УДК 004.056:004.75

М. Р. Шабан, м. Київ

ФОРМАЛІЗАЦІЯ ПРАВИЛ ПЕРЕВІРКИ ПОВНОТИ ТА НЕСУПЕРЕЧНОСТІ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИСТУ

Abstract. Information security defines as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Одним з ключових завдань при проведенні державної експертизи є ідентифікація функціонального профілю захисту (ФПЗ). Основною метою створення ФПЗ є нейтралізація загроз несанкціонованого доступу до інформації, яка забезпечується реалізацією КЗЗ політики функціональних послуг. У завдання ідентифікації входять такі підзадачі: визначення рівнів ФПБ реалізованих КСЗІ об'єкта експертизи; визначення повноти та несуперечності профілю; ідентифікація опису ФПБ у вхідних документах. При проведенні другої підзадачі необхідно враховувати правила побудови функціонального профілю захисту визначених НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Формалізація цих правил повинна створити сприятливі умови для автоматизації перевірки повноти та несуперечності ФПЗ.

Проблема безпеки складна, багатогранна та пов'язана з вирішенням широкого спектра завдань, орієнтованих на завдання побудови механізмів захисту [1, 2], іх аналізу [3] та експертизи [4]. Всі ці проблеми знайшли відображення в роботах вітчизняних вчених: Згуровский М.З., Новіков О.М., Прокофъев М.І, Задірака В.К., Анісімов А.В., Корченко О.Г., Мохор В.В., Хорошко В.О., Фаль А.М, Архипов О.Є. Так само слід звернути увагу на результати, які отримані в суміжних областях, наприклад: розробка нових нормативних документів Тимошенко А.О. [5]; розвиток теорії діагностики складних систем Коростіль Ю.М.[6]; теорії побудови систем заснованих на знаннях Яловец А.Л. [7].

Отже перед вами стоять три завдання:

- визначення рівнів ФПБ реалізованих КСЗІ об'єкта експертизи;
- визначення повноти та несуперечності профілю;
- ідентифікація опису ФПБ у вхідних документах.

Визначення рівнів ФПБ реалізованих КСЗІ об'єкта експертизи включає попередній аналіз об'єкта експертизи в ході якого шляхом пошагового опрацювання кожної ФПБ формується ФПЗ.

На этапе визначення повноти та несуперечності ФПЗ експерт повинен

перевірити відповідність отриманого на попередньому етапі ФПЗ вимогам визначаємого НД ТЗІ 2.5.004-99.

Останнє завдання, яке повинен вирішити експерт, - це опрацювати вхідні документи на предмет пошуку опису реалізації умов, які пред'являються до кожної ФПБ.

Розглянемо друге завдання більш детально.

Вимоги до ФУБ задані у вигляді таблиць показують відповідність рівня реалізованої послуги переліком необхідних вимог для її коректної роботи.

Для автоматизації перевірки повноти та несуперечності профілю формалізуємо правила, які визначені у НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Перше правило: будь-який профіль зобов'язаний включати в себе контроль цілісності КСЗІ. Позначимо профіль через множіство Fp тоді: Fp = $\{ФПБ0, ФПБ1, \ldots, ФПБN\} \cap НЦ_i \neq \emptyset$,

де ФПБN – функціональна послуга безпеки

$НЦ_i$ – «Цілісність комплексу засобів захист» і-ого рівня.

Більш детально розберемо необхідність цю умову. Розберемо ФПБ «Цілісність комплексу засобів захисту» більш детально. В умовах виконання НЦ рівня 1 сказано: «Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ»; «В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження»; «Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ». Тобто, невиконання цих правил автоматично робить неморжливим гарантування безпеки експлуатації об'єкта експертизи і унеможливлює проведення державної експертизи.

Друге правило: відповідно до НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» деякі з ФПБ є умовно пов'язаними з іншими ФПБ. Іншими словами в НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» при наявності послуг потрібна наявність інших ФПБ, наприклад: для виконання умов ФПБ КД рівня 1 необхідною умовою є виконання умов ФПБ НИ рівня 1. Формалізуємо дану умову: ФПБ КД1 = $\{УКД\ 1, УКД\ 2, \ldots, УКДN\} \cap УКД\ 7.1 \neq \emptyset$. На Рис. 1 для усіх ФПБ показані персонофікований набір необхідних умов виконання даних ФПБ.

