© Korchenko A., Davydenko A., Shaban M., Kazmirchuk S. Structural model of the DSS for the State Examination of the IISS // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 1, pp. 14-27.

DOI: 10.18372/2225-5036.26.14666

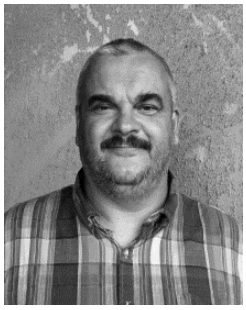
СТРУКТУРНА МОДЕЛЬ СППР ПРИ ПРОВЕДЕННІ ДЕРЖАВНИХ ЕКСПЕРТИЗ КСЗІ

Анна Корченко[2], Анатолій Давиденко[1], Максим Шабан[1], Світлана Казмірчук[2]

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова
[2]Національний авіаційний університет

КОРЧЕНКО Анна Олександрівна, д.т.н., доцент

Рік і місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, системи виявлення вторгнень, експертне оцінювання в сфері захисту інформації.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: annakor@ukr.net.
Orcid ID: 0000-0003-0016-1966.



ДАВИДЕНКО Анатолій Миколайович, к.т.н, с.н.с

Рік та місце народження: 1964 рік, м. Іркутськ, РФ.
Освіта: Національний авіаційний університет, 1986 рік.
Посада: пров.наук.спів. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, Україна з 2019 року.
Наукові інтере си: інформаційна безпека, прикладне програмування, грід-обчислення.
Публікації: більше 160 наукових публікації, серед яких наукові статті, тези і матеріали доповідей на конференціях.
E-mail: davidenkoan@gmail.com.
Orcid ID: 0000-0001-6466-1690.

ШАБАН Максим Радуйович

Рік та місце народження: 1988 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: інженер Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, Україна.
з 2017року.
Наукові інтереси: інформаційна безпека, прикладне програмування, грід-обчислення.
Публікації: більше 15 наукових публікації, серед яких наукові статті, тези і матеріали доповідей на конференціях.
E-mail: maximsaban@gmail.com.
Orcid ID: 0000-0003-2706-8235.

КАЗМІРЧУК Світлана Володимирівна, д.т.н.

Рік та місце народження: 1985 рік, м. Алмати, Казахстан.
Освіта: Національний авіаційний університет, 2006 рік.
Посада: зав. кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
Наукові інтереси: інформаційна безпека, системи менеджменту інформаційної безпеки, захист програмного забезпечення, комплексні системи захисту інформації, управління інформаційними ризиками.
Публікації: більше 90 публікацій, серед яких монографії, навчальні посібники, навчально-методичні комплекси дисциплін, наукові статті, матеріали та тези доповідей конференцій.
E-mail: sv.kazmirchuk@gmail.com.
Orcid ID: 0000-0001-6083-251X.

Анотація. *Процес проведення державних експертиз комплексних систем захисту інформації (КСЗІ) та організація електронного обігу документів, створених на етапі проектних робіт мають низку проблем, а саме: уразливість інформації, яка зберігається на постійних носіях пам'яті; велику ентропію невизначеності інформації, що збільшує ризики помилок експерта при проведенні державних експертиз КСЗІ; проблема обігу паперових документів, які були створені на етапі предпроектних робіт, що збільшує ризики розкриття інформації з обмеженим доступом. Для вирішення зазначених проблем необхідно здійснити автоматизацію окремих процесів. Поставлена мета здійснюється шляхом розробки структурної моделі системи підтримки прийняття рішень (СППР) для реалізації експертиз КСЗІ, яка формується із взаємопов'язаних баз даних смислових змінних, множини критеріїв та шаблонів документів, а також модулів виокремлення смислових змінних, ідентифікації функціонального профілю захисту та взаємодії з експертом. Для реалізації структурної моделі був розроблений програмний застосунок, що підтримує два основних процеси: перший – пов'язаний з перевіркою відповідності функціонального профілю захисту (ФПЗ) вимогам НД ТЗІ; другий – орієнтований на виділення смислових змінних з вхідних документів та їх збереження у базі даних смислових змінних (БДСЗ). Зазначені рішення дозволяють розширити функціональні можливості сучасних СППР пов'язаних з реалізацією експертиз технічного захисту інформації.*

Ключові слова: *державні експертизи КСЗІ, функціональний профіль захисту, система підтримки прийняття рішень, функціональні послуги безпеки, НД ТЗІ 2.5-004-99, експертна оцінка.*

Вступ.

Досвід використання методів математичного моделювання та інформаційних технологій в різних сферах цілеспрямованої людської діяльності призвів до розуміння багатьох принципових труднощів, що виникають при їх впровадженні в реальну практику, складається з безперервної низки дій пов'язаних з прийняттям рішень. А врахуваючи, що експерт зазвичай оперує великими масивами інформації та широким спектром обмежень, яких необхідно дотримуватись, то стає очевидним, що для забезпечення ефективності процесу прийняття рішень необхідно створювати відповідні людино-машинні (імітаційні) системи. Одним з класів таких систем є системи підтримки прийняття рішень (СППР), в межах яких можливе застосування досвіду і неформалізованих знань експерта.

Процес проведення державних експертиз комплексних систем захисту інформації (КСЗІ) та організація документообігу документів, створених на етапі проектних робіт мають низку проблем, а саме: уразливість інформації, яка зберігається на постійних носіях пам'яті; велику ентропію невизначеності інформації, що збільшує ризики помилок експерта при проведенні державних експертиз КСЗІ; проблема обігу паперових документів, які були створені на етапі предпроектних робіт, що збільшує ризики розкриття інформації з обмеженим доступом. А тому, створення СППР, що відповідає вимогам НД ТЗІ є актуальним науковим завданням.

Для досягнення поставленої мети розробимо СППР, яка підтримується двома процесами: перший – пов'язаний з перевіркою відповідності ФПЗ вимогам [4]; другий – орієнтований на виділення смислових змінних $SV^{in}_{p,i,j,b}$ з вхідних документів $\mathbf{Doc^{in}_{p}}$ та їх збереження у БДСЗ. Далі, за участю експерта формуються шаблони вихідних документів $\mathbf{Doc^{out}_{SH}}$. Оскільки перший процес детально розглянуто у [2], то приділимо увагу опису другого.

Для формування групи вихідних документів [3] необхідно сформувати шаблони документів, виділити $SV^{in}_{p,i,j,b}$ з $\mathbf{Doc^{in}_{p}}$ та розробити алгоритм наповнення шаблонів $\mathbf{Doc^{out}_{SH}}$ відповідними змінними $SV^{in}_{p,i,j,b}$.

Для цього введемо множину всіх можливих шаблонів документів

$$\mathbf{Doc_{SH}} = \left\{ \mathbf{Doc^{in}_{SH}}, \mathbf{Doc^{out}_{SH}} \right\}, \quad (1)$$

де $\mathbf{Doc^{in}_{SH}}$, $\mathbf{Doc^{out}_{SH}}$ – відповідно підмножини шаблонів вихідних та вхідних документів множини $\mathbf{Doc_{SH}}$.

Використовуючи (1) сформуємо множину шаблонів вхідних документів

$$\mathbf{Doc_{SH}^{in}} = \left\{ \bigcup_{k=1}^{v} Doc_{SH,k}^{in} \right\} = \left\{ Doc_{SH,1}^{in}, Doc_{SH,2}^{in}, ..., Doc_{SH,v}^{in} \right\}, \quad (2)$$

де $Doc_{SH,k}^{in}$ – шаблон вхідного документу з k-м ідентифікатором, а v – кількість шаблонів ($k=\overline{1,v}$).

Наприклад, для проекта **ІПМЕ**, **НАУ** тощо, з урахуванням (2) при v=18, $k=\overline{1,18}$

$$\mathbf{Doc_{SH}^{in}} = \left\{ \bigcup_{k=1}^{18} Doc_{SH,k}^{in} \right\} =$$

$$\left\{ Doc_{SH,1}^{in}, Doc_{SH,2}^{in}, ..., Doc_{SH,18}^{in} \right\} = \left\{ Doc_{SH,ПФ}, Doc_{SH,ТЗ}, .., Doc_{SH,ППВ} \right\}, \quad (3)$$

де $Doc_{SH,1}^{in} = Doc_{SH,ПФ}$, $Doc_{SH2}^{in} = Doc_{SH,ТЗ}$, $Doc_{SH,3}^{in} = Doc_{SH,ПЗТП}$, $Doc_{SH,4}^{in} = Doc_{SH,НАБ}$, $Doc_{SH,5}^{in} = Doc_{SH,НК}$, $Doc_{SH,6}^{in} = Doc_{SH,АО}$, $Doc_{SH,7}^{in} = Doc_{SH,МЗ}$, $Doc_{SH,8}^{in} = Doc_{SH,МП}$, $Doc_{SH,9}^{in} = Doc_{SH,ПЗ}$, $Doc_{SH1,10}^{in} = Doc_{SH\,ІПМЕ,ПБ}$, $Doc_{SH,11}^{in} = Doc_{SH,ПСЗІ}$, $Doc_{SH,12}^{in} = Doc_{SH,АВДЕ}$, $Doc_{SH,13}^{in} = Doc_{SH,АЗДЕ}$, $Doc_{SH,14}^{in} = Doc_{SH,ЖДЕ}$, $Doc_{SH,15}^{in} = Doc_{SH,НВДЕ}$, $Doc_{SH,16}^{in} = Doc_{SH,НППВ}$, $Doc_{SH,17}^{in} = Doc_{SH,ПМПВ}$ і $Doc_{SH,18}^{in} = Doc_{SH,ППВ}$ – відповідно шаблони документів: «Паспорт-формуляр», «Технічне завдання», «Пояснювальна записка до технічного проекту»,. «Настанова адміністратора з безпеки», «Настанова користувача», «Акт обстеження», «Модель загроз», «Модель порушника», «План захисту», «Політика безпеки», «Положення про службу захисту інформації», «Акт про введення в дослідну експлуатацію», «Акт про завершення дослідної експлуатації», «Журнал дослідної експлуатації», «Наказ про введення в дослідну експлуатацію», «Наказ про проведення попередніх випробувань», «Програма та методика попередніх випробувань» і «Протокол попередніх випробувань» для проекта **ІПМЕ, НАУ** тощо.

