системними адміністраторами для прогнозування продуктивності під час реконфігурації мережі або збільшення трафіка запитів.

1. Кузьмин А.В., Лукащук Л.А. Пакет прикладных программ для имитационного моделирования вычислительных управляющих комплексов (СИМВУК) // Тез. докл. конф. "Информационно-измерительные системы и точность в приборостроении". – М., 10–11 ноября 1982. 2. Kuzmin A., Juravchak L. The Methodology and Software of Simulation Modeling of Computing Structures // The Experience of Designing and Application of CAD Systems in Microelectronics:Proceedings of the VIIth International Conference CADSM 2003. – Lviv-Slavske, Ukraine, 18–22 February 2003. – P. 421–423.

УДК 621.396.8.

М. Медиковський, В. Пашкевич
Національний університет "Львівська політехніка"
кафедра автоматизованих систем управління

АЛГОРИТМ УПРАВЛІННЯ РИЗИКОМ ВИКОРИСТАННЯ ПОЛІГРАФІЧНИХ ДОКУМЕНТІВ

Для дослідження надійності графічних засобів захисту введено нові параметри захисту, такі як: міра роздільності двох суміжних ліній узору, міра насиченості фрагмента графічного образу, варіація роздільності вздовж суміжних ліній, локальна густина графічного засобу захисту. З використанням результатів теоретичних досліджень розроблено математичний апарат розрахунку ризику застосування графічно захищених документів. Для забезпечення оптимальної стійкості розроблено алгоритм управління величиною надійності графічних засобів захисту і функціональну блок-схему управління ризиком використання захищених документів. У роботі досліджено вплив параметрів графічних засобів захисту поліграфічних документів на міру їх стійкості.

For research of reliability of graphic facilities of defence, new parameters of defence are entered, such as: measure of divisible of two contiguous lines of pattern, measure of saturation of fragment of graphic appearance, variation of divisible along contiguous lines, local density of graphic mean of defence. With the use of results of theoretical researches the mathematical vehicle of calculation of risk of application of the graphically protected documents is developed. For providing of optimum firmness the algorithm of management by the size of reliability of graphic facilities of defence is developed and functional block- scheme of management by the risk of the use of the protected documents. In this work influence of parameters of graphic facilities of defence of polygraphs documents is explored on the measure of their firmness.

Вступ

Визначення величини ризику, якому піддається документ у разі використання засобів захисту, є ключовим елементом інформаційної технології, оскільки обрахована величина ризику є вихідною для здійснення управління по зміні рівня захисту документу в системі документообігу загалом. У межах цього підходу до факторів, які мають інтерпретацію загроз, будемо відносити тільки фактори, які властиві об'єкту, що підлягає захисту. Тому під параметрами, що характеризують існуючі загрози, розуміємо параметри, що характеризують загрози, які незалежно від характеру чи типу небезпеки, що ініціює атаку, є засобами, за допомогою яких реалізується будь-

яка атака. Перш за все зазначимо, що загроза як параметр об'єкта виникає тільки в тому випадку, коли у межах об'єкта використовують засоби захисту. Загрози як певні властивості об'єкта не створюються спеціально, а виникають у разі створення засобів захисту в результаті недосконалості технології, яку використовують для засобів захисту, в результаті змін, що можуть відбуватися в засобах захисту під впливом дій, пов'язаних з експлуатацією документа та в результаті будь-яких дій, які впливають на параметри засобів захисту.

Залежно від вимог до захисту поліграфічних документів існує багато методів його реалізації. Широкий спектр захисних технологій, насамперед, зумовлений розширенням можливостей фальсифікації документів та інтенсивним зношенням засобів захисту в процесі експлуатації. Тому в більшості випадків під системою захисту документів розуміють використання не однієї технології захисту, а комплексу захисних технологій [1]. Тоді надійність захисту документів забезпечується не досконалістю окремо взятого виду захисту, а збалансованим набором різних видів (графічним, хімічним, технологічним захистом та ін.). Тому актуальною проблемою є створення таких оригінальних засобів захисту, які відповідали б реально існуючим небезпекам, а також забезпечували б можливість керувати рівнем захисту документів.

Важливою умовою ефективного захисту документів є поєднання необхідної надійності і ефективності засобів захисту з максимальною їх зручністю у використанні. Рівень захисту документів має залежати від реальних потреб технологічних процесів, які обслуговуються відповідним документами. Тому досліджувати співвідношення параметрів технічних систем і елементів захисту поліграфічних документів важливо під час розроблення засобів автоматизованого управління документообігом.

