УДК 004.056.5

ТЕОРЕТИЧНІ ОСНОВИ ВИЗНАЧЕННЯ СТАНДАРТНИХ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

***О. К. Юдін**, д-р техн. наук, проф.; ****С. С. Бучик**, канд. техн. наук, доц.; ****С. В. Мельник**
*Національний авіаційний університет
e-mail: kszi@ukr.net
Житомирський військовий інститут імені С. П. Корольова
e-mail: s_stbu@ukr.net

У статті запропоновано, показано та проаналізовано теоретичні основи визначення стандартних профілів захищеності автоматизованої системи від несанкціонованого доступу. Висвітлено необхідні нормативні документи технічного захисту інформації, які регламентують порядок оцінки та визначення стандартних функціональних профілів захищеності інформації від несанкціонованого доступу в Україні. На основі даних документів, вперше здійснено формалізацію визначення стандартних профілів захищеності автоматизованої системи від несанкціонованого доступу. Наведено приклад визначення стандартного профілю захищеності за поданою формалізованою моделлю. Запропоновані авторами теоретичні основи дають можливість у подальшому розробити експертну систему, яка автоматизовано визначатиме стандартні профілі захищеності автоматизованої системи від несанкціонованого доступу. Це полегшить роботу адміністраторів безпеки щодо визначення профілю захищеності та створення необхідного комплексу засобів захисту, а також зменшить витрачений ресурс часу.

Ключові слова: автоматизована система, інформаційна безпека, політика безпеки інформації, правила розмежування доступу, несанкціонований доступ, комплекс засобів захисту, профіль захищеності.

The theoretical bases of determination of standard types of security of automatic system from the unauthorized access is shown, analysed and offered in the article. The necessary normative documents of technical security information, which regulate the order of estimation and determination of standard functional types of security of information from an unauthorized access in Ukraine, are reflected. On the basis of these documents, formalization of the bases of determination of standard types of security of automatic system from an unauthorized access is carried out for the first time. An example of determination of standard type of security is made after the presented formalized model. Theoretical bases offered by the authors enable in future to work out a consulting model which will determine the standard types of security of automatic system automated from an unauthorized access. It will facilitate the work of administrators of safety in relation to determination of type of security and creation of necessary complex of facilities of security, and also will decrease the spent resource of time.

Keywords: automatic system, information security, politics of security of information, rule of differentiation of access, unauthorized division, complex of facilities of security, profile of security.

Актуальність дослідження

Однією із найважливіших проблем сучасності в галузі комп'ютерних технологій вважають інформаційну безпеку (ІБ), важливою складовою якої є захист автоматизованої системи (АС) від несанкціонованого доступу (НСД).

Щоденно у світі з'являються нові програмні та апаратні засоби, які дають можливість НСД до інформації.

Тому спеціалісти з ІБ багатьох країн світу намагаються протистояти даній проблемі, використовуючи різноманітні засоби та методи. За останні роки було розроблено безліч нормативних документів ТЗІ (НД ТЗІ), спрямованих на захист АС від НСД.

Розглядаючи нормативно-правову базу України в даній галузі, слід відмітити такі документи: НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [1]; НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [2]; НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [3].

Саме вони стали основою для проведення аналізу та подальшого дослідження.

НД ТЗІ 2.5-004-99 [2], визначає, що експертна комісія проводить оцінку комп'ютерної системи (КС), таким чином є необхідність розробки методології побудови експертної системи, основою якої повинні стати теоретичні положення, які запропоновані авторами.

Тематики статті пов'язана з розробкою теоретичних основ визначення стандартних функціональних профілів захищеності (ФПЗ) АС від НСД — актуальна.

Аналіз останніх досліджень та публікацій

Тематиці визначення стандартних ФПЗ АС від НСД присвячено небагато робіт, що на думку авторів пов'язано з тим, що сам процес визна-

чення здійснюється експертною комісією та фактично єдиним документом, якій визначає підхід до визначення ФПЗ шляхом вибору зі стандартних є НД ТЗІ 2.5-005-99 [3]. При цьому сам вибір послуг безпеки, які потрібні для конкретної КС, з урахуванням середовищ та моделі загроз, залишився без уваги. НД ТЗІ 2.5-004-99 [2] надає лише методологічну базу з точки зору як нормативний документ для вибору та реалізації вимог безпеки в АС, але єдиної методології, яка б поєднувала ці документи та надавала простішу та зрозумілу інтерпретацію процесу обирання ФПЗ немає. Наразі є питання можливості обрання не лише стандартного ФПЗ, а й такого, який на основі певної методології, що реалізує визначені нормативні документи, створив умови для визначення нестандартного профілю загроз.

