може бути розпізнаним без додаткових даних, які дозволяють його відтворити або доповнити. Такі додаткові дані, як правило, розміщуються в засобах контролю відповідних документів, що використовуються для обслуговування певних технологічних процесів. Функціональна невидимість може виникати й у випадку, коли образ не має сюжету, а тільки певну інтерпретацію. В цьому випадку інтерпретація, яку описує латентна частина образу, в загальному образі відсутня.

Часткова функціональна невидимість полягає у наступному. Нехай деякий графічний образ має певну інтерпретацію, тоді латентний фрагмент образу забезпечуватиме часткову функціональну невидимість, якщо видимі фрагменти образу дозволяють здійснити повний опис інтерпретації відповідного графічного засобу захисту. Оскільки в даному випадку послуговуються уявленням про повну чи не повну інтерпретацію графічних образів, то необхідно уточнити поняття про інтерпретацію, яке використовується в даному випадку. Формально, інтерпретація визначається таким чином.

Визначення 2.1. Опис інтерпретації I являє собою сукупність об'єктів X; опис зв'язків між ними F, які можуть бути конструктивними або функціональними; сукупність параметрів P, що характеризують відповідні об'єкти та зв'язки, та множину значень A параметрів P, яка формально описується співвідношенням:

$$I = (X, F, P, A).$$

Визначення 2.2. Образом називається окрема структура $\sum$, що побудована на основі використання $\{x_{i1}, ..., x_{in}\} \subset X$, зв'язків між x_i і x_j $\{f_{i1}, ..., f_{im}\} \subset F$, в якій забезпечуються задані значення $\{a_{i1}, ..., a_{ik}\} \subset A$ параметрів $\{p_{i1}, ..., p_{ik}\} \subset P$.

Формально окремий образ Q описується співвідношенням:

$$Q_i = \sum (X, F, P).$$

Таким чином, довільний образ будується відповідно до вибраної інтерпретації I, навіть, якщо останній являє собою певну графічну абстракцію. Процес інтерпретації, який, на відміну від

опису інтерпретації I, позначатимемо літерою J буде відображенням образу Q_i в систему I, що можна записати у загальноприйнятому вигляді:

$$J: Q_i \to I, \text{ або } J(Q_i) = \Phi(\Sigma, A),$$

де Φ — деяка функція, або система правил, за допомогою якої за заданим образом Q_i вибирається відповідний фрагмент в I із заданими значеннями параметрів $\{a_{i1},...,a_{ik}\}$. В рамках опису інтерпретації I існує система правил F, яка, крім зв'язків між x_i і x_j, описує правила формування нових f_i. Оскільки говорити про наявність усіх необхідних f_i для довільного образу Q_i з області інтерпретації I не доцільно, то в процесі інтерпретації $J(Q_i)$, якщо в образі Q_i не вистачає необхідних компонент типу f_i чи x_i, то вони можуть бути в I виведеними чи підібраними таким чином, щоб відповідна інтерпретація $I^*(Q_i^*)$ не була суперечною. Очевидно, що в цьому випадку може виявитися, що вхідна інтерпретація образу $I(Q_i)$, за якою інтерпретувався образ Q_i, може не збігатися з інтерпретацією $I(Q_i^*)$, яка сформована на основі використання надмірності I та неоднозначності Q^*, що виникає внаслідок наявності в Q латентних фрагментів. Відповідно до вищезазначеного можна стверджувати, що часткова функціональна невидимість виникає, коли виявиться, що $I(Q^*) \neq I(Q)$ в результаті інтерпретаційного перетворення $J(Q^*)$.

При проектуванні образу Q_i він може проектуватися таким чином, що Q_i в рамках I може не мати однозначної інтерпретації. Процес проектування образу вважатимемо зворотним процесом до процесу інтерпретації J і позначатимемо $J^{-1}(Q_i, I)$. При доповненні Q_i певними фрагментами q_i така інтерпретація може уточнюватися. Формально процес $J^{-1}(Q_i)$, який призводить до

того, що виявляється можливою неоднозначна інтерпретація, яка описується таким співвідношенням:

$$J(Q_i^*) = I^1(Q_i^*) \vee I^2(Q_i^*) \vee \ldots \vee I_m(Q_i^*).$$

Додавання одного з допустимих доповнень q_i до образу Q_i^* в рамках процедур, що забезпечують захист документа, реалізується в процесі його контролю. При цьому для кожного окремого випадку використання документа може вибиратися наперед визначене доповнення q_i. Графічні засоби захисту, що застосовують такий спосіб побудови латентних фрагментів, відповідають випадку, коли обирається замаскований тип невидимості.

Поняття міри невидимості дещо специфічне, оскільки побутове уявлення про невидимість передбачає інтерпретацію цього поняття однозначно, або воно означає, що деякий об'єкт є видимим або невидимим. З викладеного вище випливає, що, по-перше, існує ряд різних способів формування невидимих фрагментів, по-друге, в кожному випадку розміри невидимих фрагментів та алгоритми для формування різних фрагментів є різними. Тому від розмірів невидимих фрагментів залежить можливість несанкціонованого їх відтворення. В цьому випадку міра невидимості латентного фрагмента визначатиметься параметрами, що характеризують його розмір, і може розширюватися параметрами, що характеризують складність алгоритму несанкціонованого відтворення невидимого фрагмента графічного засобу захисту.

Задача зменшення об'єму пам'яті, необхідної для опису еталонних образів, якщо процедура контролю документів ґрунтується на процедурах порівняння, може розв'язуватися завдяки використанню формальних граматик для їх опису [50]. Один із способів такого скорочення форми запису полягає на заміні слова, що описує фрагмент образу, його номером, який формується за лексографічним принципом. Тоді лексографічний номер слова в загальному вигляді запишеться таким чином:

$$< a_{i1}, a_{i2}, \ldots, a_{ik} >= n_{i1}^{k-1} + n_{i2}^{k-2} + \ldots + i_k ,$$

де $< a_{i1}, a_{i2}, ..., a_{ik} >$ — слово; $n_{i1}^{k-1} + n_{i2}^{k-2} + ... + i_k = N$ — лексографічний номер цього слова, де n — потужність алфавіту, k — номер позиції окремої літери в слові. Лексографічний номер нагадує запис числа в системі числення по модулю n. З наведеного опису видно, що чим менша потужність алфавіту, тим менша розрядність числа, яке описує номер слова, може бути досягнута. Очевидно, що величина слова також впливає на величину числа, яке визначає номер слова. Завдяки такій нумерації замість еталонних слів можна запам'ятовувати їх номери і в процесі контролю відповідне число перетворювати в слово, що описує фрагмент образу або контур всього образу. Алгоритм перетворення слова в номер і номер слова в саме слово розглянемо на двох прикладах. Нехай дано алфавіт потужності 3: $\{a,b,c\}$ і слово $cbaac$ у цьому алфавіті. Тоді лексографічний номер можна обчислити згідно зі співвідношенням:

$$3^4 3 + 3^3 2 + 3^2 1 + 3 = 303.$$

Зворотне перетворення лексографічного номера слова в цьому ж алфавіті можна продемонструвати наступним прикладом. Нехай 321 лексографічний номер слова в алфавіті $\{a,b,c\}$. Тоді перетворення цього номера в слово можна проілюструвати послідовністю перетворень:

$$321 = 106 \cdot 3 + 3 = (35 \cdot 3 + 1) \cdot 3 + 3 = (11 \cdot 3 + 2) \cdot 3^2 + 1 \cdot 3 + 3^0 =$$
$$= (3 \cdot 3 + 2) \cdot 3^3 + 2 \cdot 3^2 + +1 \cdot 3 + 3 \cdot 3^0 =$$
$$= 3 \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3 + 3 = 321.$$

Слово, яке відповідає даному номеру, складається з 3 літер, що вибираються на основі останньої суми і відповідає слову $cbbac$.

Іншим способом вирішення цієї задачі є використання до опису відповідних еталонів, алгоритмів безвтратної компресії чи інших алгоритмів архівізації [51]. Задачі оптимізації процесів аналізу графічних образів можна розв'язувати за допомогою математичних засобів, що ґрунтуються на використанні формальних граматик. Для цих цілей ефективним розширенням формальних граматик є теорія автоматів, яка дозволяє описувати та досліджувати процедури перетворень, характерні для формальних мов [52].

Таким чином, теорія автоматів та уявлення про автомат дозволяють досліджувати задачі аналізу граматик, що породжують ті чи інші мови. Оскільки опис контурів графічних образів засобів захисту ґрунтується на використанні граматик, то задачі аналізу графічних засобів доцільно розв'язувати в рамках теорії абстрактних автоматів. Розглянемо задачу оптимізації скінченного автомата і покажемо, як ця задача інтерпретується в рамках проблеми аналізу графічних засобів захисту. В цьому випадку вищезгадані задачі стосуються розв'язку проблем, пов'язаних із використанням латентних образів. Як уже зазначалось, однією з таких проблем є проблема забезпечення єдиного можливого варіанта відтворення латентних фрагментів графічного образу. Оскільки автомати являють собою моделі породження слів граматики L_i з вхідних слів, то рішення цієї проблеми може полягати у тому, щоб побудувати такий автомат, який би був оптимальним на множині вхідних і вихідних слів мови L_i. Очевидно, що оптимальний автомат на основі вхідного слова може породжувати єдине вихідне слово, яке відповідає оптимальному автомату. Оскільки вихідне слово породжується процесами переходів автомата з одного стану у інший, то він реалізує оптимальну послідовність переходів, яка по визначенню поняття оптимальності, повинна бути єдиною. Задача оптимізації автомата може розв'язуватися в рамках задачі його мінімізації. Завдяки використанню автоматних моделей процесів контролю і відновлення латентних фрагментів відповідними фрагментами їх образів у графічних засобах захисту, з'являється можливість здійснювати оцінку алгоритмів, що реалізують відповідні процеси. Можливість розв'язку задачі оцінки відповідних алгоритмів забезпечує можливість розв'язку задачі визначення допустимої довжини слів, що описують латентні фрагменти образу. Розв'язок цієї задачі ґрунтується на визначенні кількості відповідних станів автомата, на який накладено певні обмеження. В теорії автоматів відомо багато робіт, присвячених дослідженню методів отримання відповідних оцінок [53]. Згідно з ідеологією таких досліджень розглянемо твердження, що інтерпретується

безпосередньо в предметній області задач побудови та дослідження графічних засобів захисту. Насамперед зазначимо, що автомат формально описується у вигляді:

$$V = (A, Q, B, \varphi, \psi),$$

де A, Q, B — скінченний вхідний алфавіт, множина станів автомата та вихідний алфавіт; φ – функція переходів $q_t = \varphi(q_{t-1}, a_t)$, ψ – функція виходів $b_t = \psi(q_t, a_t)$, $A = \{a_1, ..., a_n\}$, $Q = \{q_1, ..., q_m\}$, $B = \{b_1, ..., b_r\}$. Змінні, що приймають значення з множин відповідних алфавітів, позначаються символами x, y, z. Тоді відповідні функції можна записати у вигляді $z = \varphi(z, x)$, $y = \psi(z, x)$. В цьому випадку обмежимося контекстно-залежними мовами (КЗМ), оскільки контури графічного образу будуються відповідно до певної інтерпретації образу, яка передбачає існування залежностей між окремими елементами слова, що відображається в рамках алгоритму функціонування автомата V. Довільний скінчений автомат можна розглядати, як деяку множину ініціальних автоматів V_q, які описуються канонічними рівняннями автомата, що мають вигляд:

$$\{q(1) = q; q(t+1) = \varphi(q(t), a(t)); b(t) = \psi(q(t), a(t))\}.$$

Тут під ініціальним автоматом V_q будемо розуміти автомат, який запускає наступну інтерпретацію процесу свого функціонування. Один ініціальний автомат має початковий стан q_0 і при певному наближенні можна стверджувати, що він описує перетворення одного слова, що подається на вхід автомата.

Твердження 2.1. Для множини ініціальних автоматів $\{V\}$ існує максимальне за довжиною вхідне слово, довжина якого не менша ніж $n(n-1)/2$.

Завдяки цьому твердженню на основі довжини слова, що описує контур графічного образу, можна визначити необхідний розмір автомата V, який може забезпечити аналіз слів тієї чи іншої довжини. Оскільки побудова процесу аналізу слів, що описують графічні образи, визначається інтерпретацією образу та вимогами

до забезпечення необхідного рівня захисту окремим засобом захисту є похідною від розмірів слова, то це твердження дозволяє оцінити відповідні розміри автомата, який необхідно збудувати, щоб забезпечити можливість аналізу або розпізнавання відповідним автоматом вхідного слова.

Нехай існують вхідні слова $\alpha \in A^*$ і $\beta \in B^*$, $|\alpha| = |\beta|$. Позначимо $F^*(\alpha,\beta) = \{q, \psi(q,\alpha) = \beta\}$, $F(\alpha,\beta) = \{\varphi(q,\alpha) : q \in F^*(\alpha,\beta)\}$. Якщо $|F(\alpha,\beta)| \geq 2$, то вибираємо найменше слово $\gamma \in A^*$, для якого існують різні описи q_1 і q_2 в $F(\alpha,\beta)$. Достатньо довести, що слово Ф можна застосувати до ініціального автомата V_{q0} з $[V]$, і довжина результату не перевищуватиме $n(n-1)/2$.

Розглянемо послідовність $a = a(1), a(2), \ldots$, де

$$a(i+1) = \Phi((a(1),\ldots,a(i), \psi(q_0, a(1)\ldots a(i))).$$

Позначимо:

$$a_i = a(1)\ldots a(i);\ \beta_i = \psi(q_0, a_i) = b(1)\ldots b(i);\ F_i^* = F^*(\alpha_i, \beta_i) \text{ та}$$
$$F_i = F(\alpha_i, \beta_i).$$

Зрозуміло, що виконується співвідношення:

$$F_{i+1} = \{\varphi(q, a(i+1)); q \in F_i; \psi(q, a(i+1)) = b(i+1)\}. \qquad (2.1)$$

Звідки випливає $|F_{i+1}| \leq |F_i|$. Припустимо, що послідовність α більша ніж $n(n-1)/2$. Тоді для довільного $i = 1,\ldots,n-1$ буде виконуватися $|F_{i(i+1)/2}| \leq n - i$. Нехай ця нерівність правильна для $i \leq n-2$.

Якщо $|F_{i(i+1)/2}| < n - i - 1$, тоді $|F_{(i+1)(i+2)/2}| \leq |F_{(i+1)/2}| \leq n - (i+1)$. Приймемо, що існує співвідношення $|F_{i(i+1)/2}| = n - i$. Якщо $F_{i(i+1)/2}$ розміщено в одному з класів еквівалентностей, то отримаємо, що в Q існує не менше ніж $|F_{i(i+1)/2}| + (i+1) = n+1$ елементів, що призводить до суперечності. Тому існують елементи q_1 і q_2 множини $F_{i(i+1)/2}$,

розміщені в різних класах розподілу або для деякого слова $\gamma \in A^*$ довжини $i+1$ справедливе $\psi(q_1,\gamma) \neq \psi(q_2,\gamma)$. Тепер методом індукції по j можна показати, що при $0 \le j \le i+1$ виконується співвідношення $\left|F_{(i(i+1)/2)+j}\right| < n-i$ або найкоротше слово в алфавіті A, для якого в $F_{(i(i+1)/2)+j}$ знайдуться два різні стани, має довжину не більшу ніж $i+1-j$. При j=0 це витікає з різних станів $q_1, q_2 \in F_{i(i+1)/2}$ словом γ довжини i+1. Припустимо, що твердження правильне при $j \le i$ і покажемо, що воно правильне для j+1. Якщо $\left|F_{(i(i+1)/2)+j}\right| < n-i$, то $\left|F_{(i(i+1)/2)+j+1}\right| \le \left|F_{(i(i+1)/2)+j}\right| < n-1$. Якщо $\left|F_{(i(i+0/2)+j}\right| = n-i$, то розглянемо найкоротше слово $c(1)...c(t)$, для якого існують різні описи $q_1, q' \in F_{(i(i+1)/2)+j}$, тоді справедливе співвідношення:

$$c(t) = \Phi(\alpha_{(i(+1)/2)+j}, \beta_{(i(i+1)/2)+j)}) = a((i(i+1)/2)+j+1).$$

Довжина цього слова менша від $i+1-j$.

Якщо $t=1$, то $\psi(q,c(1)) \neq \psi(q',c(1))$, або $\psi(q,c(1)) \vee \psi(q',c(1))$ відрізняється від $b((i(i+1)/2)+j+1)$.

З (2.1) випливає, що $\left|F_{(i(i+1)/2)+j+1}\right| < \left|F_{(i(i+1)/2)+j}\right| = n-i$. Якщо $t>1$, то слово $c(2)...c(t)$ розрізняє стани $\varphi(q,c(1))$ і $\varphi(q',c(1))$, що входить в $F_{(i(i+1)/2)+j+1}$, і довжина $t-1$ цього слова не більша від $i+1-(j+1)$. Якщо при $j=i+1$, то виконується співвідношення $\left|F_{(i(i+1)/2)+i+1}\right| < n-i$, або в $F_{(i(i+1)/2)+i+1} = F_{(i+1)(i+2)/2}$ є два стани, що відрізняються словом, довжина якого $(i+1)-(i+1)=0$. Останнє є неможливим [54]. Тому можна записати $\left|F_{(i+1)(i+2)/2}\right| \le n-(i+1)$. Таким чином, при $i=0,1,...,n-1$ правильне $\left|F_{i(i+1)/2}\right| \le n-i$. Якщо $\left|F_{n(n-1)/2}\right| \le 1$ і правильне $a_{(n(n-1)/2)+1} = \Phi(\alpha_{n(n-1)/2}, \beta_{n(n-1)/2})$, яке є не визначеним, тому довжина α не є більшою від $n(n-1)/2$, що

призводить до суперечності, яка доводить, що довжина слова α рівна довжині результату застосування Ф до V_{q0} і не перевищує $n(n-1)/2$.

Можна показати, що така оцінка не може бути покращеною. Розглянуте твердження дозволяє оцінити складність алгоритму розпізнавання вхідного слова, що описує окремий графічний засіб захисту, який можна використовувати для формування алгоритму відновлення латентних фрагментів.

Особливості використання теорії графів та методів стеганографії для побудови моделей графічних засобів захисту документів

Використання формальних граматик $L(m)$ та абстрактних автоматів в $L(m)$ є ефективним у тому випадку, коли різні вхідні слова не перетинаються між собою, або $L_i(m) \cap L_j(m) = 0$, де $(L_i(m) \& L_j(m)) \subset L(m)$. В більшості випадків, що обумовлюються відповідними інтерпретаціями графічних образів $j(h_i) \in J(H)$, таких перетинів складно уникнути. Для того щоб їх елімінувати в рамках теоретичних досліджень, що ґрунтуються на використанні формальних граматик і теорії автоматів, одне із слів α_i, що перетинається в точці a_i з α_j, розривається на два окремі слова. Якщо в деякій точці a_i перетинається m слів, то в цій точці розривається $m-1$ слово. Це призводить до перенавантаження відповідної мови $M_i(L)$. Для уникнення цього доцільно розширити формальний опис в $M_i(L)$ засобами теорії графів [55]. Не тільки розширення, але й застосування теорії графів для моделювання графічних засобів захисту, орієнтованих на використання латентних фрагментів, є доцільним у випадках, що визначаються певними способами побудови латентних фрагментів.

Досить поширеними методами побудови графічних засобів захисту є використання графічних образів, інтерпретація яких має абстрактний характер. До інтерпретацій, що не мають абстрактного

характеру, належать абстракції, що допускають побудову сюжету. Прикладами образів з абстрактними областями інтерпретації можуть слугувати різні візерунки, сітки, віньєтки і т. д. Для використання латентних фрагментів як засобів захисту в образах з абстрактною інтерпретацією J^A вони повинні зображати асиметричні структури. На відміну від образів з інтерпретацією, яка допускає існування сюжету J^S, латентні фрагменти в образах типу J^A можуть формуватися у видимій формі. Це означає, що відповідні фрагменти можуть розглядатися як латентні завдяки тому, що вони характеризуються параметрами, виявлення яких потребує додаткової інформації. Тоді йдеться про приховану або таємну інформацію, яку можна розглядати як деяку аналогію ключів, що використовуються в криптографії [56]. В цьому випадку виникає можливість таким чином формувати несиметричні сітки чи візерунки, щоби можна було створювати видимі контури графічних образів, що допускають інтерпретацію типу J^S. Виділення таких контурів може бути реалізоване і без використання таємної інформації, що потребує значного часу. Проте за рахунок надмірності відповідного графічного середовища виділення необхідного варіанта фрагмента образу може виявитися неможливим. Це пов'язано з відсутністю даних про параметри відповідного фрагмента, який при проектуванні певного образу прийнято як оригінал. Такого типу латентні фрагменти називатимемо замаскованими, оскільки його елементи надруковані, але на фоні графічного образу вони невидимі. Таким чином графічні засоби захисту, що формуються завдяки використанню друкарським технологіям, можуть мати латентні властивості за рахунок наступних способів їх формування (рис. 12):

— недодрукування окремих фрагментів образу, що призводить до їх фізичної відсутності в рамках графічного засобу захисту;
— маскування окремих фрагментів образу серед інших елементів графіки;
— сумісне використання вищенаведених першого і другого способів створення латентних фрагментів;

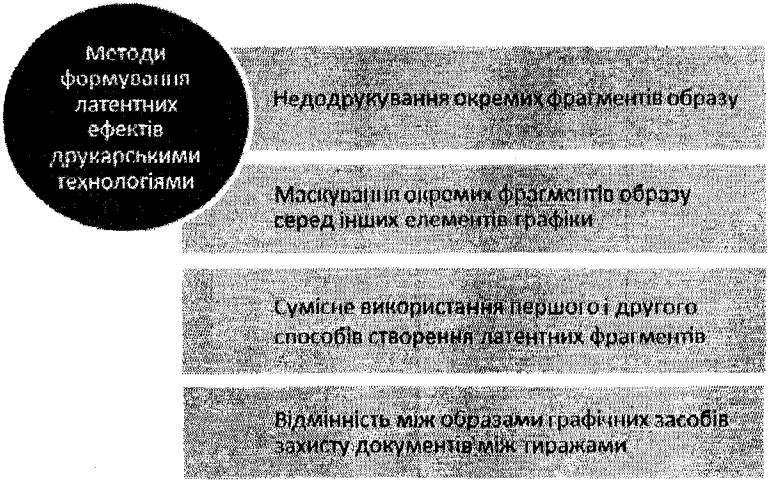


Рис. 12. Методи формування латентних ефектів друкарськими технологіями

— у випадку абстрактної інтерпретації графічних образів латентність фрагментів образу досягається за рахунок відмінностей між образами графічних засобів захисту документів між тиражами, яка є замаскованою завдяки графічній надмірності абстрактного образу і не може бути виявлена без використання спеціальних алгоритмів аналізу відповідних образів.

При застосуванні методів недодрукування окремих фрагментів для створення латентних образів засобів захисту необхідно таким чином реалізовувати латентність, щоб відсутність фрагмента була невидимою. Для цього використовується семантична надмірність графічних засобів захисту, яка може мати місце лише в тому випадку, коли інтерпретація образу є сюжетною J^S. Це означає, що образи, які застосовуються для формування латентних фрагментів, мають інтерпретацію, що відповідає реальній фізичній дійсності, яка є допустимою для користувачів документа. В цьому випадку латентні фрагменти таких образів повинні відображати семантичну надмірність в описі певного сюжету, що може вміщувати відповідну семантичну надмірність. Однак для створення

графічних засобів захисту в нашому випадку використовуються такі образи, які мають лише абстрактну інтерпретацію J^A. Однією з абстрактних моделей, яку можна використовувати для опису інтерпретації графічного засобу захисту (GZZ), є теорія графів [57]. Тому розглянемо ряд аспектів теорії графів, які можуть бути використані для розв'язку задач побудови та ідентифікації латентних фрагментів GZZ, що застосовуються в документах.

Насамперед зазначимо, що використання гільйоширних елементів, окрім загальноприйнятого їх призначення як засобів захисту, може полягати у їх інтерпретації як деякої координатної сітки, в рамках якої будуються графічні образи з $J^A(Q)$. В цьому випадку точки перетину ліній сіток розглядаються, як точки, в яких можуть розміщатися вершини графів, які складають $J^A(Q)$, а образ Q може являти собою сукупність графів, які частково або повністю друкуються на відповідних сітках і створюють абстрактний графічний засіб (GZ).

Покажемо, яким чином в абстрактній області інтерпретації можна сформулювати задачі побудови відповідних GZZ, що використовують латентні замасковані фрагменти.

Одним із факторів для вивчення закономірностей, що існують в теорії графів, є уявлення про інваріанти графів, за якими різні графи розпізнаються і, відповідно, досліджуються [58].

