Прикладом таких повноважень можуть служити повноваження на виконання операцій читання, запису, заміни інформації та інші. Відомими є моделі надання повноважень, які використовують уявлення про класи безпеки та уявлення про категорії об'єктів.

1. *Davydenko A.* Formalization level of abstraction of state information resourses access systems / A. Davydenko // Scientific letters of academic society of Michel Baludansky, ISSN 1338-9432. Volume 4, 1 2016, p.35-38.
2. *Давыденко А.Н.* Расширение теоретических возможностей математических моделей нейронных сетей обуславливаемых их использованием для решения задач защиты систем доступа / *А.Н. Давыденко* // ЗбірникнауковихпрацьІнститут проблем моделювання в енергетиці НАН України :Зб. наук. працьвип. 45 – К., 2008,– С. 112-115.
3. *Давыденко А.Н.* Анализ основных информационных компонент систем доступа / *А.Н. Давыденко* // Моделювання та інформаційнітехнології: Зб. наук. працьвип. 59. – К., 2011, – С.11-20
4. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты / *А.А. Петров* . – М. :ДМК, 2001 – 448 с.
5. *Гладков Л. А.* Генетические алгоритмы / *Л. А. Гладков, В. В. Курейчик, В. М. Курейчик*. – 2-е изд., испр. и доп . – М. :Физматлит, 2006 . – 320 с
6. *Акимов О. Е.* Дискретная математика: логика, группы, графы, фракталы / *О. Е. Акимов* . – М. : Акимова, 2005 . – 656 с.
7. *УотшемТ.Дж.* Количественные методы в финансах / *Т.ДжУотшем, К. Паррамоу*– М.: Юнити, 1999
8. *Хованов Н. В.* Анализ и синтез показателей при информационном дефиците / *Н. В. Хованов* – СПб.: Издательство Санкт-Петербургского университета, 2011

Поступила 20.03.2017р.

УДК 004.056:004.75

М. Р. Шабан, Київ

ПРОГРАМНА РЕАЛІЗАЦІЯ ПЕРЕВІРКИ ПОВНОТИ ТА НЕСУПЕРЕЧНОСТІ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИСТУ

Abstract. Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Програма «Ідентифікація функціонального профілю захисту» призначена для допомоги експерту при визначенні функціонального профіля захисту (ФПЗ) в документі типу Microsoft Word, а також допомогає [1] при аналізі ФПЗ. Головною метою цієї програми є допомога експерту при створенні ФПЗ та контроль наявності ФПЗ на відповідність умовам заданим в нормативному документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [2], а саме: визначені контролю цілісності; поглинання старшими ФПЗ молодших; перевірки пов'язаності ФПБ одна з одною.

Програма написана на мові програмування C# в середовищі розробки Visual Studio 2005. При написанні програмного коду використовувалась технологія MS Office's COM Interop, а саме бібліотека Microsoft.Office.Interop.Word та базові бібліотеки мови програмування C#.

Документ Microsoft Word є спеціалізоване COM-орієнтоване сховище даних - структуроване сховище (Structured Storage), організоване за ієрархічним принципом. Документ може містити різні типи даних: структурований текст, графіку, математичні вирази, організаційні діаграми і т.д. Концепція структурованого сховища є складовою частиною сучасної парадигми програмування на основі моделі компонентних об'єктів (Component Object Model - COM). По суті, структуроване сховище - це технологія об'єднання в одній логічній одиниці зберігання даних (файлі) об'єктів з різною природою і властивостями. Технологія COM пропонує стандартну реалізацію концепції структурованого сховища у вигляді складеного файлу (Compound File): файлова система всередині файлу. COM-сховище являє собою ієрархічну структуру колекцій об'єктів двох типів: сховищ (Storage) і потоків (Stream), яким в традиційній файлової системи відповідають каталоги і файли. Даний підхід дозволяє істотно знизити витрати зберігання в одному файлі об'єктів різної природи.

