УДК 004.056:004.75

М.Р. Шабан, Київ
О.С. Потенко, Київ
В.М. Попова, Київ

ТЕСТУВАННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОРІЄНТОВАНИХ НА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕДУР АНАЛІЗУ КІБЕРБЕЗПЕКИ

Abstract. In this article, the algorithm of the Module “identification of the functional protection profile” was considered. This algorithm was divided into two subtasks. At the first stage, the compliance of the functional protection profile with the formal criteria was determined. At the second stage, criteria were determined for compliance with functional security services in the process of semantic analysis in the input documents.

В даний час сучасні обчислювальні системи і комп'ютерні мережі дозволяють накопичувати великі масиви даних для вирішення задач обробки та аналізу. Але машинна форма подання даних містить, необхідну людині, інформацію в прихованому вигляді, і для її вилучення потрібно використовувати спеціальні методи аналізу даних. Великий обсяг інформації, з одного боку, дозволяє отримати більш точні дані, з іншого – перетворює пошук рішень в складну задачу. Аналіз даних був автоматизований. В зв’язку з вищесказаним було вирішено завдання автоматизації. В результаті чого з'явився цілий клас програмних систем, що полегшують роботу аналітиків. Такі системи прийнято називати системами підтримки прийняття рішень (СППР). Розглянемо більш детально архітектуру сучасних СППР.

Для виконання аналізу СППР [1] повинна накопичувати інформацію, володіючи засобами її введення і зберігання. Таким чином, можна виділити три основні завдання, які вирішуються в СППР. Ввід даних. Збереження даних. Аналіз даних. За ступенем «інтелектуальності» обробки даних виділяються три класи завдань аналізу:

Інформаційно-пошуковий – СППР здійснює пошук необхідних даних. Характерною рисою такого аналізу є виконання заздалегідь визначених запитів.

Оперативно-аналітичний – СППР виробляє групування і узагальнення даних в будь-якому вигляді, необхідному аналітику. На відміну від інформаційно-пошукового аналізу в даному випадку неможливо заздалегідь передбачити необхідні аналітику запити.

Інтелектуальний – СППР [4] здійснює пошук функціональних і логічних закономірностей в накопичених даних, побудова моделей і правил, які пояснюють знайдені закономірності і/або прогнозує розвиток деяких процесів.

Таким чином, узагальнена архітектура СППР може бути представлена наступним чином: підсистема введення даних, підсистема зберігання, підсистема аналізу.

Ця підсистема може бути побудована на основі:

1. Підсистеми інформаційно пошукового аналізу.
2. Підсистеми оперативного аналізу.
3. Підсистеми інтелектуального аналізу. Ця підсистема реалізує методи і алгоритми Data Mining.

На даний момент існує величезна кількість СППР, розроблених і впроваджених в різних областях людської діяльності. Темпи їх розробок постійно зростають. Слід зазначити, що хоча СППР широко застосовується в усьому світі, на просторах СНД системам цього типу поки що не приділяється належна увага.

СППР класифікується за такими ознаками:

1. СППР, орієнтовані на дані (Data-driven DSS, Data-oriented DSS);
2. СППР, орієнтовані на моделі (Model-driven DSS);
3. СППР, орієнтовані на знання (Knowledge-driven DSS);
4. СППР, орієнтовані на документи (Document-driven DSS);
5. СППР, орієнтовані на комунікації і групові СППР (Communications-Driven, Group DSS);
6. Інтер-організовані та Інтра-організовані СППР (Inter-Organizational або Intra-Організаціонал DSS);
7. Специфічно функціональні СППР або СППР загального призначення (Function-Specific або GeneralPurpose DSS);
8. СППР на базі Web (Web-Based DSS).

Залежно від даних, з якими працюють СППР, виділяють два основних їх типи СППР: EIS і DSS.

EIS (Execution Information System) – інформаційна система керівництва, ІСР. СППР цього типу є оперативними, призначеними для негайного реагування на поточну ситуацію. У більшості вони орієнтовані на непідготовленого користувача, тому мають спрощений інтерфейс, базовий набір пропонованих можливостей, фіксовані форми подання інформації та перелік вирішуваних завдань. Такі системи засновані на типових запитах, число яких відносно невелика; звіти, отримані в результаті таких запитів, представляються в максимально зручному вигляді.

DSS (Decision Support System). До систем цього типу відносять багатофункціональні системи аналізу та дослідження даних. Вони припускають глибоке опрацювання даних, яку можна використовувати в процесі прийняття рішень. Системи цього типу, на відміну від EIS, розраховані на користувачів, що мають як знання в предметній області, так і можливості використання сучасних комп'ютерних технологій. Цим системам властиві риси штучного інтелекту, за рахунок можливості опрацювання вихідних даних в конкретні висновки по поставленому завданню. Такі системи має сенс створювати, якщо є підстави для узагальнення і аналізу

даних і процесів їх обробки.

