УДК 681.3.06

МЕТОДИ ПОБУДОВИ ТА ВЕРИФІКАЦІЇ НЕСУПЕРЕЧНОСТІ І ПОВНОТИ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

О.В. ПОТІЙ, А.В. ЛЄНШИН

Проведено аналіз вимог нормативних документів в частині формування профілів захищеності. Визначені недоліки існуючого підходу до формування профілю захищеності. Сформульовані вимоги до методу формування та методу верифікації несуперечності і повноти профілів захищеності, надано їх опис. Показано, що розроблені методи відповідають вимогам із: часової складності, стандартизованості підходу (повторюваність і порівнюваність результатів), несуперечності нормативним документам, зрозумілості проміжних результатів та їх впливів на остаточний вибір, а також можливості самоперевірки особи, що використовує метод.

Ключові слова: профіль захищеності, несанкціонований доступ, методи системного аналізу.

ВСТУП

Захист інформації з обмеженим доступом, а також інформації, захист якої гарантується державою, має здійснюватися за рахунок створення комплексної системи захисту інформації (далі – КСЗІ) [1]. Основним документом, що регламентує порядок розробки та впровадження КСЗІ, є технічне завдання. Технічне завдання має містити вимоги із захисту від несанкціонованого доступу (далі – НСД), а також витоку інформації технічними каналами. Для того, щоб викласти вимоги із захисту від НСД, в Україні використовується механізм функціональних профілів захищеності (далі – ФПЗ) від НСД, що мають відповідати вербальній та/або формалізованій політиці безпеки комплексу засобів захисту комп'ютерної системи (далі – КС). У вітчизняній літературі під КС розуміється сукупність програмно-апаратних засобів, яка подана для оцінки. Тобто фактично КС є аналогом об'єкта оцінки (ТОЕ – Target Of Evaluation) за ISO/IEC 15408, відомого під назвою "Єдині критерії".

На відміну від міжнародного стандарту ISO/IEC 15408, вітчизняні документи системи технічного захисту інформації, на жаль, не містять практичних рекомендацій щодо порядку вибору функціональних послуг безпеки, що мають задовольнити цілям безпеки конкретної організації. Ось чому, сучасний український фахівець при проектуванні системи захисту інформації власноруч має боротися із проблемою відсутності науково-обґрунтованої методики розробки ФПЗ, яка б забезпечувала не лише такі важливі властивості, як порівнюваність та повторюваність результатів експертизи, але б і надавали засоби самоперевірки та інтеграції з іншими процесами зі створення КСЗІ. Єдиним механізмом, що незважаючи на свою недосконаліть закріплений у нормативних документах України, є механізм стандартних ФПЗ, що рекомендовані до використання у автоматизованих системах різного класу (відокремленої, однокористувацької робочої станції, локальної обчислювальної мережі чи розподіленої системи із передачею інформації через глобальну мережу Інтернет).

Аналіз підходу закріпленого у НД ТЗІ 2.5-004-99 показав, що використання стандартних ФПЗ можливо лише у якості відправної точки, що полегшує вибір узгодженого набору функціональних послуг для КС, що функціонує у складі автоматизованої системи певного класу. Проте, у разі необхідності врахування конкретних загроз, чи недоцільності (наприклад, з економічної точки зору) використання певної послуги безпеки виникають завдання, розв'язання яких за обсягом не поступається розробці ФПЗ з "нуля".

Зважаючи на вищезазначене, було поставлено таку ціль роботи: проаналізувати існуючи підходи до формування ФПЗ та розробити методи, які б дозволили не лише формувати ФПЗ, але і перевіряти несуперечність запропонованих варіантів та достатність послуг безпеки, що входять до складу ФПЗ. У цій статті наводяться основні результати проведених досліджень та ставляться завдання на подальше вдосконалення запропонованих методів.

1. ДОСЛІДЖЕННЯ ПІДХОДІВ З РОЗРОБКИ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ В УКРАЇНІ

У 1999 році в Україні введено в дію НД ТЗІ 2.5-004-99 [2], який визначає критерії оцінки захищеності КС від НСД та НД ТЗІ 2.5-005-99 [3], що надає нормативно-методологічну базу для вибору та реалізації вимог із захисту інформації в АС. Незважаючи на те, що минуло 11 років, а підходи до проектування та оцінювання систем захисту інформації пройшли кілька етапів еволюційного розвитку (це підтверджується наявністю вже третьої версії всесвітньо-визнаного аналогу зазначених документів – ISO/IEC 15408) в Україні ці документи не переглядалися жодного разу.

Важливим кроком у цьому напрямку, на нашу думку, є прийняття НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09, що призначені для оцінювання функціональних послуг безпеки, оцінювання рівня

гарантій коректності реалізації функціональних послуг безпеки. Але поза кадром на сьогодні залишилося питання, яким чином первинно обґрунтувати склад ФПЗ. Основним призначенням НД ТЗІ 2.5-004-99 є надання порівняльної шкали для оцінки надійності механізмів захисту та орієнтирів для розробки КС із функціями захисту інформації. Слід зауважити, що функціональні послуги з НД ТЗІ 2.5-004-99 мають по кілька рівнів, які у загальному випадку знаходяться у ієрархічній залежності (у сенсі рівня захисту, що забезпечується від загроз певного типу).

Сукупність критеріїв щодо реалізації функціональної послуги безпеки на певному рівні подані у табличному вигляді, рядки таблиці фактично є специфікаціями, наявність яких є достатньою для підтвердження реалізації у КЗЗ певного рівня заданої послуги безпеки.