В рамках теорії графів поруч з іншими проблемами досліджується відновлення графів. Оскільки в нашому випадку йтиметься про графову інтерпретацію образів типу $J^A(Q)$, то відповідний графічний образ можна представити відповідною сукупністю графів. Існує цілий ряд інваріантів, що описують і дозволяють ідентифікувати граф, який необхідно відтворити. Одним з таких інваріантів є інваріант f, який в загальному вигляді записується наступним чином:

$$F(G) = f_0(G) + f_1(G)x + f_2(G)x^2 + ... + f_l(G)x^l,$$

де $f_i(G)$ — кількість повних i — вершинних підграфів графа G. Не для всіх випадків у теорії графів проблема відновлення графів може бути розв'язана. Це означає, що коли при створенні графа G

в рамках графічного засобу GZZ укрито хоча б один його повний підграф, то відновлення такого підграфа на основі аналізу довільних інваріантів є алгоритмічно складною задачею. З цього випливає, що створення латентних підграфів у рамках GZZ з абстрактною інтерпретацією $J^A(Q)$ відповідних образів Q дозволяє створити засіб захисту, підробка якого є алгоритмічно складною задачею. Отже, розглянемо особливості розв'язку задачі захисту документа на основі використання описаного підходу.

Зазначимо, що всі документи, в яких використовуються для захисту GZZ захищаються від копіювання одним з відомих методів, наприклад, шляхом застосування мікрошрифтів чи засобу Void Pantograf. Таким чином, можна обмежитися протидією до підробки документів, що не пов'язані з їх копіюванням. До проблеми відновлення графів належить проблема оточення, яка полягає у наступному. Нехай P — довільний граф, тоді можна сформулювати таку задачу, чи існує такий граф $P^* = (x,u)$, що $O(P^*,x) \approx P$ для довільної $x \in X$. Розглянутий вище варіант побудови латентного фрагмента деякого графа можна інтерпретувати при певних модифікаціях такої побудови в рамках уявлень про проблему оточення. Для звичайних графів масова проблема визначення оточення, або що для довільного P існує таке $P^*(x,u)$, що справедливе співвідношення $\forall x \in X[O(P,x) \approx P^*]$ є алгоритмічно не розв'язною.

При формуванні образів з $J^A(Q)$ для побудови математичних моделей, в яких використовується теорія графів [59], як уже зазначалось, необхідно сформувати певну структуру простору або площини, в рамках якої можна б було будувати відповідні графи, що моделюють абстрактні образи. Застосування класичних тангірних сіток, з точки зору аналізу відповідної графіки, призводить до суттєвого алгоритмічного спрощення процесу реалізації атаки на документ, що полягає у його підробці, оскільки тангірна сітка грунтується лише на поліграфічних факторах захисту. В рамках теорії графів можна пов'язати графові структури з метрикою

площини чи простору, яка допускає інтерпретацію відповідної метрики як визначення певної структури такого простору. Така можливість ґрунтується на розв'язку таких задач теорії графів:

— по даному зваженому графу $P[q]=(x,u,q)$ знайти метричний простір (x,ρ), де $\rho=\rho_G^q$;

— для даного метричного простору (x,ρ) побудувати у вигляді чіткої реалізації такий граф $G[q\}=(x,u,q)$, щоб $\rho_p^q=\rho$.

Перша задача розв'язується згідно рівності:

$$\rho(x,y)=\rho_G^q(x,y)=\min\{[q(W)/W]\in W(x,y)\},$$

де W — маршрут; x,y — вершини графа; q — вагова функція графа G; $W(x,y)$ — множина всіх простих ланок з x в y, що називається q віддалю між вершинами x і y. Віддаль, що встановлюється функцією ρ, задовольняє аксіоми, які визначають метрику на множині точок і записуються у вигляді співвідношень:

$$A1:\forall x,y\in X\{\rho(x,y)=0\Rightarrow x=y\}$$
$$A2:\forall x,y\in X\{\rho(x,y)=\rho(y,x)\}$$
$$A3:\forall x,y,z\in X\{\rho(x,y)+\rho(x,z)>\rho(x,z)\}.$$

Як приклад розв'язку вищенаведеної задачі розглянемо наступний алгоритм [60]. Нехай маємо повний граф $P_n[q]=(x,x^2,q)$. Сформуємо симетричну матрицю $\|q_{ij}\|=\|q_{ij}\|_n^n$, де $q_{ji}=q(x_i,x_j)$ і $q_{ij}=q(x_i,x_j)$. Розглянемо тернарну операцію, що описується оператором $[\alpha,\beta\gamma]$, де $\alpha\neq\beta\neq\gamma\neq\alpha$. Результатом використання цього оператора до довільної матриці $R=\|r_{ij}\|_n^n$ буде матриця, в якій обидва елементи $r_{\beta\gamma}=r_{\gamma\beta}$ будуть замінені на $\min\{r_{\beta\gamma},r_{\beta\alpha}+r_{\alpha\gamma}\}$, а решта елементів залишиться незмінними. Покажемо, що

$$\|q_{ij}\|[1,23]...[1,(n-1)n]\cdot[2,13]...[2,(n-1)n]\cdot[3,12]...[p3,(n-1)n]...$$
$$...[n,12]...[n,1(n-1)]...[n,(n-2)(n-1)]=\|\rho_{ij}\|,$$

де $\rho_{ij} = \rho^q_{P_n}(x_i, x_j)$. Це означає, що матриця $\|\rho_{ij}\|$ задає на множині X метрику $\rho = \rho^q_p$, яка утворюється з матриці $\|q_{ij}\|$ в результаті послідовного використання оператора $[\alpha, \beta\gamma]$ до неї $n(n-1)$ разів. При цьому при кожному значенні α, $\beta\gamma$ пробігає всі $\binom{n-1}{2}$ невпорядковані пари різних чисел з множини $\{1, 2, ...\alpha - 1, \alpha + 1, ..., n\}$.

Одним із розв'язків другої задачі є граф $P_n[q] = (x, x^{[2]}, q)$, де $q(x, y) = \rho(x, y)$ при всіх $x, y \in X$. В такому графі можна єдиним чином виділити суграф $P^*[q] = (x, u, q)$, який мінімізує розв'язок з кількості ребер, з суми їх довжин та інших ознак. Нехай ребро xy графа $P_n[q]$ суттєве, якщо його довжина $q(x, y)$ скінчена і не дорівнює $q(x, y) + q(zy)$ ні для якої вершини z. Такий суграф забезпечує таку ж метрику на множині X, що і граф $P_n[q]$. Це означає, що він має всі суттєві ребра $P^*[q]$. Нехай виконується умова, якщо $xy \in x^{[2]} / u$, то $q(xy) = +\infty$, або в $P^*[q]$ існує проста ланка $Q = x(xx_1)x_1(x_1x_2)x_2...x_t(x_t y)y$ з $q(Q) = q(x, y) < +\infty$ і $t \geq 1$. При $t > 1$ замість Q можна розглянути ланку $x(xx_2)x_2...x_t(x_t y)y$, для якої q — довжина рівна $q(x, y)$ через А3 і тому, що Q є q — найкоротшою ланкою між x і y до моменту, поки не виявиться ланка виду Q, але з $t = 1$. Тому ребро (x, y), що не належить суграфу $P^*[q]$ є несуттєвим в $P_n[q]$. Нехай $x, y \in X$ — дві вершини з $q(x, y) < +\infty$, а Q_{xy} — ланка, що їх об'єднує, довжина якої $q(x, y)$ в $P_n[q]$. Якщо б хоча одне ребро (a, b) цієї ланки несуттєве, то справедливо $q(ab) = q(ac) + q(cb)$ для деякої $c \in X / \{a, b\}$. Замінюючи ділянку $aabb$ на $a(ac)c(cb)b$ в Q_{xy}, отримаємо маршрут Q^*_{xy}, для якого $q(Q^*_{xy}) = q(Q_{xy})$ із збільшеною на одиницю довжиною. Цей маршрут є простою ланкою, оскільки будь-який маршрут

графа вміщує хоча б одну просту ланку, що об'єднує ту саму пару вершин. Дійсно, якщо в маршруті $x_0u_1x_1u_2x_2...x_{r-1}u_rx_r$ всі вершини різні, то цей маршрут є простою ланкою. Нехай x_i перша з вершин маршруту, яка має повторення, а x_j останнє її повторення. Тоді, викреслюючи елементи циклічної частини маршруту між x_i і x_j, можна замінити його більш коротким у вигляді:

$$x_0u_1x_1u_2x_2...x_iu_{j+1}x_{j+1}u_{j+2}x_{j+2}...x_{r-1}u_rx_r,$$

який з'єднує x_0 з x_r. Якщо в ньому є іще повторення вершин, то попередній процес заміни можна продовжувати доти, доки не отримаємо маршрут з x_0 до x_r без вершин, що повторюються, який і є простою ланкою. Тоді проста ланка мала б q-довжину $q(Q^*_{xy}) < q(x,y)$, що є неможливим. Граф з фіксованим числом вершин не може мати простих ланок довільної довжини, а вершини x і y вибирались довільно. Тому будь-які $x, y \in X$ обов'язково з'єднуються такою простою ланкою q-довжини $q(x,y)$, яка не має несуттєвих ребер графа $P_n[q]$, а це означає, що вона повністю належить його суграфу $P^*[q]$. Таким чином, граф $P^{/\prime}[q] = P[q]$ однозначно визначається в метриці (x,ρ).

Як уже зазначалось, однією з важливих задач, що виникає при побудові та використанні латентних зображень або латентних фрагментів образів, є задача санкціонованого виявлення латентного образу. Процеси виявлення латентного образу повинні забезпечувати однозначність відповідного відновлення скритого фрагмента. Покажемо можливість розв'язку цієї задачі у випадку апроксимації контурів образів графами в деякій структурі простору. Розглянемо наступне твердження.

Твердження 2.2. Якщо зважений граф $P(x,u,q)$ апроксимує образ Q, який має абстрактну інтерпретацію $J^A(Q)$, то в $P(x,u,q)$ існують підграфи $P_i(x,u,q)$, де $i = 1,...,m$, які однозначно визначаються своїм оточенням.

Доведення цього твердження повинно грунтуватися на дослідженні моделей процесів побудови латентних фрагментів в абстрактних образах. Тому в нашому випадку розглянемо тільки ряд особливостей, визначень та умов, необхідних для побудови відповідних моделей.

При використанні Q з $J^A(Q)$ в рамках структури S метричного простору $L(x,\rho)$ можна побудувати довільний граф $P_i(x,u)$, який є елементом скінченої множини графів $P(x,u,q)$, що допустимі в межах даної структури S простору $L(x,\rho)$. При використанні латентних фрагментів для захисту документів вони можуть являти собою визначені фрагменти повного графа $P(x,u.q)$. В цьому випадку під повним графом розуміється не граф Бержа [61], а граф, всі вершини якого збігаються з виділеними точками в заданому просторі $L(x,\rho)$. Такими фрагментами можуть бути: маршрути, цикли, компоненти графа, суграфи, ланцюги, підграфи, блоки і т.д.

Виділення окремого фрагмента деякого графа призводить до появи певного типу цього фрагмента, який визначається відповідними структурними ознаками. Тому наведене твердження 2.2 доцільно розглядати окремо для кожного з типів фрагментів. Крім того, визначимося з уявленнями про оточення фрагментів, що є важливою особливістю в даному твердженні. Для цього введемо таке визначення поняття оточення фрагмента $G(x^*,u^*)$ графа $P_i(x,u,q)$, яке не залежить від того чи іншого типу виділеного фрагмента.

Визначення 2.3. Оточенням $O[G(P_i)]$ фрагмента $G(x^*,u^*)$ в графі $P_i(x,u,q)$ є множина вершин $X^0 \subset P_i(x,u,q)/G(x^*,u^*)$, які є інцидентними підмножині вершин із фрагмента $G(x^*,u^*)$ і які, в свою чергу, є інцидентними до вершин з оточення.

Різні типи фрагментів графів є спорідненими або похідними один від одного, що досягається несуттєвим, з точки зору досліджуваної задачі, розширенням параметрів або конструктивних можливостей окремого фрагмента. Наприклад, маршрут відрізня-

ється від ланцюга тим, що в маршруті можуть повторюватися окремі ребра, а суграф від підграфа відрізняється тим, що суграф утворюється шляхом викреслювання ребер між вершинами в графі $P(x,u,q)$, а при виділенні підграфа, крім ребер, викреслюються і вершини і т.д.

Наступна особливість досліджуваної задачі полягає у тому, що створення невидимого фрагмента в графі $P_i(x,u,q)$ повинно здійснюватись на основі принципів стеганографії. Це означає, що факт відсутності фрагмента, який приховується, повинен бути непомітним або невидимим для звичайного користувача. Тому усунення фрагмента з графа $P_i(x,u,q)$ має здійснюватися таким чином, щоб інваріанти, які найбільшою мірою впливають на візуальне сприйняття графа, як деякого абстрактного образу, не міняли суттєво своїх значень в межах всього графічного образу. Для дослідження цього аспекту формування латентних фрагментів образу необхідно ввести інваріанти, які безпосередньо впливають на візуальне сприйняття відповідних образів. З вищевикладеного безпосередньо випливає наступна умова або обмеження.

Умова 2.1. Укриття фрагмента абстрактного образу не повинно призводити до порушення симетрій в результуючому образі:

$$R(x,u,q) = P_i(x,u,q) / G(x^*,u^*).$$

Ця умова випливає з уявлень про відмінності між уявленням про сюжет і абстракцію. Відповідно до психофізіологічних аспектів процесів сприйняття образів [62] при поступовій елімінації сюжету його сприйняття поступово заміняється сприйняттям можливих абстракцій, що характеризують образ. До таких абстракцій належать:

- міра симетрії абстрактного образу;
- наявність візуальних або графічних особливостей у межах абстрактного образу, до яких належать: характер зміни кольорів, характер зміни контрастів та розподіл інших графічних ефектів у полі або просторі образу, який спостерігається візуально;
- абстракції, що описуються інваріантами, які характеризують графи.

Використання умови 2.1 грунтується на тому, що уявлення про симетрію є досить загальним і під її визначення можна включити всі особливості, які можна візуально спостерігати в абстрактному образі, включаючи інваріанти, які такі особливості можуть визначати. Застосування інваріантів для опису асиметрії дозволяє перейти від якісного її аналізу до кількісних оцінок величини відповідних особливостей і асиметрії в цілому.

Ключовим фактором твердження 2.2 є наявність алгоритму, який однозначно дозволяє відновити укритий фрагмент графа. Беручи до уваги умову 2.1, можна стверджувати, що відповідний, скритий фрагмент повинен бути розподілений у структурі чи середовищі графа $P(x,u,q)$. Таким чином, проблема доведення можливості існування такого алгоритму може бути зведена до проблем, що досліджуються в теорії графів і пов'язані з такими факторами, як:

— досяжність вершини x_i з вершини x_j;

— уявлення про зв'язність графів;

— проблеми ізоморфізмів підграфів;

— поняття про повноту графа;

— поняття про доорієнтованість графа і т.д.

Кожне з цих понять, в свою чергу, пов'язане з іншими поняттями, дослідження яких є доцільним у зв'язку з тим, що відповідні похідні поняття призводять до задач, які значно легше розв'язати чи які вже розв'язані в рамках теорії графів [63, 64]. Коротко прокоментуємо взаємозв'язок наведених понять з факторами, що стосуються доведення існування алгоритму виявлення скритого фрагмента з твердження 2.2.

Оскільки йдеться про наявність певного оточення $O[G(P_i)]$, то це означає, що між окремими вершинами цього оточення повинні існувати ланцюги ω_i, які є елементами латентних фрагментів. Це зокрема зумовлює актуальність питань про досяжність між двома вершинами. Очевидно, що латентні фрагменти в силу їх невидимості яка реалізується їх недодрукуванням, певним чином впливає на зв'язність графів, що обумовлює актуальність дослідження питань,

пов'язаних із зв'язністю. Для визначення способів вибору підграфів на роль латентних фрагментів таким чином, щоб задача виявлення останніх була розв'язаною, доцільно використовувати уявлення про ізоморфізм між $P_i(x,u,q)$, $G(x^*,u^*)$ та $R(x,u,q)$. Аналогічна ситуація виникає і щодо інших понять та проблем [65].

ІНФОРМАЦІЙНІ КОМПОНЕНТИ СИСТЕМИ ГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ДОКУМЕНТІВ

Основні інформаційні компоненти системи графічних засобів захисту документів

При створенні інформаційних засобів, що забезпечують функціонування алгоритмів розв'язку окремих задач у системі, можна виділити такі типи (рис. 13):

— базові інформаційні компоненти;
— спеціалізовані компоненти;
— допоміжні інформаційні компоненти;
— похідні інформаційні компоненти.

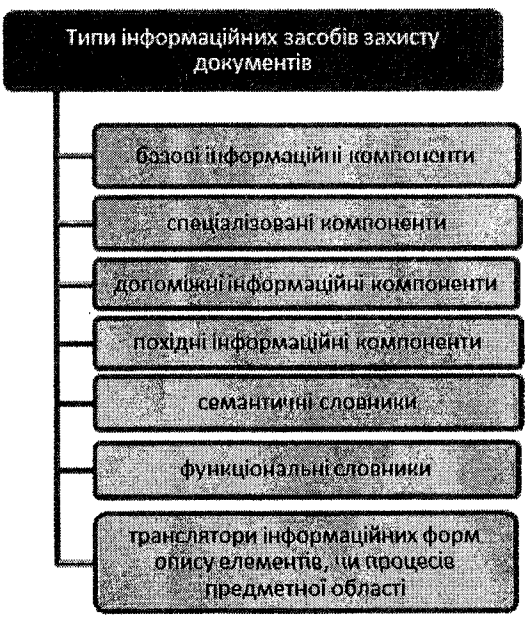


Рис. 13. Типи та компоненти інформаційних засобів захисту документів

Базові інформаційні компоненти являють собою структури, що використовуються у всіх інформаційних системах незалежно від

задач, що в них розв'язуються [66]. До таких компонент можна віднести інформаційні структури:

— семантичні словники, що описують елементи певної предметної області;
— функціональні словники, що описують процеси, які існують або можуть виникати в предметній області;
— транслятори інформаційних форм опису елементів чи процесів предметної області.

Перша і друга компоненти не являють собою унікальних структур, які було би необхідно додатково аналізувати.

Третя компонента являє собою елемент, який є більш специфічним і характерним для інформаційної системи, що ґрунтується на використанні тієї чи іншої інформаційної технології. Інформаційна форма опису елемента, що визначається в семантичному чи функціональному словнику, в більшості випадків являє собою опис деякого об'єкта природною мовою користувача відповідної системи. При цьому користувачем може бути не тільки людина, але й інша система, яка використовує власні засоби опису елементів, які можуть мати власну специфічну мову [67]. Будь-яка мова визначається правилами формування текстових фрагментів, які для зручності називатимемо реченнями або фразами [68]. Тоді така компонента як транслятор реалізує семантично допустимі способи перетворення текстових описів елементів однієї предметної області в текстові описи тих самих елементів на іншу мову. У випадку використання природних мов такі транслятори являють собою системи перекладу, які ґрунтуються на математичній лінгвістиці та інших галузях, що застосовують природні мови [69]. Оскільки інформаційні компоненти розглядаються як такі, що переважно використовують природні мови, то всі подальші їх дослідження розглядатимемо в контексті можливостей і особливостей, що визначаються природними мовами.

Спеціалізовані інформаційні компоненти відображають особливості предметної області та умови, пов'язані із специфікою дослідження та розв'язку поставлених задач. При використанні формальних засобів для опису моделей об'єктів та процесів, які у

відповідних об'єктах можуть бути реалізовані, виникає проблема рівня формалізації відповідних конструкцій. Така проблема полягає у тому, що, з одного боку, формалізація окремих аспектів досліджуваної задачі призводить до можливості отримання результатів розв'язку, які мають загальний характер. З іншого боку, що особливо характерно для прикладних задач, при певному рівні формалізації опису досліджуваних процесів та моделей втрачається ефективність інтерпретації результатів функціонування досліджуваних процесів і моделей на окремих кроках їх реалізації. Для розв'язання цієї проблеми використовуються спеціалізовані інформаційні компоненти. Наприклад, вказані компоненти можуть описувати зв'язки між вибраними формалізованими характеристиками окремих елементів предметної області. Такі описи реалізуються за допомогою мов, що використовуються при побудові інтерпретацій предметної області. Інтерпретації досить широко застосовуються в теоретичних працях, особливо в тих, що пов'язані з прикладними задачами. Беручи до уваги, що будь-яка теоретична праця використовує деяку інтерпретацію, наприклад, теорія чисел як предметна область застосовує інтерпретації арифметики [70], і рівень формалізації такої теорії пов'язаний з рівнем формалізації предметної області. У таких прикладах використання спеціалізованих інформаційних компонент є необхідним. При розв'язку прикладних задач у випадках, коли для цього необхідно використовувати формальні засоби опису, завжди застосовуються описи інтерпретації закономірностей, що існують в системі формальних засобів і відображають деяку теорію. Ці описи формуються у вигляді методик використання відповідних формальних засобів або коментарів до застосованих методів використання відповідних формальних засобів. Виділення таких інформаційних елементів в окремі спеціалізовані компоненти дозволяє отримати наступні можливості при побудові інформаційних систем:

— автоматизувати процес формування методик розв'язку задач, що потребують використання відповідних формальних засобів;

— в рамках одного розв'язку прикладної задачі об'єднати між собою формальні засоби різних теорій при формуванні відповідної методики;

— формувати та доповнювати інтерпретацію отриманих розв'язків таким чином, щоб не виникало суперечностей в описах.

Допоміжні інформаційні компоненти являють собою систему правил перетворень інтерпретаційних описів, які при використанні природних мов можуть мати такі особливості, що обумовлюються природою мови:

— надмірність;

— суперечність;

— конфліктність ситуацій;

— неповнота опису.

Оскільки однією з основних функцій інтерпретаційних описів є відображення інтерпретації формальних фрагментів та отриманих в процесі розв'язання задач результатів, то виявлення вищенаведених особливостей є обов'язковим. Допоміжні інформаційні компоненти являють собою правила, що складаються з таких частин:

— аналізу окремих фрагментів інтерпретаційного опису;

— реалізації реконструкції відповідного опису інтерпретації.

Очевидно, що аналіз окремих фрагментів, під якими вважатимемо фрази або речення, може здійснюватися лише в тому випадку, якщо існують параметри, що характеризують відповідні фрагменти та їх частини і їхні величини можуть бути виміряні. Оскільки інтерпретація найтісніше пов'язана з семантикою відповідних описів, то такі параметри називатимемо семантичними. Відповідно до вказаних особливостей введемо такі типи параметрів (рис. 14):

— семантична суперечність;

— семантичний конфлікт;

— міра надмірності;

— міра неповноти.

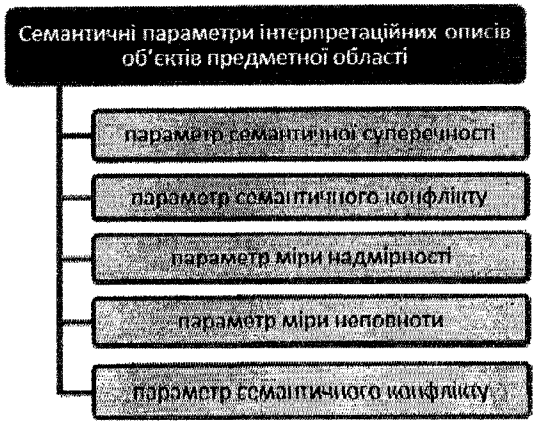


Рис. 14. Семантичні параметри інтерпретаційних описів об'єктів предметної області

Поняття семантичної суперечності сьогодні використовується в дослідженнях, пов'язаних з аналізом семантики в інформаційних системах та в дослідженнях, пов'язаних з теоретичною лінгвістикою [71, 72]. Параметр семантичної суперечності, що використовується в дослідженнях інформаційних систем, грунтується на понятті семантичної значимості окремого слова чи сукупності слів, що входять чи складають фразу або речення. Величина такої значимості визначається у вигляді її числового значення [73]. Отже, можемо визначати величини інших похідних семантичних параметрів, до яких належать: суперечність, конфліктність та міра повноти відповідного текстового виразу. Кожний графічний засіб захисту може описуватися інтерпретаційним розширенням на певній мові. При використанні стеганографічних методів формування засобів захисту ті чи інші слова формального опису графічного засобу захисту в явній або неявній формі відображені у відповідних засобах. При формуванні інтерпретаційних описів таких засобів може виникнути ситуація, коли з інтерпретаційного опису явної частини графічного засобу можна встановити окремі фрагменти неявної частини засобу або всю його неявну частину. Тому введемо уявлення про міру семантичного розширення

окремих слів у мовах, що використовуються для опису інтерпретаційних розширень. При цьому слово будемо розуміти як семантично значимий елемент, оскільки не завжди достатньо одного слова, щоб описати елементарну семантичну значимість окремих факторів з предметної області інтерпретації. Величина таких розширень визначається при формуванні семантичних словників. Розглянемо спосіб формування початкових значень величини семантичних розширень для вищеописаних випадків:

— графічний засіб захисту відображає сюжет, інтерпретація якого є доступна широкому колу споживачів;
— графічний засіб захисту є графічною абстракцією з довільними граматичними правилами;
— графічний образ являє собою графічний візерунок, особливістю якого є наявність загальних закономірностей правил побудови таких візерунків.

Коли графічний засіб захисту являє собою образ, що має загальнодоступний сюжет, то для всіх можливих предметних областей, з яких можуть створюватися графічні образи, формується семантичний словник, в якому описуються всі семантичні елементи предметної області. Формально окремий семантичний елемент описується співвідношенням:

$$x_i =< a_1,...,a_n >< P_1,...,P_m >,$$

де a_i — компонента, що описує семантичний елемент x_i, P_i — параметр, що характеризує семантичний елемент x_i.

