

УДК 004.056.5

DOI: 10.18372/2310-5461.36.12228

С. С. Бучик

д-р техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0003-0892-3494
e-mail: s_stbu@ukr.net;

Р. В. Нетребко

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

РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ТА РІВНЯ ГАРАНТІЙ АВТОМАТИЗОВАНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вступ

Необхідність інформатизації системи управління, створення баз даних та знань державних інформаційних ресурсів (ДІР) зумовлена сьогодні, насамперед, проведенням в державі нової економічної політики, зростанням кількості техногенних катастроф, загостренням військової агресії з боку інших держав. Зазначимо, що безпосередньо інформаційна війна як соціально-технічний інструмент стала важливою частиною військово-політичного втручання інших держав у життєві процеси України [1].

Наслідком цього в державі більше уваги приділяється саме питанням кібербезпеки, що в теперішній час призвело до прийняття Україною в 2016 р. «Стратегії кібербезпеки України» і на решті ухваленням Верховною Радою України 05 жовтня 2016 року Закону України «Про основні засади забезпечення кібербезпеки України».

Значну роль у протидії інформаційній війні слід приділяти захисту ДІР на основі сформованої інформаційної політики країни та впровадженню комплексного підходу до побудови систем захисту.

Провівши дослідження нормативно-правової бази (НПБ) України в галузі захисту автоматизованих систем (АС) від несанкціонованого доступу (НСД), було відмічено наступні документи: НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22 [2] із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 та НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг без-

пеки в засобах захисту інформації від несанкціонованого доступу» затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24 липня 2009 р. № 172 [3]. Проаналізовані документи стали основою для розробки програмного забезпечення. У сенсі дослідження є актуальним здійснити реалізацію програмного забезпечення 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 захисту інформації, визначення рівня захисту відображенні в працях вітчизняних і закордонних учених, серед яких І. Д. Горбенко, О. Г. Корченко, В. К. Задірака, Г. Ф. Коначович, М. В. Грайворонський, О. М. Новіков, В. Ф. Шаньгин, О. К. Юдін та багато інших. Розглянувши праці науковців було визначено, що темою визначення рівня гарантій АС від НСД присвячено небагато робіт. Це вказує на те, що даному питанню приділено не багато уваги, можливо із-за того, що процес визначення здійснюється експертною комісією та фактично єдиним документом, якій визначає підхід до визначення гарантій, є НД ТЗІ 2.7-010-09.

Дана робота є продовженням робіт авторів, в основу якої положені теоретичні основи визначення рівня гарантій автоматизованих систем від несанкціонованого доступу [7]. 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 роботи [4] авторами було розроблено інформаційну систему визначення стандартного (нестандартного) функціонального профілю захищеності (ФПЗ) [5, 8], але в даній інформаційній системі не здійснюється визначення рівня гарантій. Тому актуальним стоїть питання впровадження автоматизованої оцінки рівня гарантій.

Мета статті

Показати етапи проектування та реалізації програмного забезпечення визначення рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованої системи від несанкціонованого доступу.

Виклад основного матеріалу

Швидкий розвиток інформаційних технологій потребує значного захисту інформації користувачів різних рівнів. Починаючи з двохтисячних років розроблялась НПБ України щодо захисту інформації, оцінки ступеня захисту АС.

З визначенням стандартних функціональних профілів захищеності та рівнів гарантій пов'язана ціла низка нормативних документів технічного захисту інформації (НД ТЗІ), а саме: НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу».

Проаналізувавши дані документи було визначено, що ці документи надають лише методологічну базу з точки зору, як нормативний документ для вибору та реалізації вимог безпеки в АС, але єдиної методології, яка б поєднувала дані документи та надавала зрозумілу та просту інтерпретацію процесу обирання ФПЗ та рівнів гарантій немає. У ході дослідження методу авторами було проведено моделювання процесів.

На рис. 1 наведено головну контекстну діаграму процесу визначення ФПЗ та рівня гарантій, на рис. 2 — результат моделювання підпроцесів визначення ФПЗ та рівня гарантій проміжного рівня деталізації.