У праці [4] авторами розроблено метод формування ФПЗ від НСД на основі побудови таблиць для визначення необхідності та рівня послуг, але на відміну від запропонованих у статті теоретичних основ, він є на думку авторів більш складним та потребує від особи, що приймає рішення (ОПР) детальнішого розуміння змісту та необхідності вимог. У праці [5] авторами визначені лише певні протиріччя щодо сучасного стану нормативно-правової бази (НПБ) ТЗІ, у тому числі це стосується і визначення стандартних ФПЗ. Як усунути ці протиріччя у статті не визначено. У праці [6] розглянуто проблемні питання побудови системи захисту інформації (СЗІ) від НСД та формальна постановка завдання вибору оптимального профілю захищеності, запропоновано метод пошуку проектних альтернатив СЗІ з урахуванням ресурсних обмежень на її реалізацію. Автором статті в праці [7] подана загальна модель формування системи захисту державних інформаційних ресурсів (ДІР), у якій одним із елементів системи управління ІБ ДІР є модель вибору ФПЗ.

Таким чином, дана робота є логічним продовженням розкриття методології захисту ДІР за методом «подвійної трійки захисту», яка представлена в праці [8].

Мета статті — це розробка теоретичних основ визначення стандартних ФПЗ АС від НСД.

Виклад основного матеріалу

Розглянемо опис процесу визначення стандартного функціонального профілю захищеності АС від НСД. Для цього слід розглянути документ, за допомогою якого стає можливим завдання визначення вимог із захисту інформації (ЗІ) в КС від НСД; створення захисних КС і засобів захисту від НСД; оцінки захищеності інформації в КС та їх придатності для обробки критичної інформації (інформації, що вимагає захисту). Таким документом є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». З аналізу даного нормативного документа можна дійти висновку, що в процесі оцінки спроможності КС забезпечувати захист оброблюваної інформації від НСД розглядають вимоги двох видів: вимоги до функцій захисту (послуг безпеки); вимоги до гарантій. Для дослідження обрано лише вимоги до функцій захисту без надання певних гарантій АС. КС у такому випадку розглядається як набір функціональних послуг.

Кожна послуга являє собою набір функцій, які дозволяють протистояти певній множині загроз та можуть включати декілька рівнів. Чим вищий 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 одне одного. Рівні починаються з першого і зростають до значення n, де n —унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів. Для створення математичного опису функціональні критерії в цілому отримали буквене позначення K, а кожна група функціональних критеріїв, у свою чергу, отримала такі позначення:

- K^{conf} — критерії конфіденційності (**conf**identiality) (за даним критерієм оцінюють загрози, що відносять до несанкціонованого ознайомлення з інформацією);
- K^{int} — критерії цілісності (**int**egrity) (за даним критерієм оцінюють загрози, що відносять до несанкціонованої модифікації інформації);
- K^{av} — критерії доступності (**av**ailability) (за даним критерієм оцінюють загрози, що відносять до порушення можливості використання КС або оброблюваної інформації);
- K^{ac} — критерії спостережуваності (**ac**countability) (за даним критерієм оцінюють ідентифікацію і контроль за діями користувачів, керованість КС).

Уведення даних позначень дає можливість створити загальний математичний опис функціональних критеріїв, представлений такою множиною:

$$K = \{K^{conf}, K^{\text{int}}, K^{av}, K^{ac}\}. \quad (1)$$

Усі описані послуги є більш-менш незалежними. Якщо ж реалізація якоїсь послуги неможлива без реалізації іншої, то цей факт відбиваєть-

ся як необхідні умови для даної послуги. Рівень послуги цілісність комплексу засобів захисту НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.

Результатом оцінки КС на предмет відповідності «Критеріям оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу КС міг бути включений певний рівень послуги, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги.

Для виконання поставленої перед дослідженням мети слід виконати математичний опис даних критеріїв та отримати математичну модель системи визначення критеріїв захищеності АС від НСД. Для цього відповідно до табличних значень, відображених у документі, введемо умовні позначення.

Розглянемо це на прикладі.

Візьмемо один із критеріїв конфіденційності, а саме довірчу конфіденційність.

Довірча конфіденційність (КД). Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Існує чотири рівні довірчої конфіденційності, а саме мінімальна довірча конфіденційність, базова довірча конфіденційність, повна довірча конфіденційність, абсолютна довірча конфіденційність.

Згідно з працею [2], для визначення рівню довірчої конфіденційності користувачу надається таблиця з вимогами (табл. 1). При виконані всіх вимог, необхідних для певного рівня послуги, можна стверджувати, що обрана АС відповідає даному рівню.

Аналізуючи табл. 1, можна зробити висновок, що для всіх рівнів існують необхідні умови. Для наочності необхідні умови НІ_1 (зовнішня ідентифікація і автентифікація) та КО_1 (повторне використання об'єктів) винесені в табл. 2 та 3 відповідно. Згідно з даними таблицями для НІ_1 та КО_1 необхідні умови відсутні.