Реалізація програми включає в себе методи регулярних виразів: порівняння строк; дерево суфіксів; апроксимуючі патерни; патерни за допомогою яких можна зробити множинний вибір, часткові патерни. Показано, що технології, які поєднують в собі властивості апроксимуючих патернів і патернів, по яких можна зробити множинний вибір вирішують поставлені завдання аналізу ФПЗ і можуть бути використані для побудови системи.

Інтерфейс програми (Рис.1) представляє собою віконний додаток, який реалізований у виді GUI-програми, в якому є такі елементи управління:

1). Віконне поле типу «Listbox» пошуку функціонального профілю захисту;

2). Кнопки «Знайти», «Зупинити», «Очистити».

3). Права частнина екрану має віконне поле типу «ListView», в якому відображується номер абзацу, де було знайдено ФПЗ та сам ФПЗ;

4). Три кнопки пошуку відповідності ФПЗ умовам нормативного документу НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в

комп'ютерних системах від несанкціонованого доступу»;

5). Два віконних поля типу «TextBox» в одному з яких відображується загальна кількість абзаців документу, а в другому полі поточний абзац при обробці документа;

6). Віконне поле типу «statusStrip», яке має три положення «Очікую», «Пошук розпочато», «Пошук закінчено»;

7). Два віконних поля типу «CheckedBox» в одному з яких є можливість обрати пошук ФПЗ, а в другому полі можливість переходу до заданої частини тексту умовами пошуку ФПЗ;

8). Віконне поле типу «menuStrip», де розміщені дві вкладки: «Файл», «Допомога».

У вкладці «Файл» є можливість відкрити документ, закрити опрацьований документ, зберегти документ, а у разі необхідності є можливість не змінювати оригінал документу, а створити копію документа з новою назвою, а також вийти з програми.

Розглянемо роботу програми на прикладі пошуку функціонального профілю захисту на прикладі пакету вхідних документів державної експертизи КСЗІ типового грід-сайту.

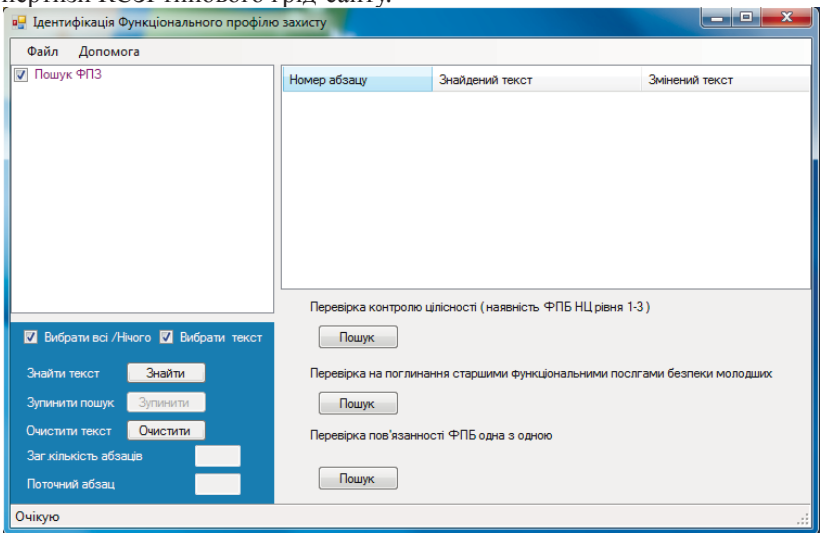

Рис.1 – Інтерфейс програми

На початку роботи експерту необхідно відкрити документ, з яким він має бажання опрацювати. Для цього потрібно зайти в меню «Файл» та натиснути по вкладці «Відкрити». Також в цьому меню є такі вкладки: «Закрити», «Зберегти», «Зберегти Як», «Вихід». За допомогою вкладки «Закрити» у експерта є можливість закрити документ з яким він працював. Вкладка «Зберегти» дозволяє зберегти зміни в документі, які відбулись під час опрацювання документу програмою. «Зберегти Як» дозволяє створити