Data Flow Diagram (DFD) — стандарт для створення моделі потоків інформації, що циркулює в АС.

Модель системи визначається, якієрархія діаграм потоків даних, що описують асинхронний процес перетворення інформації від введення у систему до отримання користувачем. DFD визначає, яким чином кожний процес перетворює вхідні дані у вихідні та дозволяє виявити залежності між процесами.

Діаграма включає наступні блоки: блок перевірки відповідності АС до вимог рівня послуги комплексу засобів захисту НЦ-1; блок отримання ФПЗ захищеності АС від несанкціонованого доступу (НСД); блок перевірки відповідності визначеного профілю захищеності до стандартного ФПЗ; блок визначення відповідності документів та блок оцінки рівня гарантій.

На основі розроблених діаграм та роботи теоретичні основи визначення рівня гарантій [7] можливо розробити програмне забезпечення для автоматизованого визначення ФПЗ та рівня гарантій. Програмне забезпечення призначене для оцінювання, визначення функціональних профілів захищеності та рівня гарантій оброблюваної інформації від несанкціонованого доступу відповідно до нормативних документів України в галузі інформаційної безпеки. Дане програмне забезпечення створюється для розробників, користувачів АС, які використовуються для обробки критичної інформації (інформації, яка потребує захисту), а також для державних органів, які здійснюють функції контролю за обробкою такої інформації.

Узявши за основу НПБ НД ТЗІ 2.5-004-99 та НД ТЗІ 2.7-010-09 було розроблено загальну блок-схема функціонування програми по визначенню ФПЗ та рівня гарантій рис. 3.

Дана блок-схема включає такі блоки:

- блок 1 – блок перевірки відповідності АС до вимог рівня послуги комплексу засобів захисту НЦ-1;
- блок 2 – блок отримання ФП захищеності АС від НСД;
- блок 3 – блок перевірки відповідності визначеного профілю захищеності до стандартного ФП;
- блок 4 – блок визначення рівня гарантій.

Перших три блоки було розглянуто у попередній статті реалізація програмного забезпечення визначення функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу [8], тому перейдемо відразу до четвертого блоку алгоритму, який наведено на рис. 4.