Предметна область D_i, що використовується для побудови графічних засобів захисту z_i, розділена на дві частини, і відповідна множина семантичних елементів розбивається на дві підкомпоненти X і A, для яких $x_i \in X$ і $a \in A$. В цьому випадку $X \cup A \subset D$. Параметр семантичного розширення визначається на основі аналізу предметної області D. Оскільки семантичний словник S_e в інформаційній системі являє собою опис D, то визначення величини розширення X' здійснюватимемо на основі

аналізу S_e. Відзначимо, що в S_e, окрім описів елементів типу $X^i = \{x_1, ..., x_n\}$, входять описи компонент, які мають власну семантику і відрізняються від X^i. Такими компонентами є семантичні зв'язки між $\overline{\overline{X_i}}$ і $\overline{\overline{X_j}}$. Приймемо наступне визначення.

Визначення 3.1. Семантичний словник S_e являє собою опис семантики всіх можливих типів компонент D.

Семантичні елементи $\overline{\overline{x_i}}$ належать до класу компонент, що ідентифікують об'єкти, які використовуються в D. Семантичні компоненти, що описують взаємозв'язки між $\overline{\overline{X_i}}$ і $\overline{\overline{X_j}}$, складатимуть окремий клас семантичних елементів з D, і формально вони описуватимуться співвідношенням:

$$\varphi_i(x_{i1}, ..., x_{im}) = < \xi_{i1}, ..., \xi_{in} >, \qquad (3.1)$$

де $\overline{\overline{x_{ij}}}$ — елемент класу об'єктів, ξ_{ij} — елемент класу взаємозв'язків. Оскільки для відображення φ_i використовується природна мова користувача, то для опису φ_i застосуємо формалізм контекстно залежних граматик [74]. Тоді в явній формі φ_i запишеться у вигляді:

$$\varphi_i(x_i, x_j) = \xi_{i1} * \xi_{i2} * ... * \xi_{in},$$

де ξ_{ij} — семантична компонента залежності між x_i і x_j, що входить до складу загальної складеної залежності φ_i і пов'язана з іншими залежностями співвідношенням:

$$\xi_{i,(k<j)} \rightarrow \xi_{ij} \rightarrow \xi_{i,(m>j)},$$

яке відображає факт конкатенації опису складових залежностей. Оскільки структура опису інтерпретації природньою мовою передбачає формальне використання лише зв'язків між x_i і x_j та ξ_i типу конкатенації, то конкатенації позначатимемо символами «*» і «→». В розширеннях контекстно залежних (КЗ) мов можуть бути

фрагменти опису, елементи яких є контекстно незалежними. В таких випадках функціональний зв'язок між відповідними елементами позначатимемо символом «*». Згідно з (3.1) φ_i може описувати залежність не тільки між двома x_i та x_j. Тоді окремі фрагменти φ_i можна записати у вигляді:

$$\xi_{im1}(x_{i1}, x_{i2}) * \xi_{i2}(x_{i1}, x_{i3}) * ... * \xi_{ik}(x_{ik}, x_{im}).$$

Умова 3.1. Елемент ξ_{ij} у φ_i може описувати зв'язок тільки між двома елементами класу X.

При використанні описів природною мовою в нормалізованій формі характерним є застосування компонент класу означень, якими описуються різні характеристики об'єктів класу X. Ці компоненти позначимо символом γ_i. Вони дозволяють розширити асортимент описів елементів з X. Як і у випадку з елементами типу ξ_{ij} опис елементів γ_i в словнику S_c відображатиме окремий клас, що формально можна записати таким чином:

$$\psi(x_i) = < \gamma_{i1}, ..., \gamma_{ik} >,$$

де γ_{ij} — ознака, якою може описуватися x_i. Всі ознаки x_i, наводяться у відповідному описі $\psi_i(x_i)$. Розширення класу X в D формально описується у вигляді:

$$\left[(x_i * \gamma_i) \neq (x_i * \gamma_j)\right] \& \left[(x_i * \gamma_i) \propto (x_i * \gamma_j)\right].$$

В більшості випадків елементи x_i для власного опису використовують не тільки a_i, а й елементи γ_i як необхідні складові. Тоді x_i описується співвідношенням:

$$x_i = < a_{i1}, ..., a_{im} > < P_{i1}, ..., P_{ik} > < \gamma_{i1}, ..., \gamma_{iq} >,$$

де γ_{ij} — виступають доповненням до $A_i = \{a_{i1}, ..., a_{im}\}$. Очевидно, що відповідно до правил граматики, навіть, якщо вони обмежені вимогами нормалізованого способу побудови текстових описів

інтерпретації, то γ_{ij} повинні комбінуватися з a_{ij} в різних фрагментах інтерпретаційного опису елемента x_i.

Визначення величини семантичного розширення, яке позначатимемо символом υ_i для кожного елемента x_i проведемо наступним чином. Вибиремо з S_c черговий елемент x_i і обчислимо з даних S_c, записаних в частині, що вміщає описи всіх можливих взаємозв'язків, кількість ξ_i, які пов'язують x_i з іншими компонентами x_j. Число таких зв'язків визначає початкове значення параметра υ для x_i, що позначимо як $\upsilon(x_i)$ або υ_i, де індекс i — відповідає індексу i в x_i. Всі семантичні параметри, запропоновані в цій роботі, мають назви, які збігаються з відповідними назвами таких параметрів в інших дослідженнях семантики інформаційних систем [75, 76]. Однак інтерпретація і, відповідно, визначення зазначених параметрів відображають особливості проведеної роботи і тому не збігаються з іншими аналогічними випадками дослідження семантики. Розглянемо визначення семантичної значимості окремого елемента x_i.

Визначення 3.2. Семантична значимість μ_i елемента x_i є величиною зворотною до величини υ_i і визначається співвідношенням:

$$\mu(x_i) = \beta_\mu / \upsilon(x_i), \text{ або } \mu_i = \beta_\mu / \upsilon_i$$

де β_μ — коефіцієнт зведення величини μ_i.

В цьому випадку семантична значимість визначає величину точності використання x_i. Наприклад, якщо υ_i приймає великі значення, то точність визначення з відповідного x_i і пов'язаного з ним іншого елемента x_j в реченні, що описує фрагмент графічного образу, є неоднозначною. У випадках, коли застосовується метод стеганографічного укриття шляхом вилучення деякого фрагмента з опису графічного образу, семантична значимість окремого

елемента x_i для реалізації відповідного фрагмента графічного образу є значною мірою бажаною, якщо μ_i має мале значення. Із збільшенням значення μ_i фрагмент, який виділяється як скрита частина графічного засобу захисту, з границею, що визначається елементом x_i, буде більш доступним для виявлення, оскільки кількість зв'язків, допустимих для цього елемента з іншими елементами з словника S_c, є меншою. Тому збільшення семантичної значимості в цьому випадку означає вищу міру однозначності інтерпретації відповідного x_i і, як наслідок, вищу міру дедуктивної залежності між x_i і x_j, з яким x_i по'єднується в рамках деякої фрази Φ_i. Міра дедуктивної залежності являє собою кількість допустимих зв'язків між x_i та іншими елементами множини X. При цьому, чим менша кількість таких зв'язків, тим вища міра дедуктивної залежності або чим більше μ_i, тим більша семантична значимість відповідного x_i. Тоді йдеться про збільшення точності семантичного значення x_i. В цьому і полягає інтерпретація параметра семантичної значимості. У випадку формування невидимих фрагментів засобів захисту щонайменше границя цих фрагментів повинна проходити через x_i, семантична значимість яких є найменша.

Якщо графічний образ являє собою абстракцію, практично немає проблеми побудови речень з елементами x_i з різною величиною $\mu_i(x_i)$. Однак виникає інша проблема, яка полягає в приховуванні границі невидимого фрагмента. Оскільки у випадку абстрактних образів є можливість формувати систему правил таким чином, щоби для x_i, які створюють границю для невидимого фрагмента $\left(G_i^N\right)$, або x_i^G величина семантичної значимості $\mu(x_i)$ була мінімальна. Тоді може виникнути ситуація, коли із значень x_i^G, що належать видимій частині G_i^V з G, можна виявити границю G_i^N, що, в свою чергу, може призвести до виявлення G_i^N.

Один із способів розв'язку цієї проблеми полягає у присвоєнні значень $\mu_i(x_i)$ граничним x_i на основі використання генераторів псевдовипадкових чисел з діапазоном, який визначається можливостями системи правил типу $\varphi(x_i)$. При цьому необхідно взяти до уваги той факт, що можливості у створенні необхідного асортименту $\varphi_i(x_i)$ обмежуються метрикою простору, в якому формується G_i як графічний засіб захисту. Зазначимо, що метрика простору для побудови G_i на площині не обмежується можливостями площини чи двомірного простору. Багатомірність простору, в якому приймається та чи інша метрика, визначається додатковими параметрами, що можуть використовуватися для побудов G_i на фізично плоскому паперовому документі. Прикладами таких параметрів можуть бути колір елементів x_i, що використовуються для побудови фраз $\Phi_i = (x_{i1}, ..., x_{ik})$; ефект тримірності графічного образу, який можна створювати різними засобами тощо [77].

Якщо G_i являє собою узор, проблема побудови фраз із заданими значеннями μ_i для граничних x_i виникає через такі обставини:

- узором називається такий графічний образ, для якого існують обмеження на способи його побудови, що визначають інтегральні характеристики графічного образу;
- при модифікації узору у зв'язку з впровадженням в нього скритих фрагментів вони повинні бути розподілені таким чином, щоб не змінилися інтегральні характеристики узору, які вказують на його тип, визначений при початкових умовах побудови графічних засобів захисту;
- необхідні значення μ_i для граничних елементів x_i повинні формуватися на основі використання правил, що визначають інтегральні параметри узору з одного боку, та з врахуванням умов забезпечення невидимості границі скритих фрагментів, з другого боку. При цьому необхідно враховувати їх взаємну суперечність.

Відповідно до зазначених особливостей можна сформулювати такі задачі, які необхідно вирішити при реалізації системи стеганографічного укриття даних для формування засобів захисту у вигляді узорів:

- створити систему виводу фраз, яка б давала можливість формувати граничні елементи x_i із заданим рівнем семантичної значимості;
- довести несуперечність відповідної системи виводу умовам, що визначають обмеження на спосіб побудови узору вибраного типу;
- визначити метод обчислення величини невидимості границі фрагмента, що усувається з загального образу графічного засобу захисту;
- сформувати правила однозначної інтерпретації невидимої частини або невидимих фрагментів графічного засобу захисту.

Методи синтезу моделей засобів захисту з інформаційними компонентами системи

Графічні засоби захисту документів та цінних паперів, що ґрунтуються на використанні стеганографічних методів досить тісно пов'язані і залежні від засобів інтерпретації основних компонент засобів захисту та системи захисту в цілому. Це насамперед зумовлено тим, що методи стеганографії орієнтовані на використання можливостей людського сприйняття візуальної інформації. Можливості людської зорової системи суттєво залежать від можливостей інтерпретації образів, які зумовлюються інформаційним забезпеченням системи захисту. У зв'язку з цим для всебічного дослідження графічних засобів захисту документів, що ґрунтуються на застосуванні стеганографічних методів, необхідно дослідити методи синтезу формальних моделей засобів захисту з інформаційними компонентами. В результаті такого синтезу формуються інформаційні моделі відповідних засобів захисту, які відрізняються між собою типом формальних засобів і

використовуються для побудови математичної моделі. В цьому випадку можна виділити такі типи інформаційних моделей (рис. 15):

— логіко-інформаційні (LIM);
— автоматно-інформаційні (AIM);
— граматично-інформаційні (GIM);
— структурно-інформаційні, які формуються на основі формальної теорії графів (SIM).

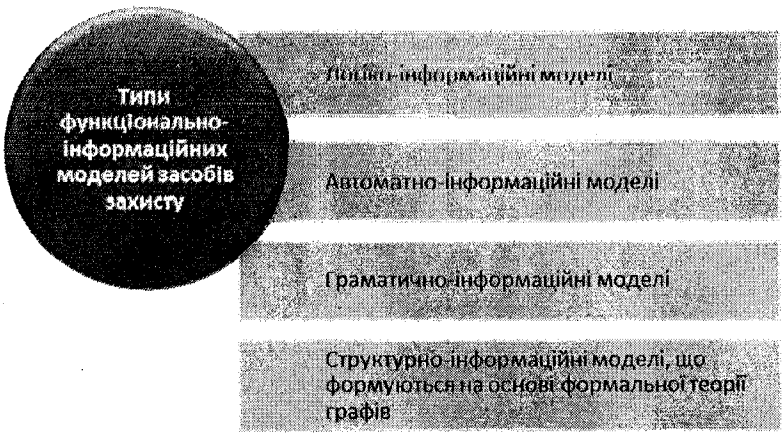


Рис. 15. Типи функціонально-інформаційних моделей засобів захисту документів

Перед дослідженням формальних засобів та методів синтезу логіко-інформаційної моделі розглянемо її на якісному рівні. Логічні засоби є найбільш загальними, з точки зору опису окремих деталей засобів захисту, тому математичні моделі, що використовують апарат математичної логіки, описують не тільки самі засоби захисту, але й їхні параметри та можливості, що проявляються на рівні методів контролю та технологій використання документів [78, 79]. При такому підході розглядати задачі максимізації рівня захисту окремого документа не завжди доцільно. Необхідний рівень захисту документів визначається такими факторами (рис. 16):

— вимогами технологічного процесу (ТР), для захисту якого використовуються документи;
— методами контролю документів, що реалізуються у відповідних ТР;
— взаємозв'язком між системами захисту всіх документів, що використовуються в рамках одного ТР;
— особливостями ТР, для обслуговування якого користуються певним комплектом документів.

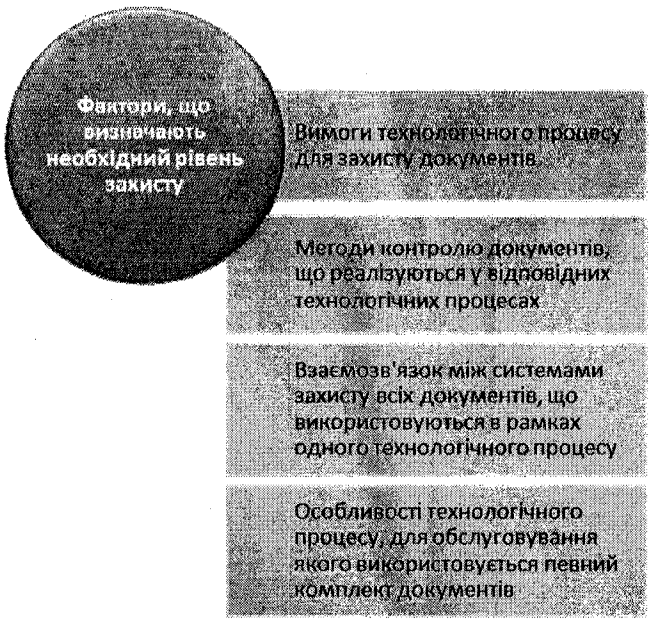


Рис. 16. Фактори, що визначають необхідний рівень захисту документів

Вимоги технологічного процесу насамперед визначають конструкцію документа, яка передбачає методи розміщення в документах змінної інформації, що безпосередньо відображає певні фрагменти ТР. Документи вказаного типу є універсальними, оскільки через змінну частину інформації, яка в них міститься, вони можуть використовуватися для різних фрагментів ТР. Можна

прийняти такий розподіл типів документів відносно їх взаємозв'язків з ТР: універсальні, персональні та індивідуальні документи.

Стосовно універсальних документів, про які мовилось вище, вони можуть використовуватись у більш ніж одному ТР. Персональні документи являють собою ті документи, що можуть використовуватися лише для одного типу ТР. Індивідуальні документи — це документи, які можуть використовуватись лише для одного фрагмента в одному технологічному процесі. Очевидно, що рівні захисту для різних типів документів є різними. До них можна віднести: абсолютний, обмежений та довільний рівні захисту.

Довільний рівень захисту характерний для документів, орієнтованих на використання в різних ТР. Зазвичай, у таких документах змінна частина інформації може мати досить широкий діапазон значень. Це означає, що змінна інформація може бути сформована в них таким чином, що рівень захисту документа, може бути заниженим. Наприклад, документи, в яких визначається тип товару, його кількість та інші параметри, можуть не бути пов'язаними з засобами захисту, і такий документ може виявитися з рівнем захисту значно нижчим, ніж той, який передбачений в документі засобами захисту.

Таким чином, важливим фактором, що визначає рівень захищеності універсального документа, є характер зв'язків між засобами захисту та різними підкласами або підтипами документів. Наприклад, колір документа, що за функціональним призначенням є універсальним, може бути пов'язаний з окремими типами змінної інформації для даного типу документів.

Засоби захисту документів з обмеженим типом рівня захисту застосовуються здебільшого у персональних документах. Обмеженість захисту в таких документах визначається тим, що як скриті дані, у відповідних засобах захисту використовуються дані, що ідентифікують технологічний процес. Типовим прикладом такого способу реалізації засобів захисту може бути застосування голографічних ідентифікаторів, інформацію з яких зчитати звичайними засобами спостереження неможливо [80].

Засоби захисту абсолютного типу являють собою дані, які безпосередньо відображають окремі форми ТР, в скритій формі містять інформацію, орієнтовану на певну методику контролю документа, що реалізується в процесі його експлуатації. Прикладом такого типу засобів захисту можуть бути дані, записані на магнітну стрічку, що знаходиться в документі. Інформація з такої стрічки зчитується спеціальними зчитувачами відповідно до методики перевірки документів.

Вищенаведений якісний аналіз визначає LIM, як деяку систему, що описує не тільки основні фрагменти засобів захисту, але й особливості ТР, який обслуговується документом та певну методику контролю документів, реалізовану у вигляді невід'ємної частини всього ТР.

Модель LIM в загальному вигляді являє собою процес використання і контролю всіх документів в окремому ТР, що можна записати таким чином:

$$TP_j = \Phi\left[L_1, \ldots L_n\right], \tag{3.2}$$

де Ф — опис системи відповідно до якої використовуються документи в TP_j; L_i — логічна функція, яка описує процес застосування засобів захисту в ТР одного з документів. Прикладом такої функції може бути співвідношення, що описує логічні залежності між параметрами окремих засобів захисту:

$$L_i = L_1\left(x_{i1}, \ldots x_{in}\right) = \left\{\left[\left(x_{i1} \,\&\, x_{i2} \,\&\, x_{i4}\right) \to \left(x_{i5} V x_{i6}\right)\right] \to x_{i3}\right\}. \tag{3.3}$$

Співвідношення (3.2) і (3.3), по суті, описують методологію контролю документа в процесі реалізації ТР на рівні вибору тих чи інших параметрів засобів захисту. В цьому випадку не виділяється окремий засіб захисту як деякий складний об'єкт, що може описуватись цілим рядом власних параметрів, а вибирається один ключовий параметр x_{ij} з власними еталонними значеннями його величини. Очевидно, що для кожного окремого засобу захисту з певним наближенням можна сформувати логіку залежностей між різними параметрами, що характеризують його компоненти. Однак таке

наближення опису окремого засобу захисту більш доцільно розглядати в рамках моделей інших типів.

В рамках моделі LIM розглянемо такі задачі, що визначають доцільність їх використання (рис. 17):

— встановлення критеріїв виявлення атаки на документ, що використовується в рамках певного ТР;
— виявлення та визначення величини небезпеки, атаки на документ і, відповідно, на ТР, що використовує документи;
— виявлення суперечностей в системах захисту документів в одному ТР;
— виявлення конфліктів, що виникають у процесі експлуатації документів, при реалізації ТР.

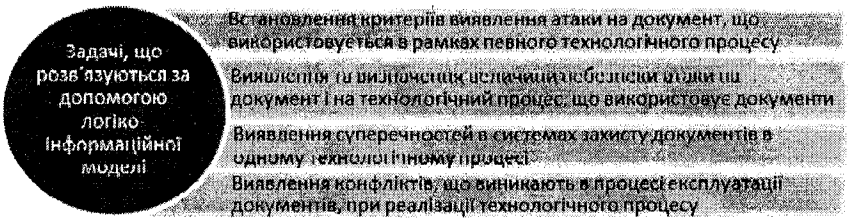


Рис. 17. Задачі, що розв'язуються за допомогою логіко-інформаційної моделі

Загалом критеріями виявлення атак можуть бути величини параметрів засобів захисту, що контролюються в процесі аналізу документів. Таких критеріїв може бути багато, оскільки засобів захисту в різних документах є також чимало і в кожному засобі захисту може використовуватись більше одного параметра. Тому критеріями виявлення атак не можуть бути окремі параметри вибраних засобів захисту. Для виявлення атак повинна використовуватися деяка структура критеріїв, яка може бути сформована в результаті синтезу моделі захисту з інформаційними компонентами, які відображають існуючі в документах загрози [81]. Оскільки документом є носій інформації, на якому розміщені засоби захисту, то можна стверджувати, що в рамках даного

дослідження загрозою є деяка властивість документа або його характеристика, що описується параметрами відповідних засобів захисту [82]. Оскільки в цьому випадку розглядаються засоби захисту, які формуються на основі використання методів стеганографії, то до базових типів загроз можна віднести такі фактори, що їх обумовлюють:

— міру видимості скритої частини або фрагмента засобу захисту, яку позначатимемо η;

— складність відновлення скритих фрагментів засобів захисту на основі їх видимих фрагментів — π;

— міру наближення виявленої інформації до даних, прихованих в фрагментах засобів захисту — λ.

Вищенаведені фактори містять локальний характер. В рамках системи захисту ТР можна визначити такі інтегральні фактори, що визначають небезпеку для всієї системи документів:

— інтенсивність атак на систему документів певного технологічного процесу $\kappa(TP)$ або κ;

— інтенсивність успішних атак κ'';

— міру адекватності системи захисту ТР рівню небезпеки для відповідного ТР — Ω.

Один із способів формування інтегральної системи критеріїв і, відповідно, синтезу моделі засобів захисту та інформаційних компонент може ґрунтуватися на використанні моделі взаємодії між небезпекою і системою захисту ТР. Вона може описуватися засобами теорії ігор [83, 84].

В загальному вигляді модель гри M можна записати:

$$M = G(SK, zz, NU, TP).$$

Приймемо, що ТР разом з системою контролю, документів (SK) представляє одного гравця, який повинен виявляти атаки, ініціалізувати реалізацію протидії атакам та визначати рівень безпеки системи захисту ТР на основі використання вищевказаних параметрів. Другий гравець становить небезпеку, що може ініціювати атаки на ТР шляхом використання різних методів фаль-

сифікації документів. По суті, другий гравець певною мірою може ототожнюватись з потенційним користувачем ТР. Першого гравця будемо ідентифікувати символами SK, оскільки система контролю документів є основним засобом, що реалізує захист ТР. Другого гравця ідентифікуємо як NU (несанкціонований учасник ТР), оскільки, за визначенням, кожний користувач може бути джерелом небезпеки, незалежно від того чи використовує він фальшиві документи свідомо. Тому, за визначенням, кожний NU системою SK сприймається, як небезпека для ТР.

Початковими умовами для першого гравця є:

1. Гравець SK має початкову методику контролю документів, яка визначає початкову стратегію поведінки SK.
2. Гравець SK має дані про певні загрози, що існують в системі захисту документів, якими може скористатися гравець NU.
3. Гравець SK при виявленні атаки може модифікувати методику контролю документів, що являє собою зміну стратегії гравця SK. Ціллю зміни стратегії гравця SK є протидія атакам, ініційованим гравцем NU. Така модифікація може використовуватись на новому циклі функціонування ТР або в рамках циклу, на якому виникла і виявлена атака, якщо до завершення циклу в ТР передбачено необхідну кількість кроків використання документів.

Початкові умови для гравця NU є:

1. Гравець NU знає про існування на об'єкті атаки загрози.
2. Гравець NU може ініціювати здійснення атаки в процесі реалізації своєї стратегії гри.
3. Гравець NU може реалізувати елементи стратегії взаємодії з SK для отримання додаткової інформації про систему захисту та елементи засобів захисту для виявлення додаткової інформації про об'єкти атаки.
4. Гравець NU може не мати повної інформації про стратегію перевірки документів ТР і, відповідно, про систему SK.

