УДК 004.056.5
DOI: 10.18372/2310-5461.34.11609

С. С. Бучик — д-р техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0003-0892-3494
e-mail: s_stbu@ukr.net;

О. К. Юдін —д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-5098-7796
e-mail: kszi@ukr.net;

Р. В. Нетребко
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0003-3212-5249
e-mail: netr_rv@ukr.net

ТЕОРЕТИЧНІ ОСНОВИ ВИЗНАЧЕННЯ РІВНЯ ГАРАНТІЙ АВТОМАТИЗОВАНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вступ

Стрімке зростання новітніх технологій, а також розвиток інфраструктури інформаційно-комунікаційних мереж державного та загального призначення призвело до створення інтегрованого інформаційного простору держави та всього суспільства. Інформаційні технології знаходять найширшого застосування в таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинена система електронних платежів, система послуг зв'язку та телебачення, системи управління транспортом, високотехнологічні виробництва (особливо атомні, хімічні тощо) і т. ін. Будь-яке несанкціоноване та протиправне втручання в інформаційний простір наведених сфер життєдіяльності держави й суспільства може призвести до тяжких та не передбачуваних наслідків [1, с. 104–105].

Досліджуючи нормативно-правову базу (НПБ) України в галузі захисту автоматизованих систем (АС) від несанкціонованого доступу (НСД), слід відмітити наступні документи: НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [2] та НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» [3]. Саме дані документи стали основою для проведення аналізу та подальшого дослідження. В розрізі продовження дослідження є актуальним здійснити аналіз теоретичних основ визначення рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу, що дозволить автоматизувати процес визначення та зменшить витрати часу та матеріальних (людських) ресурсів, які витрачаються на такий процес.

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень і публікацій показав, що питання розвитку систем захисту, їх створення, організації та дослідження процесів їх функціонування відображенні в працях вітчизняних і закордонних учених, серед яких: Горбенко І. Д., Корченко О. Г., Задірака В. К., Конахович Г. Ф., Грайворонський М. В., Новіков О. М., Шаньгин В. Ф. та багато інших. Дані праці показують основні теоретичні положення з захисту інформації, методологічні та науково-теоретичні основи побудови систем захисту, оцінки їх ефективності та принципів вибору параметрів для оцінки ефективності. Тематиці визначення рівня гарантій АС від несанкціонованого доступу (НСД) присвячено небагато робіт, що на думку авторів пов'язано з тим, що процес визначення здійснюється експертною комісією та фактично єдиним документом, якій визначає підхід до визначення гарантій є НД ТЗІ 2.7-010-09.

Дана стаття є продовженням роботи щодо теоретичних основ визначення стандартних ФПЗ на основі нормативно-правової бази (НПБ) [2] та тематики робіт над якими працює група науковців. Тому наразі стоїть питання можливості оцінки запропонованого рівня гарантій автоматизовано на основі документів НД ТЗІ 2.7-010-09 [3] та НД ТЗІ 2.5-004-99 [2].

Раніше на основі праці [4, с. 196–204] авторами була розроблена інформаційна система визначення стандартного (нестандартного) ФПЗ [5, с. 62], але в даній інформаційній системі не здійснюється визначення рівня гарантій (рис. 1).

Тому актуальним стоїть питання впровадження автоматизованої оцінки рівня гарантій.