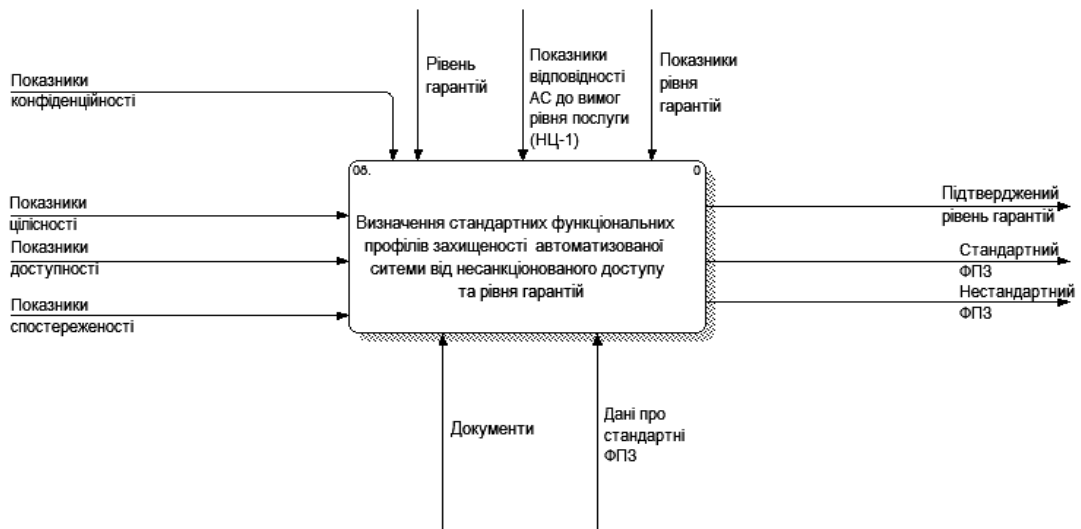


Рис. 1. Контекстна діаграма процесу визначення ФПЗ та рівня гарантій

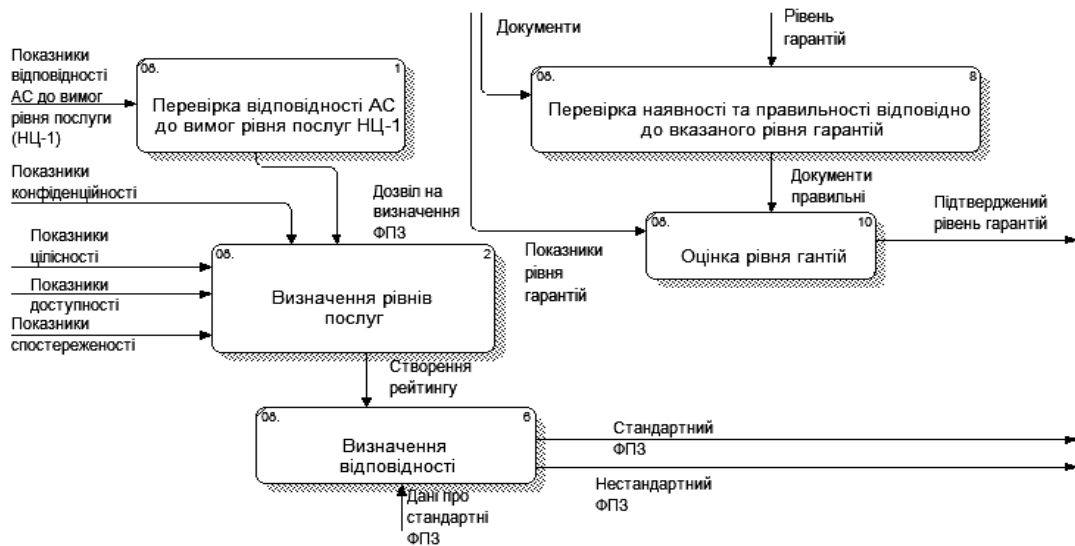


Рис. 2. Декомпована діаграма процесу визначення ФПЗ та рівня гарантій

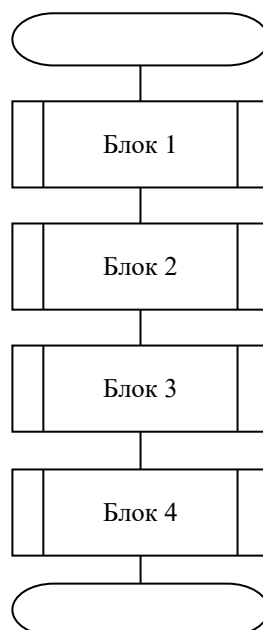


Рис. 3. Загальна блок-схема алгоритму функціонування програми

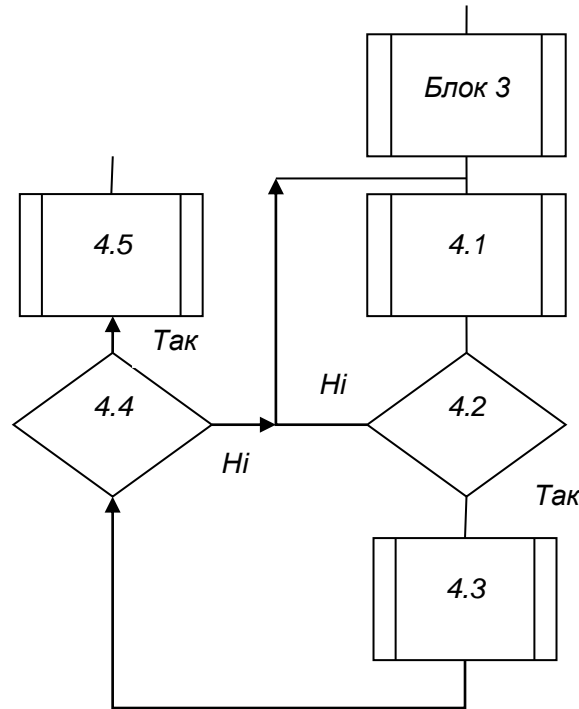


Рис. 4. Функціонування четвертого блоку алгоритму

Четвертий блок алгоритму включає такі блоки:
 4.1 — вибір рівня гарантій для оцінювання;
 4.2 — перевірка документації, що відповідає заявленому рівню перехід до блоку 4.3, якщо ні перехід до блоку 4.1;
 4.3 — оцінка рівня гарантій відповідно до критеріїв;
 4.4 — перевірка відповідності заявленого рівня гарантій, якщо так перехід до блоку 4.5, якщо ні перехід до блоку 4.1;
 4.5 — підготовка документації по визначеному рівню гарантій.