Визначення величини ризику використання документів

Оскільки існують різні за своєю значимістю документи та окремі класи документів доцільно мати можливість більш гнучко оцінювати необхідний рівень захисту документів, що дасть змогу керувати рівнем їхньої безпеки. Загальноприйнято для цього використовувати такий параметр, як величина ризику використання захищених документів [2]. У межах цієї роботи величину ризику оцінюватимемо безрозмірною величиною, яку можна визначити в процентах чи в діапазоні значень [0,1]. Завдяки такому діапазону значень цього параметра можна отримати граничні значення ризику. Якщо значення ризику дорівнює нулю, то ризик повністю відсутній, а якщо ж значення ризику дорівнює одиниці, то події, визначені як небажані, існують відносно документів. Очевидно, що величина ризику, який позначатимемо символом R, повинна займати проміжне значення. Цей параметр визначається такими факторами [3]:

- величиною протидії атакам, яку можуть забезпечувати засоби захисту;
- інтенсивністю атак, що ініціюються відносно документів;
- величиною загроз, які існують в документах, що захищаються;
- наявністю небезпек, що існують відносно документів;
- параметрами системи управління рівнем захищеності, що входить до складу інформаційної технології управління системою документообігу.

Величина ризику допускає різні способи інтерпритації цього поняття [4]. Найбільш поширений спосіб визначення величини ризику полягає у такому.

Величина ризику [1, 2] визначається імовірністю втрат, яких зазнає споживач у разі використання одного з документів або класу документів. У цьому випадку для обчислення величини ризику необхідно мати певну статистику про дані, за допомогою яких обчислюють величину ризику і за цими даними формують модель прогнозування величини ризику. У найпростішому випадку такі моделі можуть ґрунтуватися на використанні стохастичних параметрів [5]. Поняття ризику і, в першу чергу, сам параметр R є за своєю природою екстраполяційним поняттям, що визначається величиною екстраполяційного процесу в заданий момент часу, на який відповідний прогноз реалізується. У зв'язку з цим складно забезпечити обчислення величини цього параметра з високою точністю. Досить часто поняття ризику пов'язується з уявленнями про процеси та моделі

прогнозування. Моделі прогнозування відрізняються від моделей обчислення величини ризику тим, що у розв'язку задач прогнозування в більшості випадків результат прогнозування описується декількома параметрами. Це означає, що під час розв'язування задач прогнозування здійснюється передбачення стосовно перебігу цілих процесів, або передбачення змін в системах, стосовно яких реалізується модель прогнозування. У випадку визначення ризику йдеться про передбачення зміни величини окремого параметра, яким є параметр ризику.

Параметр ризику переважно використовують у тих випадках, коли існують два альтернативні фактори, вплив яких на процес чи об'єкт є протилежним. Наприклад, фактори, що визначають безпечне або небезпечне функціонування документів. У цьому випадку можна говорити про ризик як міру можливості безпечного функціонування документів. Безпечне і небезпечне функціонування документів, своєю чергою, залежить від багатьох власних факторів та параметрів, тому можна написати залежність у такій загальній формі:

$$R = F\left[f_B\left(X_{B1},...,X_{Bn}\right), f_N\left(X_{N1},...,X_{Nm}\right)\right] = F(\Omega,\Omega_N), \quad (1)$$

де f_B – функція, що описує взаємозв'язок між параметрами, стійкості документа до атак; f_N – функція, що описує взаємозв'язок між параметрами, міри податливості документів до атак.

Оскільки атакам протидіють шляхом ідентифікації документа, то міру стійкості можна вимірювати через параметри, що характеризують засоби захисту. До таких параметрів належать η – міра насиченості фрагмента графічного образу, μ – міра роздільності двох суміжних ліній узору, χ – варіація роздільності вздовж суміжних ліній, γ – локальна густина засобу захисту z_i. Крім геометричних параметрів, перерахованих вище, які є безпосередніми характеристиками графічного образу, на величину стійкості Ω впливають і графові параметри. Графові параметри в певному сенсі можна назвати функціональними, тому що їх використовують для опису процесу відтворення графічних образів, під час модифікації чи зміни графічних засобів захисту. Це також є одним з факторів стійкості засобів захисту, оскільки основний вид атаки на документи ґрунтується на підробленні засобів захисту, а саме – у несанкціонованому їх виготовленні. Опосередненими характеристиками, що впливають на стійкість графічних засобів захисту, є особливості реалізації алгоритмів формування траєкторій графічного образу, які визначаються умовами виконання окремих фрагментів чи кроків таких алгоритмів. Однією з таких характеристик є міра подібності двох фрагментів графів, що інтерполюють фрагменти різних графічних образів $\pi(G_i,G_{i+1})$. До параметрів цього типу належать такі параметри, як довжина траєкторії графу l_i, орієнтація чергового ребра α_i графу G_i та найближче оточення ε_i. Особливістю цих параметрів є те, що вони мають характер обмежень на спосіб реалізації окремих кроків алгоритму побудови траєкторії графу. Тому процес формування чергового елемента траєкторії графу, під час побудови фрагмента графічного образу, на етапі, коли локальні параметри за своїми значеннями ще далекі від необхідних, має детермінований характер, який визначається визнаним для цього графічного образу характером побудови. Наприклад, якщо для графічного образу характерними є лінії, що утворюють близькі до концентричних фігури, за наявності кількох варіантів продовження траєкторії на цьому етапі побудови, алгоритм вибирає той варіант побудови чергового ребра, який відповідає параметрам фрагмента образу. Таким параметром може бути взаємна орієнтація двох послідовних ребер чи взаємозв'язок між більшою кількістю елементів, що формують траєкторію, яка апроксимує відповідні лінії узору. Ці детерміновані алгоритми та умови вибору чергового кроку графічного засобу ми не розглядатимемо, оскільки вони відображають явні параметри чи характеристики графічного образу і тому не можуть характеризувати міру захисту, яку забезпечує відповідний образ. У зв'язку з цим функцію f_B можна побудувати, виходячи з таких позицій:

- опис кожної окремої змінної можна визначити як деяке порогове співвідношення;
- кожна із змінних, яка пов'язана з іншими змінними визначеними співвідношеннями, свою порогову структуру може відображати через порогові значення змінних або параметрів, які є для неї аргументами у функціях відповідних співвідношень;
- наближення чергового значення до своєї порогової величини має однозначно спричиняти до збільшення або зменшення величини функції f_B;

- зміна величини значення відповідних параметрів повинна приводити до інтерпретації, що не суперечить їх графічному відображенню.

Оскільки Ω визначає величину стійкості до атак, то необхідно визначитися із способом вимірювання цієї величини. Як і у випадку визначення діапазону значень величини ризику, приймемо діапазон значень, яких може набувати величина Ω, що дорівнює [0, 1]. При цьому $\Omega=0$, якщо рівень стійкості мінімальний. Це відповідає ситуації, коли графічний образ може бути повторений на основі його візуального сприйняття. Наприклад, коли як підпис, як варіант графічного образу або засобу захисту використовують символ з довільними параметрами. Величина $\Omega=1$, коли образ для свого відтворення потребує використання всіх параметрів, що його характеризують, та відтворення всіх алгоритмів, використовуваних під час його формування. У цьому випадку явно не формулюється вимога до відповідної поліграфічної технології, оскільки вона обумовлює можливість відтворення графічного образу з заданими значеннями параметрів графічних образів з суто технічного погляду.

Якщо такий параметр, як міра роздільності має метричний характер і є віддаллю між двома суміжними лініями образу в заданому фрагменті графічного образу $S(\omega)$, то складову величини стійкості Ω, що відповідає параметру роздільності μ, обчислюватимемо за допомогою виразу: $\left|\mu_{pi}-\mu_i\right| \le \delta\mu_i$, де μ_p – порогове значення віддалі між суміжними лініями, більшою від якої не повинна бути віддаль між лініями в заданому фрагменті $S(\omega)$. Виходячи з графічної інтерпретації $\delta\mu_i$, остання завжди буде додатною величиною. Якщо для вимірювання μ_i і μ_{pi} введемо, щоб $\delta\mu_i$ було цілим додатним числом, тоді $X_{Bi}=1/\delta\mu_i$ гарантує потрапляння цього параметра до діапазона [0,1]. Отже, управління величиною стійкості за параметром μ здійснюватиметься зміною допустимої величини $\delta\mu$, або μ_{pi} у заданих фрагментах графічного образу.

Параметр, що визначає міру насиченості η, вимірюють безрозмірною величиною, оскільки він є відношенням двох кутів, утворених перетином двох відрізків у вершині апроксимуючого графу. Відповідно до визначення цього параметра останній визначають у діапазоні величин [0,1]. Інтерпретація граничних значень η у межах графічного образу така. Якщо $\eta=1$, то два кути однакові і це означає, що величина кута в деякому фрагменті графічного образу є максимальною. З погляду графічного образу це означає, що віддаль між двома променями кута є максимально можлива. Якщо $\eta\approx1$, то це означає, значення більшого кута, яке у відповідному співвідношенні потрапляє до знаменника, наприклад кут α_{i+1}, є набагато більше від значення кута, яке потрапляє до чисельника, або $\alpha_{i+1} \rangle\rangle \alpha_i$. Це приводить до того, що $(\alpha_i/\alpha_{i+1}) \to 0$ і тоді $\eta=0$. У графічній інтерпретації це означає, що два промені меншого кута розміщуються на досить близькій віддалі один від одного, що ускладнює підробку засобу захисту. Тому параметр η також можна вважати пороговим параметром, значення якого потрібно забезпечити. Тоді величину стійкості в частині цього параметра можна визначити величиною відхилення η_i від величини η_p, або можна записати, що $(\eta_{pi}-\eta_i) \le \delta\eta_i$. Графічна інтерпретація цього параметра захисту полягає у тому, що для заданого рівня стійкості Ω за параметром η_i мінімальний кут у вершині повинен бути не більший ніж та його величина, яка приводить до величини параметра насиченості, яка є меншою ніж його порогова величина $\delta\eta_i$.

Аналогічним є випадок, коли йдеться про міру насичення із використанням складної сітки системи координат.