нову копію опрацьованого документу не змінюючи, при цьому, документ з яким працював експерт. «Вихід» дозволяє вийти з програми. Коли експерт натисне по вкладці «Відкрити» меню «Файл», відкривається стандарте віконне поле пошуку документу - початкове місцезнаходження якого знаходиться на диску: C:\\. Коли експерт відкриє документ, то у віконному полі типу «Title» до назви програми «Ідентифікація ФПЗ» додається назва документу типу: «Назва документу.розширення». Після того, як експерт відкрив документ йому потрібно визначити наявність в документі ФПЗ. Для цього експерту потрібно натиснути кнопку «Знайти». Під час пошуку ФПЗ кнопка «Знайти» стає неактивною, при цьому у експерта з'являється можливість зупинити пошук натиснувши кнопку «Зупинити». Під час проведення пошуку у віконному полі «Загальна кількість абзаців» буде відображена загальна кількість абзаців документу, а у полі «Поточний абзац» буде відображено той абзац, який наразі оброблюється програмою. Під час пошуку ФПЗ віконне поле типу «statusStrip» міняє своє положення з «Очікую» на «Пошук розпочато». Якщо в документі було знайдено ФПЗ, а також відмічене «CheckBox» поле «Вибрати текст», в такому разі в момент, коли ФПЗ було знайдено програмою, перейде до тієї частини документу (Рис. 2). ФПЗ буде виділений тим же кольором, що і поле «Пошук ФПЗ». У разі, якщо експерту немає необхідності в переході до тієї частини документу, де було знайдено ФПЗ, експерт може зняти галочку у віконному полі типу «CheckBox» «Вибрати текст». У випадку, якщо ФПЗ не було знайдено в документі, експерту буде дано попередження, що ФПЗ в документі відсутнє. Віконне поле типу «statusStrip» міняє своє положення з «Пошук розпочато» на «Пошук закінчено».

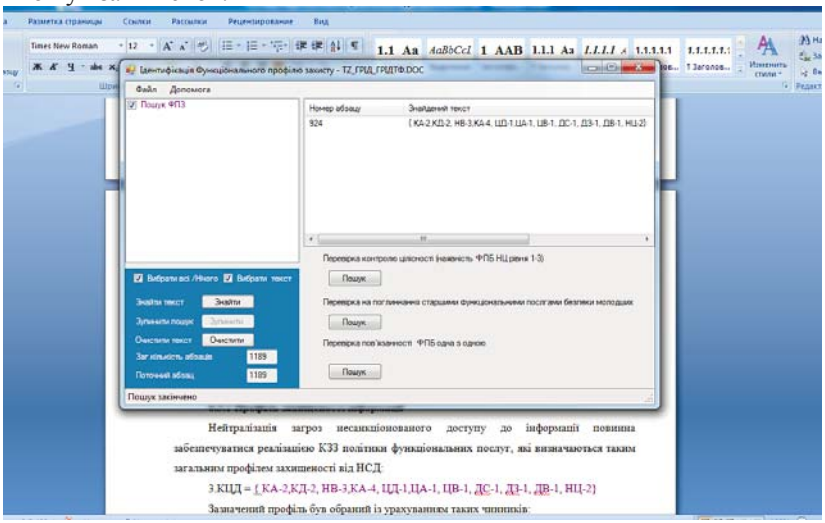

Рис.2 – Результати прошуку ФПЗ

Після того, як програмою було знайдено ФПЗ експерту необхідно провести пошук на відповідність за трьома умовам згідно з нормативним документом НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»: контроль цілісності; поглинання старшими ФПБ молодших; пов'язаність ФПБ одна з одною. Для того щоб провести пошук контролю цілісності потрібно натиснути на кнопку «Пошук» нижче поля «Перевірка контролю цілісності». Віконне поле типу «statusStrip» міняє своє положення з «Пошук закінчено» на «Пошук розпочато». У випадку, якщо в ФПЗ відсутня функціональна послуга безпеки (ФПБ) НЦ рівня 1-3, експерту буде надана можливість усунути цей недолік. Відкривається нове вікно типу «Form» (Рис. 3) з такими елементами управління: віконне поле типу «numericUpandDown», кнопками «ОК» та «Cancel» і символьною строкою типу «Lable», в якій зазначена ФПБ. Після того, як експерт обере рівень НЦ та натисне кнопку «ОК», в кінці ФПЗ з'явиться ФПБ НЦ рівня, який обрав експерт. У випадку, якщо експерт натиснув кнопку «Cancel», ФПБ НЦ не буде додано до ФПЗ, а пошук буде продовжено. Після закінчення пошуку віконне поле типу «statusStrip» міняє своє положення з «Пошук розпочато» на «Пошук закінчено».