Останнім часом до СППР відносять тільки другий тип, тобто DSS. Такий поділ систем на EIS і DSS не обов'язково означає реалізацію СППР одного з типів. Вони можуть існувати паралельно, коли кожна з систем надає свої функції для певної категорії користувачів.

Загальна схема підтримки прийняття рішень включає:

1. допомога особам які приймають рішення (ОПР) при оцінці стану керованої системи і впливів на неї;
2. виявлення вподобань ОПР;
3. генерацію можливих рішень;
4. оцінку можливих альтернатив, виходячи з переваг ОПР.

Але серед кваліфікованих СППР не має системи, що орієнтована на аналіз задач безпеки. Тому необхідно визначити методи тестування для СППР при проведенні експертизи грід-засобів на відповідність вимогам НД ТЗІ, які б відповідали критеріям оцінки безпечного обігу інформації в цьому типі СППР.

Мною була розроблена система [3], яка аналізує вхідні документи на предмет наявності ФПЗ і його ідентифікації за формальними ознаками НД ТЗІ. Заповнює шаблони вихідних документів інформацією з вхідних документів шляхом підказок експерту та аналізу вхідних документів СППР. Результатом роботи є створення групи вихідних документів. Система реалізується на платформі .NET на мові програмування C # з використанням середовища розробки Microsoft Visual Studio.

При тестуванні СППР використовувався метод квадратів [2], де види тестування перебувають у чотирьох квадрантах. В загальних випадках поділ видів тестування відбувається так: приймально-здавальне тестування, юзабіліті тестування, модульне тестування, тестування на відповідність. В нашому випадку особливий інтерес представляють юзабіліті тестування та тестування на відповідність. Тобто ті види тестування, які націлені на взаємодію з користувачем. Це пов’язано з тим, що користувач нашої СППР, за замовчуванням, вже є знавцем в області проведення державних експертиз.

В свою чергу, функціональне тестування відповідало всім вимогам, які задаються юзабіліті тестуванням та тестуванням на відповідність. Функціональне тестування (Functional Testing), яке також називають тестуванням за принципом «чорної скриньки» (“Black Box” Testing), полягає у перевірці функцій, які виконуються елементами СППР, на відповідність вимогам, проекту СППР та документації користувача.

Функціональне тестування застосовують для СППР у цілому, а також для програмних об'єктів будь-якого рівня (процедури, модуля, підсистеми, системи).

Під час реалізації функціонального тестування СППР були виконані наступні дії:

а) планування тестування:

1) розроблення плану тестування;

б) розроблення вимог до тестів:

1) визначення складових якості СППР, які оцінюються за результатами тестування;

2) визначення складових СППР, які тестувались;

3) оцінка необхідних для тестування ресурсів (бюджет, час, персонал);

в) проектування тестів:

1) проектування специфікації тестів;

г) проектування тестових процедур;

1) проектування детальних тестів;

2) проектування інструментального середовища тестування;

3) розроблення тестів;

4) розроблення детальних тестів;

5) розроблення тестових даних;

6) розроблення інструментального середовища тестування;

д) виконання тестування та оцінка його результатів:

1) виконання тестових прикладів;

2) аналіз результатів тестування;

3) розроблення звіту про тестування.

Функціональне тестування СППР було реалізовано у формі наступних методів:

- тестування транзакцій (переходів);
- тестування синтаксису;
- тестування логічних умов;

Транзакція (перехід) – це окремий процес роботи СППР з точки зору користувача або об'єкта управління. Транзакції є результатом ініціюючих (тригерних) дій, що існують обмежений період часу, наприклад, режим зміни значень параметрів, які використовують у керуючих алгоритмах.

Тестування синтаксису передбачає перевірку зовнішніх входів СППР таких, як команди оператора, дані від датчиків, інтерфейси між системами. Для виконання цього виду тестування вхідний синтаксис повинен бути описаний у вимогах до СППР та у проекті СППР. Описи вхідного синтаксису повинні включати множину користувальницьких і операторських команд, комунікаційні протоколи, логічні рішення, які відносяться до потоку транзакцій. Крім того, як джерела інформації, можуть бути використані експлуатаційна документація на СППР, а також вбудовані довідкові системи.

Тестування логічних умов застосовувалось у випадках, коли відповідні команди, які формуються СППР, залежать від набору значень логічних умов (правил). Відповідності між наборами логічних умов і станом вихідних умов змінних задають у вимогах до СППР.