Параметр зміни роздільності χ, впродовж суміжних ліній в заданому фрагменті, який визначають через параметр μ, в дискретній формі опису подає співвідношення між різними величинами міри роздільності, які визначають для послідовних точок суміжних ліній. Тому спосіб вимірювання цього параметра є аналогічним до способу вимірювання параметра роздільності. З погляду геометричної інтерпретації цей параметр визначає напрямок наближення до місця перетину двох суміжних ліній, якщо $\chi\neq0$ і не змінює знак на протилежний.

Локальна густина γ є інтегральним параметром, що характеризує в середньому всі наведені вище параметри у межах окремого фрагмента графічного образу. Цей параметр має досить важливу функцію визначення стратегії ідентифікації документа. Завдяки використанню цього параметра існує можливість детальнішої перевірки інших параметрів у вибраному фрагменті образу під час ідентифікації документа.

Загальний вираз для однієї з можливих функцій f_B можна записати у вигляді:

$$\Omega = \sum_{i=1}^{n} \sum_{j=1}^{k} \left[\left(\alpha_j X_{Bji} \right) / k \right], \qquad (2)$$

де α_j – коефіцієнт активності використання j-го засобу захисту, під час протидії атакам; X_{Bij} – параметри, які характеризують; k – кількість параметрів, що використовують для опису засобу захисту у межах одного фрагмента; n – кількість фрагментів, яку виділяють у графічних образах для здійснення контролю та виявлення атаки на документ під час його ідентифікації.

На якісному рівні загрози можна інтерпретувати так. Якщо взяти параметр захисту μ, який передбачає визначення віддалі між суміжними лініями в заданій точці, то загрозу визначає можлива неточність вимірювання цієї віддалі. Така неточність може зумовлюватися неточністю друкування цих ліній, що є складовими засобу захисту, можливостями точності засобів вимірювання такої віддалі, наприклад, параметра точності відтворення пристрою сканування, використовуваного для цієї мети, точності вибору точок, в яких здійснюється вимірювання, та іншими факторами, визначеними середовищем, в якому функціонує документ. Більше того, в процесі функціонування документа величина параметрів загроз може змінюватися, в основному, у бік збільшення, що інтерпретується як фактор, який приводить до пониження рівня захисту. Оскільки функцію $\Omega_N = f_N(X_{N1},..., X_{Nm})$, яка характеризує міру податливості до атак, опишемо в загальному вигляді, то немає необхідності детально розглядати кожний фактор, що визначає загрозу. Це обумовлено тим, що такі фактори детально описують під час розроблення методики контролю в кожному конкретному випадку. До параметрів, що описують технічні особливості загроз, належать параметри, які описують статистичні дані про кількість успішних та неуспішних або викритих атак, кількість подій ідентифікації документів, які передбачено технологією їхнього використання, кількість параметрів захисту, завдяки використанню яких вдалося виявити атаки та типи відповідних параметрів. На основі таких статистичних даних не тільки модифікують методики, що реалізуються у межах інформаційної технології, а й визначають ризик використання документів за кожний інтервал часу використання системи ідентифікації документів. Методи обчислення статистичних даних про результати, що стосуються виявлених та невиявлених атак, ґрунтуються на використанні понять про дерева подій та дерева загроз, які відображають логіко-ймовірнісні залежності між послідовностями факторів, що обумовлюють відповідні події та використовують ті чи інші загрози [6]. Отже, до співвідношення для $\Omega_N = f_N(X_{N1},..., X_{Nm})$ можна вводити параметри, отримані на основі статистичних даних про історію використання засобів захисту. Як правило, у межах методик обчислення статистичних даних про успішні та виявлені атаки, що ґрунтуються на використанні логіко-ймовірнісних дерев, обчислюють величини ризику успішного здійснення атаки на основі використання ймовірних моделей оцінки відповідних подій. Тому не вводимо до функції Ω_N складові, що відображають результати аналізу статистичних даних про події, які виникли відносно документів і які також характеризують такі параметри, як ризик використання документів. Логіко-ймовірнісний підхід у межах цієї технології використовуємо відповідно до відомих методик його реалізації [5], а обчислені величини ризику R_s – для аналізу адекватності величини ризику R, який обчислюється на основі локальних параметрів, що характеризують міру захищеності та величини загроз засобам захисту.

Розглянемо можливі способи реалізації функції F у співвідношенні $R = F(\Omega, \Omega_N)$. Виходячи з загальних уявлень про Ω і Ω_N, можна стверджувати, що параметри, які визначають Ω і Ω_N, взаємно доповнюють один одного. Це означає, що наскільки точними є вимірювання параметрів захисту, настільки менший ризик невиявлення атаки на документ, що стосується параметрів, які мають безпосередню графічну інтерпретацію, наприклад, параметри μ і η. З іншого боку, чим більші за

своїм значенням параметри, що визначають загрози, тим менший ризик. Враховуючи загальне співвідношення для Ω, можна записати таку залежність для визначення величини ризику R:

$$R = a\sum_{i=1}^{n}\left\{\left[\sum_{j=1}^{k}\left[\left(\alpha_j X_{Bij}\right)/k\right]\right]/\left[\sum_{j=1}^{m}\left[\left(\beta_j X_{Nij}\right)/m\right]\right]\right\}, \quad (3)$$

де a – коефіцієнт нормування величини R; β_j – коефіцієнт, аналогічний коефіцієнту α_j для X_{Bi}; X_{Nij} – параметри загроз, що існують у засобах захисту; m – кількість параметрів загроз.