З урахуванням (1) визначимо

$$\mathbf{Doc_{SH}^{out}} = \left\{ \bigcup_{i=1}^{z} Doc_{SH,i}^{out} \right\} = \left\{ Doc_{SH,1}^{out}, Doc_{SH,2}^{out}, ..., Doc_{SH,z}^{out} \right\}, \quad (4)$$

де $Doc_{SH,i}^{out}$ –шаблони вихідних документу, а z –кількість шаблонів ($i=\overline{1,z}$).

Наприклад, з урахуванням (4) при z=5, $i=\overline{1,5}$ для проекта **ІПМЕ**, **НАУ** тощо.

$$\mathbf{Doc_{SH}^{out}} = \left\{ \bigcup_{i=1}^{5} Doc_{SH,i}^{out} \right\} = \left\{ Doc_{SH,1}^{out}, Doc_{SH,2}^{out}, ..., Doc_{SH,5}^{out} \right\} = \quad (5)$$

$$\left\{ Doc_{SH,П}, Doc_{SH,М}, Doc_{SH,ПТ}, Doc_{SH,ЕВ}, Doc_{SH,ПВР} \right\},$$

де $Doc_{SH,1}^{out} = Doc_{SH,П}$, $Doc_{SH,2}^{out} = Doc_{SH,М}$, $Doc_{SH,3}^{out} = Doc_{SH,ПТ}$, $Doc_{SH,4}^{out} = Doc_{SH,ЕВ}$ та $Doc_{SH,5}^{out} = Doc_{SH,ПВР}$ – відповідно шаблони документів: «Програма проведення експертизи», «Методика проведення експертизи», «Перелік тестів», «Експертний висновок» та «Протокол виконання робіт» для проекта **ІПМЕ**, **НАУ** тощо.

Вхідні документи $\mathbf{Doc_p^{in}}$ представляються у відповідному форматі, що надає можливості щодо виділення в контексті $SV_{p,i,j,b}^{in}$.

Далі, побудуємо алгоритм (див. рис. 1) наповнення шаблонів вихідних документів смисловими змінними відповідних документів на основі створених $\mathbf{Doc_{SH}^{out}}$.

Робота алгоритму починається з почергового введення з бази даних шаблонів вихідних документів (БДШВД) усіх шаблонів вихідних документів множини $\mathbf{Doc_{SH}^{out}}$. Далі, завантажується з бази даних смислових змінних (БДСЗ) $SV_{p,i,j,b}^{out}$ та за участю експерта реалізується у визначеному порядку наповнення шаблонів вихідних документів.

Для реалізації вищезазначених процесів розробимо структурну модель СППР (див. рис. 2), яка складається з модулей: ідентифікації функціонального профілю захисту (ФПЗ) (МІФПЗ); виокремлення смислових змінних (МВСЗ); взаємодії з експертом (МВЕ). Також, до складу СППР входять бази даних (БД): БДСЗ; множини критеріїв (БДМК); БДШВД.

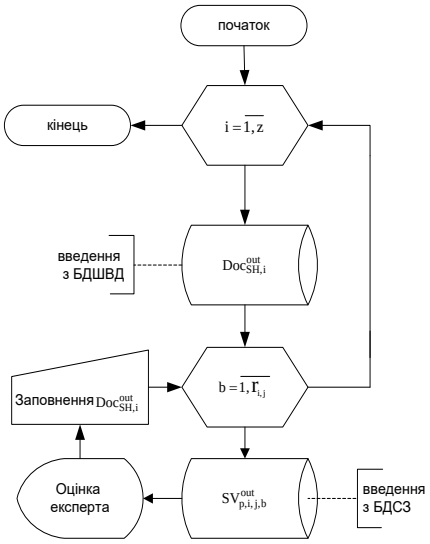


Рис. 1. Алгоритм заповнення шаблонів вихідних документів смисловими змінними

Модуль МВСЗ призначений для виокремлення $SV_{p,i,j,b}^{in}$ (див. (3) в [9]) р-го ($p=\overline{1,m}$, m – кількість можливих проектів) проекту з $\mathbf{Doc_p^{in}}$ відповідно до [3] шляхом інтерактивної взаємодії експерта з інтерфейсом СППР за допомогою низки інструкцій.

Модуль МІФПЗ за рахунок виділення $\mathbf{МК_{q,e,z}}$ з $\mathbf{Doc_p}$ реалізує процес ідентифікації функціонального профілю захисту (ФПЗ) $\mathbf{БЗ_p}$ (див. (12) в [2]) за допомогою п'яти кроків шляхом формування: 1) $\mathbf{МП_p}$ (див. (1) в [2]) функціональних послуг безпеки (ФПБ); 2) $\mathbf{МВ_p}$ (див.(3) в [2]) ФПБ; 3) множини об'єднання **(МО)** (див. (7) в [2]) ФПЗ в $\mathbf{МП_p}$ і $\mathbf{МВ_p}$; 4) $\mathbf{МО_p^{П}}$ (див. (9) в [2]) у вигляді множини порядку за індексами елементів $\mathbf{МК_{q,e,z}}$ ($z=\overline{1,w_{q,e}}$) (див. (1) в [1]); 5) $\mathbf{БЗ_p}$.

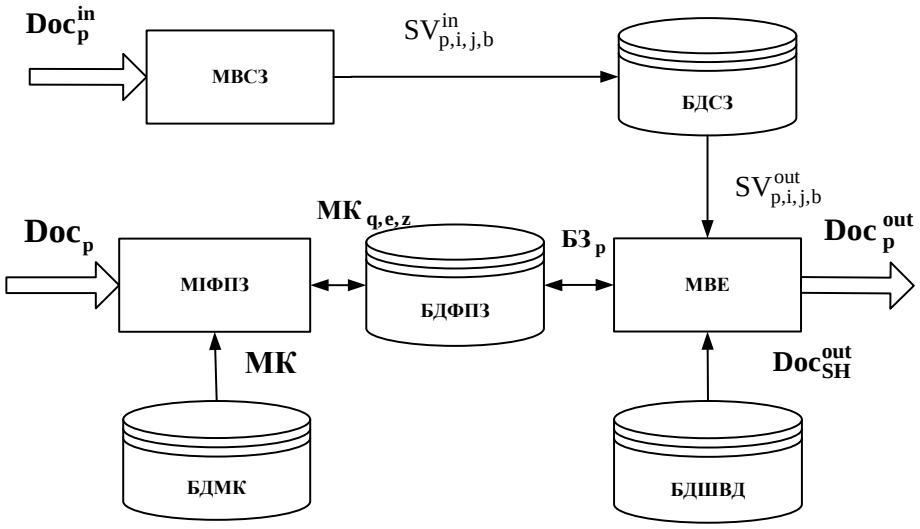


Рис. 2. Структурна модель СППР для реалізації експертиз КСЗІ

Модуль МВЕ призначений для наповнення (за участю експерта) шаблонів $\mathbf{Doc_{SH}^{out}}$ смисловими змінними $SV_{p,i,j,b}^{out}$, управління процесом генерування вихідних документів $\mathbf{Doc_p^{out}}$ з $\mathbf{Doc_{SH}^{out}}$ за допомогою відповідного інтерфейсу програми та аналізує $\mathbf{МК_{q,e,z}}$ виокремленого з $\mathbf{Doc_p}$.

База БДСЗ містить множину смислових змінних $SV_{p,i,j,b}^{out}$ (див. (3) в [9]), які були сформовані у процесі роботи модуля МВСЗ щодо виокремлення $SV_{p,i,j,b}^{in}$.

До складу БДМК входять елементи множини усіх критеріїв захищеності інформації [1] $\mathbf{МК_{q,e,y}}$, де $\mathbf{МК_{q,e,y}} \subseteq \mathbf{МК_{q,e}}$ ($y = \overline{1, w_{q,e}}$) – у-й рівень $\mathbf{МК_{q,e}}$-го елемента $\mathbf{МК_q}$-ї множини критеріїв, а $w_{q,e}$ їх максимальний рівень), які аналізує модуль МІФПЗ на предмет відповідності ФПЗ [4].

База БДШВД містить шаблони вихідних документів $\mathbf{Doc_{SH}^{out}}$, які мають у своєму складі смислові константи $SC_{p,i,j,a}^{out}$ (див. (3) в [9]), а також низку елементів, що становлять основу документа: графіка разом з призначеними атрибутами формату; параметри друкованої сторінки; список доступних стилів; макроси; елементи автотексту для вставки текстових або графічних фрагментів; панелі інструментів користувача; меню поєднання клавіш.

База БДФПЗ містить множину критеріїв $\mathbf{МК_{q,e,z}}$ для кожного проекту, які виокремлюються з множини документів $\mathbf{Doc_p}$. Далі, за допомогою експерта та МІФПЗ, відбувається перевірка $\mathbf{МК_{q,e,z}}$ вимогам [4] та складання $\mathbf{БЗ_p}$.