Таблиця 1

Вимоги для вибору рівня довірчої конфіденційності

<table>
<tr><td>КД-1. Мінімальна довірча конфіденційність</td><td colspan="2">КД-2. Базова довірча конфіденційність</td><td>КД-3. Повна довірча конфіденційність</td><td>КД-4. Абсолютна довірча конфіденційність</td></tr>
<tr><td colspan="3">Політика довірчої конфіденційності, що реалізується (комплексом засобів захисту) КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="5">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td colspan="2">процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="5">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="5">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td colspan="2">конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td colspan="2" rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td colspan="2">конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="5">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НІ-1</td><td colspan="3">НЕОБХІДНІ УМОВИ: КО-1, НІ-1</td></tr>
</table>

Таблиця 2

Необхідні умови для рівнів КД_1 та КД_2

НІ-1. Зовнішня ідентифікація і автентифікація
Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ
Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача
НЕОБХІДНІ УМОВИ : НЕМАЄ

Таблиця 3

Необхідні умови для рівнів КД_1, КД_2, КД_3 та КД_4

КО-1. Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС
Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані
Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
НЕОБХІДНІ УМОВИ: НЕМАЄ

Розібравши табл. 1 на зрозумілі компоненти, можна перейти до введення умовних позначень. Проте, для зручності та правильності математичного опису, умовні позначення надаються відразу для всіх умов, за допомогою яких можна визначити рівні відповідних послуг.

Зауваження: умови, які стосуються критеріїв конфіденційності, отримали буквене позначення «k» з цифровим індексом (1...44), критеріїв цілісності — буквене позначення «c» з цифровим індексом (1...35), критеріїв доступності — буквене позначення «d» з цифровим індексом (1...26), критеріїв спостережуваності — буквене позначення «s» з цифровим індексом (1...45).

Після введення умовних позначень, табл. 1 буде мати вигляд (табл. 4).

Необхідні умови, в свою чергу, матимуть такі умовні позначення (табл. 5).

Після введення умовних позначень слід створити матрицю знань, яку потім можна буде використати при створенні програмного продукту, який визначатиме стандартний ФПЗі АС від НСД.

Матрицю знань створено наступним чином: умовам, які виконуються у визначеній АС надаємо значення 1, а тим умовам, які не виконуються — 0. Для довірчої конфіденційності вона матиме наступний вигляд (табл. 6).

Таблиця 4

Вимоги для вибору рівня довірчої конфіденційності (з умовними позначеннями)

КД (вимоги)	***Умовні позначення***
Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься	k_1
Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС	k_2
КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	k_3
КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта	k_4
КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача, процесу і захищеного об'єкта	k_5
Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта	k_6
КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта	k_7

Продовження табл. 4

КД (вимоги)	***Умовні позначення***
КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта	k_8
КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта	k_9
КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта	k_{10}
КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес	k_{11}
КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес	k_{12}
Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	k_{13}

Таблиця 5

Необхідні умови (з умовними позначеннями)

Додаткові (необхідні) умови	***Умовні позначення***
НІ_1	
Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ	s_{10}
Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача	s_{11}
КО_1	
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС	k_{24}
Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані	k_{25}
Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною	k_{26}

Таблиця 6

Матриця знань

КД	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	s_{10}	s_{11}	k_{24}	k_{25}	k_{26}
КД_1	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0
КД_2	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1	0	0	0
КД_3	0	1	0	1	0	1	0	0	1	0	0	1	1	1	1	1	1	1
КД_4	0	1	0	0	1	1	0	0	0	1	0	1	1	1	1	1	1	1

Відповідно до табл. 6 отримаємо такі логічні рівняння.

$$КД\_1 = (k_1 \wedge k_3 \wedge k_6 \wedge k_7 \wedge k_{13}) \wedge (s_{10} \wedge s_{11}) \quad (2)$$

$$КД\_2 = (k_1 \wedge k_4 \wedge k_6 \wedge k_8 \wedge k_{11} \wedge k_{13}) \wedge (s_{10} \wedge s_{11}) \quad (3)$$

$$КД\_3 = (k_2 \wedge k_4 \wedge k_6 \wedge k_9 \wedge k_{12} \wedge k_{13}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26}) \quad (4)$$

$$КД\_4 = (k_2 \wedge k_5 \wedge k_6 \wedge k_{10} \wedge k_{12} \wedge k_{13}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26}) \quad (5)$$

Якщо один із наведених вище логічних виразів (2–5) приймає значення «1», то обирають відповідний рівень послуги, якщо значення «0» — рівень послуги відкидають. Отож, цей приклад відображає формалізацію опису визначення рівня послуги. Для наочного відображення процесу визначення одного з рівнів КД розглянемо такий приклад. Адміністратор безпеки визначив (відповідно до табл. 4) вимоги до КД, які виконуються для даної АС. Даними вимогами виявились такі твердження:

- політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона належить;
- КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта;
- запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;
- КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта;
- права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності, повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту;
- політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ;
- перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Даним вимогам відповідає наступна матриця знань (табл. 7), в якій знак питання (?) означає невідомий рівень КД.

Порівняємо отриманий набір із табл. 6, вписавши до матриці знань (табл. 8).

З табл. 8 бачимо, що даний набір відповідає рівню послуг *КД_1* (табл. 9).