Одним з базових елементів гри є опис способів представлення стратегій, яких можуть дотримуватись гравці та система критеріїв вибору можливих стратегій чи формування чергової стратегії

одним з гравців. Оскільки вибір стратегії залежить від поточного стану гри, оцінка якого тісно пов'язана з критеріями, то необхідно більш детально проаналізувати ці критерії. Згідно з прийнятою термінологією визначимо критерії у вигляді ціни гри, яка передбачає виграш одного учасника і програш другого учасника. Приймемо, що кожен ТР має свою вартість, яка на змістовному рівні визначається втратами зацікавлених сторін ТР. Наприклад, такими зацікавленими сторонами можуть бути організації, що забезпечують державну підтримку ТР; власники об'єктів, що використовуються відповідними ТР; користувачі продукції, що виробляється в результаті функціонування ТР тощо. Інтереси цих учасників захищає SK. Друга сторона, яка протидіє SK, — це NU, які можуть виступати в ролі всіх вищевказаних учасників, крім державних установ. Стратегія SK становитиме послідовність дій з контролю засобів захисту документів. Такий контроль може мати різну глибину, оскільки полягає у перевірці параметрів засобів захисту документів, то для різних засобів ці параметри позначатимемо змінними $x_{ij},...,x_{im}$, де x_{ij} — параметр i засобу захисту j. Приймемо, що окремий документ a_i може мати цілий ряд засобів захисту, які в сукупності складають систему захисту. Кожному рівню глибини контролю і кожному параметру зіставимо окремий параметр x_{ij}^k, де k — номер рівня глибини контролю. Особливістю реалізації процедур контролю є те, що результат контролю допускає бінарну інтерпретацію, що дозволяє приймати бінарну інтерпретацію змінних x_{ij}^k. Вона полягає у тому, що одне значення x_{ij}^k означає відповідність його допустимій величині, а друге — недопустимому значенню цього параметра. Тоді методику контролю, що відповідає стратегіям SK, можна представити у вигляді логічних функцій, в яких логічні оператори $\{V,\&,\rightarrow,\neg\}$ мають розширену інтерпретацію. Така стратегія поведінки SK — формальна і може бути подана у вигляді:

$$L = F_L(l_1,...,l_m), \tag{3.4}$$

де F_L – функція взаємозв'язків між окремими l_i, які можна проілюструвати таким прикладом:

$$l_i = (x_{i1} \,\&\, x_{ik}) V (x_{lm} \to x_{ik}) \,\&\, x_{il}.$$

У найпростішому випадку функція F_L являє собою опис послідовності окремих процесів контролю:

$$L = l_1 \to l_2 \to \ldots \to l_m.$$

Методика контролю часто описується логічними формулами, наприклад у вигляді співвідношення:

$$L^* = (l_1 \,\&\, (l_3 \vee l_2)) \to (l_5 \,\&\, l_6),$$

де l_i — формула, що описує логіку контролю параметрів засобу захисту zz окремого документа з ТР.

Для побудови системи критеріїв вибору чергової стратегії поведінки SK і NU необхідно враховувати такі особливості відповідної ігрової моделі:

1. Атаки на документи, незалежно від того виявлені вони чи ні, будуть змінюватися учасником NU, оскільки відсутність або наявність у процесі реалізації стратегії контролю виявиться на основі даних про відхилення результатів реалізації відповідного циклу ТР від очікуваних значень, що визначаються ціллю ТР. За результатами аналізу даних, отриманих після завершення ТР, який був успішно атакований, відповідна атака на документ буде виявлена завдяки проведенню експертизи документів a_i технологічного процесу.

2. Відповідно до першої особливості стратегія SK повинна бути змінена таким чином, щоб успішна атака була виявленою в процесі перевірки документів системою SK.

3. У випадку успішної атаки NU отримує виграш ΔW, який рівний програшу ΔV учасника SK. Якщо атака виявлена учасником SK, то NU не отримує виграшу.

4. Ціллю гри для SK є недопущення програшу, а для NU — виграш.

Для визначення умов, за яких SK повинно змінювати стратегію контролю, обмежимося такими випадками:

— в процесі реалізації контролю SK виявляє атаку;

— атака виявляється з результатів аналізу даних, отриманих після завершення ТР;

— в процесі реалізації контролю атаки на ТР не виявлено, і ТР завершився успішно.

В останньому випадку реєструється факт відсутності атаки на ТР, що може бути причиною зміни стратегії SK для спрощення процедур контролю. Очевидно, що додатковою умовою для спрощення процедури контролю є існування певної кількості реалізованих процедур або наявність статистичних даних про кількість реалізацій ТР.

Перший і другий випадок ілюструє тісну залежність ініціації зміни стратегії одним з учасників від поточної стратегії, яка реалізується іншим учасником. Нехай $G(NU)$ — стратегія учасника NU і, відповідно, $G(SK)$ — стратегія учасника SK. Тоді залежності між $G(SK)$ і $G(NU)$ формально можна описати таким чином:

$$\left\{\left[\left[G_i^1(SK)\to A_i\right]\to\left[G_{j*}^1(NU)\right]\right]\right\}\vee$$
$$\vee\left\{\left[\left[G_i^2(NU)\,\&\right]\left[G_i^2(SK)\to A_i\right]\right]\to G_{i*}^2(SK)\right\}\vee$$
$$\vee\left\{\left[K\cdot G_i^3(SK)\to\forall_i\neg A_i\right]\to G_{i*}^3(SK)\right\},$$

де верхній індекс означає номер ситуації, для якої аналізується результат застосування стратегії; * — зміну стратегії відносно попередньої стратегії; K — кількість успішних реалізацій ТР, що використовував стратегію $G_s^3(SK)$. Аналогічно до опису стратегії контролю, що здійснюється системою SK, стратегія реалізації атаки на документ учасником NU у неявному вигляді може бути записана так:

$$M_i = F_M(m_1,...,m_m), \qquad (3.5)$$

де m_i — логічна формула, що описує перевірку документів з модифікованими параметрами zz атакованого документа a_i. При реалі-

зації атаки шляхом підробки документа не всі параметри zz можуть бути відтворені з достатньою точністю, яка б відповідала вимогам оригінальних документів. Проте, NU може прийняти рішення щодо здійснення атаки на документ. Це обумовлено тим, що стратегія SK може не передбачати безпосередньої перевірки параметрів, що не можуть бути задані з необхідною адекватністю. Крім того, існує можливість укрити невідповідне значення окремого параметра zz в логічній формулі m_i, що описує zz. Все це дає змогу визначати власну стратегію NU виконання атаки, яка являє собою реалізацію можливості використання фальшивих документів в ТР. При цьому NU враховує можливості стратегії $G(SK)_i$, яку реалізує SK. В цьому сенсі можна стверджувати, що $G(NU)_i$ являє собою деяке наближення до $G(SK)_i$. Тоді міру наближення $G(NU)_i$ до $G(SK)_i$, яка значною мірою залежить від інформованості NU про zz, пов'яжемо з мірою видимості η прихованих фрагментів графічного образу. Якщо прийняти, що величина η може вимірюватись мірою наближення $G(NU)_i$ до $G(SK)_i$, то можна сформувати різні методи вимірювання міри наближеності або міри відмінності між двома системами логічних формул. Допустимість такого підходу до визначення η грунтується на наступному. Нехай існує деяка стратегія, що в явному вигляді описується функцією L_i, яку реалізує SK. Через невидимість скритих фрагментів NU реалізує стратегію атаки або виготовлення фальшивих документів для ТР таким чином, що невидимі і, відповідно, невідомі йому фрагменти будуть відсутні. Тоді чим більша різниця між M_i і L_i, тим більше значення має параметр η. В цьому випадку відсутність інформації про скриті фрагменти zz і фізична їх невидимість ототожнюються. Таким чином, параметр η являє собою інтегральний параметр невидимості скритих фрагментів всієї системи документів D_i, що обслуговують TP_i. Цей параметр можна інтерпретувати, як одну з базових складових міри

захищеності документів D_i з TP_i. При реалізації атаки на документи, окрім міри відповідності підроблених документів оригінальним, беруться до уваги процедури контролю документів, що реалізуються при їх використанні. Тому M_i можна інтерпретувати, як деяку процедуру контролю документа, яка враховується при визначенні підроблених документів. Очевидно, що в рамках M_i підроблений документ відповідає оригінальному, якщо $M_i \sim L_i$. Тоді можна вважати атаку успішною, хоча параметри a_i^* не будуть повністю відповідати параметрам a_i. З визначення, L_i формується таким чином, щоб можна було забезпечити виявлення атак на ТР. Це означає, що в процесі перевірки a_i насамперед будуть контролюватися невидимі фрагменти та їх параметри в zz. Тоді від міри видимості чи міри інформованості про відповідні фрагменти залежатиме подібність між L_i і M_i. Розглянемо наступне визначення.

Визначення 3.3. Міра невидимості η скритих фрагментів zz визначається мірою подібності M_i і L_i, що формально записується у вигляді $\eta = f(M_i, L_i)$.

Величину η можна визначити згідно зі співвідношенням:

$$\eta(M_i, L_i) = \sum_{j=1}^{n} \neg \delta_j \left[\varphi_j(M_i), \varphi_j(L_i) \right],$$

де функція δ — визначається відповідно до співвідношення:

$$\left\{ \varphi_j \left[(M_i) = \varphi_j(L_i) \right] \to (\delta = 0) \right\} V \left\{ \left[\varphi_i(M_i) = \varphi_i(L_i) \right] \to (\delta = 1) \right\},$$

$\varphi_i(M_i)$ і $\varphi_i(L_i)$ — елементарні функціональні фрагменти. Під елементарними функціональними елементами розуміємо пару змінних x_i і x_j, що об'єднані логічною функцією. Одна із змінних в $\varphi_i(L_i)$ може бути редукцією деякого фрагмента, наприклад, $x_i \,\&\, x_j = x_k^l$. Тоді допустимим є фрагмент $x_k^l \cdot x_f$.

Для визначення параметра M_i детальніше розглянемо формальні засоби побудови графічного образу (Q). Будемо розглядати графічний образ типу J^A, який формально описується як деяка мова M_i, що будується на основі граматики W_i, $W_i = (A, \Sigma, U, S)$, де $A = \{a_1, ..., a_m\}$ — множина геометричних примітивів, які використовуються для побудови окремих речень мови W_i і відображають окремі фрагменти образу Q_{ij}; $\Sigma = \{\xi_1, ..., \xi_n\}$ — правила формування речень в M_i на основі граматики W_i у вигляді продукції типу $\neg(a_1 \to a_5), \neg(a_i \to a_{i+4})$ тощо; $U = \{U_1, ..., U_m\}$ — умови вибору чергових правил продукцій і $S = \{S_1, ..., S_k\}$ — ознаки завершення побудови чергового слова та ознаки вибору початку для побудови слова.

Оскільки графічний образ будується на площині, то для формування Σ необхідно визначитися з метрикою та масштабом у відповідному просторі. Якщо прийняти, що простір визначається прямокутною системою координат, то масштаб може визначатися прямокутною сіткою, що покриває відповідну площину. Одиниця масштабу може відповідати величині відрізка геометричного примітиву a_i. В цьому випадку правила продукції описують напрямок, в якому допустиме продовження окремої траєкторії G_i.

У більшості образів Q_i типу J^A можна виділити еталонні фрагменти $\varphi_{ij} \in Q_i$. Тоді система умов U буде описувати сукупність таких еталонних фрагментів та способи їх об'єднання. Прикладом опису такого еталонного фрагмента може бути співвідношення:

$$M_i = (a_{i1} \to a_{i2} \to a_{i3}) \Rightarrow a_{i2},$$

де вираз, що знаходиться в дужках описує частину слова в M_i, від якої залежить вибір чергового геометричного примітиву, наприклад, a_{i2}.

Множина S являє собою опис умов закінчення слова, яка може мати такий вигляд:

$$S_i = (\varphi_i \to \varphi_j) \Rightarrow Q_i,$$

де S_i означає наступне. Якщо частина Q_i складається з двох еталонних фрагментів $(\varphi_i \to \varphi_j)$, послідовність яких відповідає S_i, то на цьому відповідна траєкторія закінчується. Траєкторію T, подамо у вигляді:

$$T_i = (\varphi_i \to \varphi_k \to a_j \to \ldots \to \varphi_t \to \varphi_j).$$

Очевидно, що S_i може бути частиною траєкторії T_i, яка відповідно до її інтерпретації є частиною, що завершує T_i.

Оскільки Q_i складається з видимої t_{iV} і невидимої t_{iN} частин, то приймаємо, що розподіл T_i на t_{iV} і t_{iN} здійснюється по границі $Q_2(\varphi_i)$, де Q_2 — ідентифікатор поділу T_i, а $\varphi_{i\gamma}$ — фрагмент, який розділяється в точці γ на видиму і невидиму частини. В цьому випадку можна визначити параметр π, що залежить від таких факторів:

— міри подібності невидимих фрагментів Q_{iN} до видимих фрагментів Q_i;

— вибору точки поділу або місця проведення границі Q_2 в Q_i.

Якщо візьмемо два еталонні фрагменти φ_{ij} і φ_{ik}, то різниця між ними $(\varphi_{ij} - \varphi_{ik})$ буде дорівнювати кількості графічних примітивів a_{ij}, які не збігаються в φ_{ij} і φ_{ik}. Тоді для визначення складності відновлення скритих фрагментів засобів захисту на основі їх видимих фрагментів або величини π можна використати співвідношення:

$$\pi(\varphi_{iN}) = \left[\sum_{j=1}^{m}\left[U_{ij}(\varphi_N) - U_{ij}(\varphi_V)\right]\right] + \sum_{j=1}^{k} Q_2(\varphi_{ijV}),$$

де $U_{ij}(\varphi_N)$ — фрагмент, що розміщується у невидимій частині Q_i; $U_{ij}(\varphi_V)$ — аналогічний еталонний фрагмент, який розміщується у видимій частині графічного засобу, $Q_2(\varphi_{ijV})$ — гранична точка поділу, яка розміщується в межах видимого фрагмента.

У скритих фрагментах *zz* можуть розміщуватися дані, що використовуються для процесу контролю документів системами SK [85]. Для приховування таких даних у більшості випадків застосовуються методи маскування. Однією з важливих особливостей методів маскування є друкування скритих фрагментів на графічному образі *zz*. Тому, з точки зору фізичної присутності відповідного фрагмента, цей спосіб стеганографічного укриття даних є досить специфічним і застосовується для графічних образів, що мають сюжети, або для Q^S.

Використання інформаційних компонент та стеганографічних методів у графових моделях

В межах цієї роботи графові моделі розглядаються в тісному взаємозв'язку з використанням формальних граматик для опису графічних образів засобів захисту (*zz*). Тому такі формальні описи вважатимемо графовими моделями, якщо їх аналіз будемо проводити з точки зору інтерпретації відповідних образів, як графових структур [86]. Якщо графічні образи розглядати як такі, що відображають граматичні структури, якими є слова формальної мови, при відповідному виборі елементів символів формальної граматики, що описують фрагменти графічного образу, то можна говорити про використання формальних граматик для опису графічних *zz*.

Особливістю математичних засобів теорії формальних граматик та теорії графів є їх досить високий рівень узагальнення, на якому розглядаються теоретичні проблеми, що розв'язуються в рамках їх формалізму [87]. Тому інформаційні компоненти є важливими засобами, що дозволяють пов'язати їх формалізм з предметною областю графічних *zz* документів.

Серед задач, які можна досліджувати в рамках формалізму мови $L_i(M)$, розглянемо такі:

— збереження однозначності побудови латентних частин графічного образу;

— пошук в образі кодових фрагментів, при цьому фрагменти, в яких використовуються контекстно вільні граматики, розв'язність регулярних мов, є похідними задачами.

Задачі пошуку кодових фрагментів, по суті, являють собою задачі вибору фрагментів, що підлягають укриттю на основі застосування стеганографічних методів. Одним із таких способів реалізації методу приховування інформації є недодруковування окремих фрагментів графічного образу. Це означає, що скритий фрагмент має відповідати таким вимогам:

— повинні існувати способи його відтворення;

— відповідні способи мають забезпечувати однозначність відтворення скритого фрагмента;

— для правильного відтворення повинна використовуватися додаткова інформація, яка може бути прихована в інших місцях документа або спеціальним способом (через захищені канали зв'язку) передаватися в SK.

Найпростіший спосіб відтворення може полягати на використанні еталонів недодрукованих фрагментів або еталонів повного графічного образу. Цей спосіб є настільки громіздким, що може призвести до дискредитації досліджуваного підходу в цілому.

Другий спосіб, який досліджується в цій роботі, полягає у використанні певних алгоритмів добудовування задрукованих фрагментів графічних *zz* таким чином, щоб недодруковані фрагменти однозначно і коректно доповнювали видиму частину графічного образу *zz*. В цьому випадку необхідно розв'язати такі задачі:

— сформувати методи розпізнавання коректності добудованих фрагментів;

— методи добудовування повинні забезпечувати однозначність сформованих фрагментів.

Вищенаведені задачі відображають ключові проблеми, що повинні розв'язуватися в рамках нашого підходу і можуть бути розв'язані лише на основі використання інформаційних компонент. Інтерпретація образів, для опису якої призначені інформаційні компоненти (ІК), полягає у встановленні певних закономірностей та властивостей, що характеризують абстрактний образ Q^a і тим самим звужують міру його загальності.

Інтерпретація $J^A(Q)$ полягає в описі залежностей та параметрів, що характеризують відповідний образ. Тому більш детально розглянемо відповідні залежності. Приймемо, що точки простору визначаються метрикою та дискретним масштабом, що дозволить обмежитися дискретним простором W. Найпоширеніший спосіб встановлення закономірностей ґрунтується на використанні еталонних фрагментів при побудові образу. В цьому випадку еталонні фрагменти можуть описуватися як допустимі слова φ^l в мові $L_i(M)$, наприклад:

$$\varphi_i = \left\{\left[x_{i1} \to \left(a_i, a_{i+1}, ..., a_{im}\right)\right], ..., \left[x_k \to \left(a_{i1}, a_{i2}, ..., a_{ik}\right)\right]\right\}.$$

Подальшим рівнем інтерпретації є закономірності використання окремих φ_{ie} при формуванні фрагмента образу $\varphi_i(Q)$. Такі залежності описуються логічними співвідношеннями, в яких спосіб застосування чергового φ_i може залежати від уже використаних в $\varphi_i(Q)$ фрагментів φ_{ie}. Прикладом такого співвідношення може бути:

$$\varphi_i(Q) = \left\{\left[\left(x_i \,\&\, x_j\right) V \left(x_{j1} \to x_{j2}\right)\right] \to \neg x_{j+1}\right\} \to x_q \qquad (3.6)$$

Оскільки $\varphi_i(Q)$ є послідовністю слів, то формований фрагмент φ_i визначає певний порядок використання окремих φ_{ie}. Наприклад, згідно з (3.6.) застосування x_i можливе тільки за умови використання x_j. Замість фрагмента $\left(x_i \,\&\, x_j\right)$ можна використову-

вати фрагмент $(x_{j1} \to x_{j2})$, хоча відповідно до інтерпретації диз'юнкції [88] можна використовувати два фрагменти $(x_i \,\&\, x_j)$ та $(x_{j1} \to x_{j2})$ одночасно. Логічні функції, що застосовуються в описі φ_i, мають власну інтерпретацію або власне відображення в формалізмі формальної мови. Функція & визначає необхідність безпосередньої конкатенації x_i і x_j, а диз'юнкція — допустимі варіанти реалізації відповідного фрагмента тощо. В рамках одного фрагмента φ_i використання логічних зв'язок визначає не тільки умови застосування окремих x_{ie}, але й їх послідовність. Окремий фрагмент φ_i в Q_i зіставимо з окремою траєкторією t_i, що реалізується в Q_i. Можна записати, що $(t_{ij} \in T_i) \& (T_j = Q_i)$. В рамках Q_i окремі t_i можуть перетинатися. Точки перетину t_i і t_j позначимо $p(t_i, t_j) = [t_i(x_{ij}), t_j(x_{ir})]$. Оскільки одиниця масштабу W відповідає Q_{ij}, то $p(t_{ij}, t_j)$ може реалізовуватися на початку чи наприкінці x_{ij}, що позначимо $t_i(x_i^{+}{}_j)$ або $t_i(x_i^{-}{}_j)$, де «+» означає перетин на початку x_{ij}, а «-» — наприкінці x_{ij}. Очевидно, що $p(t_i, t_j)$ не можуть існувати в довільних місцях Q_i, а їх виникнення залежить від характеру розміщення траєкторій. Обмежимося площиною для побудови φ_i, тоді кожний елемент φ_i можна ідентифікувати з його локалізацією на площині. Локалізацію точки початку еталонного слова або фрагмента траєкторії $\varphi_i(t_i)$ позначатимемо $x_i(\alpha_i^{-} \beta_{it}^{-})$.

Розглянемо ряд параметрів, що використовуються для опису особливостей різних варіантів реалізації графічних образів *zz*. Відповідні параметри ґрунтуються на вищевведених поняттях для опису графічних образів.

Така група параметрів базується на уявленнях про Q, як множини траєкторій T_i, що реалізовуються в двомірному просторі W_i. Такі параметри мають наступні типи ознак (рис. 18):

— середня довжина групи траєкторій, що мають довжини з загальною допустимою різницею, яку позначатимемо символом $\delta(t_i)$;

— міра незалежності траєкторії $\tau(t_i)$;

— міра взаємної розбіжності траєкторій $r(t_i t_j)$;

— міра автономності окремих траєкторій $a(t_i)$;

— міра однозначності траєкторії $h(t_i)$.

Рис. 18. Параметри графічної моделі засобів захисту

Траєкторії, що описують Q, можуть перетинатися між собою. Тоді виникає необхідність виділення різних траєкторій як окремих елементів Q_i. Така ідентифікація здійснюється шляхом етикетування окремих фрагментів t_i, що визначаються як такі, що належать одній траєкторії, і здійснюється в процесі побудови Q_i. Отже, всі траєкторії t_j, які мають спільні точки з t_i можна вважати траєкторіями, що перетинають t_j. Кількість таких перетинів встановлює параметр $\delta(t_i)$, який можна визначити на основі співвідношення:

$$\forall t_{ij}\left[t_{ij} \in \varphi_i \subset Q_i\right] \exists \Delta_i \left(\Delta_i = c_i\right)\left\{\delta(t_i) = \left[\sum_{j=1}^{k} \Delta(t_{ij})\right] / k\right\},$$

де φ_i — фрагмент образу Q_i, що об'єднує вибрану групу траєкторій; c_i — константа, що визначає максимально допустиме відхилення довжини траєкторії t_{ij} від t_{in} при $n \le k$, $\Delta(t_{ij})$ — максимальне відхилення t_{ij} від довжини всіх траєкторій t_{in}, що входять у групу φ_i, і яке визначається згідно зі співвідношенням:

$$\Delta t_{ij} = \max\left\{\left(\left|t_{ij} - t_{i,j+1}\right|\right),\left(\left|t_{ij} - t_{i,j+2}\right|\right),...,\left(\left|t_{ij} - t_{i,k}\right|\right)\right\}.$$

Кожна з окремих траєкторій може перетинати певну кількість інших траєкторій. Виділення типу траєкторій є можливим завдяки тому, що кожна окрема траєкторія може бути ідентифікованою [89]. Тоді міра автономності траєкторії t_i визначається кількістю перетинів інших траєкторій, що реалізуються траєкторією t_i. Між двома траєкторіями t_i і t_j у вибраних на них точках можна здійснювати вимірювання віддалі між ними. До таких точок можна віднести початкові та кінцеві точки траєкторії та точки, які залежно від встановлених умов певним чином поділяють вибрані траєкторії, наприклад, на половину чи на три рівні частини тощо. При цьому кожна окрема віддаль між відповідними точками являє собою найменший шлях між відповідними точками, що будується або може бути побудований у відповідній метриці простору W_i. Оскільки простір W_i є дискретним і спосіб переходу від однієї точки простору до суміжної визначається метрикою W_i, то кількість таких способів є обмеженою. Тому кількість можливих траєкторій r_i, що з'єднують дві вибрані точки на відповідних траєкторіях є скінченою. В цьому випадку віддаль між двома точками траєкторій t_i і t_j визначається співвідношенням:

$$r_i(\alpha^*, \beta^*) = \min\left\{r_{i1}(\alpha^*, \beta^*), r_{i2}(\alpha^*, \beta^*), ..., r_{in}(\alpha^*, \beta^*)\right\}.$$

Середня віддаль, що визначається певним способом, наприклад, як середня арифметична віддаль між вибраними точками

траєкторій, являє собою такий параметр, як розбіжність траєкторій і визначається з співвідношення:

$$r(t_i,t_j)=\left[\sum_{l=1}^{m} r_l\left(\alpha_i^*,\beta_i^*\right)\right]\Big/m .$$

Очевидно, що цей параметр можна визначати для деякої сукупності траєкторій, що об'єднуються фрагментом φ_i. Кількість пар траєкторій, між якими вимірюється віддаль, визначається комбінацією з m по η, що визначається відомими з комбінаторики способами [90]. Тоді параметр $r(\varphi_i)$ обчислюється відповідно до співвідношення:

$$r(\varphi_i)=\left[\sum\nolimits_{j=1}^{k}\left[\sum\nolimits_{j=1}^{me} r_l\left(\alpha_{\mathrm{j}}^{*e},\beta_j^{*e}\right)\right]\Big/me\right]\Big/k, \text{ де } e=\{1,2,...,k\} .$$

Міра однозначності траєкторії є відносною мірою, яка визначає залежність однієї траєкторії від інших або від однієї вибраної траєкторії. Вона позначається: $h\left[t_i,\left(t_{j1},t_{j2},...,t_{jm}\right)\right]$, якщо залежність визначається між t_i і рядом вибраних траєкторій, або — $h\left(t_i,t_j\right)$, якщо залежність траєкторії t_i встановлюється щодо однієї траєкторії t_j. Міра однозначності траєкторії визначається кількістю перетинів, які реалізуються траєкторією t_i або траєкторіями $t_{j1},t_{j2},...,t_{jm}$ траєкторії t_i. Застосування параметрів автономної траєкторії обумовлюється тим, що визначення траєкторій може здійснюватись після нанесення Q_i на d_i при виготовленні експериментальних зразків документів. Тоді в точках перетину окремої траєкторії t_i вона може продовжуватись щонайменше в трьох напрямках. Цим визначається незалежність траєкторії t_i від інших траєкторій, що її перетинають. Очевидно, що $h\left[t_i,\left(t_{j1},...,t_{jm}\right)\right]=\tau\left(t_i\right)$, якщо в h використовуються всі $t_j\in T$, що формально записується як:

$$\neg\exists\left(t_i\in T\right)\left\{h\left[t_i,\left(t_{j1},...,t_{jm}\right)\right]\right\}\rightarrow\left\{h\left[t_i,\left(t_{j1},...,t_{jm}\right)\right]=\tau\left(t_i\right)\right\} .$$

Наступна група параметрів ґрунтується на основі уявлень про Q_i, як про формальну мову $L(M)$, та теорію абстрактних автоматів. У цьому випадку Q_i описується, як графове відображення деякої мови $L(Q_i)$. До параметрів цього типу можна віднести (рис. 19):

— міру персоналізації редукцій системи формування мови або окремих слів з $L(Q_i)$;

— довжину процедури виводу одного слова x_i мови $L(Q_i)$;

— міру активності формальної граматики $L(Q_i)$.