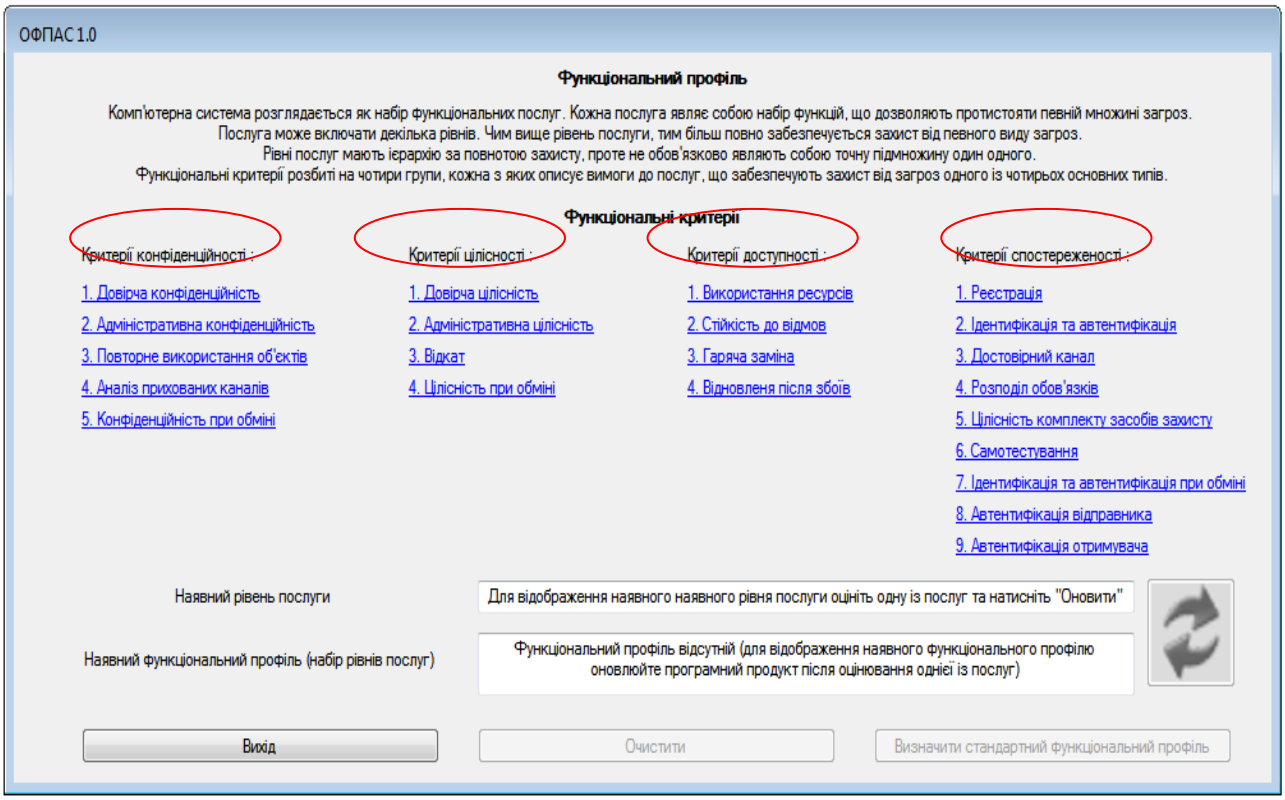

Рис. 1. Форма вибору функціонального критерію

Мета статті

Здійснити аналіз теоретичних основ оцінки рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованої системи від несанкціонованого доступу.

Виклад основного матеріалу

Автоматизована система являє собою організаційно-технічну систему, що об’єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію. Прийнято розрізняти два основних напрями технічного захисту інформації (ТЗІ) в АС — це захист АС і оброблюваної інформації від несанкціонованого доступу і захист інформації від витоку технічними каналами [6]. Забезпечення безпеки інформації АС розглядається як набір функціональних послуг.

Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз. Тому оцінка захищеності АС визначається з рівня реалізації послуг.

Окрім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в АС, критерії містять рівні гарантій, які дають змогу оцінити коректність реалізації послуг.

Рівні гарантій включають вимоги до архітектури комплексу засобів захисту (КЗЗ), середовища розробки, послідовності розробки, випробування КЗЗ, середовища функціонування і експлуатаційної документації (рис. 2).