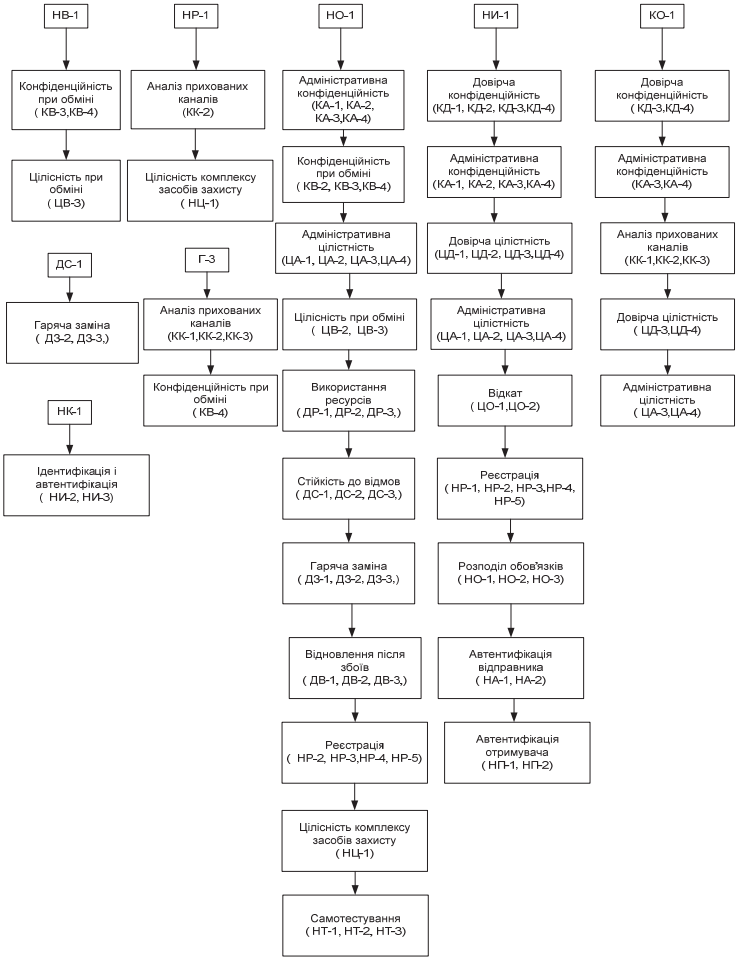

Рис.1 – Необхідний набір умов виконання для кожної ФБП

Третє правило: якщо послуга має усі 4-ри рівня, то в функціональному профілі захисту може бути тільки одна. Третє правило говорить про поглинання старшим ФПБ молодших. Тобто в одному профілі не можуть бути ФПБ однієї спрямованості різного рівня. Наприклад, якщо в ФПБ присутня послуга КД рівня 3 - це автоматично означає, що в даному ФПБ не може міститися послуги КД рівня 1 або 2. Функціональні послуги одного типу мають властивості винятковості, причому пріоритет віддається послугам вищого рівня.

У подальшому постало питання необхідності якось формалізувати, з математичної точки зору, функціональний профіль послуг безпеки (ФППБ).

Функціональний профіль послуг безпеки Fu – це функціональний профіль який включає в себе множину актуальних послуг безпеки реалізованої КСЗІ об'єкта експертизи. ФППБ залежить від 3 параметрів: Кр - група критеріїв; Ri- рівень реалізованої послуги безпеки; Ui -коньюнкція умов реалізації виконання і-тої ФПБ.

Fu (K_{p_r}, R_{i_r}, U_i);

Kp = {C, I, A, O, G};

де C - критерій конфіденційності; I - критерій цілістності; A - критерій доступності; O – критерій спостережності; G = критерій гарантій.

Ri – це кількість рівнів кожної ФПБ, яка персоніфіковано залежить від виду послуги. Максимальний рівень,згідно з нормативним документом НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», четвертий, але в залежності від ФПБ зустрічаються ФПБ з одним рівнем і тому подібне.

Ri = {1, 2, 3, 4};

де,i = 1-23 – це кількість ФПБ згідно з даним ФПЗ, де 23 – це максимальна кількість ФПБ отриманих з нормативного документу НД ТЗІ 2.5.004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Коньюнкція умов реалізації виконання і-тої ФПБ (Ui) – це сума усіх включених ФПБ до профілю захисту, де Ni – кількість умов до і-послуги; Y_{ij} – це j умова реалізації і-ої послуги.

Ui, $R_i = \bigcup_{j=1}^{Ni} Y_j$ F (i, R_i, j) (1.1)

Розглянемо приклад аналізу КД.

КД 1 = {УКД 1.1, УКД 2.1, УКД 3.1,УКД 4.1, УКД 6.1,УКД 7.1}; (1.2)

КД 2 = {УКД 1.1, УКД 2.2, УКД 3.1,УКД 4.2, УКД 5.1, УКД 6.1,УКД 7.1};

КД 3 = {УКД 1.2, УКД 2.2, УКД 3.1,УКД 4.3,УКД 5.2, УКД 6.1,УКД 7.2};

КД 4 = {УКД 1.2, УКД 2.3, УКД 3.1,УКД 4.4,УКД 5.2, УКД 6.1,УКД 7.2};

,де УКД – умова виконання ФПБ «Довірча конфіденційність».