Величина загрози використання захищених документів прямо пропорційна до точності, з якою ідентифікуються документи і обернено пропорційна до точності відображення, або точності реалізації параметрів захисту, що інтерпретуються як параметри загроз.

Доцільність використання ризику типу R, який визначають на основі аналізу параметрів засобів захисту та параметрів загроз, та ризику типу R_s, що визначається на основі статистичних даних про виявлені та невиявлені атаки, ґрунтується на тому, що розбіжності між величинами цих двох параметрів використовують для визначення необхідності здійснення керівних дій, орієнтованих на заміну параметрів засобів захисту та параметрів загроз. Необхідність ініціації управління рівнем захисту та рівнем загроз у системі ідентифікації документів визначають за співвідношенням між R і R_s:

$$\left|R - R_s\right| \le \delta R, \quad (4)$$

де δR – допустима величина відхилення між величинами ризику, визначена за параметрами засобів захисту чи параметрів загроз та величиною ризику, визначеною на основі аналізу успішних та невдалих атак. Оскільки керувати величиною ризику відносно параметрів захисту можна у двох напрямках: підвищення рівня захисту та його пониження, наведене вище співвідношення запишемо так:

$$\left\{\left[\left(R_s - R\right)\rangle 0\right] \to \left[U(R) = \varphi(\Omega + \Delta\Omega)\right]\right\} \vee \left\{\left[\left(R_s - R\right)\langle 0\right] \to \left[U(R) = \varphi(\Omega - \Delta\Omega)\right]\right\}, \quad (5)$$

де $U(R)$ – функція управління ризиком; $\varphi(\Omega+\Delta\Omega)$ – функція, котра реалізує необхідну міру підвищення стійкості засобів захисту шляхом збільшення значень параметрів засобів захисту; $\varphi(\Omega-\Delta\Omega)$ – функція, котра реалізує зменшення величин параметрів засобів захисту, що приводить до зменшення стійкості засобів захисту відносно можливих атак.

Додаткові методи захисту

Виділенням окремих фрагментів у графічному образі для ідентифікації його у межах інформаційної технології можна істотно зменшити необхідну для цього кількість операцій. Відповідно до сюжету узору в певних його місцях такі параметри, як віддаль між співбіжними кривими, яка є мірою роздільності, чи насиченість в точці перетину ліній, можуть не збігатися з тими їх величинами, які вимагаються з погляду забезпечення певної стійкості засобів захисту. Це приводить до виникнення суперечностей між сюжетом узору і вимогами до засобів захисту. Розв'язання такої суперечності, яка може спотворювати сюжет графічного образу, полягає в тому, що граничні значення параметрів засобів захисту в різних фрагментах можна змінювати так, щоб графічний образ не спотворювався, а тільки модифікувався залежно від вимог до забезпечення того чи іншого рівня захисту. В цьому випадку говорять про появу додаткового параметра захисту, який визначає номер фрагмента рисунка, який є окремим, або локальним засобом захисту. Доцільність такого подання графічних образів як засобів захисту зумовлюється ще і тим, що графічні засоби захисту у вигляді узорів досить часто використовують для створення фону всієї поверхні, на якій друкують текст документа. Тоді задруковані фрагменти графічного образу досить складно аналізувати під час проведення ідентифікації. Такого типу графічні засоби захисту документів називають дискретними графічними засобами захисту.

Завдяки використанню дискретних графічних засобів захисту з'являється можливість використовувати такі додаткові параметри захисту:

- номер фрагмента, який є графічним засобом захисту;

- міра узгодженості сюжету графічного образу з дискретними елементами графічних засобів захисту;
- порядок використання відповідних фрагментів засобу захисту в процесі ідентифікації.

Оскільки всю площину документа, заповнену графічним засобом захисту або графічним образом, розміщено в певній системі координат, яка може мати різну структуру, то, відповідно до цієї структури, на площині документів виділяють фрагменти графічного образу, які являють собою дискретну форму засобів захисту. Відповідно до цієї структури встановлюється нумерація фрагментів, які виділяються як елементи засобу захисту. У цьому випадку номер чергового фрагмента, який є дискретним елементом засобу захисту, є прихованою інформацією від не уповноважених учасників технологічного процесу системи документообігу.