Рис. 19. Параметри граматичних моделей засобів захисту

Міра персоналізації редукцій з системи Σ визначається кількістю випадків використання окремої редукції для формування кожного слова чи всього образу Q_i. Очевидно, що залежно від графічної структури Q_i міра персоналізації редукцій буде різною. На якісному рівні це означає міру однозначності вибору чергової редукції при побудові образу Q_i. Для того щоб можна було сформувати метод визначення величини цього параметра, необхідно більш детально розглянути можливі типи редукцій. Можливі типи редукцій залежать від умов, які мають задовольняти певні Q_i, що формуються на d_i. До таких умов можна віднести:

— редукції ξ_i з Σ не повинні суперечити системі логічних формул, які описують той чи інший варіант реалізації графічного образу Q_i або його фрагмента;

— редукції ξ_i мають давати можливість виконання всіх вимог, що визначаються заданими значеннями вибраних параметрів всіх типів їх груп;
— редукції повинні реалізовуватися в поточному фрагменті Q_i з врахуванням особливостей метрики простору, в якому формується відповідний образ;
— використання системи редукцій Σ не має призводити до конфліктних чи до виникнення тупикових ситуацій у графічному відображенні засобу захисту документа, як в рамках окремого zz_i, так і в рамках всієї системи захисту документа;
— система Σ повинна бути відкритою для формування нових редукцій, елімінації редукцій, що уже включені у систему Σ та модифікації редукцій, які уже використовувалися в процесі побудови Q_i.

Для зручності логічні формули, що описують окремі фрагменти $\varphi(Q)$, позначатимемо як $l_i \in L$. В цьому випадку першу умову можна формально описати співвідношенням:

$$\left[L_i(Q)\,\&\,\Sigma\right] \to \forall\left[\xi_i(\varphi_i) \to (\varphi_i\,\&\,\neg\varphi_{i+1})\right].$$

Вищевказана умова означає, що редукція ξ_i з Σ є несуперечним розширенням правил виводу $L_i(Q_i)$. Оскільки редукція ξ_i визначається інтерпретацією посилки і виводу зв'язку, який вона описує, то це означає, що кожна редукція, яка є несуперечливою в $L_i(Q_i)$ має хоча б одну індивідуальну інтерпретацію в Q_i. Оскільки параметри Q_i визначають захисні властивості графічного образу, то на кожному кроці використання вибраної редукції значення відповідного параметра повинно змінюватися. Може бути ситуація, коли окрема редукція ξ_i призводить до зміни ряду параметрів. В цьому випадку ξ_i має призводити до збільшення значення хоча б одного параметра Q_i.

Вказана обставина визначає міру персоналізації редукцій системи Σ. Таким чином міру персоналізації ξ_i можна описати:

$$\omega(\xi_i) = \left[\sum_{i=1}^{m} sign\left[\xi_i^v(Q)\right]\right] + \Delta P_i(\xi_i),$$

де $sign\left[\xi_i^v(Q_i)\right] = 1$, якщо ξ_i призвело до збільшення значення хоча б одного параметра Q_i, $\Delta P_i(\xi_i)$ — величина, на яку збільшилося значення параметра P при використанні редукції ξ_i.

Оскільки редукції $\xi_{i1},...,\xi_{im}$ можуть впливати на зміну величин параметрів через їх персоналізацію, а вимоги до образу Q визначаються на основі тих чи інших значень параметрів, то можна стверджувати, що у випадку використання персоналізованих редукцій або редукцій, міра персоналізації яких є не менше заданого рівня $\forall\xi_i\left[\mu(\xi_i) \geq C\right]$, то система Σ може забезпечувати застосування вимог, що формулюються для образів Q_i. При цьому повнота забезпечення системою Σ усіх вимог може бути виконана.

При формуванні ξ_i можуть враховуватися не тільки послідовності застосування окремих слів чи символів алфавіту A, але й координати поточного фрагмента образу, який запроектовано будувати. Така можливість з'являється за рахунок використання координат, якими може описуватися черговий елемент образу. Це зокрема дозволяє враховувати метрику простору.

Через скінченність і дискретність простору, в якому формується графічний образ, при побудові окремих фрагментів образу, що реалізується в процесі виявлення скритих частин [91], можуть виникнути конфліктні ситуації, які полягають у наступному:

— відновлюваний фрагмент порушує вимоги до образу в цілому, що проявляється у недопустимій зміні величини параметрів, які характеризують Q_i;

— може порушуватись синтаксис зв'язків між невидимими та видимими фрагментами d_i,

— можуть порушуватися умови завершення побудови окремих слів.

Довжина виводу слова являє собою кількість кроків перетворень, що здійснюються над початковим словом або початковим елементом фрагмента. При цьому довжина процесу виводу $H(\Sigma)$ і довжина слова, що генерується $H[\varphi(Q)]$, можуть бути рівними або $H(\Sigma(Q)) \geq H[\varphi(Q)]$.

Активність формальної граматики M_i визначається можливостями системи виводу слів мови $L(M_i)$. Класичною компонентою для формування мови $L(M_i)$ в граматиці M_i є система редукцій, що включає підсистему умов вибору чергової редукції при реалізації поточного кроку формування слова m_i з $L(M_i)$, та підсистема умов модифікації системи редукцій Σ [92]. Завдяки цим підсистемам можна прискорити процеси формування нових m_i і, що особливо важливо для графічних засобів захисту, які використовують скриті фрагменти, підвищення міри активності M_i призводить до покращення можливостей відновлення Q_N в Q [93].

РОЗРОБКА КОМПОНЕНТ СИСТЕМИ ЗАХИСТУ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ МЕТОДІВ УКРИТТЯ ДАНИХ У ГРАФІЧНОМУ СЕРЕДОВИЩІ

Розробка алгоритмів побудови графічних засобів захисту, що використовують стеганографічні методи укриття окремих фрагментів

Перед розглядом алгоритмів та методів побудови графічних засобів захисту, більш детально зупинимося на принципах використання та організації графічних засобів захисту на основі стеганографії. До них належать такі положення.

1. Графічний засіб захисту паперових документів повинен бути унікальним для кожного окремого документа.

2. Алгоритм побудови унікального графічного засобу захисту повинен бути в таємниці, а його виявлення має бути досить складною для розв'язку задачею.

3. Графічні засоби мають характеризуватися рядом інтегральних параметрів, які б з необхідною точністю могли ідентифікувати графічний засіб захисту для оригінального документа.

4. Графічний засіб захисту може мати невидимі фрагменти, які можуть реалізуватися такими способами:

— недодруковуванням відповідних фрагментів;

— маскуванням окремих фрагментів графічного образу, які мають свою власну інтерпретацію;

— формування окремих фрагментів псевдоневидимим способом, наприклад, фрагментів, що стають видимими при дії на них фізичних чи хімічних факторів.

Четверте положення відповідає випадку, коли графічний засіб захисту використовує принципи стеганографії. Інші положення є необхідними для можливого застосування методів стеганографії. При цьому найефективнішим способом формування невидимих фрагментів є їх недодруковування.

В рамках зазначених положень можна виділити рівні гарантування безпеки документів. Перший рівень відповідає випадку, коли графічний засіб захисту наноситься на документ повністю і є унікальним графічним образом даного екземпляра документа. В цьому випадку міра захищеності документа визначається повнотою відповідності алгоритму формування графічного засобу захисту для чергового екземпляра документа, який підробляється; алгоритму, що використовується для таких самих цілей при виготовленні оригінальних документів. Така міра відповідності не може формуватися на основі порівняння оригінального та фальшивого алгоритмів, оскільки за визначенням, зацікавленій стороні фальшивий алгоритм невідомий. Встановлювати фальшивий алгоритм за виявленим фальшивим документом не доцільно. Зацікавленою стороною при визначенні міри захищеності документа і виборі графічного, поліграфічного чи стеганографічного засобу (GPS засобу) є виробник документа. Міра відповідності засобу GPS, який реалізовано в документі, визначається на основі аналізу параметрів, що використовуються у різних випадках реалізації SK. Очевидно, що відповідні параметри можуть вимірюватися з різною точністю. Відповідно фальшивий документ може вміщувати GPS, що описуються параметрами, які відповідають з певною точністю відображенню zz на оригіналі документа. Нехай точність контролю zz системою SK по всіх параметрах відповідає величині $\Delta_0(SK)$ або Δ_0. Точність відтворення GPS засобу в документі відповідає величині Δ_d. Тоді документ при проведенні контролю засобу GPS є оригінальним, якщо справедливе співвідношення:

$$\left\{\Delta_0\left[SK\left(d_i\right)\right] \geq \Delta_0\left(d_i\right)\right\} \rightarrow \left(d_i = d_i^0\right),$$

де d_i — документ, що піддається контролю; d_i^0 — оригінальний документ. Якщо точність $\Delta_0(SK)$ не достатня, то необхідно її підвищити. Недостатність точності може виявитися на основі аналізу результатів, отриманих у процесі реалізації TP. Такий результат може інтерпретуватися використанням атакованих документів, або $d_i = d_i^a$.

Тоді співвідношення можна записати у такому вигляді:

$$\left[F(TP)\&\left(d_i^0 = d_i^a\right)\right] \to \left[\left(\Delta_0 = \Delta_0^*\right)\&\left(\Delta_0^* > \Delta_0(SK)\right)\right],$$

де $F(TP)$ — функція аналізу результату TP; Λ_0^* — нове значення точності вимірювань d_i; d_i^a — атакований документ.

Для побудови *zz* використовуватимемо параметри, що характеризують графічний образ в рамках застосування різних типів моделей його опису. Тому спосіб використання кожного з введених параметрів розглянемо в описах першого типу моделей, що являють собою моделі типу LIM. Такі моделі описуються як сукупність траєкторій $t_i \in T(Q_i)$. Однією з базових умов застосування вказаних моделей є розмітка траєкторій етикетками, що дозволяє у множині різних траєкторій, що перетинаються, виділяти окремі t_i. Основою для формування певного варіанта Q_i є параметри, за якими повинні ідентифікуватися документи. При повному контролі документів мають використовуватися всі параметри, що описують Q_i в моделях LIM. В рамках системи цих параметрів можна реалізувати певну їх класифікацію, яка впливає на рівень захисту документів. Загалом можна виділити такі фактори, що визначають в рамках відповідних параметрів критерії контролю документів:

— параметри контролю повинні відображати їх узагальнене значення для вибраного фрагмента Q_i і в цьому сенсі можна вважати їх інтегральними;

— взаємозалежності між параметрами контролю, що характеризують окремі фрагменти, мають бути визначеними, що дозволить розглядати їх як наступний інтегральний критерій контролю;

— інтерпретація відповідних параметрів видимих частин фрагмента Q_i не повинна виявляти наявність в межах їх локалізації розміщення невидимих частин відповідних фрагментів;

— при існуванні суперечностей чи конфліктів у видимих частинах фрагментів у графічному засобі *GPS* інтегральні пара-

метри мають виявляти такі факти безпосереднім значенням своєї величини чи опосередненo, шляхом виникнення певних варіантів їх інтерпретації.

Алгоритм формування графічних засобів захисту повинен грунтуватися на вищенаведених критеріях контролю документів. Оскільки вказані критерії мають функціональний характер, то необхідно розглянути їх зв'язок з параметрами, що використовуються для опису моделей різних типів [94]. Завдяки цьому виникне можливість перейти від функціональних критеріїв до відповідних параметричних критеріїв. Для формування певного Q_i необхідно виконати такі умови:

— забезпечити відмінність нового образу від образів, що уже використовувались в попередніх документах;

— необхідно, щоб прогнозування нового образу було складною для розв'язання задачею;

— наклад документів не повинен впливати на величину рівня захищеності документа, яка для кожного окремого документа може бути різною.

Виходячи з того, що в основі визначення документа знаходиться уявлення про його засоби захисту і базовим параметром, який визначає якість документа, є міра захисту, розглянемо основні фактори, які його визначають. Міру захисту документа можна визначати відповідно до таких позицій або компонент, що входять в TP:

— можливостей засобів захисту, що визначають ту чи іншу міру захищеності документів;

— засобів контролю документів або системи SK, що є основним ідентифікатором міри захищеності документів;

— технологічного процесу, що містить систему захисту і визначає споживчі та технологічні вимоги до документів, які проектуться в ньому використовувати.

Функціональна система застосування документів у процесі реалізації ТР наведена на рис. 20.

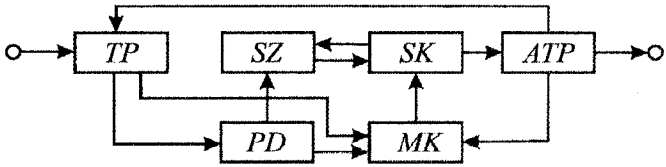


Рис. 20. Функціональна схема використання документів

На рис. 20 використовуються такі скорочення:

TP – технологічний процес, що використовує документи;

SZ – система захисту документів;

SK – система контролю документів;

PD – система проектування засобів захисту документів;

MK – методика контролю документів;

ATP – система аналізу результатів функціонування *TP*.

Приймемо стратегію проектування *SZ* документів, відповідно до якої спочатку формується макет усього графічного образу, а потім на ньому формуються невидимі фрагменти, які не будуть друкуватися. Таким чином, формування або проектування системи захисту (SZ) документів складається з таких базових етапів:

— вибір та інтерпретація системи параметрів, що визначають загальні характеристики Q_i, який позначимо — *VPI*;

— формування на основі вибраних параметрів моделей опису Q_i і реалізація синтезу моделей, що використовуються для опису Q_i, що позначимо — *MSZ*;

— формування прихованих фрагментів Q_i, що являє собою реалізацію стеганографічних методів укриття даних в Q_i, що позначимо — *SUD*;

— етап, на якому будуть формуватися правила модифікації моделей системи захисту, яка є необхідною для формування чергового екземпляра документа з власною системою захисту — *MGQ*.

В цьому випадку не розглядатимемо допоміжні етапи, такі як тестування сформованих *zz* на їх відповідність необхідному рівню

захисту чи етап, на якому здійснюється перевірка відповідності спроектованих *zz* можливостям *SK* тощо.

Приймемо, що кожен технологічний процес може використовувати один документ або систему документів, що забезпечують його реалізацію $d_i \in D$.

При використанні технологічним процесом TP_i системи документів визначається її структура SD, що можна записати у вигляді:

$$F(TP_i) \to \left\{ SD_i = f_i \left[\begin{array}{l} \varphi_1 \left[(d_1, tp_1), ..., (d_k, tp_k) \right], ... \\ ..., \varphi_m \left[(d_{m1}, tp_{m1}), ..., (d_{mk}, tp_{mk}) \right] \end{array} \right] \right\},$$

де φ_1 — фрагмент TP_i, на якому використовуються документи $\{d_1, ..., d_k\}$, а $\{tp_1, ..., tp_k\}$ — відповідні ділянки TP_i; F_i — функція, що описує загальну структуру системи використання документів в TP, що позначається як SD_i. Якщо для кожного d_i можна поставити у відповідність один або декілька tp_i, то можна стверджувати, що міра захищеності, яку забезпечує документ d_i, відповідає вартості збитків, до яких може призвести успішна атака на цей документ, і, відповідно, величина таких збитків визначається вартістю відповідного фрагмента tp_i технологічного процесу. Не будемо розглядати можливих залежностей між втратами на різних фрагментах φ_i процесу TP_i і, відповідно, залежностей між необхідними мірами захисту документів, що визначається різними $\varphi(TP_i)$. Приймемо, що всі $\varphi(tp)$ і які захищаються відповідними документами d_i, з точки зору величини збитків чи втрат, є незалежними між собою і однозначно визначають необхідну міру захисту, яку повинен забезпечувати відповідний документ. В цьому випадку на кількісному рівні необхідно розглянути спосіб визначення величини міри захисту яку забезпечує документ або підсистема захисту, що реалізується в цьому документі Sd_i, за величиною втрат, які можуть виникнути у фрагменті $\varphi_i(TP_i)$ технологічного

процесу [95]. Зазначимо, що значна частина можливих TP, в яких використовуються документи, мають економічний характер, тоді можна прийняти, що величина втрат на довільних $\varphi_i(tp_i)$ вимірюється величиною коштів.

Рівень захисту документів визначається такими факторами:

— частиною вартості системи контролю, яка здійснює контроль документів, що обслуговують відповідний фрагмент TP;

— інтенсивністю атак на відповідний фрагмент TP;

— інтенсивністю використання певних TP і відповідних $\varphi_i(tp)$;

— швидкістю реалізації окремого TP.

Вартість SK у величині коштів визначається досить однозначно, оскільки система складається з конкретних засобів контролю і процедур їх використання. Інтенсивність атак не призводить до необхідності прямо пропорційного збільшення коштів SK, якщо всі атаки виявляються в процесі реалізації TP, і якщо всі атаки успішні, то вони приводять до відповідного збільшення коштів на SK. Інтенсивність застосування TP призводить до збільшення частини коштів SK, яка визначається затратами на реалізацію процедур контролю. Якщо TP може протікати з різною швидкістю, то для певного варіанта реалізації SK існує гранична швидкість процесу функціонування TP. Оскільки всі вищенаведені фактори, крім першого, належать до факторів, які можуть прогнозуватися, то *GPS*-засіб повинен бути спроектований таким чином, щоб у випадку, коли прогнозовані фактори, незалежно від результатів прогнозування, приймають максимальні значення, то *zz* повинні забезпечувати максимально можливий рівень захисту.

Стеганографічні методи укриття даних визначаються такими умовами їх реалізації:

— забезпеченням невидимості скритих даних при звичному спостереженні;

— наданням можливості потенційному споживачеві отримати вбудовану в середовище інформацію на основі певного аналізу чи перетворень самого середовища, з використанням додат-

кової інформації, яка є доступною лише для уповноваженого користувача;

— факт можливості існування скритої в середовищі інформації не повинен бути видимим, як і приховані в ньому дані.

В цьому випадку забезпечення невидимості скритих даних реалізується шляхом недодруковування відповідних фрагментів образу, що являють собою приховані дані. Надання можливості потенційному або уповноваженому споживачеві отримати невидиму інформацію на основі аналізу чи певних перетворень середовища полягає у наступному. Оскільки графічні засоби захисту будуються таким чином, що невидимі фрагменти повинні бути безпосередньо пов'язані з видимими фрагментами, то на основі моделей, що їх описують, можна сформувати алгоритми, які дозволяють, виходячи з видимої частини графічного засобу захисту, добудувати у видимому вигляді невидимі фрагменти [96, 97]. Оскільки видимі фрагменти становлять домінуючу частину графічного образу Q_i, можна стверджувати, що видимі фрагменти Q_i є тим середовищем, в якому заховано скриті фрагменти. При цьому додатковою інформацією для отримання невидимих даних є правила виводу невидимих фрагментів з видимих. Очевидно, що способи використання відповідних правил тісно пов'язані з параметрами видимих фрагментів, що є вихідними даними для виводу невидимих частин. Тому виникає необхідність доведення однозначності виводу невидимих фрагментів у рамках вихідних даних (видимих частин) параметрів, що характеризують Q_i та прийнятих правил перетворень, що здійснюються в процесі виводу.

Остання умова, що визначає застосування стеганографічних методів, полягає в утаємненні для неуповноваженого користувача параметрів, що характеризують та їх значень, які відповідають конкретним реалізаціям *zz* у вигляді Q_i.

Розглянемо таке твердження.

Твердження 4.1. Система формування графічних образів типу J^4 є несуперечною, якщо існують співвідношення:

$$F_L[LIM,\Sigma]\to[Q(L)=Q_L]$$
$$F_G[GIM,A]\to[Q(G)=Q_G]$$
$$F_S[SIM,R]\to[Q(S)=Q_S]$$

та виконуються перетворення:

$$[f_L(Q_L)\to Q_G]\&[f_G(Q_G)\to Q_S]\&[f_L(Q_L)\to Q_S]\&$$
$$\&[f_S(Q_S)\to Q_L]\&[f_S(Q_S)\to Q_G]\&[f_G(Q_G)\to Q_L].$$

Доведення твердження складається з таких частин. В першій частині необхідно довести, несуперечність системи виводу для кожної з моделей опису образів Q_i, оскільки в кожному окремому випадку представлення Q_i використовуються різні засоби виводу. В цьому випадку засоби виводів кінцевих фрагментів φ_i і образу Q_i в цілому, по суті, формують відповідний образ, який необхідно побудувати. У випадку моделей *LIM* — це система правил логічного виводу $\Sigma=\{\xi_1,...,\xi_n\}$; в моделей *GIM* — це абстрактні автомати та відповідні автоматні перетворення A, а у моделей *SIM* — це системи редукцій, які дозволяють здійснювати перетворення та формування відповідного образу.

В другій частині доведемо функціональну еквівалентність різних моделей опису Q_i. Необхідність в цьому зумовлюється тим, що об'єкт, який необхідно сформувати, є об'єктом, інтерпретація якого являє собою певну абстракцію, що визначається досить спеціалізованими умовами, які описують функціональні можливості відповідного об'єкта і не може проектуватися на ті чи інші фрагменти природних областей інтерпретації.

У третій частині покажемо, що застосування прийнятих способів представлення Q_i не призводить до виникнення конфліктів. Конфлікти можуть полягати в тому, що використання параметрів для опису Q_i в рамках однієї моделі не призводить до появи суперечностей в інших способах опису одного і того самого об'єкта Q_i.

Оскільки правила виводу відображають процес формування чергового елемента Q_i, то кожне з правил визначає умови формування чергового елементу $\varphi_i(Q_i)$. В рамках *LIM* складовою, що відображає інформаційну компоненту, є система умов вибору правила побудови фрагмента образу на поточному кроці виводу. Таке розширення являє собою введення функцій розвитку еталонних фрагментів $\varphi_i^e(x_i)$, що описуються співвідношеннями:

$$\xi_1 : \left\{ \varphi_i^e(x_i) \,\&\, \left[\left[\left[(P_i + \Delta P_i) \right] > P_i^d \right] = b_i \right] \,\&\, \exists \xi_i \left[\xi_i \left[\varphi_i^e(x_i) \right] \neq b_i \right] \right\} \rightarrow$$
$$\rightarrow \xi_i \left[\varphi_i^e(x_i), x_j \right],$$

де P_i — поточне значення параметра, що аналізується на даному етапі формування $\varphi_i(Q_i)$; P_i^d — граничне значення цього параметра; b_i — ознака переходу P_i за допустимі границі; x_j — геометричний примітив, що використовується на поточному кроці формування Q_i, якщо їх більше одного; ΔP_i — величина зміни параметра P_i при реалізації чергового кроку формування Q_i.

Другий тип розширення системи Σ передбачає можливість враховування конфігурації попередньої частини фрагмента $\varphi_i(x_i)$, якщо він не є фрагментом типу φ_i^e. Таке розширення записується як:

$$\xi_2 : \left\{ \begin{array}{l} \left[\varphi_i(x_i) * x_{i1} * \ldots * x_{ik} \right] \,\&\, \forall x_{ij} \left[\varphi_{i+1}(x_i, \ldots, x_{ik}) \neq b_k \right] \,\& \\ \&\exists \xi_i \left[\xi_i \left[\varphi_{i+1}(x_i, \ldots, x_k, x_m) \right] = \alpha \right] \end{array} \right\} \rightarrow \xi_i(\varphi_i, x_m),$$

де $\left[\varphi_i(x_i) * x_{i1} * \ldots * x_{ik} \right]$ — фрагмент Q_i; x_m — черговий геометричний примітив, α — інтерпретація значення логічної формули $\xi_i[\varphi_{i+1}(x_i, \ldots, x_k, x_m)]$, що прийнята в системі Σ, наприклад, α_i може дорівнювати 1, що є загальноприйнятим для класичних логічних систем.

Для доведення несуперечності Σ_i в цілому $F_L[LIM, \Sigma]$, припустимо, що в $F_L[LIM, \Sigma] \rightarrow (Q_L \,\&\, \neg Q_L)$, що означає можливість

виводу двох суперечних образів Q_L і $\neg Q_L$. Ця суперечність означає, що значення параметрів P_i, які описують два різні образи Q_i^L і $Q_i^{L^*}$ є різними. Відповідно до розширень $\xi_i \in \Sigma$ умови формування чергових елементів x_i при побудові образів Q_i передбачають перевірку відповідності сформованої частини Q_i значенням заданих P_i. Тому, якщо є можливим $Q_L \,\&\, Q_i^L$, то система Σ в рамках системи виводу, що прийнята для предикатів є суперечлива. Це суперечить твердженням про несуперечність вузького числення предикатів, що доводиться в математичній логіці [84,85]. Тому система $F_L[LIM, \Sigma]$ — несуперечлива.