Таблиця 7

Матриця знань отриманого набору

КД	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	s_{10}	s_{11}	k_{24}	k_{25}	k_{26}
?	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0

Таблиця 8

Порівняльна матриця знань

КД	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	s_{10}	s_{11}	k_{24}	k_{25}	k_{26}
?	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0
КД_1	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0
КД_2	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1	0	0	0
КД_3	0	1	0	1	0	1	0	0	1	0	0	1	1	1	1	1	1	1
КД_4	0	1	0	0	1	1	0	0	0	1	0	1	1	1	1	1	1	1

Таблиця 9

Результат порівняння отриманого набору із стандартними наборами рівнів КД

КД	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	s_{10}	s_{11}	k_{24}	k_{25}	k_{26}
?	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0
КД_1	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0

Отож, відповідно до табл. 9, як вираз для математичного опису даної АС оберемо логічний вираз (2).

Даний приклад чітко ілюструє процес визначення стандартного рівню послуги.

Відповідно до НД ТЗІ 2.5-004-99 [2] формалізуємо усі представлені функціональні критерії (послуги, рівні послуг) до наступних логічних рівнянь.

Функціональні критерії (формула (1)):

1. Критерії конфіденційності (для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом). Конфіденційність забезпечується такими послугами (підмножина (6)): довірча конфіденційність (КД), адміністративна конфіденційність (КА), повторне використання об'єктів (КО), аналіз прихованих каналів (КК), конфіденційність при обміні (КВ)

$$K^{conf} = \{КД, КА, КО, КК, КВ\}. \quad (6)$$

1.1. Довірча конфіденційність. Дана послуга поділяється на наступні рівні (підмножина (7)): мінімальна довірча конфіденційність (КД_1), базова довірча конфіденційність (КД_2), повна довірча конфіденційність (КД_3), абсолютна довірча конфіденційність (КД_4).

1.2. Адміністративна конфіденційність. Дана послуга поділяється на наступні рівні (підмножина (12)): мінімальна адміністративна конфіденційність (КА_1), базова адміністративна конфіденційність (КА_2), повна адміністративна конфіденційність (КА_3), абсолютна адміністративна конфіденційність (КА_4).

1.3. Повторне використання об'єктів. Дана послуга має один рівень (підмножина (17)): повторне використання об'єктів (КО_1).

1.4. Аналіз прихованих каналів. Дана послуга поділяється на наступні рівні (підмножина (19)): виявлення прихованих каналів (КК_1), контроль прихованих каналів (КК_2), перекриття прихованих каналів (КК_3).

1.5. Конфіденційність при обміні. Дана послуга поділяється на наступні рівні (підмножина (23)): мінімальна конфіденційність при обміні (КВ_1), базова конфіденційність при обміні (КВ_2), повна конфіденційність при обміні (КВ_3), абсолютна конфіденційність при обміні (КВ_4).

.

$$КД = \{КД\_1, КД\_2, КД\_3, КД\_4\} \quad (7)$$

$$КД = \begin{cases} КД\_1 = (k_1 \wedge k_3 \wedge k_6 \wedge k_7 \wedge k_{13}) \wedge (s_{10} \wedge s_{11}) & (8) \\ КД\_2 = (k_1 \wedge k_4 \wedge k_6 \wedge k_8 \wedge k_{11} \wedge k_{13}) \wedge (s_{10} \wedge s_{11}) & (9) \\ КД\_3 = (k_2 \wedge k_4 \wedge k_6 \wedge k_9 \wedge k_{12} \wedge k_{13}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26}) & (10) \\ КД\_4 = (k_2 \wedge k_5 \wedge k_6 \wedge k_{10} \wedge k_{12} \wedge k_{13}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26}) & (11) \end{cases}$$

$$КА = \{КА\_1, КА\_2, КА\_3, КА\_4\} \quad (12)$$

$$КА = \begin{cases} КА\_1 = (k_{14} \wedge k_3 \wedge k_{16} \wedge k_{17} \wedge k_{23}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (13) \\ КА\_2 = (k_{14} \wedge k_4 \wedge k_{16} \wedge k_{18} \wedge k_{21} \wedge k_{23}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (14) \\ КА\_3 = (k_{15} \wedge k_4 \wedge k_{16} \wedge k_{19} \wedge k_{22} \wedge k_{23}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26} \wedge s_{19} \wedge s_{22}) & (15) \\ КА\_4 = (k_{15} \wedge k_5 \wedge k_{16} \wedge k_{20} \wedge k_{22} \wedge k_{23}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26} \wedge s_{19} \wedge s_{22}) & (16) \end{cases}$$

$$КО = \{КО\_1\} \quad (17)$$

$$КО\_1 = (k_{24} \wedge k_{25} \wedge k_{26}) \quad (18)$$

$$КК = \{КК\_1, КК\_2, КК\_3\} \quad (19)$$

$$КК = \begin{cases} КК\_1 = (k_{27} \wedge k_{28} \wedge k_{29} \wedge k_{30}) \wedge (s_1 \wedge s_2) & (20) \\ КК\_2 = (k_{27} \wedge k_{28} \wedge k_{29} \wedge k_{30} \wedge k_{32}) \wedge (s_{10} \wedge s_{11} \wedge s_1 \wedge s_2 \wedge s_4 \wedge s_5) & (21) \\ КК\_3 = (k_{27} \wedge k_{31}) \wedge (k_{24} \wedge k_{25} \wedge k_{26} \wedge s_1 \wedge s_2) & (22) \end{cases}$$