При проведенні державних експертиз КСЗІ відповідно до алгоритму функціонування СППР здійснюється за допомогою трьох процедур: виокремлення та запис смислових змінних $SV_{p,i,j,b}^{in}$ БДСЗ; формування контенту на основі смислових змінних і шаблонів $\mathbf{Doc_{SH}^{out}}$; ідентифікування функціонального профілю захисту.

Процес роботи починається з аналізу вхідних документів р-го проекту $\mathbf{Doc_p^{in}}$ на предмет наявності в них $SV_{p,i,j,b}^{in}$ (рис. 3, вершини 1-3). Якщо вони є, то відбувається відкриття БДСЗ та запис відповідних $SV_{p,i,j,b}^{in}$ у БД (рис. 3, вершини 4-5).

Далі, відбувається відкриття шаблонів вихідних документів (рис. 3, вершини 6-7) для формування контенту на основі відповідних смислових змінних (рис. 3, вершини 8-9). У результаті цього отримаємо вихідний документ р-го проекту $\mathbf{Doc_p^{out}}$ (рис. 3, вершина 10).

Наступним, здійснюється аналіз ФПЗ на предмет відповідності його формальним ознакам [4] та аналіз вихідного документа р-го проекту $\mathbf{Doc_p^{out}}$ на предмет наявності ФПЗ (рис. 3, вершини 11-13). Таким чином, за участю експерта формується $\mathbf{МП_p}$ для р-го проекту (див. рис. 3, вершину 14). Після створення групи ФПБ перевіряється наявність похідних від цих ФПБ (рис. 3, вершину 16). Якщо експертом прийнято рішення у сформованій **МВ** підвищити окремі рівні ФПБ (рис. 3, вершини 16-17), то з **МВ** вилучаються відповідні рівні елементів **МК** та об'єднуються з множиною значень табличної функції **ФПЕ** [2] від кожного з вилучених елементів. Далі, формується проміжна множина **МО**, що об'єднує **МП** і **МВ** (рис. 3, вершину 18), яка упорядковується за індексами $\mathbf{МО_p^{П}}$ (рис. 3, вершину 19) та мінімізується (рис. 3, вершина 20).

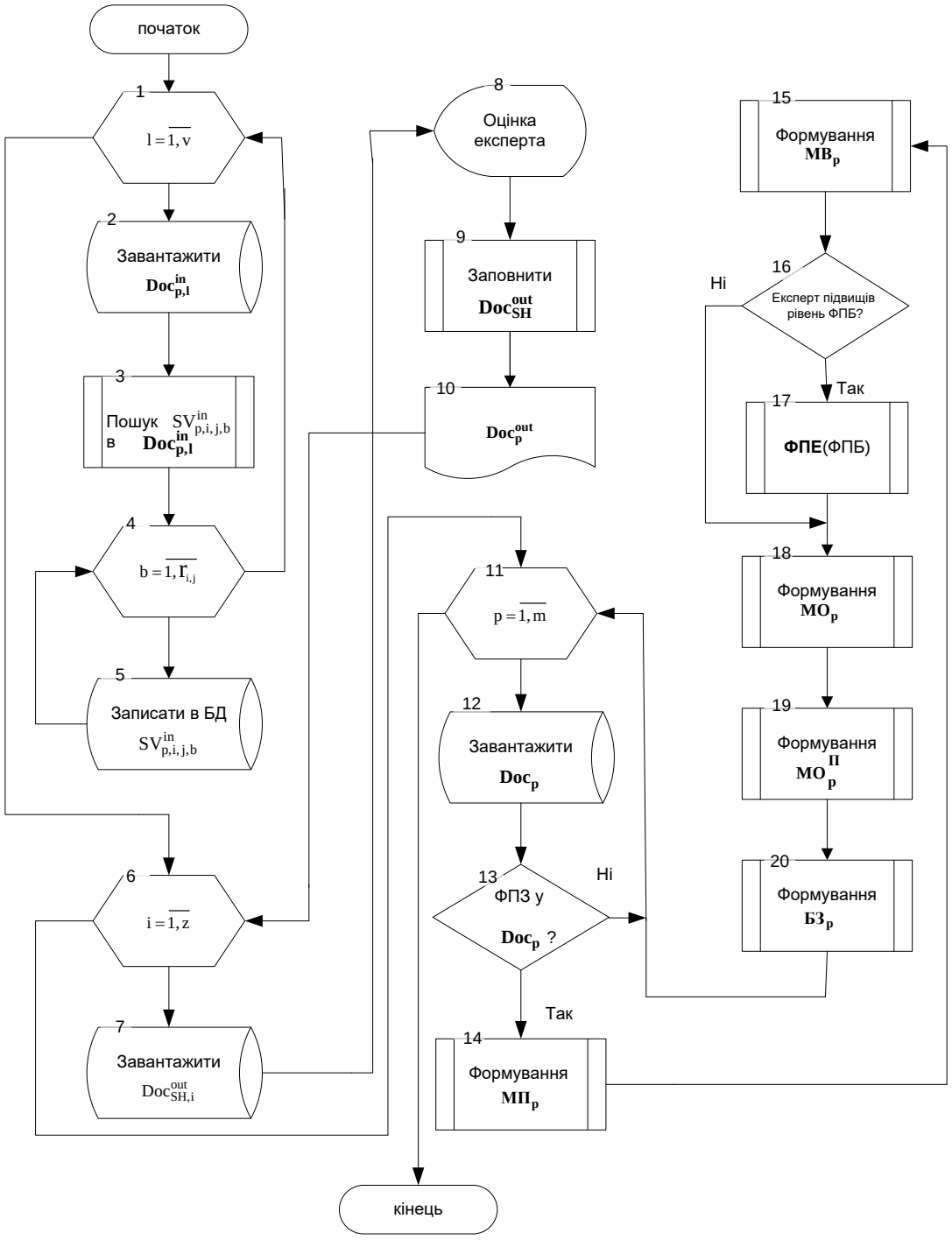


Рис. 3. Алгоритм роботи СППР при проведенні державних експертиз КСЗІ

Для реалізації МІФПЗ, з урахуванням моделі [1] та [2], розробимо алгоритмічне забезпечення, яке (відповідно до запропонованої структурної моделі СППР) можна застосовувати в процесі проведення державних експертиз КСЗІ (див. рис. 2]). Основою МІФПЗ є модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах [1]. В основу алгоритма реалізації МІФПЗ (рис. 4) закладено базовий клас DocumentEngine, що поєднує низку наступних зумовлених процесів (методів класу):

– RegularExpressionFind (Пошук $\mathbf{БЗ_p}$ $(p=\overline{1,m})$ та виклик FindNS, FindDuplicate, FindLinks);

– FindNS (Ініціалізація **МП ФПБ** (див. (1) в [2]) для НЦ рівня визначеного експертом. Відповідно до [4] ФПЗ повинен містити ФПБ НЦ рівня 1);

– FindDuplicate (Перевірка наявності в ФПЗ ФПБ, які повторюються (див. (11) в [2]). Реалізується шляхом мінімізації сформованої **МО** у вигляді множини порядку);

– FindLinks (Формування **МВ** (див. (3) в [2]) та перевірка наявності похідних елементів від $МП_{p,f}$).