У випадку використання *GIM* система формування слів відповідної мови ґрунтується на основі застосування уявлень про абстрактні автомати. В цьому випадку уявлення про абстрактний автомат буде дещо модифіковане. Як відомо, автомат A визначається співвідношенням:

$$A_i = \left(x_i, y_i, H_i, \lambda_i, \delta_i, h_i^0\right),$$

де y_i — вихідний алфавіт, H_i — множина внутрішніх станів, що може описуватися в алфавіті x_i, λ_i і δ_i — як і в класичному визначенні абстрактного автомата A [86] являють собою перетворення поточного стану автомата в новий стан, або $\lambda_i\left(h_i(A), x_i\right) = h_j(A)$; δ_i — це перетворення $\delta_i\left(h_i(A), x_i\right) = \omega_j(x_i)$, де ω_i – слово, щодо цього було сформоване автоматом A за m тактів роботи, в яке увійшов елемент x_i, що доповнив слово ω_i на такті $m+1$. В цьому випадку множина станів автомата описується власним алфавітом H_i. Особливістю даного автомата є наявність зворотного зв'язку. Це означає, що на вхід автомата A може подаватися на кожному такті черговий елемент вихідного слова y_i. Необхідність такої модифікації зумовлюється тим, що $\omega_i(y_i)$ представляє $\varphi_i(Q_i)$, а $\omega_i(\varphi_i)$ залежить від $\omega_{i-1}(y_i)$, яке отримане

на попередньому кроці. Очевидно, що реалізація контекстної залежності може здійснюватися і на основі формування системи внутрішніх станів автомата, але тоді H_i буде більш громіздким.

Суперечність *GIM* буде полягати у тому, що автомат A_i на основі двох однакових вхідних слів $\omega_i(x_i)$ міг би продукувати різні вихідні слова $\omega_i(y)\&\omega_j(y_j)$, або це можна записати у вигляді: $\left[\omega_i(x_i)\to A_i\right]\to\left[\omega_i(y_i)\vee\omega_j(y_j)\right]$.

Покажемо, що в рамках *GIM* такого автомата A_i не існує. Припустимо, що існує такий автомат A_i^*, для якого правильне $A_i^*\left[\omega_i(x_i)\right]\to\left[\omega_i(y_i)\vee\omega_j(y_j)\right]$. Наведене співвідношення можна інтерпретувати таким чином. Автомат A^* не розпізнає вхідного слова $\omega_i(x_i)$ і тоді можливо, що $A_i^*\left[\omega_i(x_i)\right]\to\left[\omega_i(y_i)\vee\omega_j(y_j)\right]$. Зазначимо, що $\omega_i(y_i)$ і $\omega_j(y_j)$ можуть генеруватися A_i^* в різних циклах перетворення $\omega_i(x_i)$. Це означає, що повинно існувати:

$$\left[A_i^*\left[\omega_i(x_i)\right]\to\omega_i(y_i)\right]\&\left[A_i^*\left[\omega_i(x_i)\right]\to\omega_j(y_j)\right].$$

Якщо $A_i^*\left[\omega_i(x_i)\right]\to\left[\omega_i(y_i)\vee\omega_j(y_j)\right]$, то це означає, що автомат A_i^* не розпізнає слова $\omega_i(x_i)$. Відповідно до твердження 2.1. існує визначена довжина вхідного слова для відповідних A_i, яка завжди буде розпізнаватися певним автоматом A_i^*.

Тому випадок, коли $A_i^*\left[\omega_i(x_i)\right]\to\left[\omega_i(y_i)\vee\omega_j(y_j)\right]$ є неможливим. Розглянемо ситуацію, коли $\omega_i(x_i)$ надаються на вхід A_i^* в різних циклах роботи A_i. Нехай при виконанні першого циклу перетворення $\omega_i(x_i)$ автоматом A_i^* існує: $A_i^*\left[\omega_i(x_i)\right]\to\omega_i(y_i)$. Це означає, що на кожному кроці функціонування A_i^* виконувались

перетворення: $\left[\lambda_i\left[y_i\left(A_i^*\right),x_i\right]\to h_j\left(A_i^*\right)\right]\&\left[\delta\left[h_j\left(A_i^*\right)\right]\to y_i\right]$. Для цілого циклу функціонування автомата A_i^* можна записати:

$$\forall_i\left\{\left[\lambda_i\left(h_i,x_i\right)\to h_j\right]\&\left[\delta\left(h_j\right)\to y_i\right]\right\}. \qquad (4.1)$$

Для наступного циклу роботи A_i^* згідно з припущенням можна записати:

$$\forall_i\left\{\left[\lambda_i\left(h_i,x_i\right)\to h_j\right]\&\left[\delta\left(h_j\right)\to y_j\right]\right\}. \qquad (4.2)$$

Оскільки справедливе $\left[\delta\left(h_j\right)\to y_i\right]$, то h_j з (4.1) і h_j з (4.2) не дорівнюють одне другому. Це означає, що перетворення $\lambda_i\left(h_i,x_i\right)$ є неоднозначне. Така неоднозначність λ_i може обумовлюватися лише тим, що h_j з (4.1) і h_j з (4.2) є різними, оскільки x_i є однаковим для (4.1) і (4.2) з визначення. Згідно з визначенням автомата $A_i = A_i^*$, якщо $x_i = x_i^*$, то:

$$\left(\forall x\in x\right)\lambda\left(A\right)\left(h\left(A\right),x\right)=\lambda\left(A^*\right)\left(h\left(A^*\right),x\right).$$

Отже, для того щоб $\lambda A\left(h_i\left(A\right),x\right)\neq\lambda A^*\left(h_i\left(A^*\right),x\right)$, необхідно щоб одне і теж вхідне слово $\omega_i\left(x_i\right)$ на деякому етапі функціонування A в одному випадку призводило до використання стану h_i, а в другому — до використання h_j. Спосіб реалізації поточного кроку при перетворенні $\omega_i\left(x_i\right)$ визначається попередніми кроками перетворення $\omega_{i-1}\left(x_i\right)$ та всіма поточними станами автомата. Тому на довільному кроці перетворень $\omega_i\left(x_i\right)$ та на довільному циклі перетворень одного і того ж вихідного слова будуть повторюватися відповідні стани автомата. Це означає, що завжди $\lambda A\left(h_i\left(A\right),x\right)=\lambda A^*\left(h_i\left(A^*\right),x\right)$ при $A=A^*$. А це, в свою чергу, доводить неможливість виникнення в *GIM* суперечності в процесі побудови $\omega_i\left(y_i\right)$.

Суперечність в *SIM* полягатиме у виникненні ситуації, при якій формування фрагмента структури відповідно до умов їх завершення не будуть закінчені, а структурне оточення поточної точки фрагмента не дасть можливості продовження побудови відповідного $\varphi_i(Q_i)$. Наявність суперечності в *SIM* означає неможливість побудови у ньому всіх $\varphi_i(Q_i)$ відповідно до вибраної стратегії формування Q_i. Стратегія формування Q_i вибирається на основі заданих значень глобальних параметрів відповідного Q_i. Кожний з глобальних параметрів P^G, будучи певною абстрактною характеристикою, може бути зведеним до певного масштабу, який визначає спосіб його визначення. Залежно від характеру абстракції Q_i можна сформулювати різного типу параметри. Оскільки допустимі способи визначення P_i^G передбачають методи обчислення його величини, то для доведення розглянемо P_i^G наступних типів:

— міра симетрій P_S^G визначається точністю повторення структури вибраних фрагментів Q_i;

— візуальні особливості в межах Q_i, що позначаються як параметр P_O^G;

— параметр, який описується вибраним графовим інваріантом за умови що Q_i допускає структурну інтерпретацію, яку позначимо P_G^G.

Параметр P_S^G описується двома складовими:

— кількістю симетричних зразків, що розміщуються в образі Q_i, або які вибрані в цьому образі;

— мірою подібності між зразками одного класу.

Формально це записується у вигляді:

$$P_S^G = \sum_{i=1}^{m} \sum_{j=1}^{k-f(i)} mp_{ji},$$

де mp_{ji} — кількість відмінностей, що існують між парами вибраних фрагментів подібності, які належать до класу j; m —

кількість клонів подібних фрагментів. Для визначення P_O^G вводиться поняття про траєкторію аналізу структури Q_i. Така траєкторія визначає порядок переходу від $\varphi_i(Q_i)$ до $\varphi_j(Q_i)$. Тоді P_O^G означає кількість відмінностей між характеристиками φ_i і φ_j, що вибрані для його опису і стосуються $\varphi_i(Q_i)$ в цілому. Якщо в Q_i для визначення P_S^G сформовано один клас $\varphi_i(Q_i)$, то $P_O^G = 0$. Величина P_O^G визначається з співвідношення:

$$P_0^G = \sum_{i=1}^{m} mv_i ,$$

де mv_i – величина відмінності між парою вибраних класів $\varphi_i(Q_i)$. Параметри P_G^G визначаються відповідно до відомих способів визначення інваріантів графів [98]. Наприклад, для такого інваріанта, як степінь вершини графа, спосіб визначення його величини залежить від визначення самого інваріанта. Стратегія формування Q_i визначається як $M=F(\delta P_i^G, \ldots, \delta P_i^G)$, де δ визначає доступний діапазон значень P_i^G. Для формування Q_i в $W(\rho)$ можна використовувати методи, що відповідають співвідношенню $\rho(x,y) = P_G^q(x,y) = \min\left\{\left[q(W)/W\right] \in W(x,y)\right\}$, де q_i — вагова функція графа G, що визначається глобальними параметрами. Як відомо [99], застосування таких методів призводить до побудови графа $P^P[q] = P[q]$, який однозначно визначається в метриці (x,ρ). Це означає, що в SIM не виникає суперечностей.

Доведемо можливість перетворення однієї форми опису Q_i в іншу. Кожна інформаційна компонента системи LIM, GIM і SIM є однакова, оскільки вона відображає інтерпретацію окремих формальних елементів у предметній області $J(Q_i)$. Тому розглянемо взаємозв'язок між формальними компонентами L, G, S. Кожна з компонент складається з частини, яка використовується для формального опису Q_i та частини, що являє собою правила

перетворень формальних описів. Реалізація перетворень, що стосується двомісних логічних функцій, передбачає проведення аналізу двох змінних, що входять у відповідний вираз. Тому достатньо показати, що при перетворенні в G, яке реалізується в рамках автомата A при реалізації однієї операції також проводиться аналіз двох змінних. В L базовими фрагментами логічних функцій є $y_i = x_i \,\&\, x_j$, $y_i = x_i \vee x_j$, $y_i = x_i \to x_j$ і $y_i = \neg x_i$. В рамках формалізму A значення елемента y_i на кожному кроці перетворень залежить від чергового x_i, що подається на вхід A та від стану автомата q_i, що відповідає моменту подачі на вхід A елемента x_i. Ця ситуація описується функціями $q_i = \lambda(x_i, q_i)$ та $y_i = \lambda(x_i, q_i)$, які входять у визначення A. Оскільки область визначення x_i і x_j для $L \in \{0,1\}$, то область визначення для q_i чи q_j може бути зведена до $\{0,1\}$, оскільки таке зведення являє собою звуження можливої області визначення для q_i чи q_j автомата A. Оскільки справедливе $y_i = x_i \to x_j = x_i \vee \neg x_j$, то цей випадок зводиться до попередніх випадків. Реалізація функції $y_i = \neg x_i$ відповідає випадку, коли $q_i = \lambda(x_i, q_i) = q_i$, що є можливою редукцією станів автомата A, а q_i відповідає інтерпретації, що описується одномісною функцією $\neg$. Зворотне перетворення $G \to L$ можливе при умові редукції функціональних можливостей A_i до системи виводу Σ_i в L, що виконується завдяки тому, що об'єкт Q_i, який описується засобами A_i, може бути представлений в LIM. Між системою виводу Σ_L з L і системою Σ_S з S, якщо S є графом, існує однозначний зв'язок. Для підтвердження цього розглянемо відповідність інтерпретації базових функцій в L з базовими елементами в S. Кожній базовій функції з L відповідатиме певний фрагмент структури з S. При цьому ребра графа V_i будуть відповідати змінним, а вершини фрагмента s_i будуть ідентифіку-

вати логічні функції. Така відповідність між s_i і l_i наведена на рис. 21.

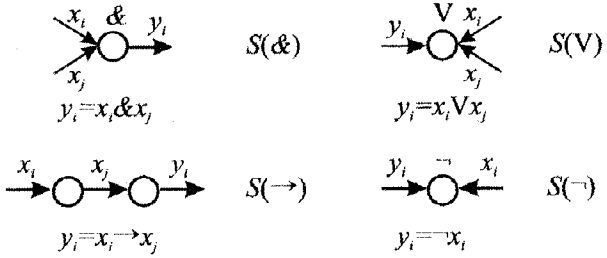


Рис. 21. Структури $s_i \in S$, що відповідають $l_i \in L$

У випадку перетворення $y_i = x_i \to x_j$ у структуру $S(\to)$ використовуються дві вершини, оскільки для відтворення функції $\to$ необхідно застосувати дві функції $\vee$ та $\neg$ або & та $\neg$. Зворотне перетворення є однозначне або виконується $S \to L$, оскільки області інтерпретації для x_i і y_i в L і l_i та V_i для S є еквівалентними.

Відсутність конфліктів між різними представленнями Q_i випливає з несуперечності моделей *LIM*, *GIM* і *SIM* та підтверджується тим, що є можливим перехід від однієї моделі опису до іншої або:

$$\left[Q_i(LIM) \to Q_i(GIM)\right] \& \left[Q_i(LIM) \to Q_i(SIM)\right]$$

і навпаки [100]. З вищевикладеного випливає, що здійснення таких переходів призводить лише до звуження допустимих функціональних можливостей в окремих моделях [101].

Реалізація методів контролю документів із стеганографічними методами захисту

Обмежимося ситуацією, коли латентний фрагмент засобу захисту формується шляхом недодруковування. Для здійснення контролю або ідентифікації документа на його оригінальність необхідно здійснити такі дії:

— перевірити інтегральні параметри графічного засобу захисту, якщо він має абстрактну інтерпретацію типу $J^S(Q_i)$;

— визначити місце розміщення латентних фрагментів $\varphi''(Q_i)$ в межах Q_i та їх типи;

— відновити латентні фрагменти та перевірити їх ідентичність до латентних фрагментів оригінального образу;

— на основі проведених перевірок встановити міру захищеності документа та її відповідність до рівня захисту встановленого для даного документа.

Інтегральні параметри графічного образу суттєво залежать від типу образу, наприклад, параметри, що характеризують спосіб застосування кольорів у площині образу, основні осі симетрії, частину покриття окремих фрагментів поверхні документа тощо.

Задача знаходження латентного фрагмента є необхідною складовою проблеми використання латентних образів, оскільки виявлення їх місця розміщення на основі аналізу тільки видимої частини є нерозв'язною [102]. Розв'язок цієї задачі грунтується на даних, що передбачають різну складність розв'язку, а саме:

— на основі використання ключа, який містить таємну інформацію, що може передаватись уповноваженим користувачам незалежно від захищеного документа;

— прихованих ключів, скритих у фрагментах Q_i, які являють собою графічний засіб захисту (zz);

— на основі використання інформації про способи побудови Q_i в цілому та про способи формування в його середовищі латентних фрагментів.

Використання ключів з метою виявлення розміщення патентних фрагментів є типовим для стеганографічних систем, особливо, коли йдеться про застосування графічного середовища. Ключі, приховані безпосередньо в графічному середовищі, зазвичай, використовують для укриття методи маскування, які найефективніші, якщо як Q_i застосовуються образи, що мають сюжетну інтер-

претацію або $I(Q) = J^S(Q_i)$. Це обумовлюється тим, що наявність сюжету призводить до концентрації інтерпретації в окремих фрагментах образу, залишаючи інші фрагменти графічно надмірними [103]. Ключі, пов'язані з відображенням інформації про способи формування латентних фрагментів, дозволяють в рамках вибраної для даного Q_i системи виводу відтворити процес формування видимої частини фрагментів φ_i, що безпосередньо пов'язана з невидимою частиною. Очевидно, що в цьому випадку в рамках образу Q_i повинні бути виділені точки у видимій частині Q_i, з яких необхідно починати процес формування $\varphi_i^v \to \varphi_j^n$, що визначається певним ключем.

Для того щоб можна було конструктивно використовувати інтегральні характеристики необхідно розв'язати такі задачі:

— визначення інтегральних характеристик в межах поля відображення образу Q_i;

— визначення способів або механізмів визначення величини значень відповідних характеристик;

— розпізнавання інтегральних параметрів відповідного документа, оскільки у документів з різними типами абстрактних Q_i такі характеристики можуть бути різними;

— визначення точності виміряних або обчислюваних значень інтегральних параметрів.

Задача локалізації фрагментів, для яких необхідне визначення інтегральних параметрів, може розв'язуватися на основі таких методів:

— визначення координат фрагмента Q_i, для якого обчислюється відповідний параметр;

— сканування необхідних фрагментів образу;

— адаптивний пошук фрагмента за очікуваними значеннями інтегрального параметра.

Метод визначення координат передбачає необхідність введення системи координат для площини [104], в якій розміщується графічний

засіб захисту. Така система координат може застосовуватися явним або не явним чином. У першому випадку система координат повинна наноситися на документ друкарським методом, що дозволяє її ідентифікувати при проведенні контролю документа. При цьому масштаб не мусить задаватися явним чином. Очевидно, що така система координат має відповідати геометрії всього документа чи геометрії тих його частин, на яких розміщуються засоби захисту. В більшості випадків така система координат є прямокутною. В другому випадку система координат разом з відповідним масштабом формується в рамках засобів контролю. Тоді в межах поля документа повинні розміщуватися точки позиціонування документа для здійснення контролю. Очевидно, що позиціонування документа може здійснюватися відповідно до конструкції на основі використання його базових конструктивних параметрів, що здебільшого здійснюється при перевірці документів з застосуванням машинозчитувальних методів.

Окрім визначення системи координат, в межах графічного засобу чи в засобах захисту, що орієнтовані на певний вид документа, повинні задаватися координати базових точок розміщення фрагментів, в межах яких необхідно вимірювати інтегральні параметри. Такі координати не мають являти собою метричні одиниці виміру на площині документа. Вони можуть визначати координати розміщення тих чи інших фрагментів через різні значення параметрів, що характеризують відповідні фрагменти [105]. В цьому випадку масштабна сітка має бути багатомірною і не прив'язаною до геометрії площини, на якій розміщується графічний образ. Наприклад, якщо інтегральний параметр P_i являє собою густину ліній у певному фрагменті Q_i, то у точках координатних ліній, які є прямокутними проекціями вибраних точок відповідного фрагмента, записуються значення цього параметра. Оскільки параметри Q_i в площині рисунка не передбачають впорядкованості, то відповідні значення вибраних точок фрагмента, що розміщуються на осях координат, відносно осей координат не будуть впорядкованими за величиною. Завзвичай, такого типу масштабування реалізується неявним чином щодо образу документа, і формується в межах засобів контролю. Очевидно, що для

різних параметрів необхідно формувати окремі масштабні поділи системи координат. Це пов'язано з тим, що для різних параметрів, які стосуються одного фрагмента образу, точка зведення може збігатися на площині, що призведе до необхідності суміщення відповідних точок поділу осей координат.

Метод сканування образу з ціллю виявлення або локалізації відповідних фрагментів може бути реалізований тільки в рамках засобів контрою або методів контролю документів, що залежить від їх функціональних можливостей. Техніка сканування графічних образів на сьогодні досить поширена і добре розвинена, тому її використання в процесах контролю документів не є проблематичне. Алгоритми аналізу результатів сканування можуть бути орієнтовані на обчисленнях окремих параметрів засобу захисту. Процес сканування може прив'язуватися до базових ознак, що характеризують геометрію документа, що дозволяє по заданому приблизному значенню параметра визначити геометричні чи метричні координати відповідного $\varphi_i(Q_i)$ на площині документа.

Метод адаптивного пошуку необхідного фрагмента документа складається з таких частин:

— визначення початкової дислокації фрагментів засобів захисту на площині розміщення образу Q_i в документі d_i;

— вимірювання параметра в початковому наближенні точності вимірювань;

— адаптаційної модифікації траєкторії пошуку необхідного фрагмента образу.

Для реалізації процесу визначення початкової локалізації фрагмента, параметри якого необхідно вимірювати, використовується алгоритм грубого сканування AGS, який полягає в наступному:

1. Вибирається діапазон значення параметра P_i фрагмента φ_i, в якому змінюється його величина. Цей діапазон визначає φ_i як окремий фрагмент Q_i. При цьому вибраний P_i є характерним для φ_i. Це означає, що за P_i визначається факт існування φ_i в Q_i заданого типу.

2. Починаючи з базової точки документа, AGS здійснює згідно з визначеною траєкторією реалізацію сканування графічного образу, яка полягає у наступному. На заданому відрізку траєкторії, наприклад, зчитується кількість ліній, які перетинає пристрій протягом прийнятої одиниці траєкторії, якщо як P_i прийнято густину рисунка або його насиченість. Якщо P_i попадає в діапазон $\left[\alpha(P_i), \beta(P_i)\right]$, то вважається, що початкова точка φ_i визначена.
3. Виходячи з початкової точки, відповідно до локальної траєкторії сканування визначається область всього φ_i. Для цього використовується перевірка P_i на відповідність цих значень заданому діапазону. Якщо виявиться, що на наступних кроках локального сканування фрагмент φ_i відсутній, що встановлюється шляхом попадання поточного значення P_i в $\left[\alpha(P_i), \beta(P_i)\right]$, то виявлення φ_i завершено.
4. Локальна траєкторія сканування φ_i є неперервною в базовій системі координат документа і, незалежно від вибраного способу масштабування, дає можливість визначити місце знаходження φ_i в рамках системи координат з впорядкованим масштабом. Завдяки цьому після завершення процесу сканування на цьому кроці алгоритм AGS формує координати виявленого фрагмента та його границі в межах площини документа.

Після завершення роботи алгоритму AGS необхідно провести більш детальний аналіз φ_i з ціллю виявлення в ньому латентних частин або фрагментів φ_i''. Для розв'язання цієї задачі використовуються такі підходи:

— для визначення початкової точки латентного фрагмента застосовується алгоритм обчислення локальних параметрів, що характеризують відповідний фрагмент і на основі проведеного аналізу визначається:

а) факт наявності φ_i^n в φ_i;

б) локалізація φ_i^N в φ_i з точністю, яка необхідна для відтворювання в явному вигляді φ_i^N;

в) міра адекватності виявленого φ_i^N реальному або еталонному фрагменту φ_i^N;

— для визначення початкової точки розміщення φ^N використовується стеганографічний ключ, що може вміщувати різну кількість інформації, необхідну для явного відтворення φ_i^N;

— для відтворення φ_i^N застосовується метод адаптаційного формування φ_i^N, в якому на кожному кроці формування чергового наближення φ_i^N до φ_i^{NE} можна формувати такий φ_i^{NJ}, який буде наближатися до φ^{NE}.

Оскільки φ_i^{NE} в φ_i є розподіленим, то в рамках системи впровадження φ_i^N в φ_i існує відповідний підавтомат, який однозначно описує спосіб побудови φ_i^N. Початковий стан такого автомата та його перший вхідний символ відповідає початковій точці фрагмента φ_i^N. Згідно з твердженням 2.1 для відповідного автомата існує максимально допустимий розмір вхідного слова, яке може бути ним розпізнане або, відповідно, сформоване вихідне слово обмеженої довжини. Це означає, що для кожного окремого φ_i^N повинен існувати власний підавтомат, що описує процес формування відповідного φ_i^N.

При формуванні розподілених φ_i^N встановлюється безпосередній зв'язок між індексацією окремих символів та координатами вершин окремих геометричних примітивів x_i, що використовуються для побудови Q_i. Така відповідність визначається окремою системою правил виводу заданого способу позиціонування φ_i^N в середовищі φ_i. Таким чином, при реалізації першого способу виявлення φ_i^N в Q_i засоби, що реалізують відповідні процеси в тій чи інший організації

контролю документів, являтимуть собою досить складні алгоритми виявлення φ_i^N. Також до недоліків вказаного методу виявлення φ_i^N можна віднести те, що алгоритми виявлення φ_i^N досить точно відображають алгоритми формування φ_i^N, що є суттєвим фактором, який впливає на забезпечення стійкості засобів захисту від підробок.

При використанні стеганографічних ключів для легального розпізнавання в φ_i фрагментів φ_i^N в рамках засобів контролю можна реалізувати лише фрагменти автоматів розпізнавання φ_i^N, а початкові точки відповідних підфрагментів φ_i^N задаються значеннями їх координат в базовій системі координат документа. В цьому випадку виникає проблема передачі ключа, що відповідає окремому індивідуальному документу d_i. Цю проблему можна оминути шляхом створення системи виводу чергових вхідних даних для підавтомата Q_i, що розрізняє підфрагмент $f_i^N \in \varphi_i^N$. Таким чином можна розділити інформацію про алгоритм формування Q_i і, відповідно, φ_i^N на окремі фрагменти, за якими його відтворення виявляється складною задачею. При застосуванні такого підходу існує можливість зменшити кількість даних, які необхідно передавати разом з ключем.