$$КВ = \{КВ\_1, КВ\_2, КВ\_3, КВ\_4\} \quad (23)$$

$$КВ = \begin{cases} КВ\_1 = (k_{33} \wedge k_{35} \wedge k_{36}) & (24) \\ КВ\_2 = (k_{33} \wedge k_{35} \wedge k_{36} \wedge k_{37} \wedge k_{38} \wedge k_{40}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (25) \\ КВ\_3 = (k_{34} \wedge k_{35} \wedge k_{36} \wedge k_{37} \wedge k_{39} \wedge k_{41} \wedge k_{42}) \wedge & (26) \\ (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22} \wedge s_{33} \wedge s_{34} \wedge s_{35}) & \\ КВ\_4 = (k_{34} \wedge k_{35} \wedge k_{36} \wedge k_{37} \wedge k_{39} \wedge k_{41} \wedge k_{42} \wedge k_{43} \wedge k_{44}) \wedge & (27) \\ (s_{10} \wedge s_{11} \wedge s_1 \wedge s_2 \wedge s_4 \wedge s_5 \wedge s_{19} \wedge s_{22} \wedge s_{33} \wedge s_{34} \wedge s_{35}) & \end{cases}$$

2. Критерії цілісності (для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації). Цілісність забезпечується такими послугами (підмножина (28)): довірча цілісність (ЦД), адміністративна цілісність (ЦА), відкат (ЦО), цілісність при обміні (ЦВ).

2.1. Довірча цілісність. Дана послуга поділяється на наступні рівні (підмножина (29)): мінімальна довірча цілісність (ЦД_1), базова довірча цілісність (ЦД_2), повна довірча цілісність (ЦД_3), абсолютна довірча цілісність (ЦД_4).

2.2. Адміністративна цілісність. Дана послуга поділяється на наступні рівні (підмножина (34)): мінімальна адміністративна цілісність (ЦА_1), базова адміністративна цілісність (ЦА_2), повна адміністративна цілісність (ЦА_3), абсолютна адміністративна цілісність (ЦА_4).

2.3. Відкат. Дана послуга поділяється на наступні рівні (підмножина (39)): обмежений відкат (ЦО_1), повний відкат (ЦО_2).

2.4. Цілісність при обміні. Дана послуга поділяється на наступні рівні (підмножина (42)): мінімальна цілісність при обміні (ЦВ_1), базова цілісність при обміні (ЦВ_2), повна цілісність при обміні (ЦВ_3).

3. Критерії доступності (для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів). Доступність забезпечується такими послугами (підмножина (45)): використання ресурсів (ДР), стійкість до відмов (ДС), гаряча заміна (ДЗ), відновлення після збоїв (ДВ).

3.1. Використання ресурсів. Дана послуга поділяється на наступні рівні (підмножина (46)): квоти (ДР_1), недопущення захоплення ресурсів (ДР_2), пріоритетність використання ресурсів (ДР_3).

$$K^{\text{int}} = \{ЦД, ЦА, ЦО, ЦВ\} \tag{28}$$

$$ЦД = \{ЦД\_1, ЦД\_2, ЦД\_3, ЦД\_4\} \tag{29}$$

$$ЦД = \begin{cases} ЦД\_1 = (c_1 \wedge c_3 \wedge c_6 \wedge c_7 \wedge c_{13}) \wedge (s_{10} \wedge s_{11}) & (30) \\ ЦД\_2 = (c_1 \wedge c_4 \wedge c_6 \wedge c_8 \wedge c_{11} \wedge c_{13}) \wedge (s_{10} \wedge s_{11}) & (31) \\ ЦД\_3 = (c_2 \wedge c_4 \wedge c_6 \wedge c_9 \wedge c_{12} \wedge c_{13}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26}) & (32) \\ ЦД\_4 = (c_2 \wedge c_5 \wedge c_6 \wedge c_{10} \wedge c_{12} \wedge c_{13}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26}) & (33) \end{cases}$$

$$ЦА = \{ЦА\_1, ЦА\_2, ЦА\_3, ЦА\_4\} \tag{34}$$

$$ЦА = \begin{cases} ЦА\_1 = (c_{14} \wedge c_3 \wedge c_{16} \wedge c_{17} \wedge c_{23}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (35) \\ ЦА\_2 = (c_{14} \wedge c_4 \wedge c_{16} \wedge c_{18} \wedge c_{21} \wedge c_{23}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (36) \\ ЦА\_3 = (c_{15} \wedge c_4 \wedge c_{16} \wedge c_{19} \wedge c_{22} \wedge c_{23}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26} \wedge s_{19} \wedge s_{22}) & (37) \\ ЦА\_4 = (c_{15} \wedge c_5 \wedge c_{16} \wedge c_{20} \wedge c_{22} \wedge c_{23}) \wedge (s_{10} \wedge s_{11} \wedge k_{24} \wedge k_{25} \wedge k_{26} \wedge s_{19} \wedge s_{22}) & (38) \end{cases}$$