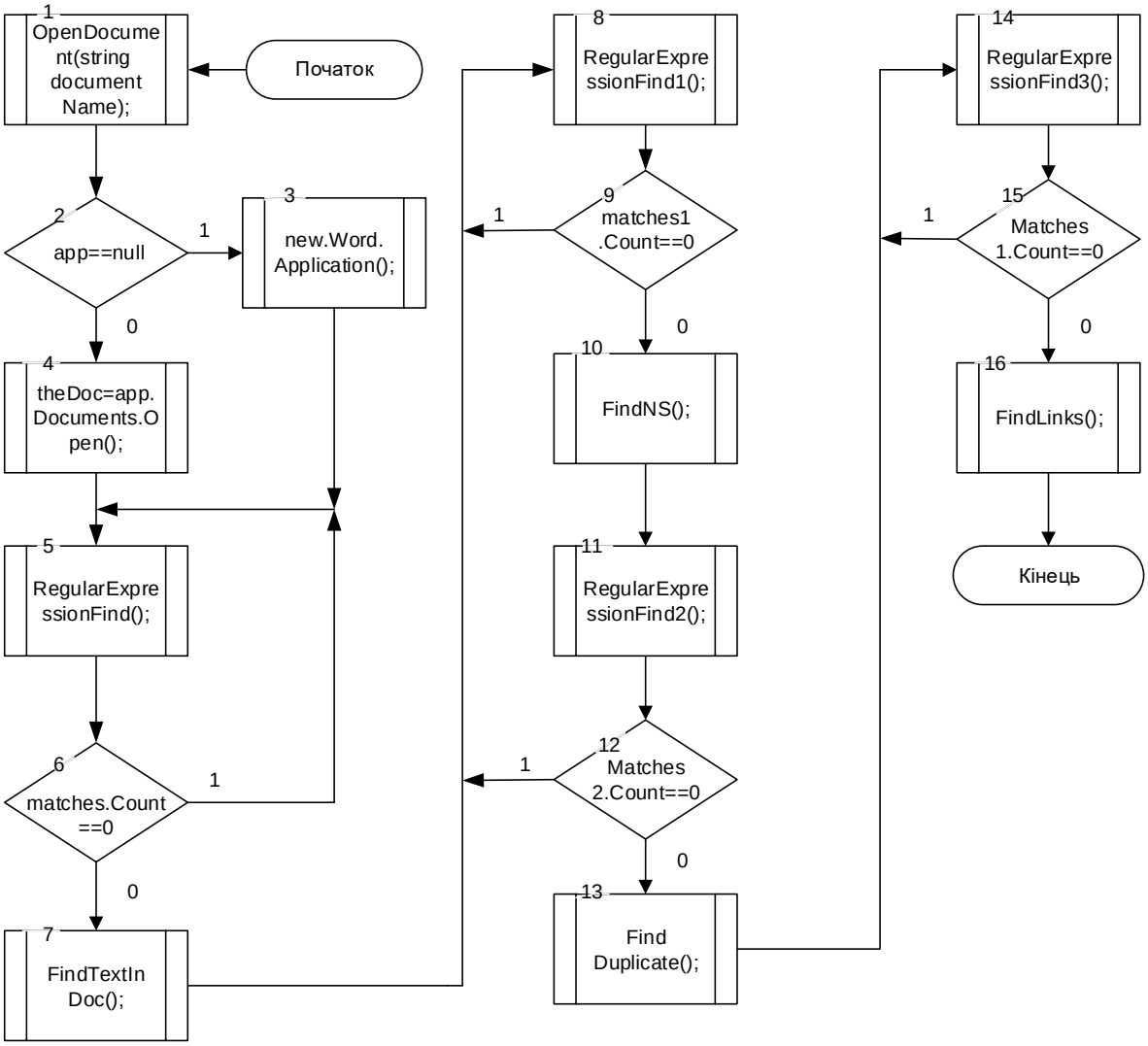


Рис. 4. Алгоритм реалізації МІФПЗ СППР

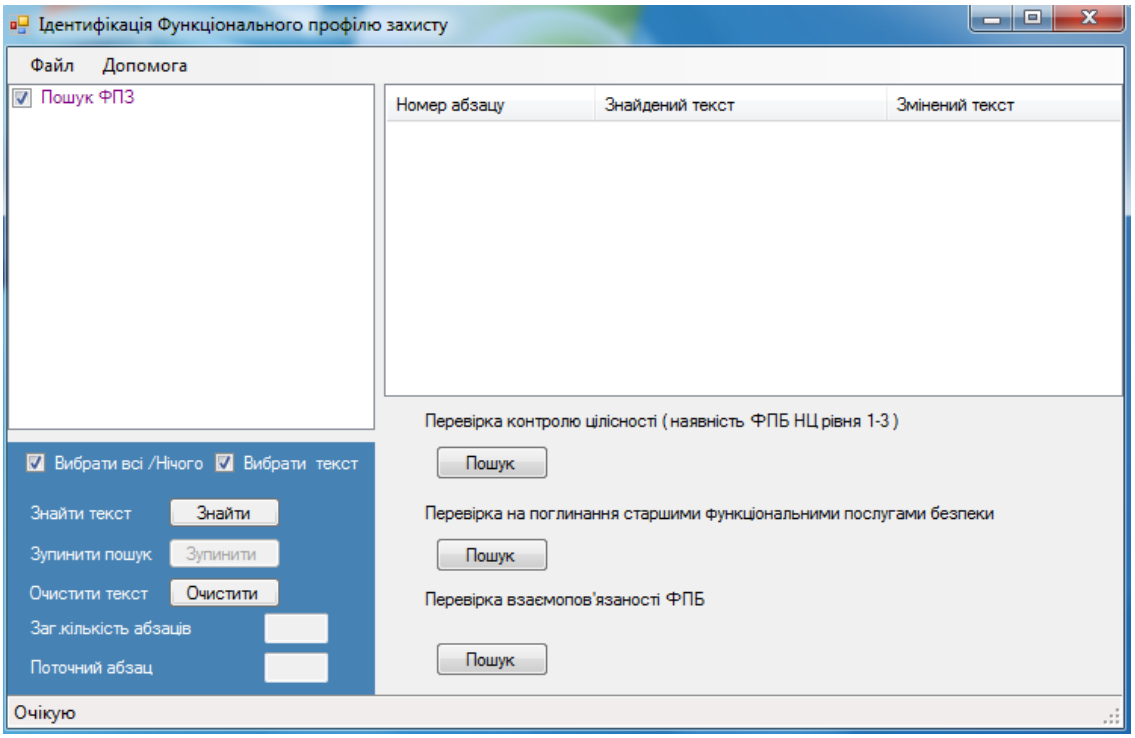


Рис. 5. Віконний інтерфейс модуля МІФПЗ СППР при проведенні державних експертиз КСЗІ

Відповідний програмний застосунок, що реалізує алгоритм на рис. 4 ініціює запуск графічного інтерфейса програми (рис. 5) за допомогою Main() (рис. 6).

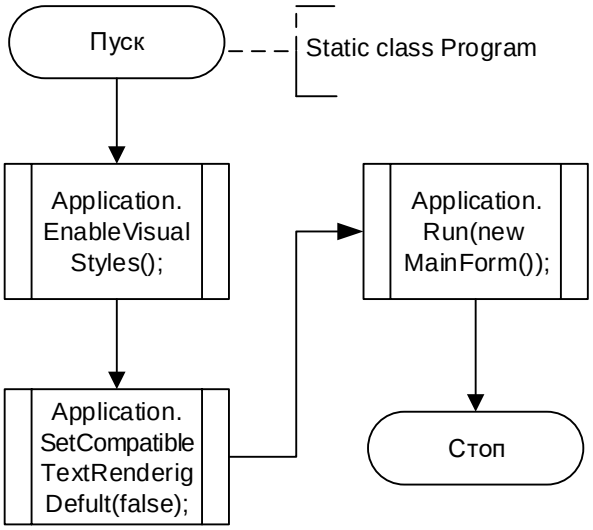


Рис. 6. Алгоритм реалізації Main() статичного класу Program

Далі, здійснюється пошук (рис. 8) ФПЗ в $\mathbf{Doc_p^{out}}$ (рис. 4, вершини 5, 8, 11 та 14) і за його результатами, експерт приймає рішення про подальші кроки щодо аналізу профіля (рис. 7).

Знайдений ФПЗ (рис. 9) відображається у графічному інтерфейсі програми і виділяється в $\mathbf{Doc_p^{out}}$ кольором (рис. 10).

Далі (рис. 4, вершина 10), відповідно до структури СППР (див. рис. 2) за участю експерта визначається необхідний НЦ рівень.

На наступному етапі (рис. 4, вершина 16) викликається FindLinks (рис. 14), який дозволяє перевірити наявність взаємопов'язаних ФПЗ отримавши дані з таблиць похідних елементів від $МП_{p,f}$ (див. табл. (1) в [2]).

Наприклад, необхідною умовою виконання ФПБ КД-2 є ФПБ НИ рівня 1 та вище (рис. 14).

Наступним (рис. 4, вершини 13), реалізується перевірка на наявність повторювань ФПБ у ФПЗ (рис. 15). Розглядаються два випадки: ФПБ з однаковим рівнем; ФПБ з різним рівнем.

Наприклад, якщо у профілі є: КД – 1, КД – 2, КД – 4, то відповідно до (див. (9) в [2]) залишиться КД – 4, а ФПБ з більш низьким рівнем будуть вилучені з ФПЗ (рис. 16).

Відповідно до запропонованої структурної моделі СППР здійснена програмна реалізація алгоритмічного забезпечення МІФПЗ, яка була застосована при проведенні державних експертиз КСЗІ. При створенні зазначеного програмного застосунка використовувалась мова програмування C# в середовищі розробки Visual Studio 2005, а при написанні програмного коду – технологія MS Office's COM Interop, а саме бібліотека Microsoft.Office.Interop.Word та базові бібліотеки мови програмування C#. Практичне використання програми, розробленої відповідно до структурної моделі (див. рис. 2), підтвердило теоретичні результати щодо пошуку (див. рис. 10) та аналізу (див. рис. 12, 13, 16) ФПЗ на предмет відповідності його формальним ознакам [4].