У табл. 1 наведено формалізоване подання специфікації на прикладі послуги "Довірча конфіденційність". У таблиці 1 не вказані конкретні вимоги, а використовуються лише такі позначення: знак "+" на перетині рядка (що вказує на специфікацію) та стовпця (що визначає рівень послуги) позначає, що відповідна специфікація є обов'язковою для визначеного рівня послуги, знак "–" вказує на відсутність необхідності реалізації вимог відповідної специфікації, а об'єднані комірки позначають, що вимоги не відрізняються для рівнів послуг, що визначаються відповідними стовпцями.

У документі [3] визначено підхід до визначення ФПЗ шляхом вибору з множини стандартних ФПЗ. Зважаючи на те, що цей підхід є єдиним, що визначений у НД ТЗІ та для спрощення викладення матеріалів, далі у статті використовується термін "стандартний підхід". Стандартний підхід базується на таких припущеннях:

а) Усі АС можна віднести до одного з трьох класів за наступними ознаками: конфігурація апаратних засобів, їх фізичне розміщення, кількість категорій оброблюваної інформації, кількість користувачів і категорій користувачів.

б) У межах класу АС можна віднести до одного з підкласів, що визначені за критерієм необхідності забезпечення: конфіденційності, цілісності та доступності інформації. Таким чином, кількість сполучень з трьох властивостей зумовлює наявність семи підкласів АС (табл. 2).

в) Вимоги до безпеки АС різних класів суттєво відрізняються, що дозволяє сформувати для їх підкласів множини стандартних ФПЗ, що знаходяться у ієрархічній залежності (реалізація забезпечує наростаючу захищеність від загроз певного типу).

г) Для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Визначено такі етапи застосування стандартного підходу для визначення ФПЗ для КС, що використовується у складі АС.

Е1) Визначення класу АС. Е2) Визначення, яке сполучення вимог конфіденційності, цілісності, доступності висувається до АС. Е3) Визначення призначення АС та вибір підказки ("маски"), яку треба використовувати у цьому випадку для вибору одного зі стандартних ФПЗ (використовуючи довідковий додаток А з НД ТЗІ 2.5-005-99). Якщо призначення АС відрізняється від наведених у [3], необхідно власноруч обрати підмножину стандартних ФПЗ, відповідно до класу АС, у якій експлуатується КС. Е4) Аналіз сутності вимог, відібраних стандартних ФПЗ. Е5) Вибір одного зі стандартних ФПЗ, що найбільш відповідає політиці безпеки КЗЗ КС. Е6) У випадку, коли жоден із стандартних ФПЗ не підходить повною мірою, необхідно змінити рівень послуги, що міститься у стандартному ФПЗ, або додати нову послугу. При цьому необхідно врахувати залежності між послугами, що визначені у НД ТЗІ 2.5-004-99.

Визначимо переваги та недоліки, що притаманні стандартному підходу. Основними перевагами є відносна простота за рахунок: наявності готових шаблонів ФПЗ для КС, можливості звуження простору вибору за рахунок визначення призначення АС (автоматизації діяльності органів державної влади, автоматизації банківської діяльності, керування технологічними процесами, довідково-пошукові системи), до складу якої входять КС, врахування необхідних зв'язків між послугами, що входять до складу стандартних ФПЗ. До основних недоліків слід віднести: значну

Таблиця 1

Приклад специфікації послуги "Довірча конфіденційність" з НД ТЗІ 2.5-004-99

Специфікація \ Рівні послуги	КД-1	КД-2	КД-3	КД-4
Множина об'єктів, яких стосується політика послуги	+		+	
Атрибути доступу, що використовує КЗЗ	+	+		+
Обробка запитів на зміну прав доступу	+	+	+	+
Правила керування доступом до об'єктів домену	+	+	+	+
Правила керування доступом до процесів домену	–	+	+	
Початкові права доступу та правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	+			
Необхідні умови (залежності послуги)	НИ-1		КО-1, НИ-1	

складність (особливо часову) детального аналізу послуг безпеки, що входять до складу стандартних ФПЗ, відсутність формалізованого (та зрозумілого користувачу) зв'язку між включеними до стандартного ФПЗ послугами безпеки (їх рівнями) та загрозами і ризиками для конкретної КС. Власне кажучи, недоліки стандартного методу є наслідком його основної переваги. Стандартний ФПЗ не може повністю відповідати вимогам довільної КС, якщо кількість стандартних ФПЗ не дорівнює загальній кількості можливих ФПЗ, а у випадку рівності цих величин це вже не стандартні ФПЗ, а "припустимі профілі". Звісно, що використання у стандартному підході "припустимих профілів" призвело б до надвеликої складності їх належного аналізу. Кількість стандартних ФПЗ для окремих підкласів [3] визначені у табл. 2.

Таблиця 2

Результати кількісного аналізу стандартних ФПЗ з НД ТЗІ 2.5-005-99

Клас АС	Кількість стандартних ФПЗ для підкласів АС							Загальна кількість стандартних ФПЗ
	К	Ц	Д	КЦ	КД	ЦД	КЦД	
АС-1	2	2	4	2	4	4	4	22
АС-2	6	5	4	6	4	4	5	34
АС-3	6	5	4	6	4	4	5	34

Проведений аналіз [2] показав, що послуги безпеки вважаються більш-менш незалежними, за небагатьма виключеннями: послуга НЦ (цілісність КЗЗ) перший рівень якої, тобто НЦ-1, є обов'язковим для реалізації усіх інших послуг безпеки, а також деякими іншими залежностями, основними з яких є необхідність у реалізації послуг НО (розподіл обов'язків) та НИ (ідентифікація та автентифікація). Як видно з припущення б) щодо стандартного методу така властивість інформації як "спостереженість" не використовується для розбиття АС на підкласи. У роботі [3] цей факт пояснюється тим, що послуги спостереженості є необхідною умовою для реалізації інших послуг, а з іншого боку завжди важлива для КС. Проте швидше за все, не внесення властивості "спостережність" як такої, що визначає підклас, зумовлено тим, що розробники намагалися зменшити обсяг роботи особи, яка приймає рішення (ОПР) щодо вибору ФПЗ за рахунок зменшення кількості стандартних ФПЗ.

