УДК 004.056

Б. В. Дурняк
Українська академія друкарства
В. З. Пашкевич
Національний університет «Львівська політехніка»

МОДЕЛІ ГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ДОКУМЕНТІВ

Визначається загальна модель графічних засобів захисту документів, яка дає можливість управляти рівнем захисту документів, не змінюючи його технологію.

Модель, засоби захисту, документ

Залежно від вимог до захисту документів на паперових носіях існує цілий ряд методів їх захисту. Сьогодні надійний захист документів можна забезпечити збалансованим набором різних видів захисту та їх ідентифікацією на всіх етапах використання. Проте існує проблема створення надійних і недорогих засобів захисту документів, оскільки наявні засоби доволі дорогі з погляду реалізації технологічних процесів їх виготовлення.

Розв'язання цієї проблеми можливе завдяки використанню моделей графічних засобів захисту, які дають можливість виконувати такі функції [3]:

модель у цілому відображає зв'язки засобів захисту з параметрами, що характеризують їх реальне використання в процесі обігу документів;

модель описує загальну мету керування, яка виражається рівнем захищеності для кожного окремого документа;

у межах моделі можна досліджувати стійкість систем захисту документів.

Загальна модель графічного засобу захисту в межах запропонованого підходу — це синтез таких окремих моделей та компонент, які наведені на рис. 1.

Моделі графічних засобів захисту будуються на основі методів формальних описів, що використовуються для їх подання [2]. До таких формальних описів також належать методи графового подання засобів захисту та геометричні параметри, що описують відповідний засіб, як деякий геометричний образ. Модель графічного засобу захисту є синтезом його формального опису, геометричних параметрів, що характеризують образ та опис процесів, які пов'язані з функціонуванням засобу захисту і передусім процесів, пов'язаних з протидією атакам, що ініціюються загрозами. Крім того, будь-яка модель, що є компонентою загальної (ZM), використовує засоби інтерпретації всіх компонент, що формально подані в моделі. Такі засоби реалізуються в межах окремої групи моделей, що входять у ZM, якими є інформаційні моделі [7].

Моделі процесу генерації та модифікації виділяються в окрему компоненту у зв'язку з тим, що процеси протидії атакам значною мірою пов'язані з ними. Протидія у цьому випадку розглядається як послідовність дій, яка реалізується зі сторони системи захисту і складається щонайменше з дій спрямованих на розпізнавання атаки та дій [5], що передбачають захист відповідних документів від атаки. Фізична природа графічних засобів захисту, що в межах цього підходу є графічними образами — така, що вони не можуть здійснювати будь-які дії пов'язані з протидією атакам. Така протидія може бути реалізована тільки в межах загальної моделі захисту (рис. 1).

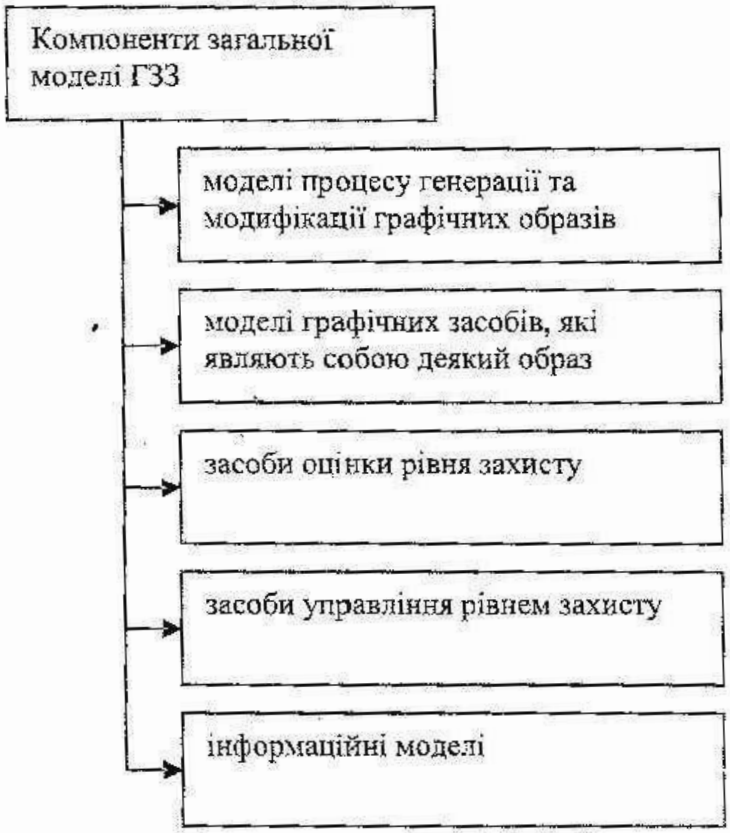

Рис. 1. Компоненти опису графічних засобів захисту

Наступна модель, що виокремлена як компонента загальної моделі, є інформаційною (ІМ) [3]. Необхідність у такому відокремленні полягає в тому, що інформаційні елементи, які входять до складу цієї моделі, не тільки виконують функції інтерпретації всіх компонент ZM, а й реалізують суто інформаційні процеси, що описуються за допомогою параметрів інформаційного характеру. Ці інформаційні процеси і відповідні параметри не дублюють процесів, які описуються іншими моделями, а є незалежними від них в тому сенсі, що їх результати можуть мати нову непередбачувану відповідними моделями інтерпретацію процесів, які можуть відбуватися в межах ZM.