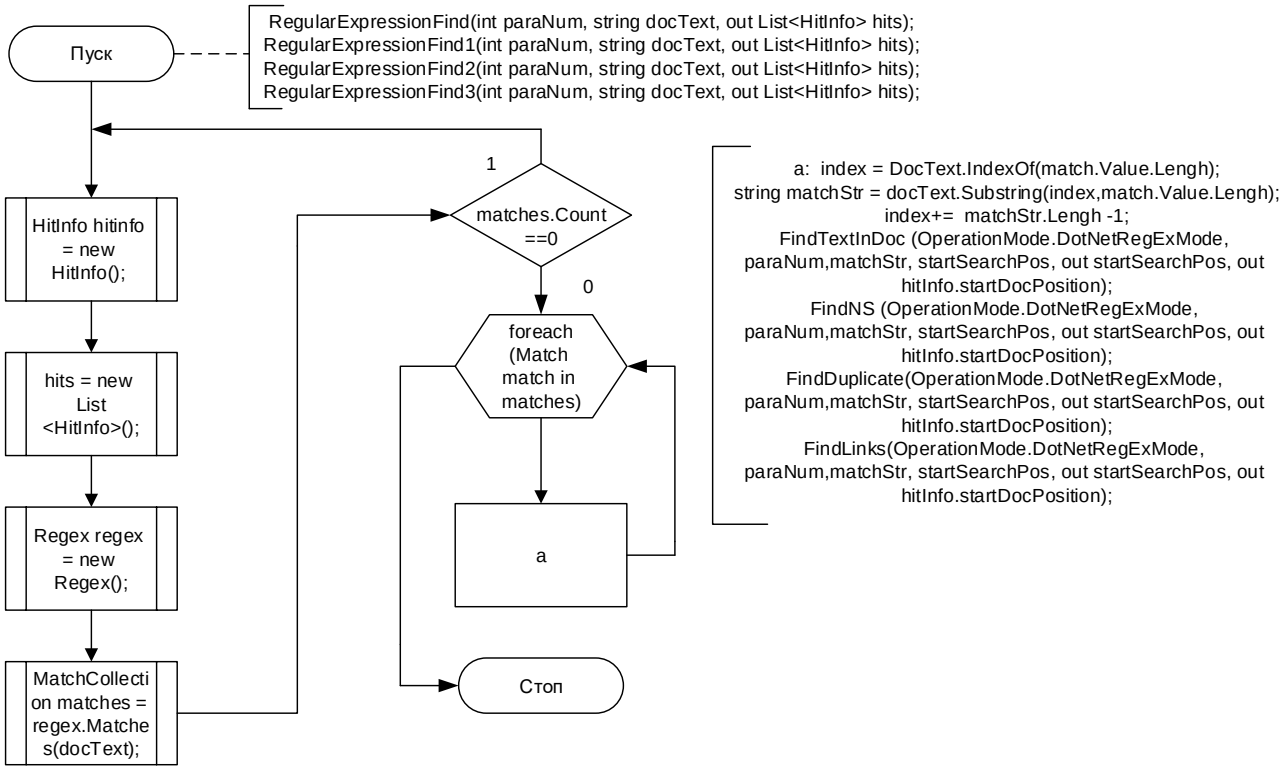


Рис. 7. Алгоритм реалізації RegularExpressionFind

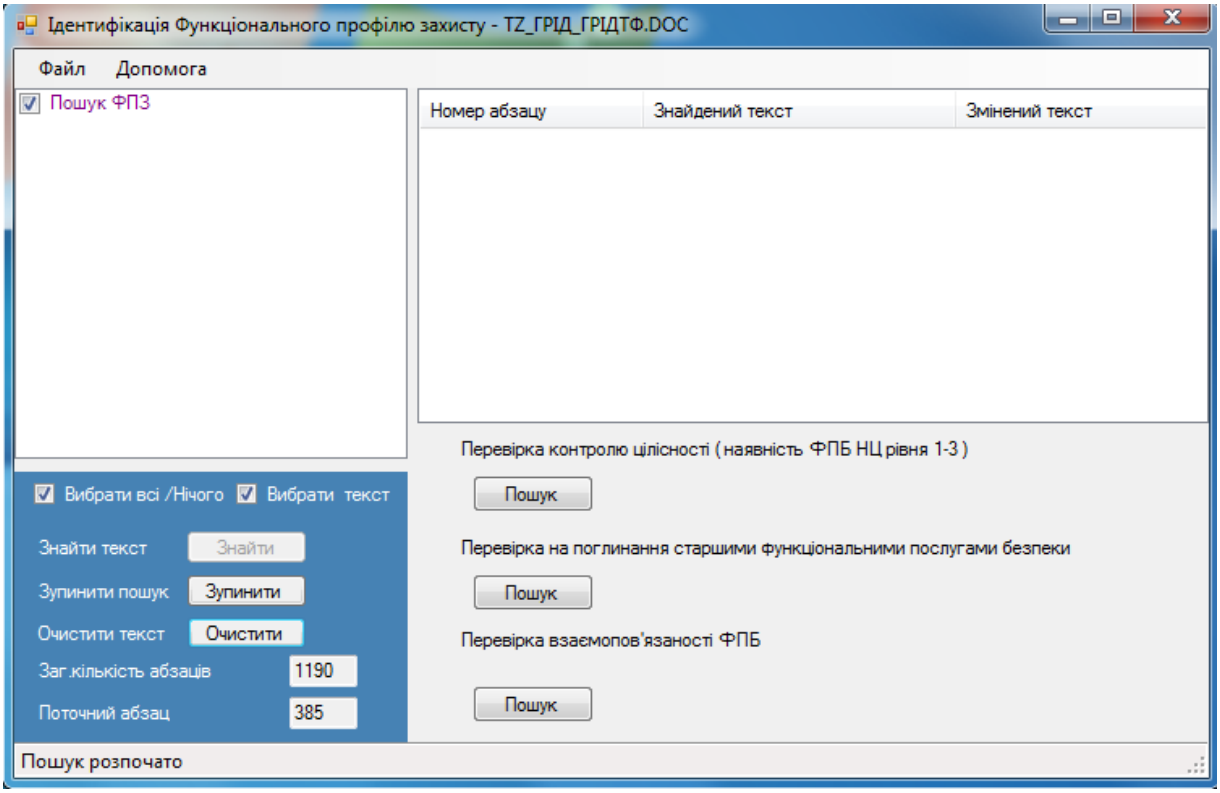


Рис. 8. Приклад реалізації алгоритма RegularExpressionFind

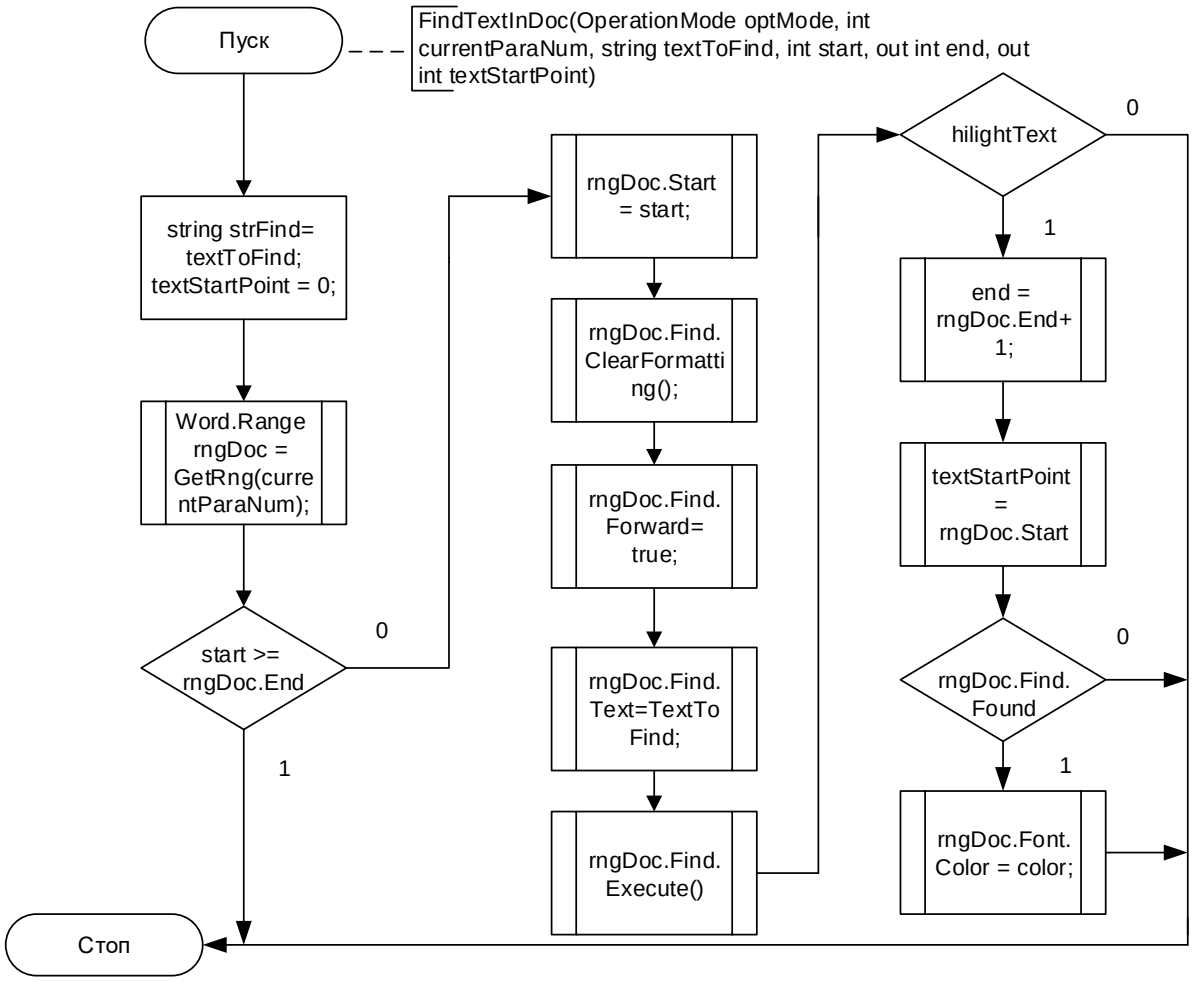