У рамках вищенаведеного підходу при використанні ключів їх передача для кожного окремого документа розв'язується такими способами:

— ключ, що передається разом з відповідним документом у вигляді певної сукупності цифр, шифрується за допомогою вибраних криптографічних шифрів [106, 107]. Тоді криптографічний ключ є універсальним для цілого ряду документів, а спосіб його передачі може реалізуватися методами розподілу криптографічних ключів, для реалізації яких використовуються відповідні системи сертифікації криптоключів [108, 109];

— ключ передається відкритим способом в межах відповідного документа у вигляді штрих-кодів чи відповідних чисел, що описують координати фрагментів φ_i^N, $f_i^N \in \varphi_i^N$;

— стеганографічний ключ може розміщуватися в середовищі Q_i чи φ_i за допомогою маскування. В цьому випадку розміри ключа обмежуються можливостями графічного середовища відповідно до образу Q_i;

— стеганоключ, що являє собою певну послідовність цифр, які також ідентифікують документ за його серійним номером, в зашифрованій або відкритій формі може передаватися до систем контролю на основі використання систем розподілу ключів;

— завдяки тому, що стеганоключі можуть являти собою комбіновані способи опису даних, необхідних для виявлення φ_i^N, то вони можуть складатися з частин, які є сталими для певного класу документів. Наприклад, алгоритми формування окремих підфрагментів $f_i^N \in \varphi_i^N$ та частин, що є змінними для кожного екземпляра документів або координати розміщення початкових точок окремих фрагментів φ_i^N чи їх підфрагментів f_i^N.

Оскільки образи Q_i являють собою відповідні абстракції з $J^A(Q_i)$, а різні документи повинні забезпечувати певні рівні захисту, то точність виявлення в Q_i може бути різною. Зрозуміло, що документи, які забезпечують різні рівні захисту, можуть обслуговуватися різними за складністю методами контролю. Оскільки методи контролю документів, що застосовують стеганографічні методи захисту, не є методами порогового типу або такими, що ґрунтуються на використанні еталонів, то в них можуть виникнути фактори, що призводять до досягнення різного рівня точності розпізнавання ідентичності документа. Таким чином рівень захисту для певного документа визначає методику контролю, яка повинна застосовуватися в кожному окремому випадку. Тому методика контролю може розглядатися як параметр, що додатково характеризує документ. Оскільки ця інформація залежить від фрагмента технологічного процесу, який захищає певний документ, то вона не може містити таємницю високого рівня [110]. Тому виникає задача

визначення відповідності рівня захищеності документа не тільки методиці, що використовується для його контролю, але й до отриманих результатів контролю і методу його реалізації. Загальна блок-схема реалізації процесу контролю документа наведена на рисунку 22.

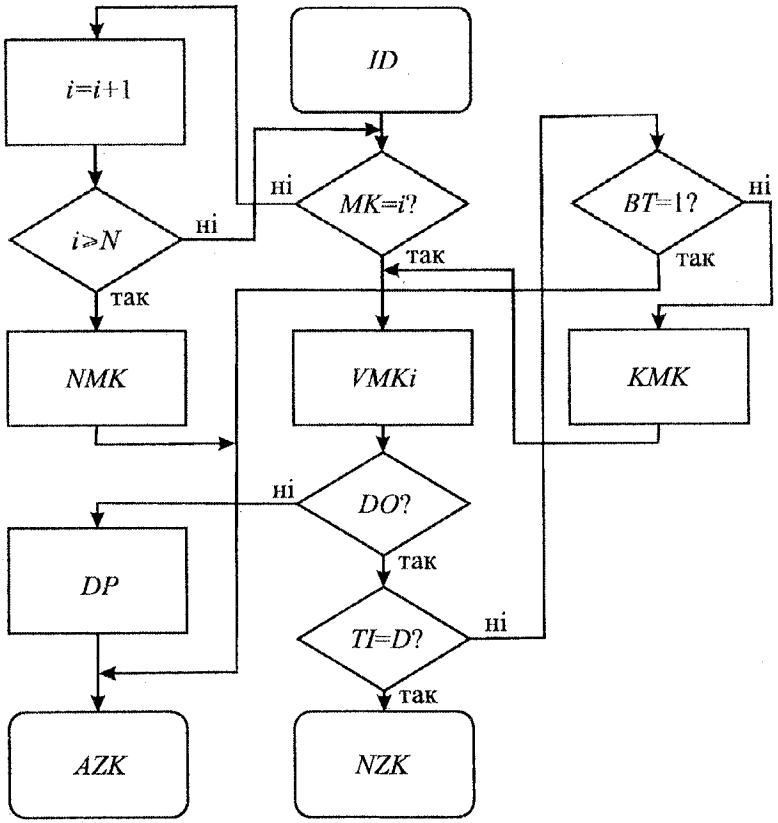


Рис. 22. Блок-схема реалізації процесу контролю документів

На рис. 22 прийнято такі скорочення:

ID — ідентифікація документа;

MK_i — реалізація вибраної методики;

DO — перевірка оригінальності документа;

TI = MKD — перевірка точності ідентифікації документа;

NZK — нормальне завершення контролю;
BTI — перевірка наявності ознаки модифікації;
KMK — корекція методики контролю;
$I \geq N$ — перевірка вибору всіх методик;
NMK — необхідна методика контролю відсутня;
DP — документ підроблений;
AZK — аварійне завершення контролю.

Загальна організація системи захисту технологічних процесів на основі використання документів

У рамках системи захисту документів (SK) відповідно до прийнятих визначень інтегрального параметра невидимості елементів засобів захисту (zz), він характеризує міру збіжності стратегії контролю документа $G(SK)$ зі стратегією реалізації атаки $G(NU)$. Це зумовлюється тим, що базовими елементами захисту є елементи, що формуються в документі d невидимим способом, а атака являє собою таку підробку zz, яка б в рамках використовуваної $G(SK)$ виявилась невидимою. Оскільки стратегія контролю може змінюватися залежно від ситуації, що пов'язана з реалізацією технологічного процесу TP, а стратегія реалізації атаки змінюється залежно від TP, то загальну організацію використання документів при реалізації TP можна подати у вигляді деякої моделі гри. Оскільки реалізація стратегій $G(SK)$ і $G(NU)$ може описуватися у вигляді логічних формул $L(x_1,...x_n)$ і $M(x_1,...x_m)$, відповідно, а ціль гри — у вигляді функції, що максимізує різницю між L_i і M_i, то функція цілі може бути описана у вигляді виводу M_i з L_i, довжина якого має бути мінімізована [111, 112]. Можливість існування різних стратегій $G(SK)$ зумовлена тим, що TP захищається не одним, а сукупністю документів. Не розпізнавання атаки в рамках документів може призводити до різних втрат. Якщо величина втрат нижча від вартості виготов-

лення засобів захисту документів, які б відповідні втрати могли виявити, то стратегія $G(SK)$ може допускати такий стан справ у процесі захисту TP, принаймні протягом певного періоду реалізації TP. Теоретично можливо уявити собі ситуацію, коли TP може не потребувати взагалі ніяких засобів захисту у вигляді документів, якщо з якоїсь причини втрати при його реалізації чи реалізації його фрагментів є принципово неможливими. Такі причини можуть обумовлювати фізичні, природні чи технічні фактори. Наприклад, якщо існує деяка повністю автоматизована технологічна лінія, що реалізує вищевказаний TP, то фрагменти такого процесу не потребують системи захисту, що реалізується за допомогою документів.

Для формального опису загальної організації системи захисту, що ґрунтується на використанні документів, застосовується модель гри, функція вартості якої описується системою логічних формул, L_i і M_i, що в кожному окремому випадку відображають значення їх змінних, у вигляді стратегії реалізації процесів контролю документів TP.

Оскільки в наведеній грі кількість стратегій реалізацій одного ходу може бути нескінченою, то відповідна гра є нескінченною. Нескінченність практично полягає в тому, що вартість реалізації підробки засобів захисту в межах одного документа і, відповідно, в межах усіх документів, що використовуються для захисту TP, є достатньо великою.

Стратегія $G(NU)$ описується логічними формулами M_i, і M_i^P, де M_i^P — повна стратегія атаки документа, а M_i — наближена стратегія атаки документа. Формально це описується як:

$$M^P = L_i\left[m_1\left(x_{11},...x_{1p}\right),...,m_k\left(x_{k1},...,x_{kr}\right)\right]$$

$$M_i = L_j\left[m_1\left(x_{11},...,\overline{\overline{Y}}_{si},...,\overline{\overline{Y}}_{1i},...,x_{1r}\right),...,m_k\left(x_{k1},...,\overline{\overline{Y}}_{ki},...,\overline{\overline{Y}}_{kr},...,\overline{\overline{X}}_{kr}\right)\right],$$

де $\left[\left(x_{ij}\right) > \overline{\alpha}\left(x_{ij}\right) \to \left(x_{ij} = 0\right)\right] \vee \left[\left[x_{ij} \le \overline{\alpha}\left(x_{ij}\right)\right] \to \left(x_{ij} \le 1\right)\right]$; $\overline{\alpha}\left(x_{ij}\right)$ — порогове значення параметра $P\left(x_{ij}\right)$, з точки зору zz оригінального

документа d в GD_i; $\overline{\overline{Y}}_{ij}$ — визначається аналогічними співвідношенням, за винятком того, що величина порогу визначається виразом $\alpha^*(x_{ij})+\delta^*(x_{ij})$, де $\delta^*(x_{ij})$ — певне відхилення значення $P^*(x_{ij})$ засобу zz у більшу сторону. Тому співвідношення можна записати у вигляді $Y_{ij}=f_i(x_{ij})$, де f_i — лінійна функція. В загальному випадку f_i — довільна функція.

Стратегія $G(SK)$ описується аналогічно до стратегії $G(NU)$:

$$L^P = L\left[l_1(x_{11},...,x_{1r}),...,l_k(x_{k1},...,x_{kr})\right]$$

$$L_i = L\left[l_1\left(x_{11},...,\overline{\overline{Y}}_{1i},...,\overline{\overline{Y}}_{1r},...,x_{1r}\right),...,l_k\left(x_{k1},...,\overline{\overline{Y}}_{ki},...,\overline{\overline{Y}}_{kr},...,x_{kr}\right)\right].$$

Очевидно, що у випадку використання різних стратегій двома гравцями при реалізації одного ходу кожним можливі ситуації, що описуються співвідношеннями:

$$\left[\left[\left(G(SK)=L^P\right)\vee\left(G(SK)=L\right)\right]\&\left[G(NU)=M^P\right]\right]\rightarrow$$
$$\rightarrow\left[V(NU)=1\right],$$

$$\left[\begin{array}{l}\left(G(SK)=L\right)\&\left(G(NU)=M\right)\&\\ \left(\delta^M\left(\overline{\overline{X}}_{ij}\right)<\delta^L\left(\overline{\overline{X}}_{ij}\right)\right)\vee\left(G(NU)=M^P\right)\end{array}\right]\rightarrow\left[V(NU)=1\right],$$

$$\left[\begin{array}{l}\left(G(SK)=L\right)\&\left(G(NU)=M\right)\&\\ \&\left(\delta^M\left(\overline{\overline{X}}_{ij}\right)\right)>\left(\delta^L\left(\overline{\overline{X}}_{ij}\right)\right)\vee\left[\left(G(NU)=L^P\right)\right]\end{array}\right]\rightarrow\left[V(NU)=0\right].$$

З наведених співвідношень випливає, що виграш в результаті атаки на документ можна ідентифікувати множиною $\{0,1\}$, оскільки його досягнуто або не досягнуто гравцем NU. В цьому випадку гравець SK отримує програш, який для зручності називатимемо $V(SK)=0$. Якщо $V(NU)=0$, то будемо записувати, що $V(SK)=1$. Гра між NU і SK триває протягом багаторазового використання TP.

Кожний окремий TP відповідає одному кроку реалізації гри. В цьому випадку гру можна віднести до класу антагоністичних нескінченних ігор, в яких кожен крок гри може реалізуватися на основі даних про стратегії в попередніх кроках [113].

Приймемо, що $\Gamma(SK, NU)$ може складатися з довільної кількості кроків, а модифікація стратегії SK полягає у виборі стратегій на кожному кроці гри, що в різній мірі може наближатися до нової стратегії контролю чи віддалятися від неї. Це обумовлюється тим, що міра наближення L_i до L^P призводить до збільшення ціни реалізації стратегії і, крім цілі гри, що полягає у виграші на кожному кроці гри, стратегія повинна вибиратися таким чином, щоб вартість її реалізації була мінімальною при забезпеченні виграшу на відповідному кроці. Для цього встановимо фактори, що визначають вартість реалізації окремої стратегії. Приймемо, що змінні, які будуть ідентифікувати відповідні фактори, будуть використовуватися у випадку аналізу та опису окремої стратегії $G(NU)$. Оскільки фактори будуть ті ж самі і лише їхній вплив на результат гри, на окремому ході буде протилежний, то до них можна віднести:

— повноту контролю zz, що використовуються в d_i;

— точність вимірювання окремих величин параметрів;

— логічну структуру процесу контролю документів.

Повнота контролю документів відображається при формальному описі стратегій кількістю змінних, що ідентифікують параметри zz і, відповідно, використовуються в логічних формулах L_i, що описують окремі стратегії. Точність вимірювання величини окремих параметрів описується величиною збільшення порогу допустимого відхилення, що позначається як $\delta(x_{ij})$. Логічна структура процесу контролю описується логічною структурою формули L_i та формулами $m_i l_i$ [114].

Оскільки в цій роботі розробляються стеганографічні методи захисту, то вищевказані фактори необхідно більш точно наблизити

до невидимих фрагментів $\varphi_i U$ образу Q_i. Оскільки $\varphi_i U$ формується у вигляді недодрукування в межах Q_i, то повнота контролю означає виявлення всіх геометричних примітивів чи частин, з яких складаються фрагменти $\varphi_i U$ в процесі реалізації контролю у відповідності $G(SK) = L_i$. Точність вимірювання величини окремих параметрів відповідає точності відтворення геометричного положення або орієнтації окремих геометричних примітивів, з яких складаються фрагменти $\varphi_i U$. В цьому випадку одиницею виміру $\delta(x_{ij})$ є кількість x_{ij}, орієнтація чи локалізація яких не відповідає $\varphi_i U$. Тому одиниці вимірювання повноти та точності контролю x_{ij} збігаються. Логічна структура процесу контролю документів також суттєво впливає на результат контролю. Образ Q_i, що відіграє роль графічного засобу захисту, має певну вибрану структуру, якій підпорядковується процес побудови zz та його скритих фрагментів. Відповідно до цієї структури формуються параметри zz. Вони не можуть суттєво відрізнятися від цієї структури, оскільки $\varphi_i U$ формуються шляхом недодруковування елементів Q_i. Якщо залежність $\varphi_i U$ і, відповідно, параметрів x_{ij} засобів zz від структури Q_i буде недостатньою, то в процесі контролю $\varphi_i U$ буде неможливо однозначно відновити, що призведе до дискредитації відповідного zz.

Процедура, що реалізується SK і описується співвідношенням L_i, виводиться з структури Q_i і значною мірою є апроксимуючою функцією відповідної структури. Це відображає глобальну роль впливу L_i на результат контролю d_i. Логічна функція L_i відіграє і локальну роль впливу на аналіз zz. Оскільки x_{ij} з L_i безпосередньо ідентифікують параметри геометричних елементів та компонент φ_i^N, то послідовність їх перевірки та взаємозв'язок між їхніми значеннями, що описується в L_i, безпосередньо впливає на результат аналізу. Наприклад, нехай x_{ij} характеризує кількість виявлених

компонентів в φ_i^N, або повноту φ_i^N, тоді $x_{i(j+1)}$ може характеризувати точність вимірювання φ_i^N. Оскільки повнота x_{ij} встановлює повноту контролю, то $x_{i(j+1)}$ залежить від x_{ij} і орієнтація елементів в φ_i^N може аналізуватися або досліджуватися лише у випадку виявлення відповідної компоненти в режимі порівняння з орієнтацією тієї ж компоненти, сформованої згідно з оригінальним алгоритмом формування φ_i^N в складі Q_i у видимій формі. Оскільки формула L_i для окремої стратегії $G(SK)$ являє собою таємницю в системі захисту, то вона є недоступною для NU, а особливо її повна формула L_i^P. Згідно з наведеним визначенням η, що описує особливості використання інтерпретації відповідного параметра невидимості скритих фрагментів, невидимість являє собою міру здатності NU відтворити $Q_i = \Sigma\varphi_i^W + \Sigma\varphi_i^N$ таким чином, щоб $Q_i^F \to Q_i^E$. Вона проявляється шляхом наближення $M_i \to L_i$. Оскільки L_i в $G(SK)$ може реалізуватися з різною мірою наближення до L_i^P, то зміна такого наближення призводить до зміни величини видимості η. Оскільки η актуальний лише в процесі його використання NU, то $\eta = F_M[L_i - M_i]$, або: $\eta^* = F_L[L^P - L_i]$. Приймемо, що функція $F_L = \Delta[L^P \to L_i]$, де Δ – довжина виводу L_i з L^P. В цьому випадку $\eta^* = h$, де h – ціле число, рівне крокам виводу L_i з L^P. Якщо справедлива рівність $M_i = L_i$, то можна це інтерпретувати як видимість скритих $\varphi^n \in Q_i$, тому що NU може їх викрити. При цьому, якщо $L_i = L^P$, то видимість обмежується можливостями L_i. Отже, якщо $L_i \to L^P$, а $M_i = const$, то видимість η зростає, а якщо $L_i \to M_i$, то невидимість $\varphi_i U$ знижується і $\eta = 0$, коли $L_i = M_i$. Таким чином, η не означає фізичної невидимості $\varphi_i U$, а здатність NU сформувати таку M_i наближену до L_i. Очевидно, що може виникнути

ситуація, коли $M_i = 0$. Тоді атака на d_i не здійснювалась. Оскільки реалізація L_i в SK потребує затрат, то при $M_i = 0$ досить, щоб $(L_i = \min) \vee (L_i = 0)$ і тільки при $M_i \to L_i$ необхідно, щоб $\Delta^* = F[L_i \to M_i]$ була завжди мінімальною. Тоді величина затрат на L_i буде мінімально необхідною для того, щоб $V(NU) = 0$. Очевидно, що на кожному кроці реалізації гри $\Gamma(SK, NU)$ зі сторони NU здійснюється модифікація M_i так, щоб $M_i \to L_i$. Тому можна стверджувати, що до змін величин η_i призводить модифікація L_i.

Отже, загальна організація системи захисту TP, що базується на застосуванні стеганографічних методів та засобах захисту, ґрунтуватиметься на моделі з теорії ігор. Така організація передбачає використання дворівневої моделі [115]. На першому рівні застосовується модель гри, в якій формуються чергові стратегії з ціллю їх використання на етапі обслуговування одного циклу функціонування TP. Цей цикл визначається початком та завершенням його функціонування. Модель гри на цьому етапі являє собою антагоністичну однокрокову гру. Завершення кроку збігається з завершенням окремого TP, після чого визначається виграш кожного з учасників. На основі даних, отриманих після завершення TP, та даних про умови протікання та завершення попередніх TP, формується стратегія чергового кроку гри [116]. На другому рівні організації системи захисту TP використовується модель в рамках якої здійснюється аналіз процесу захисту TP в межах одного циклу функціонування TP. Процедура контролю, яка виконується відповідно до стратегії $G_i(SK) = M_i$, супроводжується формуванням можливої стратегії реалізації атаки $G_i(SK) = M_i$. При перевірці кожного з параметрів x_{ij} з L_i відповідно до логіки, що описується в $L_i = L(l_1, ..., l_k)$, формується $M_i = L(m_s, ..., m_k)$ таким чином:

1. Якщо при перевірці параметра x_{ij} не виявлено відхилення від умов, що описуються в рамках L_i і в описі її інтерпретації, то в формулу M_i вноситься фрагмент, що вміщує x_{ij} з L_i в такому ж вигляді і з таким значенням відповідної змінної в описі її інтерпретації.
2. Якщо при перевірці x_{ij} у zz документа відповідно до фрагмента з L_i виявились відхилення величини параметра від його опису, що розміщений в інтерпретації x_{ij}, то в M_i у відповідне місце вноситься змінна x_{ij}^* з інтерпретацією, що відображає відповідну відмінність $x_{ij} \in L_i$ і $x_{ij}^* \in M_i$.
3. Якщо при перевірці zz з d_i виявляється на деякому кроці, що параметр x_{ij} з L_i в d_i відсутній, то фрагмент, що вміщує x_{ij} в M_i, не переноситься, а M_i на подальших кроках перевірки формується таким чином, щоб не допускати синтаксичних помилок у фрагменті $M_i = L(m_s,...,m_k)$.
4. Якщо виконуються випадки п. 2 і 3, то в SK фіксується факт виявлення атаки на відповідні документи $d_i \in D_i$ на TP_i в цілому, і процес TP переривається як такий, що не може завершитися успішно, але процес перевірки d_i продовжується.
5. Якщо випадки п. 2 і 3 не виконуються, то при завершенні TP він перевіряється системою SK, чи отримані результати процесу функціонування TP відповідають його цілі, що сформована замовником TP.
6. Якщо ціль $C_i(TP) = C_i(SK,TP)$, то процес TP вважається не атакованим, і цей факт фіксується в SK і, відповідно, документи $d_i \in D_i$ не атаковані.
7. Якщо $C_i(TP) \neq C_i(SK,TP)$, то процес TP і відповідні документи вважаються успішно атакованими.

8. Процеси перевірки $d_i \in D_i$, на рівні моделі функціонування якої описано в п. 1, 2, 3, 4, 5, 6 і 7, завершуються, і управління передається в модель гри.

На основі даних, отриманих на моделі другого рівня, відповідно до алгоритму реалізації моделі гри [117] формується нова стратегія $G_j(SK)$, для якої виконується умова:

$$\left|L^P - L_j\right| < \left|L^P - L_i\right|,$$

або умова типу:

$$\left|L^P - L_j\right| = \Delta + \left|L^P - L_j\right|,$$

де Δ — визначає величину підвищення рівня безпеки $d_i \in D_i$, що обслуговують TP [118]. Формально відповідна модель гри описується у вигляді функції:

$$\Gamma\left[SK, NU, M(SK), M(NU)\right],$$

де $M(SK)$ і $M(NU)$ виграші SK і NU, відповідно.

Блок-схема загальної організації системи захисту TP за допомогою $d_i \in D_i$ наведена на рис. 23.

Скорочення, прийняті на рис. 23:

ITP — ініціалізація TP;

PU — початкова установка ознак;

VSL_1 — вибір поточної стратегії контролю документів;

PNS — перевірка, чи параметри, що підлягають контролю у вибраній стратегії, не вичерпані;

PSU — перевірка чергового параметра системи захисту документів на його відповідність оригінальному значенню;

VPL — вибір чергового параметра системи захисту;

VPM — формування чергового фрагмента $G(NU)$, що відповідає параметру, який контролюється;

FMA — формування фрагмента $G(NU)$ при виявленні атаки на документ;

TPT — установка ознаки наявності атаки на документ;

C_i — ціль *TP*, визначена споживачем *TP*;

C_i^* — ціль *TP*, досягнута після завершення *TP*;

FNSG — формування наступної стратегії моделі гри при успішному завершенні *TP*;

UZTP — успішне завершення *TP*;

FSGA — формування чергової стратегії в моделі гри при виявленні атаки чи успішно проведеній атаці;

NZTP — неуспішне завершення *TP*.

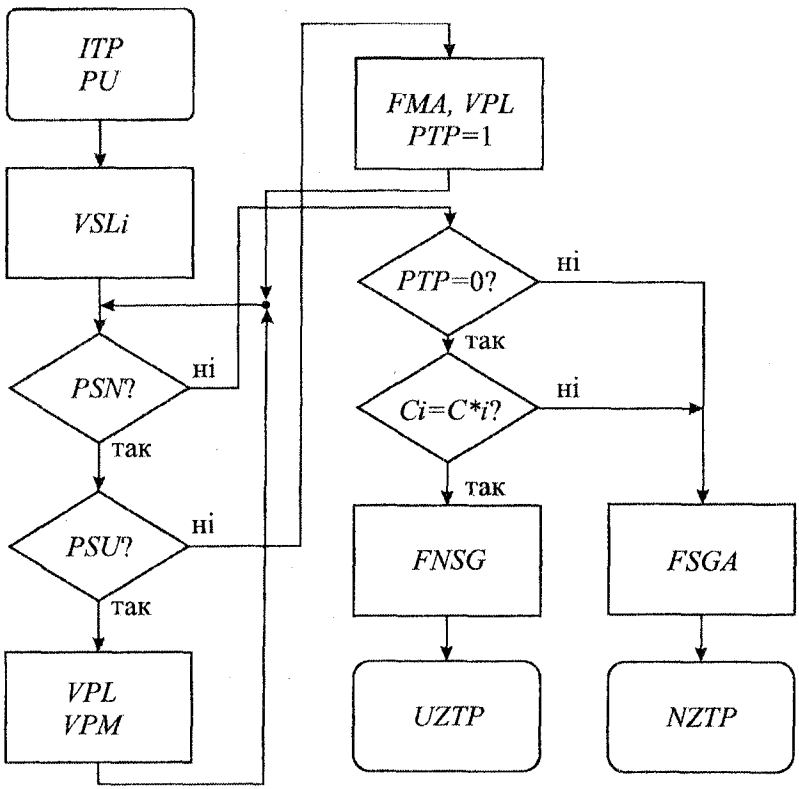


Рис. 23. Блок-схема загальної організації системи захисту *TP* і контролю документів

ВИСНОВКИ

У монографії розв'язано актуальну науково-прикладну задачу розробки математичних моделей графічних засобів захисту документів, що дало змогу дослідити графічні засоби, які забезпечують різний рівень захисту, та сформувати модель системи захисту, що описує процес контролю документів при їх використанні в технологічних процесах. При цьому отримано такі основні результати.