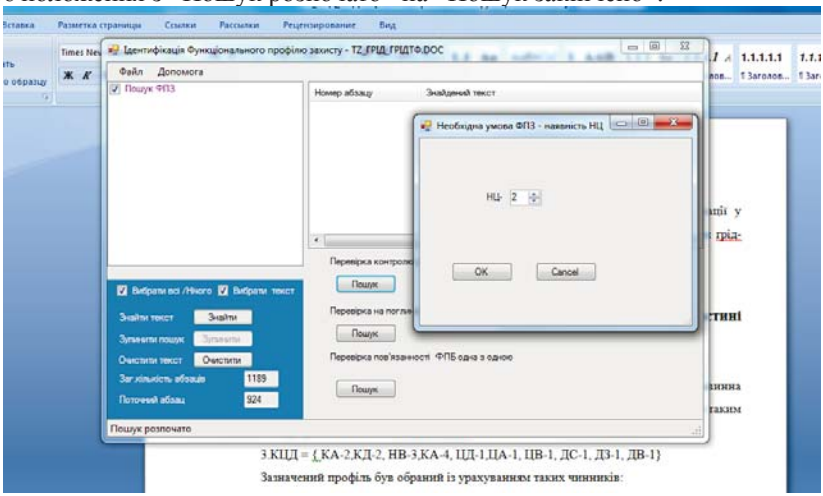

Рис.3 – Приклад перевірки контролю цілісності

Наступним етапом роботи експерта є перевірка ФПЗ на поглинання старшими ФПБ молодших. Для цього необхідно натиснути кнопку «Пошук » нижче поля «Перевірка на поглинання старшими ФПБ молодших». Віконне поле типу «statusStrip» міняє своє положення з «Пошук закінчено» на «Пошук розпочато». У випадку, якщо, наприклад, у профілі є: КД – 1, КД - 2, КД – 4, в ФПЗ залишиться старша ФПБ, тобто КД - 4, а ФПБ з більш низьким рівнем будуть прибрані програмою з ФПЗ.

Останнім етапом роботи експерта з програмою є перевірки пов'язаності ФПБ. Для цього експерту необхідно натиснути кнопку «Пошук» під однойменним текстовим полем. Наприклад, в документі я створив ФПЗ, який містить ФПБ КД рівня 4, але не містить ФПБ, які є необхідними умовами для КД рівня 4. Згідно з нормативним документом НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» необхідними умовами для ФПБ КД рівня 4 є наявність в ФПЗ ФПБ НИ рівнів 1-4 та КО рівня 1. У цьому випадку відкривається нове вікно типу «Form» (Рис. 4) з такими елементами управління: віконне поле типу «numericUpandDown», кнопками «ОК» та «Cancel» і символьною строкою типу «Lable», на якій зазначена ФПБ. Після того, як експерт обере рівень НИ та натисне кнопку «ОК», в кінці ФПЗ з'явиться ФПБ НИ рівня, який обрав експерт. У випадку, якщо експерт натиснув кнопку «Cancel», ФПБ НИ не буде додано до ФПЗ, а пошук буде продовжено. Після закінчення пошуку віконне поле типу «statusStrip» міняє своє положення з «Пошук розпочато» на «Пошук закінчено». Результатами роботи програми буде включення у кінець профілю НИ рівня 3 та КО рівня 1. Якщо необхідна умова ФПБ має один рівень, згідно з НД ТЗІ 2.5-004-99, то ця ФПБ буде додана до ФПЗ автоматично.