2. ДОСЛІДЖЕННЯ НЕСУПЕРЕЧНОСТІ ТА ДОСТАТНОСТІ СТАНДАРТНИХ ФПЗ, ЩО ВИЗНАЧЕНІ У НД ТЗІ 2.5-005-99

Перед тим як викласти результати дослідження несуперечності та достатності стандартних ФПЗ наведемо семантику їх опису, як вона визначається у НД ТЗІ 2.5-005 -99:

1.Д.4 = {ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}. (1)

Опис профілю складається з трьох частин: буквено-числового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Як визначається НД ТЗІ 2.5-005-99: "Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків." Отже для розробки ФПЗ для конкретної КС необхідно проведення аналізу та оцінки ризиків є обов'язковим.

Задамо собі питання: "Яку частину можливого простору припустимих варіантів ФПЗ покривають стандартні ФПЗ?". Для надання відповіді обчислимо граничні значення кількості "припустимих" ФПЗ із застосуванням комбінаторного підходу. Нехай існує множина $\{abcd\}$, така, що $a=\overline{1,N_a}$, $b=\overline{1,N_b}$, $c=\overline{1,N_c}$, $d=\overline{1,N_d}$, тоді кількість можливих варіантів розраховуватиметься як:

$$M_{abcd} = N_a \cdot N_b \cdot N_c \cdot N_d . \qquad (2)$$

Розглянемо кілька прикладів для ілюстрації способу застосування виразу (2).

Приклад 1:

Нехай: $N_a = N_b = N_c = N_d = 10$, тоді кількість можливих варіантів: $M_{abcd} = 10^4$ (0-9999). Такий результат легко зрозумілий, оскільки така множина дорівнює діапазону десяткових цифр чотиризначного PIN-коду, з яким кожен з нас зустрічається у повсякденній практиці використання кредитних карток.

Приклад 2:

Нехай: $N_a = 2, N_b = 2, N_c = 3$, тоді кількість можливих варіантів: $M_{abcd} = 2 \cdot 2 \cdot 3 = 12$ (дивись дані таблиці 3).

Таблиця 3

Множина варіантів комбінацій для прикладу 2

A	b	c
1	1	1
1	1	2
1	1	3
1	2	1
1	2	2
1	2	3

a	b	c
2	1	1
2	1	2
2	1	3
2	2	1
2	2	2
2	2	3

Розглянувши ці прості приклади, можна безпосередньо перейти до розрахунку нижньої (S_L) та верхньої (S_H) границі кількості "припусти-

мих" ФПЗ. Для обчислення нижньої границі нам необхідно знати кількість рівнів для кожної i – й послуги безпеки, тобто знати множину $\{N_i\}, i=\overline{1,I}$, де I - загальна кількість послуг безпеки (для випадку НД ТЗІ 2.5-004-99: $I=22$). Використовуючи вираз (2) та дані таблиці 4, маємо, що $S_L \approx 7\cdot 10^9$ варіантів. Така оцінка справедлива, якщо ми вважатимемо, що в довільному ФПЗ обов'язково мають бути представлені усі функціональні послуги, але такої вимоги не висувається, тому кількість можливих рівнів для кожної i-ої послуги (враховуючи нульовий рівень, коли послуги відсутні у ФПЗ) дорівнюватиме $N_i^+ = N_i + 1$. Отже $S_H \approx 6{,}3\cdot 10^{12}$. Вихідні дані та результати розрахунків зведені до табл. 4.

Таблиця 4

Розрахунок верхньої та нижньої границі кількості можливих ФПЗ

i	Послуга	N_i	N_i^+	i	Послуга	N_i	N_i^+
1	КД	4	5	12	ДЗ	3	4
2	КА	4	5	13	ДВ	3	4
3	КО	1	2	14	НР	5	6
4	КК	3	4	15	НИ	3	4
5	КВ	4	5	16	НК	2	3
6	ЦД	4	5	17	НО	3	4
7	ЦА	4	5	18	НЦ	3	3*
8	ЦО	1	2	19	НТ	3	4
9	ЦВ	3	4	20	НВ	3	4
10	ДР	3	4	21	НА	2	3
11	ДС	3	4	22	НП	2	3
Кількість варіантів							
Нижня границя:		7 255 941 120		Верхня границя:		6 370 099 200 000	

* Оскільки будь-який ФПЗ має включати послугу НЦ, послуга не має нульового рівня.

Розгляд НД ТЗІ 1.1-002-99 "Загальні положення про захист інформації в КС від НСД" показує, що при наданні послуг конфіденційності та цілісності може бути використаний довірчий або адміністративний принципи керування доступом.

Під довірчим керуванням доступом слід розуміти таке керування, при якому засоби захисту дозволяють звичайним користувачам управляти (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами), тобто призначення і передача повноважень не вимагають адміністративного втручання.

Адміністративне керування доступом – керування, при якому керувати потоками інформації між користувачами та об'єктами дозволено лише адміністраторам (авторизованим користувачам).

Не важко помітити, що ці принципи є взаємовиключними, тобто не можуть одночасно застосовуватися до одного і того ж об'єкта. Множини об'єктів КС, до якої мають застосовуватися послуги з довірчим чи адміністративним принципом керування доступу, зведені до табл. 5.

У ході дослідження несуперечності стандартних ФПЗ було з'ясовано, що деякі з них вказують на необхідність одночасного застосування послуг, що базуються на різних принципах керування доступом, але відносяться до всіх об'єктів КС. Результати проведеного аналізу з врахування семантики ФПЗ та даних табл. 5 зведені до табл. 6.