В разі, коли розглядається КСЗІ [5], повнота тестів визначається функціональним профілем захисту (ФПЗ), а обсяг тестів визначається рівнем гарантій. Таким чином, наприклад, для ФПЗ {КА-2, КД-2, ЦА-1, ЦД-1, ДС-1, ДЗ-1 ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}була побудована тестова таблиця, що складається з 13-ти функціональних послуг безпеки (ФПБ), де ФПБ Базова Адміністративна Конфіденційність (КА) має одинадцять вимог технічного захисту серед яких: щодо захисту інформацію та об’єктів, що містять технологічну інформацію; щодо розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта; щодо запитів на зміну прав доступу, які обробляються КЗЗ, можуть тільки в тому випадку, якщо вони надходять від адміністратора; щодо прав доступу до кожного захищеного об'єкта, визначеного політикою безпеки, повинні встановлюватися в момент його створення або ініціалізації. Базова довірча конфіденційність (КД) має одинадцять вимог технічного захисту серед яких: щодо користувачів, програмного забезпечення, призначеного для запуску завдань, а також об’єктів, що містять інформацію користувачів; щодо КЗЗ, яка повинна здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта; щодо можливості КЗЗ надавати користувачу право, для кожного захищеного об'єкта, одержувати інформацію від об'єкта; права доступу до кожного захищеного об'єкта; Мінімальна адміністративна цілісність (ЦА) має шість вимог технічного захисту серед яких: щодо можливості здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта; можливості на зміну прав доступу; щодо прав доступу до кожного захищеного об'єкта, які повинні встановлюватися в момент його створення або ініціалізації. Мінімальна довірча цілісність (ЦД) має одинадцять вимог технічного захисту серед яких: щодо розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта; щодо можливості надавати користувачу, для кожного захищеного об'єкта, право модифікувати об'єкт. Стійкість при обмежених відмовах (ДС) має шість вимог технічного захисту серед яких: щодо можливості КЗЗ бути спроможною повідомити адміністратора про відмову через журнал або сигналізацію. Модернізація (ДЗ) має три вимоги технічного захисту серед яких: щодо можливості створення порядку модернізації компонентів, при виконанні якого не знижується рівень безпеки інформації та не потрібна додаткова державна експертиза. Ручне відновлення (ДВ) має чотири вимоги технічного захисту серед яких: щодо необхідності існування ручних процедур, за допомогою яких можна безпечним чином повернути компоненти системи до нормального функціонування. Захищений журнал (НР) має п’ять вимог технічного захисту серед яких: щодо журналу, повинен

містити інформацію про дату, час, місце, результат події. Одиночна ідентифікація і автентифікація (НИ) має п’ять вимог технічного захисту серед яких: щодо необхідності кожному користувачу однозначно ідентифікуватися КЗЗ. Однонаправлений достовірний канал (НК) має дві вимоги технічного захисту серед яких: щодо необхідності використання достовірного каналу для початкової ідентифікації і автентифікації. Виділення адміністратора (НО) має три вимоги технічного захисту серед яких: шодо політики розподілу обов'язків, яка повинна визначити ролі адміністратора. КЗЗ з гарантованою цілісністю (НЦ) має п’ять вимог технічного захисту серед яких: щодо необхідності всім послугам безпеки бути доступним тільки через інтерфейс засобів захисту. Самотестування при старті (НТ) має п’ять вимог технічного захисту серед яких: щодо необхідності виконання тестів тільки за запитом користувача, який має відповідні повноваження. Все вище зазначене дозволило вийти на рівень гарантій Г-3.

Висновок. В даній статті розглянуті існуючи класифікації СППР. Запропоновано розширення цієї класифікації СППР-орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки. Показана пряма залежність набору тестів від функціонального профілю захисту.

1. Система підтримки прийняття рішень щодо забезпечення інформаційної, антивірусної та фізичної безпеки комп’ютерних систем органів внутрішніх 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., Пайщик І.І., Давиденко А.М. та ін. / Київ 2010, 189 с.

2. *Шабан М.Р.* Разработка методики проведения комплексных систем защиты информации / М.Р. Шабан, А.Н. Давиденко // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім Г.Є. Пухова НАН України. – Київ, 2014. – Вип. 73. – С.114-121.

3. *Шабан М.Р.* Реалізація програмного модуля підтримки прийняття рішень при проведенні експертизи грід-засобів на відповідність вимогам НД ТЗІ / М.Р. Шабан // Збірка праць конференції «Моделювання 2018». – 2018. – С.259-262.

4. *Кузнєцова М.О.* Інформаційні системи підтримки прийняття управлінських рішень / М.О. Кузнецова, Г.Ю. Коблянська // Формування ринкових відносин в Україні. – 2012. – № 9. – С.154-157.

5. *Головань С.М.* Про термінологію в області безпеки інформації / С.М. Головань, А.М. Давиденко, Л.М. Щербак // Зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2013. – Вип. 66. – С.31-35.

Поступила 27.08.2018р.