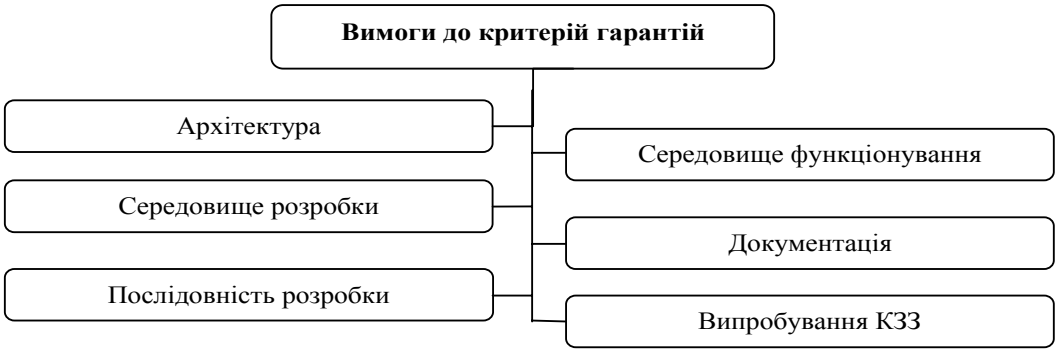

Рис. 2. Вимоги критерій гарантій

Уводиться сім рівнів гарантій, ці рівні є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру впевненості в тому, що послуги, які надаються, дозволяють протистояти певним загрозам, а механізми, що їх реалізують, у свою чергу, коректно реалізовані, і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації АС [2].

Гарантії забезпечуються як в процесі розробки, так і в процесі оцінки.

У процесі розробки гарантії забезпечуються діями розробника щодо забезпечення коректності розробки.

У процесі оцінки гарантії забезпечуються шляхом перевірки додержання розробником вимог, аналізу документації, процедур розробки і постачання, а також іншими діями експертів, які проводять оцінку.

Критерії гарантій, розглядаються в нормативному документі НД ТЗІ 2.5-004-99, містять в собі вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, експлуатаційної документації та випробувань КЗЗ. Згідно з вимогами цього документа, оцінювання відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам здійснюється шляхом проведення експертизи [3].

Розглянемо вимоги до рівня гарантій більш детально. Оцінювання рівня гарантій функціональних послуг безпеки (ФПБ) передбачає виконання таких дій:

– перший етап — ознайомлення з оцінювальною АС, збирання та аналіз документів, що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваної АС;

– другий етап — розроблення програми перевірки дотримання вимог до рівня гарантій у процесі розроблення, виробництва та постачання замовнику оцінюваної АС;

– третій етап — розроблення методики перевірки дотримання вимог до рівня гарантій у процесі розроблення, виробництва та постачання замовнику оцінюваної АС;

– четвертий етап — виконання оцінювання рівня гарантій згідно з розробленими програмою та методикою;

– п’ятий етап — аналіз та документування результатів оцінювання рівня гарантій [3].

Тому виходячи з даного порядку можна представити роботу експерта при подані на експертизу розробником або заявником АС разом з проектною, супровідною та експлуатаційною документацією та з визначеними в проектній документації функціональними специфікаціями АС наступною діаграмою (рис. 3).