На деякому інтервалі існування двох співбіжних кривих віддаль між ними відповідно до сюжету графічного образу змінюється відповідно до співвідношення, яке можна запозичити з визначення параметра зміни роздільної здатності $\chi = d\mu(L_i, L_{i+1}) / dL_i = \beta_i$. Це означає, що для кожної одиниці довжини двох ліній визначено величину зміни віддалі між цими кривими. Цю зміну віддалі під час проектування графічного образу визначає його сюжет. Нехай фрагмент засобу захисту графічного образу $\varphi_i(z)$ містить частину цих ліній і відповідно до вимог стійкості $\Omega_i[\varphi_i(z)]$, віддаль між лініями L_i і L_{i+1} у фрагменті $\varphi_i(z)$ має бути не більшою ніж β_i^z. При цьому $(\beta_i^z - \beta_i) \neq 0$, а справедливе $(\beta_i^z - \beta_i) = \delta\beta_i$. Тоді виникає суперечність між вимогами сюжету до розміщення фрагмента ліній L_i і L_{i+1} між собою та вимогами міри стійкості до засобів захисту, які визначають необхідну віддаль як β_i^z. Для розв'язання цієї суперечності вводять поняття узгодженості сюжету графічного образу. У нашому випадку параметром узгодженості є допустима модифікація віддалі між лініями, яка не змінює сюжет. Цю міру допустимої модифікації узору визначають на етапі проектування образу, і процес визначення міри узгодженості має евристичний характер. Суть евристичного методу ґрунтується на визначенні таких модифікацій як допустимих, які не приводили б до виникнення ефекту появи аномальних фрагментів у відповідному образі. Аномальність полягає у такій зміні геометричних параметрів деякого фрагмента, за якої величини цих геометричних параметрів істотно відрізняються від відповідних величин геометричних параметрів фрагментів, що оточують модифікований фрагмент.

Можливість використання впорядкованості фрагментів як параметра засобу захисту, обґрунтовується так. Якщо б, наприклад, такий параметр, як міра роздільності для всіх фрагментів дискретного засобу захисту був однаковий, то це істотно понизило б рівень захищеності, який забезпечує відповідний графічний засіб захисту. Тому для різних графічних фрагментів дискретного засобу захисту встановлюють різні значення гранично допустимих величин параметрів захисту. Очевидно, що для графічних образів діапазон графічних значень є різним, але завжди визначеним. Наприклад, приймемо, що цей діапазон задано як $[\beta^z_{max}, \beta^z_{min}]$. Відповідні величини граничних значень, або величини порогів, β_i^z задаються дискретно у межах цього діапазону. Це означає, що, наприклад, в діапазоні $[\beta^z_{max}, \beta^z_{min}]$ можна вибрати тільки r-значень величини порогу для відповідного параметра захисту. Оскільки геометричні параметри за своєю інтерпретацією близькі між собою, наприклад μ і χ, то для них у межах діапазону можна задати однакову кількість величин для визначення допустимих порогових значень. У цьому випадку кількість порогових величин навіть для одного параметра можна вважати основою для подання чисел. Якщо таких порогів тільки два, то основою подання чисел є двійкова система і т. д. аж до десяткової системи подання чисел. Тоді окрему величину порогу можна інтерпретувати як окремий розряд запису числа у відповідній системі числення. Оскільки фіксована кількість порогів визначається на етапі проектування графічного засобу та засобів захисту, то кількість допустимих порогових значень для різних типів параметрів захисту є відомою, як і конкретний поріг для чергового фрагмента засобу захисту. Доцільно вибір того чи іншого порогу підпорядкувати необхідності запису певного числа в межах певної кількості фрагментів захисту. Кількість фрагментів захисту, вибраних для запису того

чи іншого числа, може визначатися кількістю величин порогових значень параметра захисту в заданому діапазоні. Це, в своєю чергою, визначає основу числа, яке мають записати.

Розроблення алгоритму управління ризиком

Розглянемо функціональну блок-схему підсистеми управління величиною ризику використання захищених документів. У межах цієї підсистеми використовують функції визначення величини ризику, ідентифікації документів та зміни міри стійкості документів до атак. Така блок-схема підсистеми управління величиною ризику наведена на рисунку з такими позначеннями:

ВІД – виконання ідентифікації документа;

ОВР – обчислення величини ризику конструктивного типу, яку визначають за параметрами захисту;

ФЗПЗ – формування загального параметра захисту документів за конструктивними параметрами захисту графічних засобів;

ЛПЗ – вибір локального параметра захисту;

МЗЗП$_i$ – модифікація засобу захисту за *i*-м параметром захистома

ФОАД – формування ознаки атаки на документ;

P_i:i=i+1 – вибір чергового параметра захисту;

НЗІД – нормальне завершення ідентифікації документа;

АЗР – аварійне завершення роботи з реєстрацією виявленої атаки на документ;

УЗР – умовне завершення роботи через високий ризик використання документа;

$R_s \le R$ – перевірка, чи статистичний ризик менший від ризику конструктивного;

$R \le \delta R$ – перевірка умови, чи конструктивний ризик не перевищує заданої величини ризику;