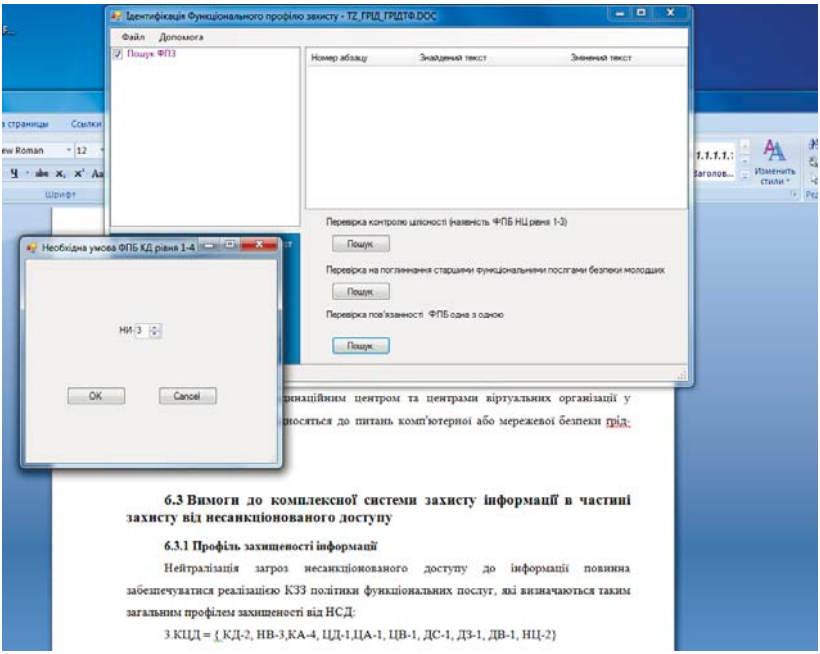

Рис.4 - Вибір експерта рівня НИ, яка є необхідною умовою ФПБ КД рівня 4

Висновок. Таким чином був проаналізован документ «Технічне завдання» [3] типового грід-сайту на прикладі Інституту кібернетики ім. В.М.Глушкова на предмет наявності в ньому ФПЗ. Результатом роботи програми стало виконання завдань з пошуку ФПЗ та аналіз ФПЗ на предмет відповідності трьом умовам згідно з нормативним документом НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Аналіз виконання показав багаторазове збільшення швидкості обробки документа при стовідсотковій відсутності помилок, а саме - програма усунула з ФПЗ однотипні послуги, виконала перевірку цілісності та повноти [4]. Приблизний час обробки документів склало: «Технічне завдання» – 17сек; «Пояснювальна записка до технічного проекту» – 43 сек.; «Акт обстеження» – 7 сек.; «Політика безпеки інформації» – 12 сек. Програма виконувалась на робочій станції з такими технічними характеристиками: центральний процесор Intel Core i5-4670 з частотою 3.4 ГГц; оперативна пам'ять - 8 ГБ.

1. *Давиденко А.М.* Система підтримки прийняття рішень щодо забезпечення інформаційної, антивірусної та фізичної безпеки комп'ю т е р н и х систем органів внутішніх справ України «ТОРСІОН - 3»// Міністерство внутрішніх справ України, Державний науково-дослідний інститут МВС України, Департамент документального забезпечення та режиму МВС України, Методичні рекомендації / Шорошев В.В., Пающик І.І., Давиденко А.М. та ін./ Київ 2010, 189 с.

2. *Корченко О.Г.* Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Корченко, В. Бурячок, С. Гнатюк // Безпека інформації. - 2013. - Т. 19, № 1. - С. 40-44.

3. *Корченко О.Г.* Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах / О. Корченко, Ю. Дрейс, І. Лозова // Захист інформації. - 2016. - Т. 18, № 1. - С. 39-47.

4. *Давиденко А.М.* Про термінологію в області безпеки інформації / С. М. Головань, А. М. Давиденко, Л. М. Щербак // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова. - 2013. - Вип. 66. - С. 31-35.

Поступила 12.04.2017р.