$$ЦО = \{ЦО\_1, ЦО\_2\} \tag{39}$$

$$ЦО = \begin{cases} ЦО\_1 = (c_{24} \wedge c_{25}) \wedge (s_{10} \wedge s_{11}) & (40) \\ ЦО\_2 = (c_{24} \wedge c_{26}) \wedge (s_{10} \wedge s_{11}) & (41) \end{cases}$$

$$ЦВ = \{ЦВ\_1, ЦВ\_2, ЦВ\_3\} \tag{42}$$

$$ЦВ = \begin{cases} ЦВ\_1 = (c_{27} \wedge c_{28}) & (43) \\ ЦВ\_2 = (c_{27} \wedge c_{28} \wedge c_{30} \wedge c_{32} \wedge c_{34}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (44) \\ ЦВ\_3 = (c_{27} \wedge c_{29} \wedge c_{31} \wedge c_{33} \wedge c_{34} \wedge c_{35}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22} \wedge s_{33} \wedge s_{34} \wedge s_{35}) & (44) \end{cases}$$

$$K^{av} = \{ДР, ДС, ДЗ, ДВ\} \tag{45}$$

$$ДР = \{ДР\_1, ДР\_2, ДР\_3\} \tag{46}$$

$$ДР = \begin{cases} ДР\_1 = (d_1 \wedge d_3 \wedge d_5) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (47) \\ ДР\_2 = (d_2 \wedge d_3 \wedge d_5 \wedge d_6) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (48) \\ ДР\_3 = (d_2 \wedge d_4 \wedge d_5 \wedge d_7) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (49) \end{cases}$$

3.2. Стійкість до відмов. Дана послуга поділяється на наступні рівні (підмножина (50)): стійкість за обмежених відмов (ДС_1), стійкість з погіршенням характеристик обслуговування (ДС_2), стійкість без погіршення характеристик обслуговування (ДС_3).

3.3. Гаряча заміна. Дана послуга поділяється на такі рівні (підмножина (54)): модернізація (ДЗ_1), обмежена гаряча заміна (ДЗ_2), гаряча заміна будь-якого компонента (ДЗ_3).

3.4. Відновлення після збоїв. Дана послуга поділяється на такі рівні (підмножина (58)): ручне відновлення (ДВ_1), автоматизоване відновлення (ДВ_2), вибіркове відновлення (ДВ_3).

4. Критерії спостережуваності (для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереження, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції). Доступність забезпечується такими послугами (підмножина (62)): реєстрація (аудит) (НР), ідентифікація і автентифікація (НІ), достовірний канал (НК), розподіл обов'язків (НО), цілісність КЗЗ (НЦ), самотестування (НТ), ідентифікація і автентифікація при обміні (НВ), автентифікація відправника (НА), автентифікація отримувача (НП).

4.1. Реєстрація. Дана послуга поділяється на наступні рівні (підмножина (63)): зовнішній аналіз (НР_1), захищений журнал (НР_2), сигналізація про небезпеку (НР_3), детальна реєстрація (НР_4), аналіз в реальному часі (НР_5).

4.2. Ідентифікація і автентифікація. Дана послуга поділяється на наступні рівні (підмножина (69)): зовнішня ідентифікація і автентифікація (НІ_1), одиночна ідентифікація і автентифікація (НІ_2), множинна ідентифікація і автентифікація (НІ_3).

$$ДС = \{ДС\_1, ДС\_2, ДС\_3\} \tag{50}$$

$$ДС = \begin{cases} ДС\_1 = (d_8 \wedge d_9 \wedge d_{11} \wedge d_{12} \wedge d_{14}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (51) \\ ДС\_2 = (d_8 \wedge d_{10} \wedge d_{11} \wedge d_{12} \wedge d_{14}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (52) \\ ДС\_3 = (d_8 \wedge d_{10} \wedge d_{11} \wedge d_{13} \wedge d_{14}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (53) \end{cases}$$

$$ДЗ = \{ДЗ\_1, ДЗ\_2, ДЗ\_3\} \tag{54}$$

$$ДЗ = \begin{cases} ДЗ\_1 = (d_{15} \wedge d_{18}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (55) \\ ДЗ\_2 = (d_{16} \wedge d_{19}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22} \wedge d_8 \wedge d_9 \wedge d_{11} \wedge d_{12} \wedge d_{14}) & (56) \\ ДЗ\_3 = (d_{17} \wedge d_{19}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22} \wedge d_8 \wedge d_9 \wedge d_{11} \wedge d_{12} \wedge d_{14}) & (57) \end{cases}$$