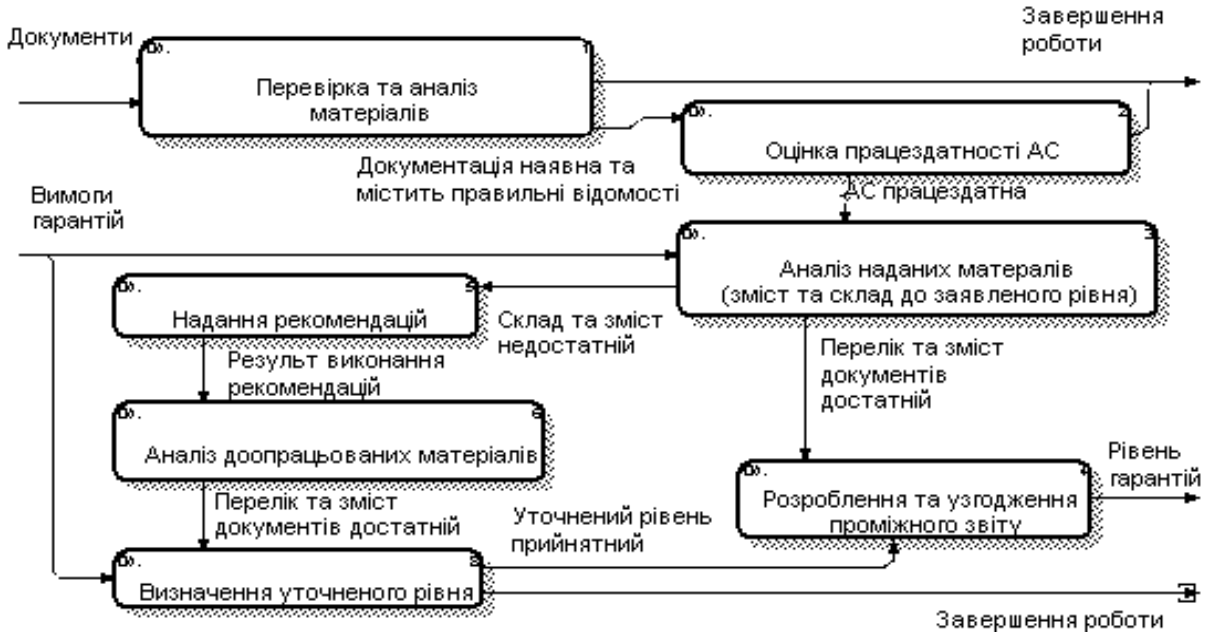

Рис. 3. Порядок роботи експерта

Виконуючи перший етап експерти перевіряють документацію на наявність функціональних специфікацій АС, якщо вони відсутні, експерт оцінює систему до вимог рівня гарантій Г-1.

Робота експерта відповідно до діаграми, яка представлена на (рис. 3), полягає в такому:

– проводиться перевірка факту надання експлуатаційної документації на АС та наявності в ній відомостей, необхідних для виконання подальших робіт з оцінювання працездатності АС. У випадку відсутності документації подальші роботи мають припинятися;

– якщо перший процес відбувся успішно проводиться оцінювання працездатності надано-

го АС та визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності АС подальші роботи мають припинятися;

– після чого проводиться аналіз, згідно з методичними рекомендаціями, наданих розробником або заявником матеріалів з метою попереднього визначення відповідності їх складу та змісту вимогам до рівня гарантій, визначеного розробником АС або заявником відповідно до заявленого рівня гарантій;

– за деяких невідповідностях, що аналізувалися у попередньому процесі, проводиться повторний аналіз складу та змісту доопрацьованих або додатково наданих розробником (заявником) матеріалів з метою визначення їх достатності для проведення подальших перевірок на відповідність вимогам до заявленого рівня гарантій або необхідності зниження заявленого рівня гарантій до такого, який випливає зі складу та змісту наданих матеріалів;

– потім відбувається прийняття рішення про прийнятність уточненого рівня гарантій, відповідність вимогам до якого має бути підтверджено в процесі експертизи та про продовження робіт;

– якщо даний рівень гарантій обраний, проводиться документування отриманих результатів у погодженому з розробником (заявником) проміжному звіті з обов'язковою фіксацією уточненого рівня гарантій як такого, відповідність вимогам до якого має бути підтверджено в процесі експертизи. Основною роботою експерта є збір та оцінка всіх необхідних документів перелік яких подано в таблиці рекомендований склад матеріалів (документів) [3]. Назви документів не є обов'язковими, допускається об'єднання схожих за змістом документів в один.

Рекомендації щодо змісту документів, які надаються експерту викладені в нормативному документі НД ТЗІ 2.7-010-09 в додатку А.

Відповідно до переліку та змісту представлених документів визначається подальше опрацювання документів та визначення вимог критеріїв гарантій. Вимоги представлені в нормативному документі НД ТЗІ 2.5-004-99. Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ.

Виходячи з даних критеріїв можна представити коефіцієнт гарантії позначенням — K^{gar}. Вимоги до архітектури представимо таким коефіцієнтом — K^{arh}, середовища розробки — K^{sr}, послідовності розробки — K^{pr}, середовища функціонування — K^{sf}, документації — K^{d} і випробувань — K^{v}.