Таблиця 5

Визначення множини об'єктів для послуг КД, КА, ЦД, ЦА

№	Рівні послуги	Політика ПОСЛУГИ, що реалізується КЗЗ, повинна
1	КД–1, КД-2, ЦД-1, ЦД-2, КА–1, КА-2, ЦА-1, ЦА-2	визначати множину об'єктів КС, до яких вона відноситься
2	КД–3, КД-4, ЦД-3, ЦД-4, КА–3, КА-4, ЦА-3, ЦА-4	відноситись до всіх об'єктів КС

Підводячи підсумки вищенаведеного, можна стверджувати, що:

– стандартні ФПЗ перекривають незначну частину простору припустимих ФПЗ;

– у стандартних ФПЗ присутні неточності типу "друкарські помилки" та "несумісне використання рівнів послуг";

– згідно рекомендацій з НД ТЗІ 2.5-005-99 для побудови адекватної загрозам системи захисту обов'язково необхідно здійснювати аналіз ризиків, результати якого мають використовуватися для уточнення чи розробки ФПЗ;

– уточнення стандартного ФПЗ за складністю можна порівняти з формуванням ФПЗ наново.

3. МЕТОД ПОБУДОВИ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ВІД НСД

Проведений у першому розділі аналіз та недоліки стандартного підходу дозволив сформулювати такі вимоги до методу, що розробляється [4]:

– зручність застосування (В1);

– зрозумілість проміжних результатів та їх впливу на остаточний склад ФПЗ (В2);

– врахування вимог нормативних документів у сфері ТЗІ (В3);

– коректність переходів між різними етапи визначення складу ФПЗ (В4);

– можливість самоперевірки ОПР (В5);

– наявність формалізованого процесу вибору та можливість використання результатів для документування ходу вибору елементів ФПЗ (В6);

– можливість інтеграції з іншими етапами побудови КСЗІ (В7).

Під В1 розуміється, логічність та ненадлишковість викладення текстової частини та використання у методі допоміжного інструментарію (наприклад, опитувальних листів, таблиць, формул, рисунків), що дозволять ОПР зосередитися на виконанні безпосередньо вирішуваної задачі

Таблиця 6

Стандартні ФПЗ, що не задовольняють висунутим вимогам

№	СФПЗ	Зауваження
1	1.К.1	Не зрозуміло, яким чином забезпечується конфіденційність інформації, що обробляється, оскільки послуги конфіденційності відсутні у СФПЗ
2	1.Ц.1	Не зрозуміло, яким чином забезпечується цілісність інформації, що обробляється, оскільки послуги цілісності відсутні у СФПЗ
3	1.КЦ.1	Не зрозуміло, яким чином забезпечується конфіденційність та цілісність інформації, що обробляється, оскільки послуги конфіденційності та цілісності відсутні у СФПЗ
4	2.К.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
5	2.К.6	Одночасна наявність послуг: КД-4, КА-4 є неможливою
6	2.Ц.5	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
7	2.КЦ.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
8	2.КЦ.6	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою
9	2.КД.3	Одночасна наявність послуг: КД-3, КА-3 є неможливою
10	2.КД.4	Одночасна наявність послуг: КД-4, КА-4 є неможливою
11	2.ЦД.4	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
12	2.КЦД.4	Одночасна наявність послуг: КД-3, КА-3 є неможливою
13	2.КЦД.5	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою
14	3.К.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
15	3.К.6	Одночасна наявність послуг: КД-4, КА-4 є неможливою
16	3.Ц.5	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
17	3.КЦ.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
18	3.КЦ.6	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою
19	3.КД.3	Одночасна наявність послуг: КД-3, КА-3 є неможливою
20	3.КД.4	Одночасна наявність послуг: КД-4, КА-4 є неможливою
21	3.ЦД.4	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
22	3.КЦД.4	Одночасна наявність послуг: КД-3, КА-3 є неможливою
23	3.КЦД.5	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою

– виборі елементів ФПЗ, а не на вивченні особливостей методу.

Під В2 розуміється можливість ОПР відстежувати, яким чином її вибір на певному кроці впливає на проміжні/остаточні результати. Реалізація цієї вимоги необхідна для більшого залучення та творчої реалізації потенціалу ОПР, та надання можливості пошуку причин невідповідності (якщо такі є) сформованого ФПЗ наперед визначеним цілям або вимогам більш високого рівня, а також надання можливості вдосконалення/уточнення сформованого ФПЗ.

Вимога В3 передбачає несуперечність вимогам/підходам, що викладені у діючих нормативних документах, а також розвиток принципів, що були задекларовані в них.

Для задоволення В4 алгоритм, що має бути покладений у основу метода, має забезпечувати відсутність "тупикових" ситуацій, тобто випадків, в яких виникає неоднозначність трактування результатів (проміжних/остаточних) методу.

Необхідність виконання вимоги В5 полягає у підвищенні якості результатів процесу формування ФПЗ, зокрема несуперечності положенням НД ТЗІ, а також надання ОПР можливості проконтролювати правильність своїх дій.

Вимога В6 висувається з метою підвищення рівня гарантій стосовно процесу розробки ФПЗ та загальної зрілості процесів захисту інформації.

Під В7 необхідно розуміти можливість використання результатів методу для виконання інших робіт зі створення КСЗІ, а також врахування у методі результатів попередніх етапів (наприклад, вимоги політики безпеки та моделі загроз).

Аналіз підстав для ранжирування рівнів послуг (табл. 7) показує, що формально можна виділити 15 таких груп. Проте кожний рівень послуги, залежить передусім від загрози, що блокується чи попереджається. Таке спостереження підтверджується аналізом вимог НД ТЗІ 2.5-004-99:

1. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів.

2. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

3. Рівні починаються з першого (1) і зростають до значення n, де n — унікальне для кожного виду послуг.

Твердження 1. Вибір рівня послуги однозначно зумовлюється загрозою, якій має протистояти КЗЗ чи КСЗІ.