$$ДВ = \{ДВ\_1, ДВ\_2, ДВ\_3\} \tag{58}$$

$$ДВ = \begin{cases} ДВ\_1 = (d_{20} \wedge d_{21} \wedge d_{25}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (59) \\ ДВ\_2 = (d_{20} \wedge d_{22} \wedge d_{24} \wedge d_{25}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (60) \\ ДВ\_3 = (d_{20} \wedge d_{23} \wedge d_{24} \wedge d_{26}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (61) \end{cases}$$

$$K^{ac} = \{НР, НІ, НК, НО, НЦ, НТ, НВ, НА, НП\} \tag{62}$$

$$НР = \{НР\_1, НР\_2, НР\_3, НР\_4, НР\_5\} \tag{63}$$

$$НР = \begin{cases} НР\_1 = (s_1 \wedge s_2 \wedge s_4 \wedge s_5) \wedge (s_{10} \wedge s_{11}) & (64) \\ НР\_2 = (s_1 \wedge s_2 \wedge s_4 \wedge s_6 \wedge s_7) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (65) \\ НР\_3 = (s_1 \wedge s_2 \wedge s_4 \wedge s_6 \wedge s_7 \wedge s_8) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (66) \\ НР\_4 = (s_1 \wedge s_3 \wedge s_4 \wedge s_6 \wedge s_7 \wedge s_8) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (67) \\ НР\_5 = (s_1 \wedge s_3 \wedge s_4 \wedge s_6 \wedge s_7 \wedge s_8 \wedge s_9) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (68) \end{cases}$$

$$НІ = \{НІ\_1, НІ\_2, НІ\_3\} \tag{69}$$

$$НІ = \begin{cases} НІ\_1 = (s_{10} \wedge s_{11}) & (70) \\ НІ\_2 = (s_{10} \wedge s_{12} \wedge s_{14}) \wedge (s_{15} \wedge s_{16}) & (71) \\ НІ\_3 = (s_{10} \wedge s_{13} \wedge s_{14}) \wedge (s_{15} \wedge s_{16}) & (72) \end{cases}$$

4.3. Достовірний канал. Дана послуга поділяється на наступні рівні (підмножина (73)): односпрямований достовірний канал (НК_1), двоспрамований достовірний канал (НК_2).

4.4. Розподіл обов'язків. Дана послуга поділяється на наступні рівні (підмножина (76)): виділення адміністратора (НО_1), розподіл обов'язків адміністраторів (НО_2), розподіл обов'язків на підставі привілеїв (НО_3).

4.5. Цілісність комплексу засобів захисту. Дана послуга поділяється на такі рівні (підмножина (80)): КЗЗ з контролем цілісності (НЦ_1), КЗЗ з гарантованою цілісністю (НЦ_2), КЗЗ з функціями диспетчера доступу (НЦ_3).

4.6. Самотестування. Дана послуга поділяється на такі рівні (підмножина (84)): самотестування за запитом (НТ_1), самотестування при старті (НТ_2), самотестування в реальному часі (НТ_3).

4.7. Ідентифікація і автентифікація при обміні. Дана послуга поділяється на такі рівні (підмножина (88)): автентифікація вузла (НВ_1), автентифікація джерела даних (НВ_2), автентифікація з підтвердженням (НВ_3).

4.8. Автентифікація відправника. Дана послуга поділяється на такі рівні (підмножина (92)): базова автентифікація відправника (НА_1), автентифікація відправника з підтвердженням (НА_2).

4.9. Автентифікація отримувача. Дана послуга поділяється на наступні рівні (підмножина (95)): базова автентифікація отримувача (НП_1), автентифікація отримувача з підтвердженням (НП_2).

$$НК = \{НК\_1, НК\_2\} \tag{73}$$

$$НК = \begin{cases} НК\_1 = (s_{15} \wedge s_{16}) & (74) \\ НК\_2 = (s_{15} \wedge s_{17} \wedge s_{18}) & (75) \end{cases}$$

$$НО = \{НО\_1, НО\_2, НО\_3\} \tag{76}$$

$$НО = \begin{cases} НО\_1 = (s_{19} \wedge s_{22}) \wedge (s_{10} \wedge s_{11}) & (77) \\ НО\_2 = (s_{19} \wedge s_{20} \wedge s_{22}) \wedge (s_{10} \wedge s_{11}) & (78) \\ НО\_3 = (s_{19} \wedge s_{20} \wedge s_{21} \wedge s_{22}) \wedge (s_{10} \wedge s_{11}) & (79) \end{cases}$$

$$НЦ = \{НЦ\_1, НЦ\_2, НЦ\_3\} \tag{80}$$

$$НЦ = \begin{cases} НЦ\_1 = (s_{23} \wedge s_{25} \wedge s_{27}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22} \wedge s_1 \wedge s_2 \wedge s_4 \wedge s_5) & (81) \\ НЦ\_2 = (s_{24} \wedge s_{26} \wedge s_{27}) & (82) \\ НЦ\_3 = (s_{24} \wedge s_{26} \wedge s_{28}) & (83) \end{cases}$$