На основі цього побудуємо матрицю значень для кожного рівня ФПБ КД використовуючи рівняння Ui, $R_i = \bigcup_{j=1}^{Ni} Y_j$ F (i, R_i, j) ,

де U = КД, Y = УКД, $\overline{КД} = \overline{УКД}$;

$$КД = \begin{Bmatrix} КД1 \\ КД2 \\ КД3 \\ КД4 \end{Bmatrix} \quad (1.3)$$

Виходячи з цього представимо вектор УКД у вигляді добутку матриц:

$$\text{УКД} = \{\text{УКД1 УКД2 УКД3 УКД4 УКД5 УКД6 УКД7}\} \begin{Bmatrix} 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 4 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{Bmatrix} \quad (1.4)$$

Тоді для КД 1 це буде мати вигляд такий:

$$\text{КД 1} = \text{УКД}\{1\ 2\ 3\ 4\ 5\ 6\ 7\} \begin{Bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{Bmatrix} \quad (1.5)$$

Для КД 2:

$$\text{КД 2} = \text{УКД}\{1\ 2\ 3\ 4\ 5\ 6\ 7\} \begin{Bmatrix} 1 \\ 2 \\ 1 \\ 2 \\ 1 \\ 1 \\ 1 \end{Bmatrix} \quad (1.6)$$

Для КД 3:

$$\text{КД 3} = \text{УКД}\{1\ 2\ 3\ 4\ 5\ 6\ 7\} \begin{Bmatrix} 2 \\ 2 \\ 1 \\ 3 \\ 2 \\ 1 \\ 2 \end{Bmatrix} \quad (1.7)$$

Для КД 4:

$$\text{КД 4} = \text{УКД}\{1\ 2\ 3\ 4\ 5\ 6\ 7\} \begin{Bmatrix} 2 \\ 3 \\ 1 \\ 4 \\ 2 \\ 1 \\ 2 \end{Bmatrix} \quad (1.8)$$

Опис 1.5 - 1.8 є окремими випадками формули 1.1 за умови i = 1. Проведемо обчислення за формулою 1.3, для цього порахуємо добуток матриц згідно з правилом множення матриц: перший елемент першої матриці множимо на перший елемент другої матриці. Далі множимо другий елемент

першої матриці на другий елемент другої матриці і т.д. Коли число столбців в першому сомножнику рівне числу рядків у другому; в цьому випадку говорять, що форма матриц узгоджена. Як наслідок, отримаємо первинний вигляд КД 1 вигляду:

КД1= {УКД 1.1, УКД 2.1, УКД 3.1,УКД 4.1,УКД 6.1,УКД 7.1 }.

Підводячи підсумок слід зазначити, що ми розглянули окремий випадок коньюнкції умов реалізації виконання ФПБ КД. Розглянутий випадок підтверджує відповідність 1.2 до рівняння 1.1. Рівняння 1.1. дозволяє формалізувати процедуру перевірки повноти та несуперечності функціонального профілю захисту. На основі чого був написан програмний модуль для системи підтримки прийняття рішень під час проведення державної експертизи на відповідність інформації циркулюючої в грід-системі.

Висновок. Таким чином, завдання визначення повноти та несуперечності ФПЗ може бути зведена до перевірки запропонованих вище правил, а саме: правило контролю цілістності КСЗІ; правило контролю взаємозв'язку одних ФПБ по відношенню до інших; правило контролю рівнів ФПБ, що дозволяє автоматизувати цей процес шляхом побудови відповідної комп'ютерної системи підтримки прийняття рішень під час проведення державної експертизи на відповідність інформації циркулюючої в грід-системі. Проведена робота дає теоретичну основу для практичної реалізації системи автоматизації перевірки повноти та несуперечності ФПЗ.

1. *Д.П. Зегжда, М.О. Калинин* Методика анализа защищенности информационніх систем //Проблемі информационной безопасности. Компьютерные системы 2002. № 3. С. 7-12.
2. *Алексей Лукацкий* Уверенность безопасников в своих силах поколебалась [Електронний ресурс] – Режим доступу: http://gblogs.cisco.com/ru/asr2016-2/ – Заголовок з екрану.
3. *Крис Касперски* Жизненный цикл червей [Електронний ресурс] – Режим доступу: http://www.allasm.ru/vir_03.php – Заголовок з екрану.
4. *А.Н. Давиденко, М.Р. Шабан* Разработка методики проведения экспертиз комплексных систем защиты информации// Зб. наук. праць ІПМЕ НАН України. – Київ, 2014– Вип. 73. – С. 114-121.
5. *О. М. Новіков, А. О. Тимошенко* Логіко-функціональні моделі безпеки інформації в інформаційно-обчислювальних системах з відкритою архітектурою // Наук. вісті НТУУ "КПІ". - 2002. - № 2. - С. 40-46. - Бібліогр.: 15 назв. - укр.
6. *Я. Гильгурт, Б. В. Дурняк, Ю. М. Коростиль* Противодействие атакам алгоритмической сложности на системы обнаружения вторжений // Моделювання та інформаційні технології. - 2014. - Вип. 71. - С. 3-12.
7. *А.Л. Яловец* Представление и обработка знаний с точки зрения математического моделирования/ А.Л. Яловец – М. Наукова Думка, 2011. –358 с.

Поступила 14.09.2016 р.