При розробці методу було зроблено спробу представити необхідні дії ОПР у вигляді алгоритму (рис. 1). Проте на практиці це виявилось не

Таблиця 7

Результати аналізу підстав ранжирування функціональних послуг з НД ТЗІ 2.5-004-99

№	Позначення	Підстава ранжирування рівнів послуг
1	КД, КА, КВ, ЦД, ЦА, ЦВ	повнота захисту і вибірковість керування
2	ДЗ, НВ	повнота реалізації
3	КО	-
4	КК	здійснення виявлення, контролю або перекриття прихованих каналів
5	ЦО	множина операцій, для яких забезпечується відкат
6	ДР	повнота захисту і вибірковість керування доступністю послуг КС
7	ДС	спроможність КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови
8	ДВ	міра автоматизації процесу відновлення
9	НР	повнота і вибірковість контролю, складність засобів аналізу даних журналів реєстрації і спроможність вияву потенційних порушень
10	НИ	число задіяних механізмів автентифікації
11	НК	гнучкість надання можливості КЗЗ або користувачу ініціювати захищений обмін
12	НО	вибірковість керування можливостями користувачів і адміністраторів
13	НЦ	міра здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами
14	НТ	можливість виконання тестів у процесі запуску або штатної роботи
15	НА, НП	можливість підтвердження результатів перевірки незалежною третьою стороною

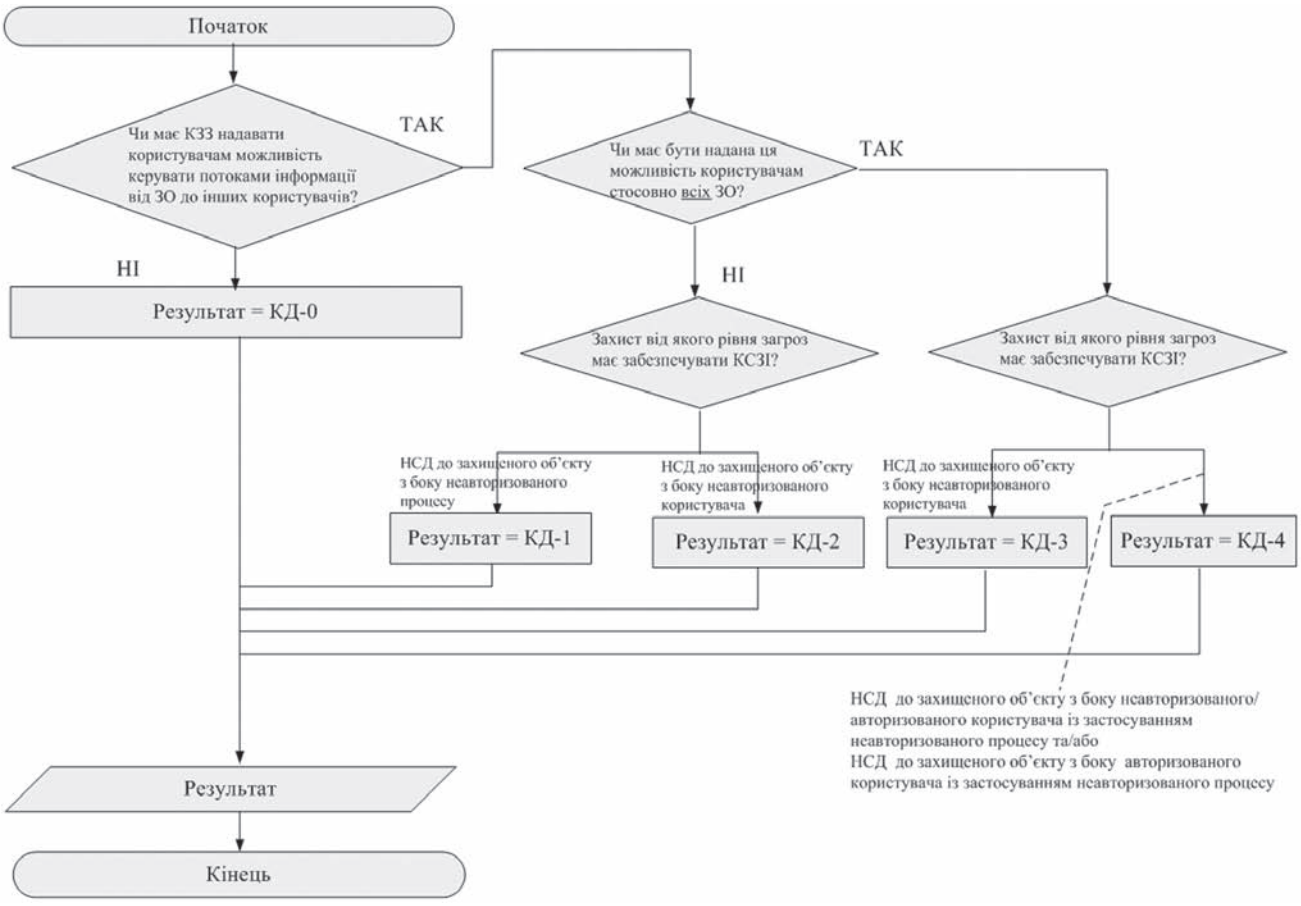

Рис. 1. Алгоритм визначення необхідності включення (та/або рівня) послуги "Довірча конфіденційність"

зручним (вимога В1). Тому алгоритми з'ясування необхідності та рівня послуги безпеки були подані у табличному вигляді (табл. 8).