$$НТ = \{НТ\_1, НТ\_2, НТ\_3\} \tag{84}$$

$$НТ = \begin{cases} НТ\_1 = (s_{29} \wedge s_{30}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (85) \\ НТ\_2 = (s_{29} \wedge s_{30} \wedge s_{31}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (86) \\ НТ\_3 = (s_{29} \wedge s_{30} \wedge s_{31} \wedge s_{32}) \wedge (s_{10} \wedge s_{11} \wedge s_{19} \wedge s_{22}) & (87) \end{cases}$$

$$НВ = \{НВ\_1, НВ\_2, НВ\_3\} \tag{88}$$

$$НВ = \begin{cases} НВ\_1 = (s_{33} \wedge s_{34} \wedge s_{35}) & (89) \\ НВ\_2 = (s_{33} \wedge s_{34} \wedge s_{35} \wedge s_{36}) & (90) \\ НВ\_3 = (s_{33} \wedge s_{34} \wedge s_{35} \wedge s_{36} \wedge s_{37}) & (91) \end{cases}$$

$$НА = \{НА\_1, НА\_2\} \tag{92}$$

$$НА = \begin{cases} НА\_1 = (s_{38} \wedge s_{40}) \wedge (s_{10} \wedge s_{11}) & (93) \\ НА\_2 = (s_{38} \wedge s_{39} \wedge s_{40} \wedge s_{41}) \wedge (s_{10} \wedge s_{11}) & (94) \end{cases}$$

$$НП = \{НП\_1, НП\_2\} \tag{95}$$

$$НП = \begin{cases} НП\_1 = (s_{42} \wedge s_{44}) \wedge (s_{10} \wedge s_{11}) & (96) \\ НП\_2 = (s_{42} \wedge s_{43} \wedge s_{44} \wedge s_{45}) \wedge (s_{10} \wedge s_{11}) & (97) \end{cases}$$

Визначивши критерії захищеності АС від НСД та їх математичний опис, з'являється можливість визначити один із стандартних ФПЗ.

Для стандартних ФПЗ не вимагається ані зв'язаної з ними політики безпеки, ані рівня гарантій, хоч їх наявність і допускається в разі необхідності.

Основні результати

Основними результатами автори вважають, що вперше здійснено формалізацію основ визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу.

Запропоновані авторами теоретичні основи дають можливість у подальшому розробити експертну систему, яка визначатиме стандартні профілі захищеності автоматизованої системи від несанкціонованого доступу автоматизовано.

Висновок

Таким чином, у статті запропоновано, показано та проаналізовано теоретичні основи визначення стандартних ФПЗ АС від НСД.

Висвітлено необхідні НД ТЗІ, які регламентують порядок оцінки та визначення стандартних ФПЗ інформації від несанкціонованого доступу в Україні.

На основі даних документів, вперше здійснено формалізацію основ визначення стандартних ФПЗ АС від НСД.

Наведено приклад визначення стандартного ФПЗ за представленою формалізованою моделлю. Запропоновані авторами теоретичні основи дають можливість в подальшому розробити експертну систему, яка визначатиме стандартні ФПЗ АС від НСД.

Це полегшить роботу адміністраторів безпеки щодо визначення профілю захищеності та створення необхідного комплексу засобів захисту, а також зменшить витрачений ресурс часу.

ЛІТЕРАТУРА

1. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99 [Електронний ресурс]. — Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41650.

2. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 2.5-004-99. — [Електронний ресурс]. — Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41649.

3. *Класифікація* автоматизованих систем та стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу : НД ТЗІ 2.5-005-99. — [Електронний ресурс]. — Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41648.

4. *Лєншин А. В*. Метод формування функціональних профілів захищеності від несанкціонованого доступу // А. В. Лєншин, П. В. Буслов. // Радіоелектронні і комп'ютерні системи : науч. тр. — Х. : Нац. аэрокосм. ун-т «ХАИ», 2010. — Вып. 7(48). — С. 77 — 81. — Режим доступу: http://www.khai.edu/csp/ nauchportal/Arhiv/ REKS/2010/ REKS710/Lyenshyn.pdf

5. *Паламарчук Н. А*. Сучасний стан нормативно-правової бази в галузі технічного захисту інформації // Н. А. Паламарчук, Ю. І. Хлапонін, В. В. Овсянніков // Збірник наукових праць ВІТІ НТУУ «КПІ» — К. : ВІТІ НТУУ «КПІ», 2011. — №3. — С. 78 — 82. — Режим доступу: http://viti.edu.ua/files/zbk/2011/11_3_2011.pdf.

6. *Шевченко В. Л*. Метод пошуку проектних альтернатив системи захисту інформації // В. Л. Шевченко, Д. С. Берестов // Сучасний захист інформації — К.: ДУТ, 2015. — №3. — С. 22 — 27.

7. *Юдін О. К*. Загальна модель формування системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології. — 2015. — № 4 (28). — С. 332–337.

8. *Юдін О. К*. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 214 с.

Стаття надійшла до редакції 14.04.2016