Засоби оцінки рівня захищеності документів являють собою компоненту, яка визначає поточне значення рівня безпеки документа впродовж періоду його

існування. Ця функція є ключовою для моделі захисту в цілому, оскільки вона не тільки описує в тій чи іншій формі вигляд засобу захисту, а насамперед дає можливість відображати процеси функціонування моделі. Процес функціонування засобів рівня захищеності передбачає не тільки аналіз самих засобів захисту, але й подій, які свідчать про виникнення атак, результати їх впливу на документи і, відповідно, про успішність чи невдачу кожної з атак та інформації, що стосується безпеки документів [7].

Засоби управління рівнем захисту здійснюють управління загальною моделлю захисту. Критерієм управляючих для них дій є заданий або визначений рівень захисту, якому мають відповідати [6] документи захищені відповідними засобами захисту. Функції засобів управління рівнем захисту документів наведені на рис. 2.

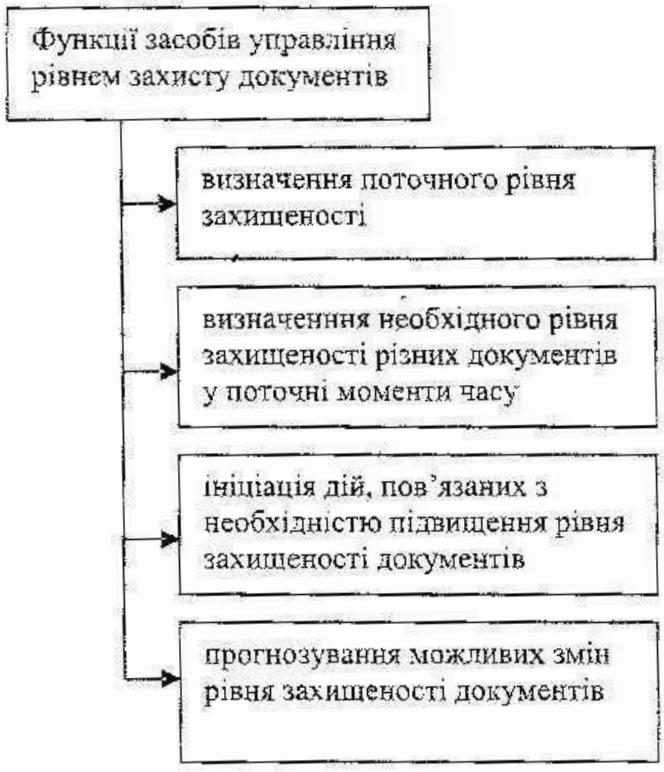

Рис. 2. Функції засобів управління рівнем захисту документів

Функції визначення поточного значення рівня захищеності доволі тісно пов'язані з його оцінкою. Однак між визначенням рівня захищеності і його оцінкою є суттєві відмінності, характерні для задачі управління моделлю ZM. Оцінення рівня захищеності здійснюється в межах визначеної шкали оцінок, яка використовується потенціальними користувачами документів і безпосередньо пов'язана з предметною областю, в якій відповідний документ використовується. Одним з прикладів формування оцінки рівня захищеності може бути її визначення шляхом оцінення втрат [4, 8], до яких може призвести успішна атака на документ, якщо відомо, що цей засіб захисту має захищати його від відповідних атак.

Друга особливість оцінення рівня захищеності полягає в тому, що вона визначається на весь період функціонування цілого тиражу однакових документів. Рівень захищеності у разі визначення його поточного значення, визначається на основі власних параметрів засобів захисту, якими захищені документи. Його величина визначається для кожного тиражу документів з урахуванням даних про здійснені атаки та про кількість успішних атак. Ці дані накопичуються і, залежно від зміни їх значень, рівень захисту може змінюватися в часі. Кількість атак, що завершились успішно, визначається на основі аналізу технологічного процесу використання конкретного типу документів або на основі аналізу використання ряду документів, який здійснюється у разі виявлення порушень у виконанні технологічного процесу. У результаті такого аналізу може виявитися, що причиною порушення технологічного процесу є успішна атака на документ, стосовно якого передбачається оцінювати рівень захищеності. При цьому сам документ за технологічними параметрами засобу захисту, завдяки успішності атаки, може бути визнано непідробленим та непідміненим, що відповідає основному типу атак на документи. До неуспішних атак належать ті, які вдалося виявити завдяки перевірці засобів захисту, і за їх параметрами було виявлено, що документ є підробленим або підміненим.