Рис. 9. Алгоритм реалізації FindTextInDoc

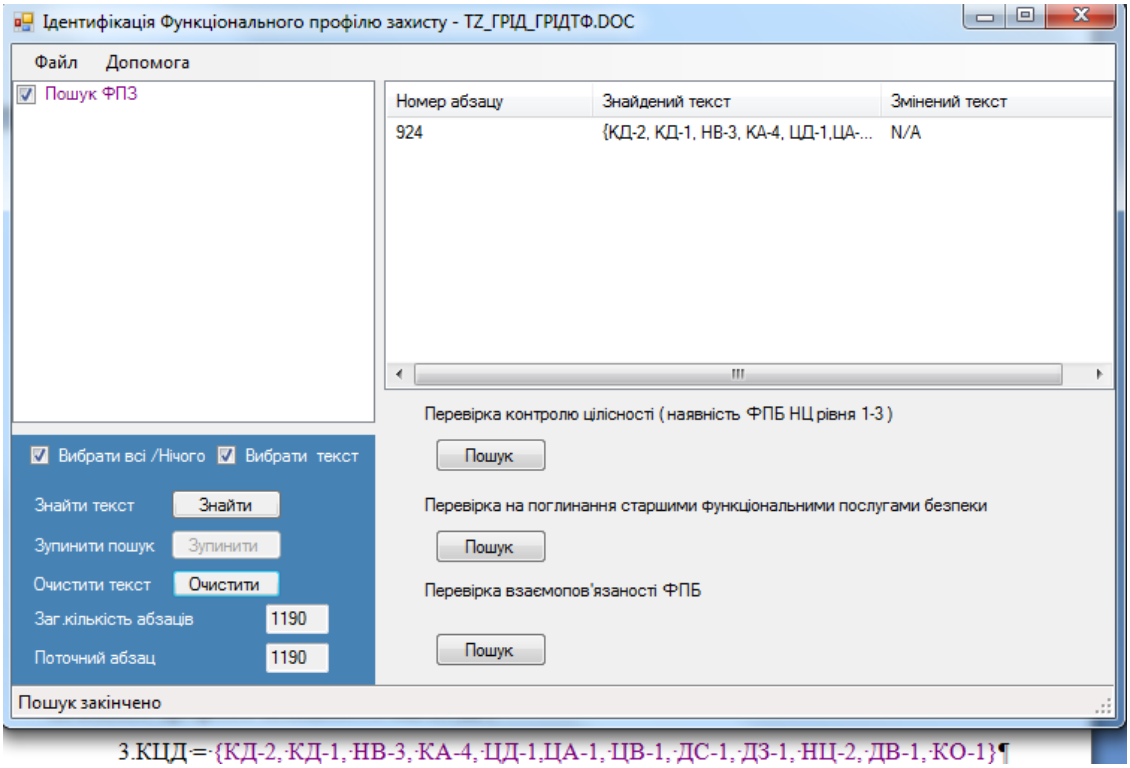


Рис. 10. Приклад реалізації алгоритма FindTextInDoc

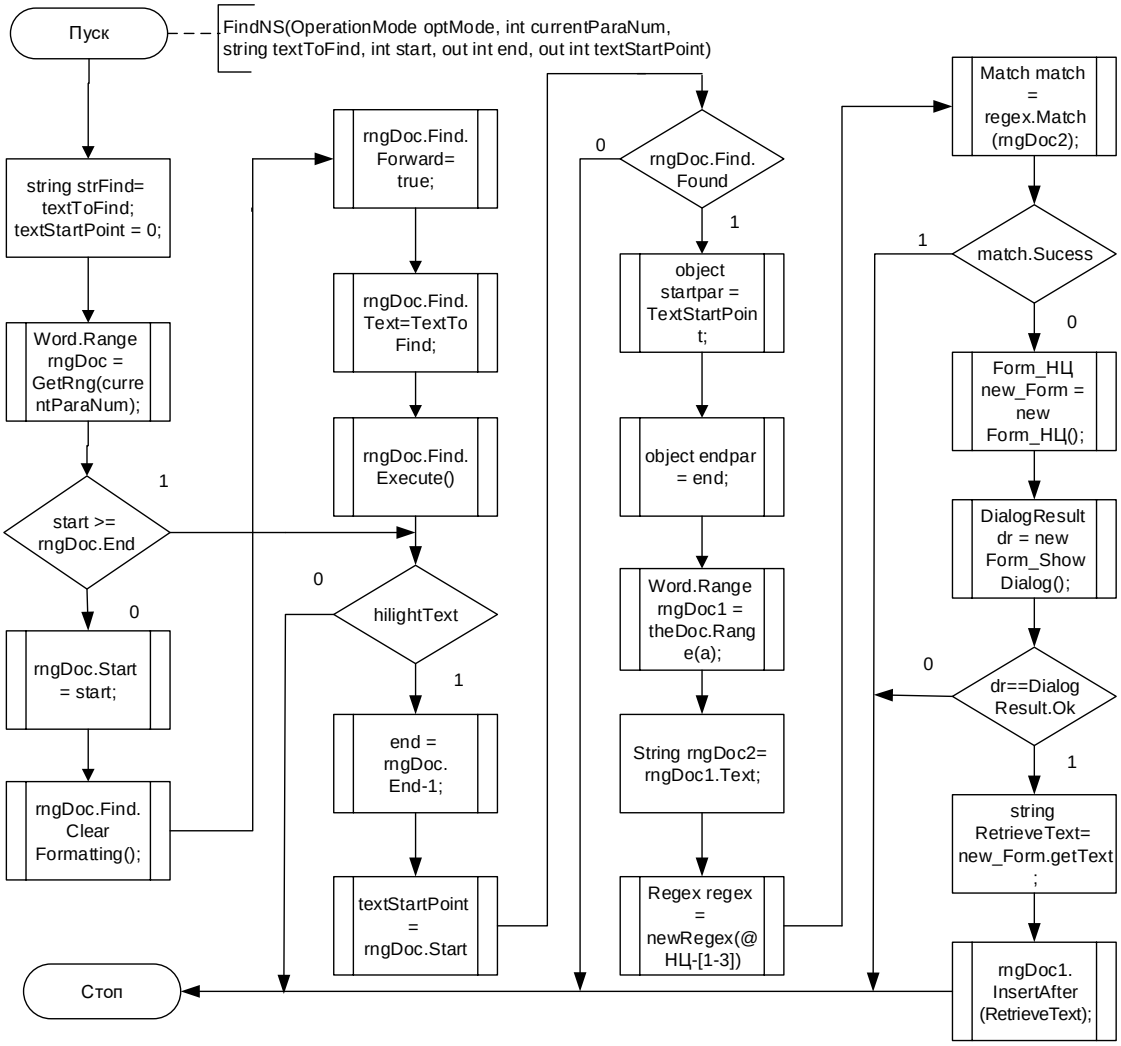
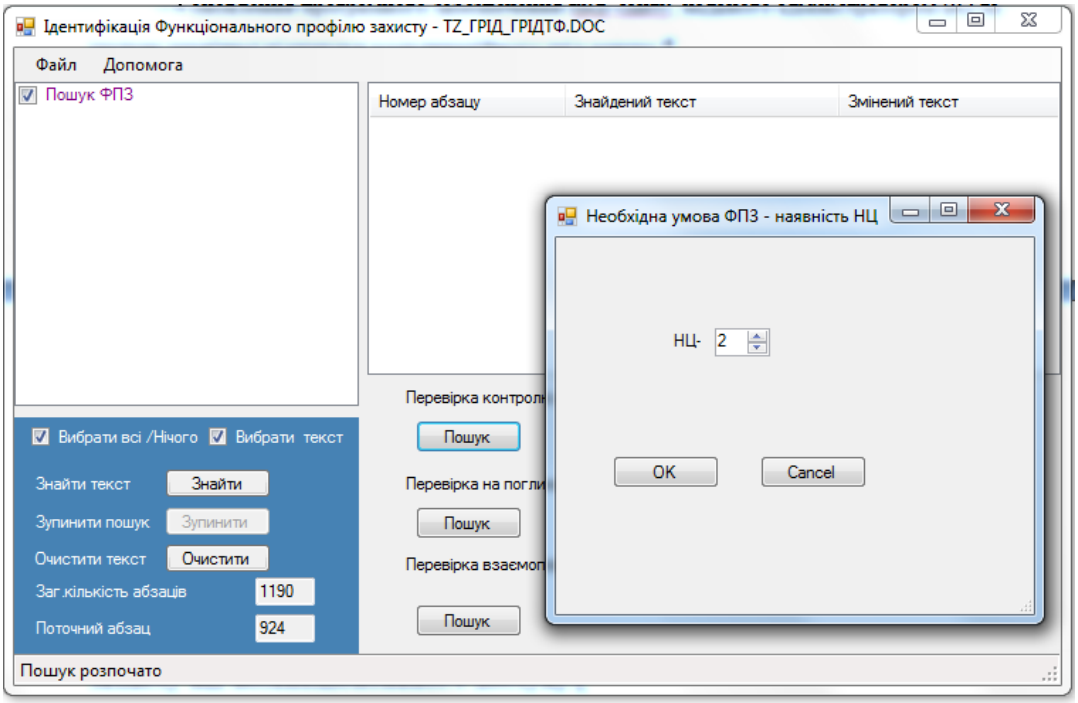