Таблиця містить 8 основних стовпців: "№", "Запитання", "Відповіді", "Результат", "Перехід до". Стовпець "№" визначає номер кроку експерта по роботі з даною послугою. Стовпець "Запитання" містить формулювання питання закритого типу (тобто такого, що передбачає наявність готових відповідей). Стовпець "Відповіді" розбитий на два підстовпця, в яких по групах наведені варіанти відповідей, з яких має обрати експерт. Стовпець "Результат" також розбито на два підстовпця, в яких наведено зміст отриманого результату, а також його тип "П" (проміжний) чи "О" (остаточний). У останньому стовпці "Перехід до" визначено, до якого кроку слід перейти експерту і яку групу варіантів відповідей він має використовувати при наданні подальших оцінок.

Усього метод містить двадцять дві таких таблиці (за кількістю визначених у НД ТЗІ 2.5-004-99 послуг безпеки). Усі таблиці мають вищеописану структуру (табл. 8) і відрізняються лише наповненням та кількістю кроків (а отже і кількістю рядків), що має пройти експерт.

4.МЕТОД ВЕРИФІКАЦІЇ ПОВНОТИ І НЕСУПЕРЕЧНОСТІ ФПЗ ВІД НСД

Результати дослідження несуперечності стандартних ФПЗ наведені у розділі 2, дозволяють стверджувати, що розробник ФПЗ буде зіткатися із задачею перевіряння розробленого ним ФПЗ.

У загальному випадку розробник ФПЗ може припустити помилки трьох видів:

– не повністю перекрити існуючи загрози;

– не включити до складу ФПЗ залежні (підтримуючі) послуги;

– включити послуги, що не можуть використовуватися спільно.

Для першого виду помилки характерна неможливість її викриття без повторного аналізу загроз, і отже її відсутність пропонується забезпечувати за рахунок запропонованого у статті методу (розділ 3).

Помилки другого та третього виду викриваються достатньо легко за рахунок використання матриць (таблиць) залежностей. Одним із прикладів таких матриць залежностей є морфологічна скринька (рис. 2). У такій таблиці на перетині рядків та стовпців визначається, чи може сумісно використовуватися послуги певних рівнів. Враховуючи те, що основна кількість помилок відноситься до виду "неповнота ФПЗ", у такій морфологічній скриньці слід включити так звані "нульові рівні" послуг. Включення нульового рівня послуги дозволяє у матричному вигляді задати заборону на відсутність послуги у разі використання залежної від неї послуги.

Як видно з рис. 2, користуватися морфологічною скринькою, складеною на основі врахування залежності між функціональними послугами, що визначені у НД ТЗІ 2.5-004-99, незручно унаслідок її надвеликого розміру. До того ж, у разі врахування лише безпосередніх залежностей (як це зроблено у таблицях НД ТЗІ 2.5-004-99) використання морфологічної скриньки може призвести до певних непорозумінь, наприклад, вказано, що рівні

Таблиця 8

Визначення необхідності включення (та/або рівня) послуги "Довірча конфіденційність" табличним способом

№	Запитання	Відповіді		Результат		Перехід до
		Гр.	Варіанти відповіді	Зміст	Тип*	
1	Чи має КЗЗ надавати користувачам (не адміністраторам) можливість керувати потоками інформації від захищених об'єктів КС до інших користувачів?	а)	Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно окремих захищених об'єктів.	Максимальний рівень послуги: "КД-2"	П	п.2 гр. а)
			Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно всіх захищених об'єктів.	Мінімальний рівень послуги: "КД-3"	П	п.2 гр. б)
			Ні. КЗЗ має заборонити таку можливість.	У профіль не потрібно включати послугу "КД"	О	
2	Захист від якого рівня загроз має забезпечувати КСЗІ?	а)	НСД до захищеного об'єкту із застосуванням неавторизованого процесу	Рівень послуги: "КД-1"	О	
			НСД до захищеного об'єкту з боку неавторизованого користувача	Рівень послуги: "КД-2"	О	
		б)	НСД до захищеного об'єкту з боку неавторизованого користувача	Рівень послуги: "КД-3"	О	
			НСД до захищеного об'єкту з боку неавторизованого/авторизованого користувача із застосуванням неавторизованого процесу та/або НСД до захищеного об'єкту з боку авторизованого користувача із застосуванням неавторизованого процесу	Рівень послуги: "КД-4"	О	

послуги ДС (ДЗ, ДВ тощо) можуть використовуватися без послуги НИ, але ж це не вірно, оскільки послуга ДС вимагає наявності хоча б першого рівня послуги НО, що в свою чергу тягне за собою щонайменше перший рівень послуги НИ.

Для усунення зазначених недоліків, пропонується розбити морфологічну скриньку на частини. У одній частині (представлена табл. 9) елементом на перетині рядка та стовпця буде визначатися можливість одночасної наявності у ФПЗ послуг з певними рівнями (якщо стоїть "х" одночасно використовувати відповідні рівні послуг у одному ФПЗ заборонено). У другій частині (представлена табл. 10) елементом на перетині рядка та стовпця буде визначатися наявність помилки "неповнота ФПЗ".

Враховуючи те, що велика кількість рівнів послуг ускладнює роботу експерта (розробника), було запропоновано вдосконалений спосіб виявлення помилок типу "неповнота ФПЗ" (таблиці 10 та 11), що має наступні переваги:

– зменшення розмірності таблиці;

– прискорення процесу роботи з таблицями перевірки;

– врахування перехресних посилань (врахування неявної залежності ПОСЛУГА → НО → НИ);

– простота підрахунку послуг, що залежать (обчислення суми по рядкам).

Зменшення розмірності таблиці було досягнуто за рахунок групування рівнів послуг безпеки по групах (11 груп).