$П_к \le П_п$ – перевірка умови, чи поточний конструктивний параметр захисту менший від заданого порогового значення цього параметра;

$П_л = 0$ – перевірка умови, чи за всіма локальними параметрами захисту проведено пороговий контроль;

$i \le П_з$ – перевірка умови, чи всі параметри захисту документа аналізувались;

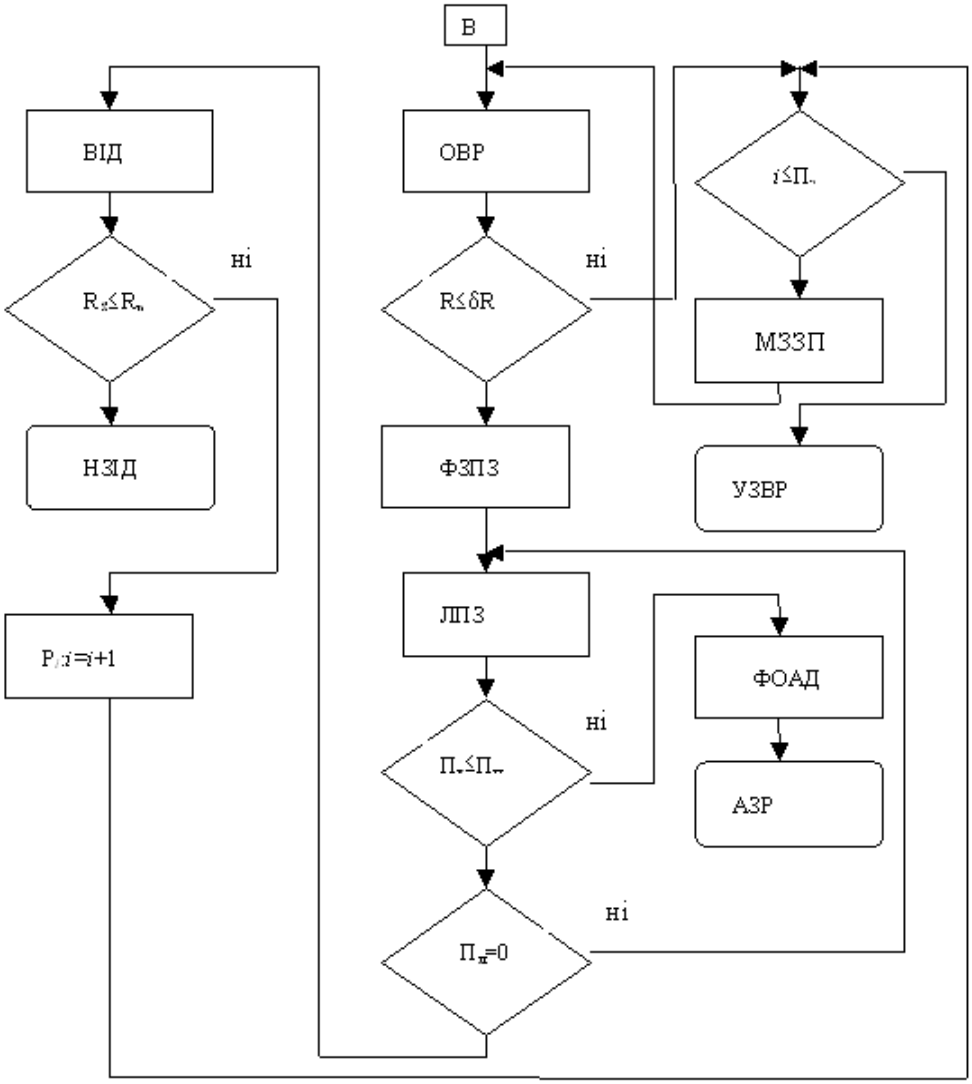
В – вхідна точка підсистеми управління величиною ризику використання документа.

Оскільки у цьому випадку йдеться про паперові документи, то необхідно детальніше прокоментувати процес управління ризиком використання документів. Насамперед треба зазначити, що система і відповідно, інформаційна технологія ідентифікації документів, на основі якої створено систему, складається з таких функціональних систем:

- системи управління і виготовлення документа;
- системи використання та ідентифікації документів.

Ці дві системи взаємозв'язані між собою і складаються з ряду підсистем, частина яких стосується інформаційної технології ідентифікації документів.

Початкове значення допустимого ризику визначає замовник документа, і систему захисту будують так, щоб вона забезпечувала необхідний рівень ризику. Формування системи управління ризиком починається з формування загального параметра захисту ФЗПЗ. Під час формування цього параметра перевіряють, чи конструктивний ризик не перевищує заданої замовником величини ризику ($R \le \delta R$). Якщо умова $R \le \delta R$ виконується за кожним параметром захисту, то формування загального параметра ФЗПЗ закінчується. Якщо ж умова $R \le \delta R$ не виконується хоча б за одним з параметрів, то модифікується засіб захисту за *i*-м параметром МЗЗП$_i$. Після цього за всіма локальними параметрами захисту (ЛПЗ) перевіряють умову, чи поточний конструктивний параметр захисту менший від заданого порогового значення цього параметра ($П_к \le П_п$). Невиконання умови $П_к \le П_п$ хоча б за одним з параметрів захисту означає появу атаки на документ (ФОАД), і робота підсистеми завершується в аварійному випадку (АЗР).