Уведення даних коефіцієнтів дає можливість створити загальний математичний опис вимог гарантій, поданий такою множиною:

$$K^{gar} = \{K^{arh}, K^{sr}, K^{pr}, K^{sf}, K^{d}, K^{v}\}. \qquad (1)$$

Для того щоб АС одержала певний рівень гарантій, повинні бути задоволені всі вимоги, визначені для заданого рівня в кожному із розділів документа [3]. Розглянемо визначення вимог гарантій на прикладі архітектури [2].

Уведемо позначення вимог перейшовши до умовних позначень. Умови, які стосуються вимог архітектури, отримали буквене позначення «a» з цифровим індексом (1...5), до середовища розробки отримали буквене позначення «r» з цифровим індексом (1...7), послідовності розробки отримали буквене позначення «pr» з цифровим індексом (1...5), середовища функціонування отримали буквене позначення «sf» з цифровим індексом (1...3), документації отримали буквене позначення «d» з цифровим індексом (1...5) і випробувань отримали буквене позначення «v» з цифровим індексом (1...4). Після введення умовних позначень, таблиця буде мати наступний вигляд результат представлений в табл. 1.

Підставивши умовні позначення слід створити матрицю знань, яку потім можна буде використати при створенні програмного продукту, який визначатиме рівень гарантій. Матрицю знань створено так: вимогам, які виконуються у визначеній АС надаємо значення 1, а тим умовам, які не виконуються — 0. Для вимог архітектури відповідно до семи рівнів гарантій матриця буде мати такий вигляд (табл. 2).

Таблиця 1

Вимоги до архітектури КЗЗ (з умовними позначеннями)

Архітектура (вимоги)	Умовні позначення
КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені	a_1
КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень	a_2

Продовження табл. 1

Архітектура (вимоги)	Умовні позначення
Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня	a_3
З боку Розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки. Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту	a_4
Розробка ПЗ переважно має бути спрямована на мінімізацію складності КЗЗ. КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою. Цей механізм повинен відігравати центральну роль в реалізації внутрішньої структури КЗЗ. Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи як модульність побудови і приховання (локалізація) даних	a_5

Таблиця 2

Матриця знань

K^{arh} Рівень гарантій	$K^{arh}{}_1$	$K^{arh}{}_2$	$K^{arh}{}_3$	$K^{arh}{}_4$	$K^{arh}{}_5$	$K^{arh}{}_6$	$K^{arh}{}_7$
a_1	1	1	1	1	1	1	1
a_2	0	0	1	1	1	1	1
a_3	0	0	0	1	1	1	1
a_4	0	0	0	0	1	1	1
a_5	0	0	0	0	1	1	1

Відповідно до матриці (табл. 2) отримаємо наступні логічні рівняння.

$$K^{arh}{}_1 = K^{arh}{}_2 = a_1; \quad (2)$$

$$K^{arh}{}_3 = a_1 \wedge a_2; \quad (3)$$

$$K^{arh}{}_4 = a_1 \wedge a_2 \wedge a_3; \quad (4)$$

$$K^{arh}_5 = K^{arh}_6 = K^{arh}_7 = a_1 \wedge a_2 \wedge a_3 \wedge a_4 \wedge a_5. \quad (5)$$

Якщо один із наведених вище логічних виразів (2–5) приймає значення «1», то обирають відповідну вимогу, якщо значення «0» — вимога відкидається.

Отож, дані рівняння відображають формалізацію основ до вимог архітектури по визначенню рівня гарантій.

Відповідно до НД ТЗІ 2.7-004-99 формалізуємо усі представлені вимоги до наступних логічних рівнянь.