Для прискорення процесу роботи з таблицями перевірки було запропоновано використовувати так звані "індекси послуги" (табл. 11). Сутність індексів послуг полягає у наступному: розробник виписує номери, що відповідають рівню послуги (табл. 11) та ставить прапорці у стовпцях з цими порядковими номерами (табл. 10). За рахунок

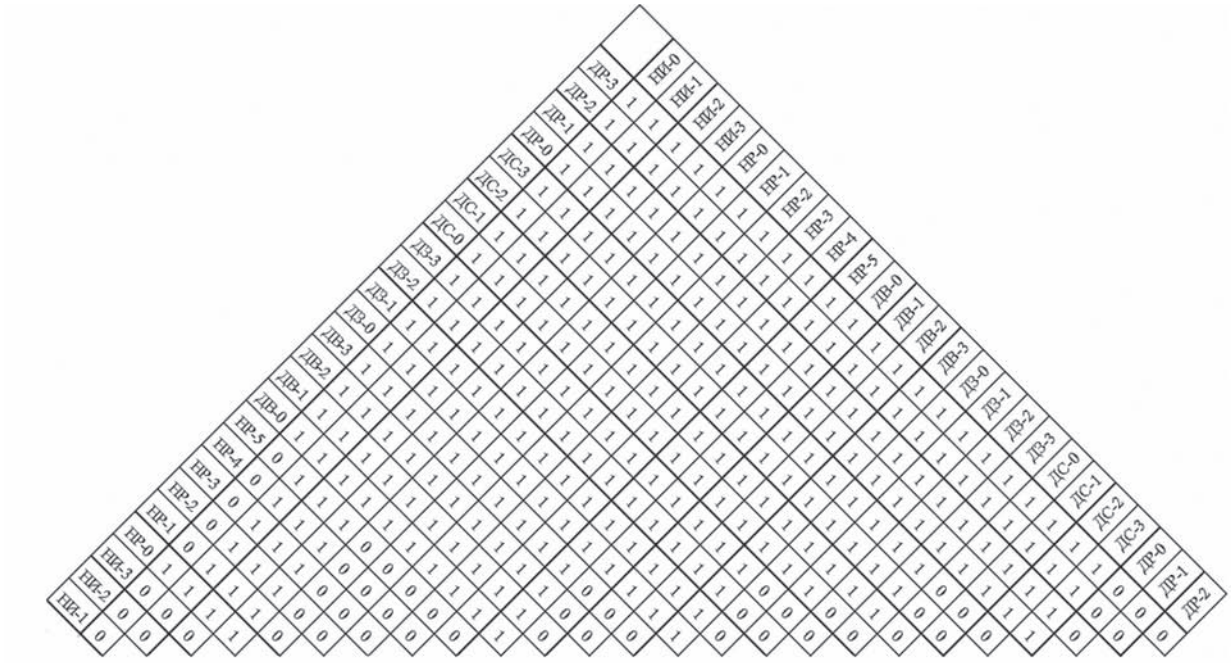

Рис. 2. Фрагмент (26х26) морфологічної скриньки для виявлення помилок типу "неповнота ФПЗ" (реальний розмір повної морфологічної скриньки 89х89)

Таблиця 9

Таблиця перевірки несуперечності послуг з ФПЗ

			Наявність послуги															
			КД-1	КД-2	КД-3	КД-4	КА-1	КА-2	КА-3	КА-4	ЦД-1	ЦД-2	ЦД-3	ЦД-4	ЦА-1	ЦА-2	ЦА-3	ЦА-4
			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Наявність послуги	КД-1	☐							x	x								
	КД-2	☐							x	x								
	КД-3	☐							x	x								
	КД-4	☐							x	x								
	КА-1	☐			x	x												
	КА-2	☐			x	x												
	КА-3	☐			x	x												
	КА-4	☐			x	x												
	ЦД-1	☐															x	x
	ЦД-2	☐															x	x
	ЦД-3	☐															x	x
	ЦД-4	☐															x	x
	ЦА-1	☐											x	x				
	ЦА-2	☐											x	x				
	ЦА-3	☐											x	x				
	ЦА-4	☐											x	x				

Таблиця 10

Виявлення помилок типу “Неповнота ФПЗ”

			Наявність послуги																																			
			КО-1	КВ-1	ЦВ-1	НИ-1	НК-1,2	НЦ-2,3	НВ-1,2,3	КД-1,2	ЦД-1,2	ЦО-1,2	НР-1	НО-1,2,3	НА-1,2	НП-1,2	КА-1,2	КВ-2	ЦА-1,2	ЦВ-2	ДР-1,2, 3	ДС-1,2, 3	ДЗ-1	ДВ-1, 2, 3	НР-2,3,4,5	НТ-1,2, 3	КД-3,4	ЦД-3,4	КА-3,4	ЦА-3,4	КВ-3	ЦВ-3	НЦ-1	КВ-4	ДЗ-2,3	НИ-2,3	КК-1, 3	КК-2	Сума
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
Відсутність послуги	НЦ	☐	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	
	НИ	☐								x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			x	
	КО	☐																									x	x	x	x						x	x	
	НО	☐															x	x	x	x	x	x	x	x	x	x			x	x	x	x	x	x				
	НВ	☐																													x	x		x				
	НР	☐																															x	x				x	
	НК	☐																																		x			
	ДС	☐																																	x			
Код помилки			П0							П1							П2										П3		П4		П5		П6	П7	П8	П9	П10	П11	
Кількість помилок			0																																			

Таблиця 11

Прискорення пошуку за рахунок обчислення індексу послуги

Назва послуги	Позначення послуги	Рівні послуги					Індекс послуги
		1	2	3	4	5	
Довірча конфіденційність	КД	8	8	25	25		
Адміністративна конфіденційність	КА	15	15	27	27		
Повторне використання об'єктів	КО	1					
Аналіз прихованих каналів	КК	35	36	35			
Конфіденційність при обміні	КВ	2	16	30	32		
Довірча цілісність	ЦД	9	9	26	26		
Адміністративна цілісність	ЦА	17	17	28	28		
Відкат	ЦО	10	10				
Цілісність при обміні	ЦВ	3	18	30			
Використання ресурсів	ДР	19	19	19			
Стійкість до відмов	ДС	20	20	20			
Гаряча заміна	ДЗ	21	33	33			
Відновлення після збоїв	ДВ	22	22	22			
Реєстрація	НР	11	23	23	23	23	
Ідентифікація і автентифікація	НІ	4	34	34			
Достовірний канал	НК	5	5				
Розподіл обов'язків	НО	12	12	12			
Цілісність КЗЗ	НЦ	31	6	6			
Самотестування	НТ	24	24	24			
Автентифікація при обміні	НВ	7	7	7			
Автентифікація відправника	НА	13	13				
Автентифікація одержувача	НП	14	14				