Функціональна блок-схема підсистеми управління ризиком використання документу

Коли документ вже виготовлено і він потрапляє до споживача, то перш за все використовують систему ідентифікації документів. У результаті ідентифікації виявляють атаку на документ або перевіряють, чи документ не є підробленим. У цій системі виявляються також атаки, які були успішними. За допомогою аналізу досягнення мети сформульовано в документі. На основі таких даних за певний період використання документів розраховують статистичний ризик, який відображає об'єктивний інтерес до документів не уповноважених осіб. Якщо статистичний ризик R_s більший від величини конструктивного ризику $R_к$, обчисленого на основі аналізу параметрів захисту, то для наступного тиражу цього типу документів засоби захисту модифікують так, щоб $R_s \leq R_к$. Якщо в процесі експлуатації виявилося, що R_s значно менше за $R_к$, то у наступному тиражі цього типу документів зменшується рівень стійкості засобів захисту незалежно від вимог замовника.

Висновки

Внаслідок реалізації логіко-математичних процедур, пов'язаних з формуванням дискретних графічних засобів захисту, появляється можливість вписувати до засобів захисту певні числа, подані у вибраній системі числення. Цю можливість можна розвинути до вписування в графічний образ в закодованому вигляді окремих речень чи фрагментів текстів, які, з погляду забезпечення стійкості текстів та стійкості засобів захисту документів, можуть мати додаткові функції захисту документів. Очевидно, що прочитати так закодований або захований текст можна лише у межах

інформаційної системи ідентифікації документів, оскільки тільки ця система містить всю необхідну інформацію про порогові значення параметрів захисту, про кількість допустимих порогових значень, що можуть бути заданими у визначеному діапазоні та інформацію про порядок нумерації фрагментів. Для того, щоб показати безпосередню функцію захисту, яка реалізується шляхом використання так закодованих текстів, необхідно розглянути безпосередню взаємодію засобів захисту з атаками на документи, які ініціюються відповідними небезпеками.

Запропонований у роботі алгоритм функціонування системи управління ризиком використання документів дає змогу виявляти атаки на документи на всіх етапах технологічного процесу їхнього використання, а також керувати ризиком використання документів шляхом підвищення або зниження стійкості засобів захисту до атак. Використання запропонованої системи забезпечує оптимальну стійкість документів до атак. Отримані залежності між параметрами елементів захисту і технологічних процесів можна застосовувати для моделювання динаміки системи захисту та керування даними. Таку систему управління ризиком використання документів можна застосовувати як елемент автоматизованої системи управління документообігом.

1. Копшин А.А. Защита полиграфической продукции от фальсификации. – М.: ООО "Синус", 1999. 2. Давиденко А.М., Головань С.М., Щербак Л.М. Процес оцінки безпеки документообігу: Зб. наук. праць ІПМЕ НАН України. – 2005. – Вип. 31. – С. 30–34. 3. Современные технологии анализа рисков в информационных системах. – М.: Компютерная неделя, 2001. – № 37(307). 4. Андрианов В.В., Зефиров С.Л. Защит информационных технологий. – Пенза: Изд-во Пенз. гос. техн. ун-та, 1997. – 31 с. 5. Вентцель Е.С. Теория случайных процессов и её инженерные приложения. – М.: Наука, 1990. 6. Хенли Э.Дж., Кумамато Х. Надёжность технических систем и оценка риска. – М.: Мир, 1984.

УДК 004.8

Ю. Нікольський
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

ЗАСТОСУВАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ АНАЛІЗУ СИТУАЦІЙ З МЕТОЮ ВИЯВЛЕННЯ ПЕРЕДУМОВ СПРАЦЮВАННЯ ЗАХИСТІВ НА ЕНЕРГОБЛОКАХ

Запропоновано загальний підхід до моделювання інформаційного об'єкта та принципи побудови системи прийняття рішень у випадку прогнозування спрацювання захистів на електростанціях. Побудовано алгоритми попереднього аналізу потоків інформації з метою конструювання нейромережі для прийняття рішень.

The general approach to modeling the information objects and the principles of building the making decision system for forecasting the defense systems making at the power-stations is proposed. The special algorithms of preliminary information flow analysis were built by applying the neural network.

Постановка проблеми у загальному вигляді

Мета виконаного дослідження полягає у розробленні математичної моделі прийняття рішень про локалізацію місця виникнення та початкових стадій розвитку ситуацій, що спричиняють спрацювання систем захисту енергоблоків теплових та атомних електростанцій. Результатом цих досліджень є розроблення засобів попередження персоналу про розвиток ситуацій та їхню