Оскільки документ розглядається як засіб захисту технологічного процесу його використання, то він має відображати динаміку розвитку, яка передусім, стосується змін параметрів захисту чи самих засобів захисту [7]. Ці процеси реалізуються у сфері використання документів і сьогодні вони являють собою заміну одних зразків іншими, тому виникає потреба у збільшенні захисних властивостей окремих засобів захисту в документах, наприклад, у паперових грошових знаках. У межах цього підходу передбачається створити механізми більш гнучкої реалізації відповідних процесів управління рівнем захищеності документів шляхом зміни параметрів засобів захисту. Гнучкість такого управління полягає у тому, що зміна значень параметрів засобів захисту не вимагає складних і дорогих змін у технологічному процесі використання модифікованих документів поряд з немодифікованими, які є допустимими впродовж деякого перехідного періоду, що може бути значно коротшим, ніж перехідний період, який використовується при заміні документів у межах наявних підходів [1].

Визначення потрібного рівня захищеності ґрунтується не тільки на аналізі атак, що ініціюються небезпеками стосовно документів, а й на основі аналізу змін у технологічних процесах, які вони обслуговують, оскільки говорити про їх засоби захисту та документи, як про окремі об'єкти, некоректно. У цьому разі процес управління рівнем їх захисту здійснюватиметься з випередженням, але не із запізненням, як це має місце у випадку управління рівнем захисту на основі аналізу атак, що діють на документи. Можливість здійснювати управління рівнем захисту документів з випередженням ґрунтується на тому, що будь-який технологічний процес, перш ніж впроваджуватися в ту чи іншу предметну область, проектується. На стадії проектування

технологічного процесу визначаються потрібні документи, що мають його обслуговувати, та необхідні рівні захисту цих документів. Визначення рівня захисту в цьому разі грунтується на оцінюванні критичності самого технологічного процесу та аналізі величин вартості і ризику кожного етапу технологічного процесу, на яких передбачається використовувати документи. Цей же аналіз може використовуватись і під час модифікації технологічних процесів для впровадження необхідних змін у засоби захисту документів. У цьому разі управління рівнем захищеності документів здійснюється з точністю до величини зміни у процесах, які обслуговуються в режимі випередження [7].

Структурні моделі графічних засобів захисту дають можливість здійснювати управління мірою захищеності документів у процесі їх експлуатації. Доцільність такого управління полягає у тому, що виготовлення графічних засобів захисту з високим рівнем стійкості є дорогим. Що нижчим є рівень стійкості, то нижчою буде ціна виготовлення засобів захисту. Запропонована модель графічних засобів захисту дає можливість управляти рівнем захисту документів, не змінюючи технологію захисту, що є суттєвою економічною перевагою під час забезпечення надійного та недорогого захисту.

1. Дурняк Б. В. Основні небезпеки в системах автоматизованого документообігу / Б. В. Дурняк // Моделювання та інформаційні технології : зб. наук. пр. — К., 2003. — Вип. 23. — С. 121–128. 2. Капустій Б. О. Системи розпізнавання образів з малими базами даних / Б. О. Капустій, Б. П. Русин, В. А. Таянов. — Львів : СПОЛОМ, 2006. — 152 с. 3. Киричок П. О. Захист цінних паперів та документів суворого обліку: моногр. / П. О. Киричок, Ю. М. Коростіль, А. В. Шевчук. — К. : НТУУ «КПІ», 2008. — 368 с. 4. Копшин А. А. Защита полиграфической продукции от фальсификации / А. А. Копшин. — М. : Синус, 1999. — 160 с. 5. Організація збору і попередня підготовка захисту інформації в автоматизованих інформаційних системах / А. М. Давиденко, С. М. Головань, О. О. Мелешко, Л. М. Щербак // Зб. наук. пр. НАН України. Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. — К., 2005. — Вип. 34. — С. 20–26. 6. Орел С. М. Ризик. Основні поняття : навч. посіб. / С. М. Орел, М. С. Мальований. — Львів : Вид-во Нац. ун-ту «Львів. політехніка», 2008. — 88 с. 7. Пашкевич В. З. Аналіз методів побудови графічних засобів захисту / В. З. Пашкевич // Зб. наук. пр. НАН України. Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. — К., 2005. — Вип. 30. — С. 101–108. 8. Симонов С. Современные технологии анализа рисков в информационных системах / С. Симонов // Компьютерная неделя. — М., 2001. — № 37 (307). — С. 10–17.

МОДЕЛИ ГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ДОКУМЕНТОВ

Определяется общая модель графических средств защиты документов, которая позволяет управлять уровнем защиты документов, не изменяя его технологию.

MODELS OF GRAPHIC FACILITIES OF DEFENCE OF DOCUMENTS

We worked out the general model of graphic protection means of documents which allows to provide their optimum protection according to real existing risks of their falsification.

Стаття надійшла 20.04.10