того, що ФПЗ за визначенням є: “.. упорядкований перелік рівнів функціональних послуг” (упорядкованість визначається порядком викладення специфікацій послуг у НД ТЗІ 2.5-004-99) перевірка відсутності помилок другого та третього виду для ФПЗ будь-якої складності займає не більше кількох хвилин.

Слід звернути увагу, що при користуванні таблицею 10, прапорець у послугах, що зазначені ліворуч (залежні послуги) позначає, що послуга відсутня у ФПЗ, що верифікується, а прапорці у стовпцях навпаки позначають, що послуга із зазначеним рівнем включена до складу ФПЗ, що верифікується.

Загальний алгоритм роботи експерта з перевіряння несуперечності та повноти ФПЗ може бути викладений у такий спосіб:

– виписати ФПЗ, що верифікується;

– перевірити за табл. 9, чи не присутні в ФПЗ послуги, що не можуть одночасно використовуватися;

– перевірити (з використанням табл. 10 та 11), чи включені до ФПЗ усі залежні послуги;

– у випадку відсутності у ФПЗ, що верифікується, залежних послуг, підрахувати (підсумувавши кількість “x” у рядку) кількість елементів, що зумовили цю помилку;

– підготувати звіт з результатів перевірки.

Розроблений метод верифікації несуперечності та повноти ФПЗ від НСД може використовуватися як для перевірки ФПЗ, що розроблені за методом, викладеним у розділі 3, так і для перевірки будь-якого іншого ФПЗ, що розроблений згідно вимог, що висуваються НД ТЗІ 2.5-004-99 [2].

ВИСНОВКИ

1. Нормативне та методичне забезпечення з організації діяльності із запобігання загрозам НСД відстає від світового рівня. Наявні нормативні документи, зокрема, не надають методів формування та перевіряння ФПЗ.

2. Існуючий підхід, заснований на стандартних ФПЗ, призводе до висунення недостатніх або надмірних вимог до захисту КС.

3. Запропоновані методи дозволяють підвищити ефективність діяльності експерта з розробки та верифікації ФПЗ за рахунок:

– зручності використання;

– зрозумілості проміжних результатів;

– можливості самоперевірки;

– забезпечення повторюваності та порівнюваності результатів;

– врахування результатів інших етапів побудови КСЗІ.

Література.

[1] НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999 р. / ТОВ "ІКТ". – К: ДСТСЗІ СБ України, 1999. – 21 с. – (Нормативний документ системи технічного захисту інформації).

[2] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999 р. / ТОВ "ІКТ". – К: ДСТСЗІ СБ України, 1999. – 59 с. – (Нормативний документ системи технічного захисту інформації).

[3] НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від " 28 " квітня 1999 р. /ТОВ "ІКТ2. – К: ДСТСЗІ СБ України, 1999. – 22 с. – (Нормативний документ системи технічного захисту інформації).

[4] *Лєншин А.В., Буслов П.В.* Метод формування функціональних профілів захищеності від несанкціонованого доступу //Науково-технічний журнал "Радіоелектронні і комп'ютерні системи". – Харків: ХАІ, 2010. – Том 7. – С. 77-81

Надійшла до редколегії 9.07.2010.

Потій Олександр Володимирович, доцент, доктор техн. наук, професор кафедри БІТ ХНУРЕ. Область наукових інтересів: системний аналіз процесів захисту інформації, управління захистом інформації.

Лєншин Анатолій Валерійович, канд. техн. наук, доцент кафедри БІТ ХНУРЕ. Область наукових інтересів: побудова КСЗІ, інфраструктура відкритих ключів.

УДК 681.3.06

Методы построения и верификации непротиворечивости и полноты функциональных профилей защищенности от несанкционированного доступа / А.В.Потий, А.В Леншин // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 479–488.

Проведен анализ требований нормативных документов в части формирования профилей защищенности. Определены недостатки существующего подхода к формированию профиля защищенности. Сформулированы требования к методу формирования и методу проверки непротиворечивости и полноты профилей защищенности, дано их описание. Показано, что разработанные методы соответствуют требованиям по: временной сложности, стандартизированности подхода (повторяемость и сравнимость результатов), непротиворечивости требованиям нормативных документов, понятности промежуточных результатов и их воздействий на окончательный выбор, а также возможности самопроверки лица, использующего метод.

Ключевые слова: профиль защищенности, несанкционированный доступ, методы системного анализа.

Табл. 11. Ил.02. Библиогр.: 04 назв.

UDC 681.3.06

Methods of constructing and verifying consistency and completeness of functional protection profiles against unauthorized access / A V. Potii, A.V. Lenshin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 479-488.

The analysis of normative documents requirements concerning protection profiles is conducted. Shortcomings of the existing approach to designing protection profiles are identified. Requirements to the methods of designing and verifying consistency and completeness of protection profiles against unauthorized access are formulated and their descriptions are given. It is shown that the developed methods comply with the requirements of time complexity, approach standardization (repeatability and comparability of results), consistency to the requirements of the normative documents, understandability of interim results and their impact on the final choice, as well as the possibility of self-verification for a person using the method.

Key words: protection profile, unauthorized access, system analysis methods.

Tab. 11. Fig. 02. Ref.: 04 items.