Вимоги архітектури K^{arh} визначаються за допомогою системи рівнянь

$$K^{arh} = \begin{cases} K^{arh}{}_1 = K^{arh}{}_2 = a \\ K^{arh}_3 = a_1 \wedge a_2; \\ K^{arh}_4 = a_1 \wedge a_2 \wedge a_3; \\ K^{arh}_5 = K^{arh}_6 = K^{arh}_7 = a_1 \wedge a_2 \wedge a_3 \wedge a_4 \wedge a_5. \end{cases} \quad (6)$$

Вимоги середовища розробки K^{sr} визначаються за допомогою системи рівнянь

$$K^{sr} = \begin{cases} K^{sr}_1 = K^{sr}_2 = r_1 \wedge r_4; \\ K^{sr}_3 = r_1 \wedge r_2 \wedge r_4; \\ K^{sr}_4 = K^{sr}_5 = r_1 \wedge r_2 \wedge r_3 \wedge r_4 \wedge r_5 \wedge r_6; \\ K^{sr}_6 = K^{sr}_7 = r_1 \wedge r_2 \wedge r_3 \wedge r_4 \wedge r_5 \wedge r_6 \wedge r_7. \end{cases} \quad (7)$$

Вимоги послідовність розробки K^{pr} визначаються за допомогою системи рівнянь

$$K^{pr} = \begin{cases} K^{pr}_1 = pr_1 \wedge pr_3 \wedge pr_4; \\ K^{pr}_2 = K^{pr}_3 = K^{pr}_4 = K^{pr}_5 = K^{pr}_6 = K^{pr}_7 = \\ = pr_1 \wedge pr_2 \wedge pr_3 \wedge pr_4. \end{cases} \quad (8)$$

Вимоги послідовність розробки K^{sf} визначаються за допомогою системи рівнянь

$$K^{sf} = \begin{cases} K^{sf}_1 = K^{sf}_2 = sf;_1 \\ K^{sf}_3 = K^{sf}_4 = K^{sf}_5 = sf_1 \wedge sf_2; \\ K^{sf}_6 = K^{sf}_7 = sf_1 \wedge sf_2 \wedge sf_3. \end{cases} \quad (9)$$

Вимоги документації K^d визначаються за допомогою рівняння

$$K^d = K^d_1 = K^d_2 = K^d_3 = K^d_4 = K^d_5 = K^d_6 = K^d_7 = \\ = d_1 \wedge d_2 \wedge d_3 \wedge d_4 \wedge d_5. \quad (19)$$

Вимоги випробування КЗЗ K^v визначаються за допомогою системи рівнянь

$$K^v = \begin{cases} K_1^v = v_1 \wedge v_2; \\ K_2^v = K_3^v = v_1 \wedge v_2 \wedge v_3; \\ K_4^v = K_5^v = K_6^v = K_7^v = v_1 \wedge v_2 \wedge v_3 \wedge v_4. \end{cases} \quad (10)$$

Визначивши вимоги гарантій та їх математичний опис, з'являється можливість визначити один із рівнів гарантій.

Висновки

Таким чином, у роботі запропоновано, показано та проаналізовано теоретичні основи визначення рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації АС від НСД. Висвітлено необхідні НД ТЗІ, які регламентують порядок оцінки та визначення рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації АС від НСД в Україні. На основі нормативних документів, здійснено формалізацію визначення (узгодження) рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації АС від НСД. Запропоновані авторами теоретичні основи надають можливості в подальшому розробити експертну систему, яка визначатиме рівні гарантій АС від НСД. Це полегшіть роботу експертів щодо визначення гарантій безпеки АС від НСД, зменшить витрачений на це ресурс часу. У сукупності з автоматизацією процесу визначення стандартних (нестандартних) профілів захищеності АС від НСД, реалізація викладених в статті результатів надасть можливість у подальшому удосконалити інформаційну систему розроблену групою авторів з урахуванням гарантій безпеки.

Перспективи подальших досліджень

Основними результатами автори вважають здійснення формалізації визначення рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу. Запропоновані авторами теоретичні основи дають можливість у подальшому розробити експертну систему, яка допоможе експертам визначати гарантії безпеки автоматизованої системи від несанкціонованого доступу автоматизовано.

ЛІТЕРАТУРА

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

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. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-010-09 [Електронний ресурс]. — Режим доступу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=103247.

4. **Юдін О. К**. Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу / О. К. Юдін, С. С. Бучик, С. В. Мельник // Наукоємні технології. — 2016. — № 2 (30). — С.195 — 205, doi.org/10.18372/2310-5461.30.10564.