Рис. 11. Алгоритм реалізації FindNS

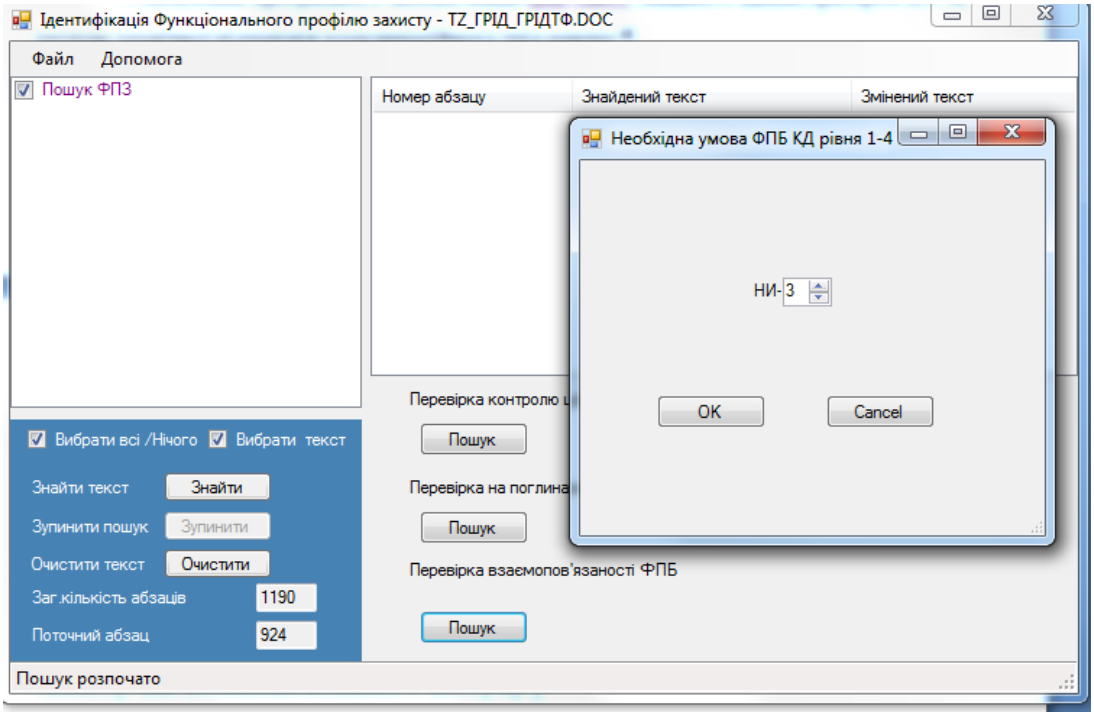


- **6.3.1 Профіль захищеності інформації**

Нейтралізація загроз несанкціонованого доступу до інформації повинна забезпечуватися реалізацією КЗЗ політики функціональних послуг, які визначаються таким загальним профілем захищеності від НСД:

3.КЦД = {КД-2, КД-1, НВ-3, КА-4, ЦД-1,ЦА-1, ЦВ-1, ДС-1, ДЗ-1, ДВ-1, КО-1}

Рис. 12. Приклад реалізації алгоритма FindNS



- **6.3.1 Профіль захищеності інформації**

Нейтралізація загроз несанкціонованого доступу до інформації повинна забезпечуватися реалізацією КЗЗ політики функціональних послуг, які визначаються таким загальним профілем захищеності від НСД:

3.КЦД = {КД-2, КД-1, НВ-3, КА-4, ЦД-1,ЦА-1, ЦВ-1, ДС-1, ДЗ-1, НЦ-2, ДВ-1, КО-1}

Рис. 13. Приклад реалізації алгоритма FindLinks

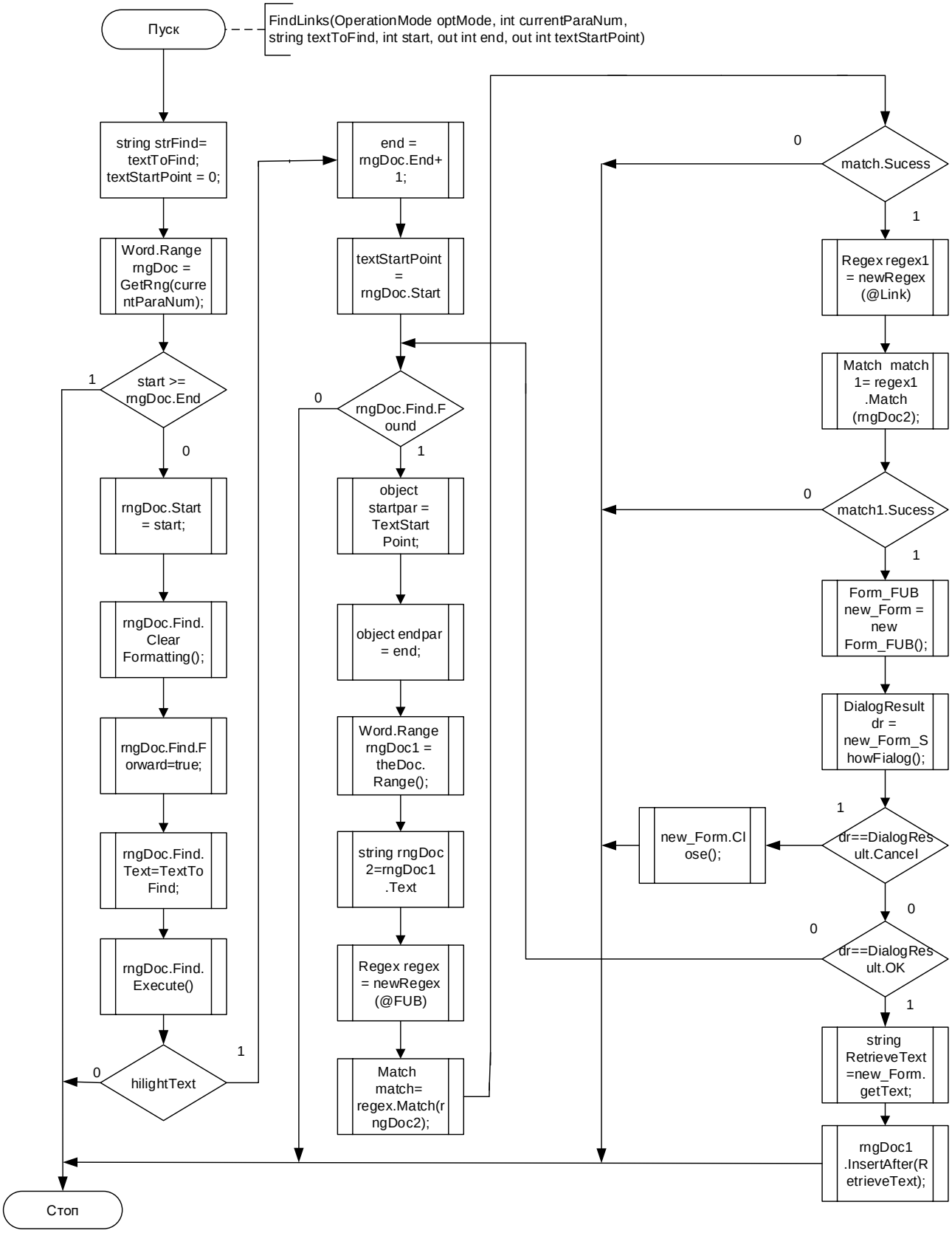


Рис. 14. Алгоритм реалізації FindLinks

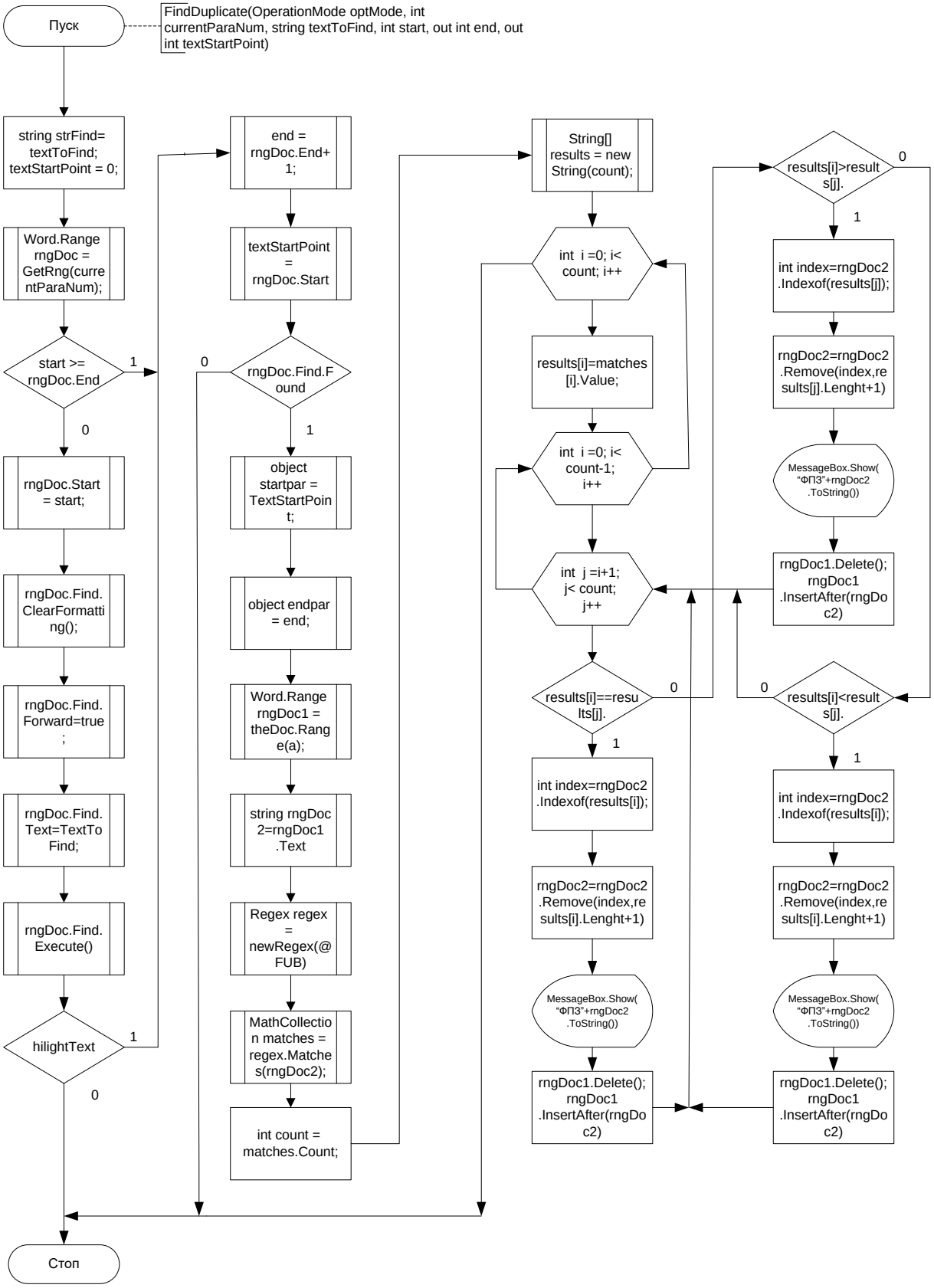
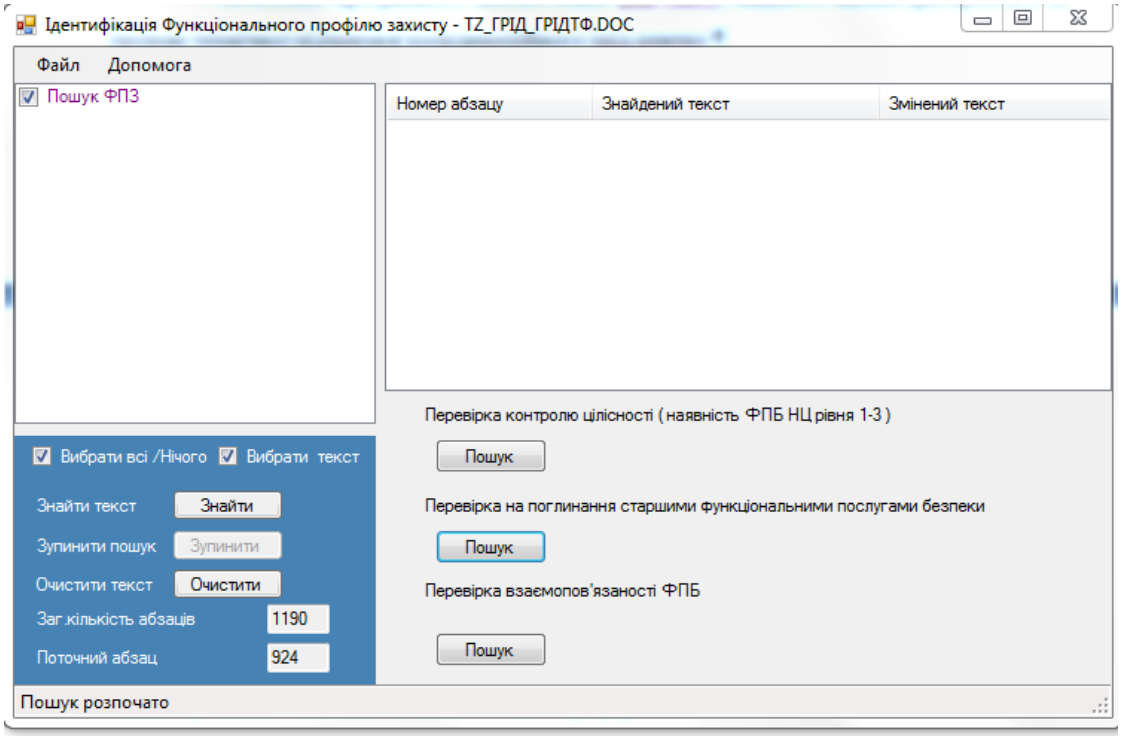


Рис. 15. Алгоритм реалізації FindDuplicate



- **6.3.1 Профіль захищеності інформації**

Нейтралізація загроз несанкціонованого доступу до інформації повинна забезпечуватися реалізацією КЗЗ політики функціональних послуг, які визначаються таким загальним профілем захищеності від НСД:

3.КЦД={КД-2, НВ-3, КА-4, ЦД-1,ЦА-1, ЦВ-1, ДС-1, ДЗ-1, НЦ-2, ДВ-1, КО-1}

Рис. 16. Приклад реалізації алгоритма FindDuplicate

Висновок. Таким чином, запропонована структурна модель СППР, яка за рахунок взаємопов'язаних баз даних смислових змінних, множини критеріїв та шаблонів документів, а також модулів виокремлення смислових змінних, ідентифікації функціонального профілю захисту та взаємодії з експертом дозволяє розширити функціональні можливості сучасних СППР пов'язаних з реалізацією експертиз технічного захисту інформації.

ЛІТЕРАТУРА

[1]. О. Корченко, А. Давиденко, М. Шабан, "Модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах", *Безпека інформації*, Том 25, №2, С. 122-126, 2019.

[2]. А. Давиденко, М. Шабан, О. Корченко, І. Іванченко, "Метод ідентифікації функціонального профілю захисту", *Захист інформації*, Том 21, №4, С. 251-258, 2019.

[3]. О. Корченко, А. Давиденко, М. Шабан, "Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ", *Захист інформації*, Том 21, №2, С. 88-96, 2019.

[4]. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

УДК 004.056:004.75

Корченко А.А., Давиденко А.Н., Шабан М.Р., Казмирчук С.В. Структурная модель СППР при проведении государственной экспертизы КСЗИ

Аннотация. *Процесс проведения государственных экспертиз комплексных систем защиты информации (КСЗИ) и организация электронного оборота документов, созданных на этапе проектных работ имеют ряд проблем, а именно: уязвимость информации, хранящейся на постоянных носителях памяти; большую энтропию неопределенности информации, увеличивает риски ошибок эксперта при проведении государственных экспертиз КСЗИ; проблема обращения бумажных документов, которые были созданы на этапе предпроектных работ, увеличивает риски раскрытия информации с ограниченным доступом. Для решения указанных проблем необходимо осуществить автоматизацию отдельных процессов. Поставленная цель осуществляется путем разработки структурной модели системы поддержки принятия решений (СППР) для реализации экспертиз КСЗИ, которая формируется из взаимосвязанных баз данных смысловых переменных, множества критериев и шаблонов документов, а также модулей выделение смысловых переменных, идентификации функционального профиля защиты и взаимодействия с экспертом. Для реализации структурной модели было разработано программное приложение, поддерживающее два основных процесса: первый - связан с проверкой соответствия функционального профиля защиты (ФПЗ) требованиям НД ТЗИ; второй - ориентирован на*

выделение смысловых переменных из входящих документов и их сохранения в базе данных смысловых переменных (БДСП). Указанные решения позволяют расширить функциональные возможности современных СППР связанных с реализацией экспертиз технической защиты информации.
Ключевые слова: *государственные экспертизы КСЗИ, функциональный профиль защиты, система поддержки принятия решений, НД ТЗИ 2.5-004-99, экспертная оценка.*

Korchenko A., Davydenko A., Shaban M., Kazmirchuk S. Structural model of the DSS for the State Examination of the IISS

Abstract. *The process of conducting state examinations of integrated information security systems (IISS) and the organization of electronic circulation of documents created at the stage of design work have a number of problems, namely: the vulnerability of information stored on permanent storage media; greater entropy of information uncertainty, increases the risks of expert errors in conducting state examinations of IISS; the problem of handling paper documents that were created at the pre-design stage increases the risks of information disclosure with limited access. To solve these problems, it is necessary to automate individual processes. The goal is carried out by developing a structural model of a decision support system (DSS) for the implementation of IISS examinations, which is formed from interconnected databases of semantic variables, a variety of criteria and document templates, as well as modules for extracting semantic variables, identifying a functional defense profile and interacting with an expert. To implement the structural model, a software application was developed that supports two main processes: the first is to verify the compliance of the functional security profile (FSP) with the requirements of the ND TPI; the second is focused on extracting semantic variables from incoming documents and storing them in a database of semantic variables (DBSV). These solutions allow you to expand the functionality of modern DSS related to the implementation of examinations of technical protection of information. Thus, a structural model of DSS was proposed, which due to interconnected DBSV, set of criteria and templates of documents as well as modules for separating semantic variables, identification of FSP and interaction with the expert allows to expand the functionality of modern DSS related with the implementation of examinations of technical protection of information.*
Keywords: *IISS state examinations, functional security profile, decision support system, ND TPI 2.5-004-99, expert review.*

Корченко Анна Олександрівна, доктор технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Корченко Анна Александровна, доктор технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Korchenko Anna, Dr Eng (Information security), Associate Professor of IT-Security Academic Department, National Aviation University.

Давиденко Анатолій Миколайович, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник відділу Теорії моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.
Давиденко Анатолий Николаевич, кандидат технических наук, старший научный сотрудник, ведущий научный сотрудник отдела Теории моделирования Института проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины.
Davydenko Anatoly, Candidate of Technical Sciences, Senior Researcher, Leading Researcher of Department of Modelling Theory, Pukhov Institute for Modelling in En-ergy Engineering of NAS of Ukraine.

Шабан Максим Радуйович, інженер Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова.
Шабан Максим Радович, инженер Института проблем моделирования в енергетике им. Г.Е. Пухова.
Shaban Maxim, engineer Pukhov Institute for Modelling in Energy Engineering.

Казмірчук Світлана Володимирівна, доктор технічних наук, зав. кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
Казмирчук Светлана Владимировна, доктор технических наук, зав. кафедры компьютеризированных систем защиты информации Национального авиационного университета.
Kazmirchuk Svitlana, Dr Eng (Information security), Head of Computerised Information Security Systems Academic Department, National Aviation University.

Отримано *10 квітня 2020 року*, затверджено редколегією *22 квітня 2020 року*