На основі аналізу сучасних засобів захисту документів та цінних паперів показано, що найперспективнішими щодо практичної реалізації графічних засобів захисту є інформаційні технології, що дозволяють створити засоби захисту, які відповідають вимогам реальних технологічних процесів, що використовують документи з відповідними засобами, які визначають необхідний рівень захисту, допустиму вартість відповідних засобів захисту та засобів контролю документів.

Уперше розроблено моделі графічних засобів захисту, які описуються засобами формальних граматик, що дозволяє дослідити можливості формування засобів захисту на рівні безпосередньої апроксимації графічних образів відповідними графічними структурами, завдяки чому стало можливим розв'язати задачу формування та коректного відновлення скритих фрагментів графічних засобів захисту.

Запропоновано та обґрунтовано математичні моделі графічних засобів захисту, що являють собою абстрактні образи із застосуванням принципів стеганографії для реалізації необхідних рівнів захисту, які визначаються параметрами алгоритмів відновлення прихованих фрагментів графічних образів.

Уперше розроблено методи синтезу моделей засобів захисту з інформаційними компонентами, що використовують моделі теорії гри, в якій описується взаємодія засобів захисту документів, що реалізується системою контролю документів з атаками, що здійснюються неуповноваженими учасниками технологічного процесу.

Запропоновано спосіб використання методів стеганографії для забезпечення графічних засобів захисту ознаками, що надають їм захисні властивості, які визначаються ключовим параметром, що являє собою міру невидимості окремих фрагментів засобів захисту і дозволяє змінювати їх значення при повторному виготовленні окремих екземплярів документів залежно від реальної небезпеки, що виникає стосовно відповідного технологічного процесу.

Розроблено алгоритми побудови графічних засобів захисту із можливістю визначення рівня захисту завдяки застосуванню інформаційної технології, яка включає не тільки математичні моделі різних рівнів опису графічних засобів захисту, а й інформаційні компоненти та процеси використання документів з відповідними засобами захисту в технологічних процесах.

Розроблено методи організації системи контролю документів у рамках ігрової моделі, що описує використання документів у технологічних процесах, засоби контролю та аналізу реального рівня небезпеки для технологічних процесів і відповідних документів, який визначається на основі обчислень виявлених атак, успішних атак та загальної кількості повних циклів використання документів технологічними процесами.

CONCLUSIONS

The monograph solved urgent scientific applied task of mathematical models development of graphic means of documents protection with the help of which it became possible to investigate graphical means that provide different level of protection, and to form the model of protection system that describes the process of document control while their use in the industrial processes. Thus, we got the following basic results.

Based on the analysis of modern methods of documents and securities protection had been shown that the most promising as to the practical implementation of the graphic protection means are information technologies that can create means of protection that meet the requirements of real technological processes were the documents with the appropriate means are used, that determine the necessary level of protection, allowable costs of the appropriate protection means and means of documents control.

For the first time had been developed the models of graphic protection means described by means of formal grammars what allows to investigate the possibility of forming the protection means directly on the level of graphic images approximation by the relevant graphic structures, so that it became possible to solve the problem of formation and correct renewal of the hidden fragments of graphic means of protection.

Were suggested and grounded the mathematical models of graphic protection means that are abstract images with the use of steganography principles for implementation the necessary levels of protection which are defined by the parameters of algorithms renewal of the graphic images hidden fragments.

For the first time the methods of synthesis of the protection means models with the information components that use the game theory model, in which the interaction of document protection means which is realized through the document control system with the attacks made by the non commissioned participants of the technological process is described.

A method of steganography using techniques for providing graphic protection means by the features which ensure their safety properties which are defined by the key parameter that is a measure of invisibility of the individual fragments of the protection means and enable them to their values while re making of some copies of documents based on the real danger, which appears according to the appropriate technological process had been suggested.

Algorithms of graphic protection means construction which have the ability to determine the protection level due to the informational technology usage which includes not only mathematical models of different levels of graphic protection means description, but also the information components and processes of document using with the appropriate means of protection in the technological processes have been worked out.

Methods of document control system organization in the game model frames that describes the use of documents in technological processes, means of control and analysis of the actual level of danger for the technological processes and appropriate documents, which is based on the computation expression of the detected, successful attacks and the total number of full cycles of the documents usage by the technological processes have been worked out.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мельников О. В. Технологія плоского офсетного друку / Мельников О. В. [за ред. д-ра техн. наук, проф. Е. Т. Лазаренка. – 2-е вид., випр.]. — Львів : УАД, 2007. — 388 с.
2. Лазаренко Е. Т. Захист друкованої продукції / Е. Т. Лазаренко, В. З. Маїк, А. В. Шевчук, С. В. Жидецький. — Львів : УАД, 2007. — 104 с.
3. Матвеева Р. В. Основы полиграфического производства / Р. В. Матвеева, Г. Г. Трубникова, Д. А. Шифрина. — М. : Книга, 1994. — 312 с.
4. Пикок Д. Издательское дело / Д. Пикок. — М. : Эком., 1988. — 398 с.
5. Артем'єва Е. Ю. Основи психології суб'єктивної семантики / Е. Ю. Артем'єва. — М. : Зміст, 1999. — 350 с.
6. Шмельов А. Г. Введення в експериментальну психосемантику / А. Г. Шмельов. — М. : МГУ, 1983. — 157 с.
7. Дж. Пейдж Крауч. Основы флексографии / Дж. Пейдж Крауч, А. В. Макаров. — М. : Принт-Медиа центр, 2004. — 161 с.
8. Бланки цінних паперів і документів суворого обліку та звітності. Загальні технічні вимоги: ДСТУ 4010-2001 — [Чинний від 2001-06-01]. — К. : Держспоживстандарт України, 2001. — 43 с.
9. Петренко В. Ф. Введение в экспериментальную психосемантику. Исследование форм репрезентации в обыденном сознании / В. Ф. Петренко. — М. : МГУ, 1983. — 175 с.
10. Киричок П. О. Захист цінних паперів та документів суворого обліку / П. О. Киричок, Ю. М. Коростиль, А. В. Шевчук. — К. : НТУУ «КПІ», 2008. — 368 с.
11. Жалніна О. Електрокінетичні властивості паперу / О. Жалніна // Друкарство. — 2002. — № 3(44).

12. Киппхан Г. Энциклопедия по печатным средствам информации. Технологии и способы производства / Г. Киппхан. — М. : МГУП, 2003. — 1280 с.

13. Иродов И. Е. Волновые процессы. Основные законны / И. Е. Иродов. — М. : Физмат, 1999. — 256 с.

14. Беляков В. А. Диффракционная оптика периодических сред сложной структуры / В. А. Беляков. — М. : Наука, 1988. — 256 с.

15. Волкова Л. А. Издательско-полиграфическая техника и технология / Л. А. Волкова. — М. : МГУ «Мир книги», 1999. — 224 с.

16. Стефанов С. Полиграфия и технологии печати / С. Стефанов. — М. : Либроком, 2009. — 144 с.

17. Вильсон Д. Дж. Основы офсетной печати / Д. Дж. Вильсон. — М. : Принт-Медиа центр, 2005. — 220 с.

18. Шевчук А. В. Металографічний друк — ефективний спосіб захисту цінних паперів та документів суворого обліку / А. В. Шевчук // Друкарство. — 2004. — № 3(56).

19. Багая П. И. Химия и технология защитных средств документации / П. И. Багая. — М. : Машиностроение, 1975. — 450 с.

20. Коншин А. А. Защита полиграфической продукции от фальсификации / А. А. Коншин. — М. : ООО «Синус», 1999. — 160 с.

21. Ингрем С. Основы трафаретной печати / С. Ингрем. — М. : Принт-Медиа центр, 2004. — 186 с.

22. Нельсон Р. Э. Что полиграфист должен знать о красках / Р. Э. Нельсон. — М. : Принт-Медиа центр, 2005. — 328 с.

23. Кондрашов Г. А. Физические методы интенсификации процессов химической технологи / Г. А. Кондрашов. — М. : Химия 1990. — 208 с.

24. Душкин С. С. Магнитная подготовка на химических предприятиях / С. С. Душкин, В. Н. Евстратон. — М. : Химия, 1986. — 142 с.

25. Барсуков В. С. Стеганографическая технология защиты документов, авторских прав и информации / В. С. Барсуков // Обзор специальной техники. — 2000. — № 2. — С. 31–40.

26. Генне О. В. Основные положения стеганографии / О. В. Генне // Защита информации. Конфидент. — 2000. — № 3.

27. Шевчук А. В. Захист друкованої продукції за допомогою змішування фарб / А. В. Шевчук, З. Есенфельд // Друкарство. — 2000. — № 4(33).

28. Валиев С. Защита ценных умаг / С. Валиев, Б. Эльтазаров. — М. : ЧеРо, 1997. — 156 с.

29. Пуйплато О. Грошовий документ, захищений друкованою графікою та кодовими знаками / О. Пуйплато // Banque de France. — Франція : 9104782, 1991.

30. Коншин А. А. Защита полиграфической продукции от фальсификации / А. А. Коншин. — М. : ООО «Синус», 1999. — 157 с.

31. Грибулин В. Г. Цифровая стеганография / В. Г. Грибулин, И. Н. Оков, И. В. Туринцев. — М. : СОЛОН-ПРЕС, 2002. — 272 с.

32. Коханович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Коханович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

33. Гуцалюк М. В. Ідентифікація фізичних осіб як протидія організованій злочинності та тероризму [Електронний ресурс] / М. В. Гуцалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2005. — № 11. – http://mndc.naiau.kiev.ua/Gurnal/11text/g11_24.htm.

34. CAO DOC 9303 Machine Readable Travel Documents. [Електронний ресурс]. — http://www2.icao.int/en/mrtd.

35. Дурняк Б. В. Методи стеганографії в задачах захисту документів / Б. В. Дурняк, Д. В. Музика // Збірник наукових праць. — К. : НАН України ІПМЕ, 2007. — № 42. — С. 57–64.

36. Митрофанов С. П. Применение ЭВМ в технологической подготовке серийного производства / С. П. Митрофанов, Ю. А. Гульнов, Д. Д. Куликов. — М. : Машиностроение, 1981 — 287 с.

37. Сабат В. І. Методи захисту документів в системах документообігу / В. І. Сабат// Комп'ютерні технології друкарства. — Л : УАД, 2004. — № 12. — С. 297–305.

38. Лескин А. А. Алгебраические модели гибких производственных систем / А. А. Лескин. — Л. : Наука, 1986. — 150 с.

39. Брагг Р. Система безопасности Windows 2000 / Р. М. Брагг. — СПб. : Издательский дом «Вильямс», 2001. — 592 с.

40. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. — М. : ДМК Пресс, 2002. — 656 с.

41. Тейз А. Логический подход к искусственному интеллекту: от классической логики к логическому программированию / А. Тейз, П. Грибомон, Ж. Луи и др. [Пер. с франц]. — М. : Мир, 1990. — 432 с.

42. Кустов В. Н. Методы встраивания скрытых сообщений / В. Н. Кустов, А. А. Федорчук // Защита информации. Конфидент. — 2000. — № 3.

43. Стародубцев Г. В. Разработка инструментального средства построения интеллектуальных объектно-ориентированных моделей для поддержки принятия решений / Г. В. Стародубцев, М. П. Силич, В. А. Силич // Известия Томского политехнического университета. — 2006. — № 7. — С. 165–168.

44. Алгоритмы и структуры систем обработки информации: Сб. науч. Тр. — Тула : ТПИ, 1989. — 122 с.

45. Бирбков Б. В. Теория смысла Готлоба Фреге / Б. В. Бирбков // Применение логики в науке и технике. — М. : Изд-во АН СССР, 1960. — С. 502–555.

46. Клини С. Математическая логика / С. Клини. — М. : Мир, 1973. — 480 с.

47. Дурняк Б. В. Логічні способи опису графічних засобів захисту документів та цінних паперів / Б. В. Дурняк, Д. В. Музика // Збірник наукових праць. — К. : НАН України ІПМЕ, 2007. — № 43. — С. 46–54.

48. Валькман Ю. Р. Принципы построения алгебры и логики текстов и контекстов математических моделей / Ю. Р. Валькман // Труды III конф. по искусственному интеллекту «КИИ-92». — Тверь, 1992. — С. 48–53.

49. Булатов В. Увидеть невидимое / В. Булатов, В. Дмитриев // КомпьютерПресс, 1993. — № 4. — С. 20–26.

50. Саломаа А. Жемчужины теории формальных языков / А. Саломаа [Пер. с англ.]. — М. : Мир, 1986. — 160 с.

51. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. — М. : ДИАЛОГ-МИФИ, 2002. — 384 с.

52. Кудрявцев В. Б. Введение в теорию абстрактных автоматов / В. Б. Кудрявцев, А. С. Подколзин, Ш. Ушчумлич. — М. : Изд-во. Моск. Ун-та, 1985. —174 с.

53. Карацуба А. А. Решение одной задачи из теории конечных автоматов / А. А. Карацуба // УМН. — М., 1960. — № 3(93). — С. 157-159.

54. Музика Д. В. Використання формальних граматик та теорії автоматів, для опису та дослідження графічних засобів захисту / Д. В. Музика // Моделювання та інформаційні технології : зб. наук. пр. [НАН України ІПМЕ]. – К., 2007. — № 43. — С. 48–57.

55. Зыков А. А. Основы теории графов / А. А. Зыков. — М. : Наука, 1987. — 389 с.

56. Смарт Н. Криптографія / Н. Смарт. — М. : ТЕХНОСФЕРА, 2005. — 528 с.

57. Харари Ф. Теория графов / Ф. Харари. — М. : Мир, 1973. — 300 с.

58. Кристофидес П. Теория графов. Алгоритмический поход / П. Кристофидес. — М. : Мир, 1978. — 432 с.

59. Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део. — М. : Мир, 1980. — 478 с.

60. Берж К. Теория графов и ее применения / К. Берж. — М. : Изд. иностранной литературы, 1962. — 320 с.

61. Солсо Р. Когнитивная психология / Р. Солсо. — СПб. : Питер, 2006. — 589 с.

62. Салий В. Н. Алгебраические основы теории дискретных систем / В. Н. Салий, А. М. Богомолов. — М. : Физико-математическая литература, 1997. — 368 с.

63. Кормен Т. Х. Алгоритмы построение и анализ / Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест // Клиффорд Штайн. [2-е изд.]. — М. : «Вильямс», 2006. — 1296 с.

64. Кук Д. Компьютерная математика / Д. Кук, Г. Бейз. — М. : Наука, 1990. — 384 с.

65. Дурняк Б. В. Особливості використання теорії графів та методів стеганографії, для побудови графічних засобів захисту документів / Б. В. Дурняк, Д. В. Музика // Моделювання та інформаційні технології: зб. наук. пр. [ІПМЕ ім. Г. Є. Пухова НАН України]. — К., 2007. — № 44. — С. 39–48.

66. Современные проблемы математического и информационного моделирования. Перспективы разработки и внедрения инновационных IT-решений: сб. науч. тр. / Тюм. гос. ун-т; гл. ред. В. Н. Кутрунов. — Тюмень : Изд-во ТюмГУ, 2008. — 164 с.

67. Лотман Ю. М. Текст в тексте / Ю. М. Лотман // ТЗС. — М., 1981. — Вып. 14. — С. 3–18;

68. Львова С. И. Язык в речевом обращении / С. И. Львова. — М. : Просвещение, 1991. — 190 с.

69. Плоткин Б. И. Универсальная алгебра, алгебраическая логика и базы даннях / Б. И. Плоткин. — М. : Наука, 1991. — 446 с.

70. Федоров Б. И. Логика компьютерного диалога / Б. И. Федоров, З. О. Джалиашвили. — М. : ТОО «Онега», 1994. — 238 с.

71. Козеренко Е. Б. Концептуально-лингвистическое моделирование в интеллектуальных системах на основе расширенных семантических сетей: автореф. дис. на соиск. учен. степ. кандидата наук: спец. 05.13.17 «Теоретические основы информатики» / Е. Б. Козеренко. — М., 1995. — 21 с.

72. Математическое моделирование и управление в сложных системах: сб. науч. тр. — М. : МГАПИ, 1997. — 189 с.

73. Сабат В. І. Теоретичні особливості захисту інформації на основі використання її семантики / В. І. Сабат // Моделювання та інформаційні технології: зб. наук. праць. [ІПМЕ ім. Г. Є. Пухова НАН України]. — К., 2003. — Вип. 22. — С. 97–105.

74. Муромцев Ю. Л. Моделирование и оптимизация сложных систем при изменениях состояния функционирования / Муромцев Ю. Л. — Воронеж: Изд-во Воронеж. ун-та, 1993. — 162 с.

75. Крамер Г. Математические методы статистики / Крамер Г. — М. : Мир, 1975. — 648 с.

76. Дурняк Б. В. Семантичний захист інформації в системах документообігу / Б. В. Дурняк, В. І. Сабат // Монографія. — Л. : УАД, 2010. — 160 с.

77. Дурняк Б. В. Основні інформаційні компоненти системи графічних засобів захисту документів / Б. В. Дурняк, Д. В. Музика // Моделювання та інформаційні технології: зб. наук. пр. [НАН України ІПМЕ]. — К., 2008. — № 46. — С. 52–59.

78. Музика В. П. Особливості формування графічних засобів захисту документів з використанням методів укриття фрагментів графів / В. П. Музика, Д. В. Музика // Моделювання: міжнародна наукова конференція, 14-16 травня, 2008 р.: тези доповідей. — К., 2008.

79. Дурняк Б. В. Методи стеганографічного захисту інформації в автоматизованих системах документообігу / Б. В. Дурняк, В. І. Сабат, Д. В. Музика // Моделювання та інформаційні технології: зб. наук. пр. [ІПМЕ ім. Г. Є. Пухова НАН України]. — К., 2010. — Вип. 54. — С. 210–215.

80. Молчанов А. А. Моделирование и проектирование сложных систем / А. А. Молчанов. — К. : Вища шк., 1988. — 359 с.

81. Белоусов А. И. Дискретная математика / А. И. Белоусов, С. Б. Ткачев. — М. : МГТУ им. Н. Э. Баумана, 2001. — 743 с.

82. Сабат В. І. Моделювання семантики загроз документів / В. І. Сабат // Зб. наук. праць. [ІПМЕ ім. Г. Є. Пухова НАН України]. — К., 2003. — Вип. 23. — С. 139–147.

83. Донской В. И. Дискретная математика / В. И. Донской. — Симферополь : СОНАТ, 2000. — 354 с.

84. Емеличев В. А. Лекции по теории графов / В. А. Емеличев, О. И. Мельников, В. И. Сараванов, Р. И. Тышкевич. — М. : Наука, 1990. — 384 с.

85. Дурняк Б. В. Задачі логіко-інформаційних моделей засобів захисту / Б. В. Дурняк, Д. В. Музика // Моделювання: XXVII науково-технічна конференція, 10-11 січня 2008 р.: тези доповідей. — К., 2008.

86. Евстигнеев В. А. Теория графов / В. А. Евстигнеев, В. Н. Касьянов. — Новосибирск : Наука, 1994. — 360 с.

87. Шенфилд Дж. Математическая логика / Дж. Шенфилд. — М. : Наука, 1975. — 528 с.

88. Плесневич Г. С. Алгоритмы в теории графов / Г. С. Плесневич, М. С. Саратов. — Ашхабад : Илым, 1981. — 311 с.

89. Майника Э. Алгоритмы оптимизации в сетях и графах / Э. Майника. — М. : Мир, 1981. — 323 с.

90. Методы дискретного анализа в теории графов и схем / Отв. Ред. Ю. Л. Васильев. — Новосибирск : ИМ, 1985. — 111 с.

91. Плюшкявичус Р. Математическая логика и ее применение / Под ред. Р. Плюшкявичуса. — Вильнюс : Ин-т математики и кибернетики, 1985. — 138 с.

92. Романенко А. Г. Моделирование информационных систем / А. Г. Романенко. — М. : МГИАИ, 1988. — 83 с.

93. Музика В. П. Використання інформаційних компонент в графових моделях графічних засобів захисту / В. П. Музика, Д. В. Музика // Моделювання та інформаційні технології: зб. наук. пр. [НАН України ІПМЕ]. — К., 2008. — № 45. — С. 81-87.

94. Брук В. М. Большие системы управления: критериальная оценка и моделирование / В. М. Брук, М. В. Копейкин. — Л. : СЗПИ, 1984. — 75 с.

95. Вирт Н. Алгоритмы + структуры данных — программы / Н. Вирт. — М. : Мир, 1985. — 406 с.

96. Голуб А. П. Алгоритмы управления и математические модели систем автоматического управления / А. П. Голуб. — Харьков : УзПИ, 1986. — 85 с.

97. Математическое моделирование процессов управления и обработки информации: межвед. сб. — М. : МИФИ, 1993. — 203 с.

98. Лозовану Д. Д. Экстримально-комбинаторные задачи и алгоритмы их решения / Д. Д. Лозовану. — Кишинев : Штиинца, 1991. — 221 с.

99. Кравченко В. А. Алгоритмы решения задач многокритериальной оптимизации / В. А. Кравченко. — М. : МИЭМ, 1988. — 72 с.

100. Дурняк Б. В. Контроль документів, що використовують стеганографічні методи захисту / Б. В. Дурняк, Д. В. Музика // Збірник наукових праць [НАН України ІПМЕ]. — К., 2008. — № 45. — С. 83–90.

101. Афанасьєва О. Ю. Аналіз окремих семантичних параметрів, що використовуються в стеганосистемах / О. Ю. Афанасьєва, В. І. Сабат // Моделювання та інформаційні технології: зб. наук. пр. [ІПМЕ ім. Г. Є. Пухова НАН України]. — К., 2008. — Вип. 46. — С. 127–132.

102. Козлов К. П. Алгоритмы: Учебное пособие / К. П. Козлов. — Л. : ЛГПИ, 1989. — 38 с.

103. Прикладные задачи оптимального управления: модели, методы, алгоритмы: сб. тр. — М. : ИПУ, 1990. — 118 с.

104. Девенпорт Джеймс. Компьютерная алгебра: системы и алгоритмы алгебраических вичислений / Джеймс Девенпорт. — М. : Мир, 1991. — 30 с.

105. Советов Б. Я. Моделирование систем / Б. Я. Советов, С. А. Яковлев. — М. : Высш. шк., 1985.— 271 с.

106. Червенчук В. Д. Логические функции, таблицы решений и аксиоматическое моделирование / В. Д. Червенчук. — Омск : ОмПИ, 1989. — 80 с.

107. Линдон Р. Заметки по логике / Р. Линдон. — М. : Мир, 1968. — 128 с.

108. Бузин А. Ю. АПЛ. Язык интерактивного математического моделирования / А. Ю. Бузин. — М. : Изд-во Рос. ун-та дружбы народов, 1996. — 56 с.

109. Чень Ч. Математическая логика и автоматическое доказательство теорем / Ч. Чень, Р. Ли. — М. : Наука, 1983. — 385 с.

110. Музика Д. В. Особливості використання стеганографії для захисту паперових документів / Д. В. Музика // Сучасні інформаційно-комунікаційні технології COMINFO' 2007: III Міжнародна науково-технічна конференція, 25–28 вересня, 2007 р.: тези доповідей. — Ялта, 2007.

111. Успенский В. А. Теория алгоритмов: основные открытия и приложения / В. А. Успенский, А. Л. Семенов. — М. : Наука, 1987. — 288 с.

112. Самарский А. А. Математическое моделирование: Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов. — М. : Наука, 1997. — 316 с.

113. Сысоев В. В. Системное моделирование: Учебное пособие / В. В. Сысоев. — Воронеж : ВТИ, 1991. — 78 с.

114. Джордж Ф. Основы кібернетики / Ф. Джордж. — М. : Радио и связь, 1984. — 272 с.

115. Новиков П. С. Элементы математической логики / П. С. Новико. — М. : Наука, 1973. — 400 с.

116. Гладкий А. В. Элементы математической логики / А. В. Гладкий, И. А. Мельничук. — М. : Мир, 1969.

117. Плоткин Б. И. Элементы алгебраической теории автоматов / Б. И. Плоткин, Л. Я. Гринглаз, А. А. Гварамия. — М. : Высш. шк. 1994. — 191 с.

118. Таланов В. А. Логические модели языков. Учебное пособие / В. А. Таланов. — Горький : ГГУ, 1985. — 64 с.

Наукове видання

Дурняк Богдан Васильович
Музика Дмитро Валентинович
Сабат Володимир Іванович

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ДОКУМЕНТІВ

Монографія

Художнє оформлення та верстання *В. І. Сабат*
Обкладинка *В. І. Сабат*
Редактор *Г. Я. Шевчук*

Свідоцтво про внесення до Державного реєстру
ДК № 3050 від 11.12.2007 р.

Підписано до друку 13.05.2014. Формат 60×84/16
Папір офсетний. Гарнітура «Times».
Умов. друк. арк. 9,3. Обл.-вид. арк. 10,64.
Друк офсетний. Тираж 300 примірників.
Зам. № 100.

Видавництво Української академії друкарства
79020, Львів, вул. Підголоско, 19
Віддруковано в НЛПТ Української академії друкарства
79008, м. Львів, пл. Митна, 1