5. А. с. 66492 Україна. Комп'ютерна програма. Інформаційна система визначення функціонального профілю захищеності автоматизованої системи від несанкціонованого доступу / С. С. Бучик, С. В. Мельник (Україна). — № 67055; заявл. 10.05.16; опубл. 28.10.16, Бюл. № 42.

6. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99 [Електронний ресурс]. — Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340.

Бучик С. С., Юдін, О. К., Нетребко Р. В.

ТЕОРЕТИЧНІ ОСНОВИ ВИЗНАЧЕННЯ РІВНЯ ГАРАНТІЙ АВТОМАТИЗОВАНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У статті запропоновано, показано та проаналізовано теоретичні основи визначення рівня гарантій автоматизованих систем від несанкціонованого доступу. Висвітлено необхідні нормативні документи технічного захисту інформації, які регламентують порядок оцінки та визначення рівня гарантій автоматизованих систем від несанкціонованого доступу в Україні. Розглянуто алгоритм дій експерта. На основі даних документів, вперше здійснено формалізацію основ визначення рівня гарантій автоматизованих систем від несанкціонованого доступу. Запропоновані авторами теоретичні основи дають можливість в подальшому удосконалити експертну систему, яка автоматизовано визначатиме функціональний профіль захищеності та рівень гарантій автоматизованої системи від несанкціонованого доступу. Це полегшить роботу експертів щодо визначення профілю захищеності, рівня гарантій та створення необхідного комплексу засобів захисту, а також зменшить витрачений ресурс часу та матеріальних ресурсів.

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

Бучик С. С., Юдин О. К., Нетребко Р. В.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОПРЕДЕЛЕНИЯ УРОВНЯ ГАРАНТИЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В статье предложены, показаны и проанализированы теоретические основы определения уровня гарантий автоматизированных систем от несанкционированного доступа. Отражены необходимые нормативные документы технической защиты информации, которые регламентируют порядок оценки и определения уровня гарантий автоматизированных систем от несанкционированного доступа в Украине. Рассмотрен алгоритм действий эксперта. На основе данных документов, впервые осуществлена формализация основ определения уровня гарантий автоматизированных систем от несанкционированного доступа. Предложены авторами теоретические основы дают возможность в дальнейшем усовершенствовать экспертную систему, которая автоматизировано будет определять функциональный профиль защищенности и уровень гарантий автоматизированной системы от несанкционированного доступа. Это облегчит работу экспертов относительно определения профиля защищенности, уровня гарантий и создания необходимого комплекса средств защиты, а также уменьшит потраченный ресурс времени и материальные ресурсы.

Ключевые слова: автоматизированная система, информационная безопасность, политика безопасности информации, правила разграничения доступа, несанкционированный доступ, комплекс средств защиты, профиль защищенности.

Buchyk S., Yudin O., Netrebko R.

THEORETICAL BASIS FOR DETERMINING THE LEVEL OF GUARANTEES OF AUTOMATED SYSTEMS FROM UNAUTHORIZED ACCESS

The article suggests, shows and analyzes the theoretical basis for determining the level of guarantees of automated systems from unauthorized access. The necessary normative documents of technical protection of information that regulate the procedure for assessing and determining the level of guarantees of automated systems from unauthorized access in Ukraine are reflected. The algorithm of the expert's actions is considered. On the basis of these documents, formalization of the basis for determining the level of guarantees of automated systems against unauthorized access was carried out for the first time. The authors proposed theoretical foundations that make it possible to further improve the expert system that will automatically determine the functional profile of security and the level of guarantees of the automated system from unauthorized access. This will facilitate the work of experts regarding the definition of the security profile, the level of guarantees and the creation of the necessary set of protective equipment, as well as reduce the spent resource of time and material resources.

Keywords: automated system, information security, information security policy, access control rules, unauthorized access, complex of protection facilities, security profile.

Стаття надійшла до редакції 04.05.2017 р.
Прийнято до друку 12.05.2017 р.
Рецензент – д-р техн. наук, проф. Литвиненко О. Є.