Ідея алгоритму ґрунтується на такому: користувач (адміністратор безпеки) послідовно повинен визначити рівні усіх послуг. Для здійснення даної процедури користувачеві надається опитувач, у якому він повинен обрати відповідь, яка задовольняє наявні критерії.

Рівень гарантій містить перевірку наявності та складу потрібних документів, а також оцінку критеріїв відповідно до обраного рівня гарантій.

На основі НПБ та розроблених діаграм, алгоритмів функціонування було розроблено програмне забезпечення ОФПАС 2.0. Процес визначення ФПЗ було розглянуто в статті [8], тому зупинимось безпосередньо на оцінці рівня гарантій.

Перед тим, як визначити ФПЗ і рівень гарантій необхідно перевірити виконання вимог та необхідних умов для рівня послуги цілісність комплексу засобів захисту (КЗЗ) НЦ-1, оскільки даний рівень послуги є необхідною умовою абсолютною для всіх рівнів всіх послуг (рис. 5).

Якщо рівень НЦ-1 підтверджено, відкривається можливість вибору запропонованого рівня гарантій. На вкладці вибирається потрібний рівень гарантій (рис. 6).

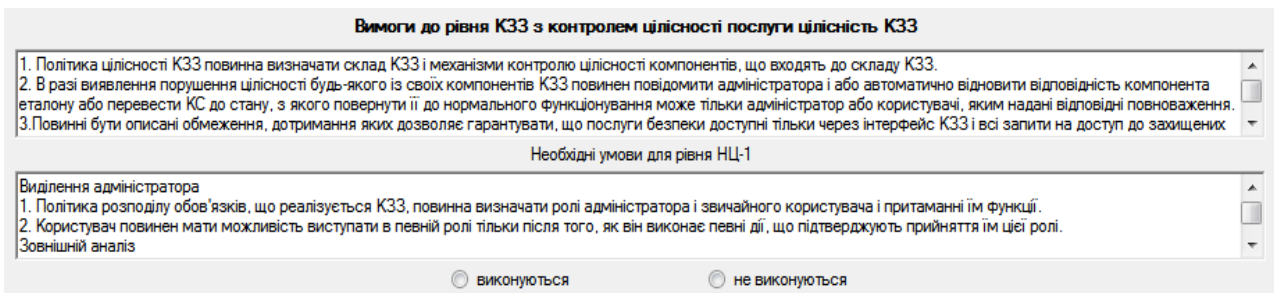


Рис. 5. Визначення рівня НЦ-1

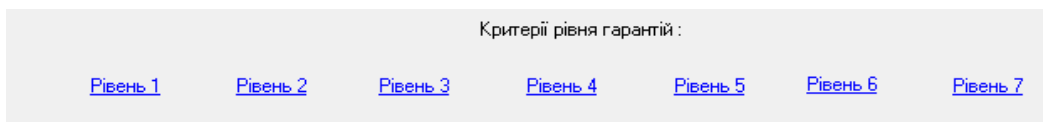


Рис. 6. Панель вибору рівня гарантій

Після чого для кожного рівня пропонується перелік необхідних документів та критерії, які потрібно обрати, якщо вони відповідають заявленому рівню при перевірці експертом (рис. 7).

Якщо перелік не відповідає заявленому рівню виникає помилка (повідомлення про невідповід-

ність документації) та повідомлення про невідповідність критерію (рис. 8, 9). У випадку якщо обрані вкладки відповідають заявленому рівню, виникає підтвердження, що заявлений рівень підтверджений (рис. 10), що дозволяє експерту виконувати оформлення документації.

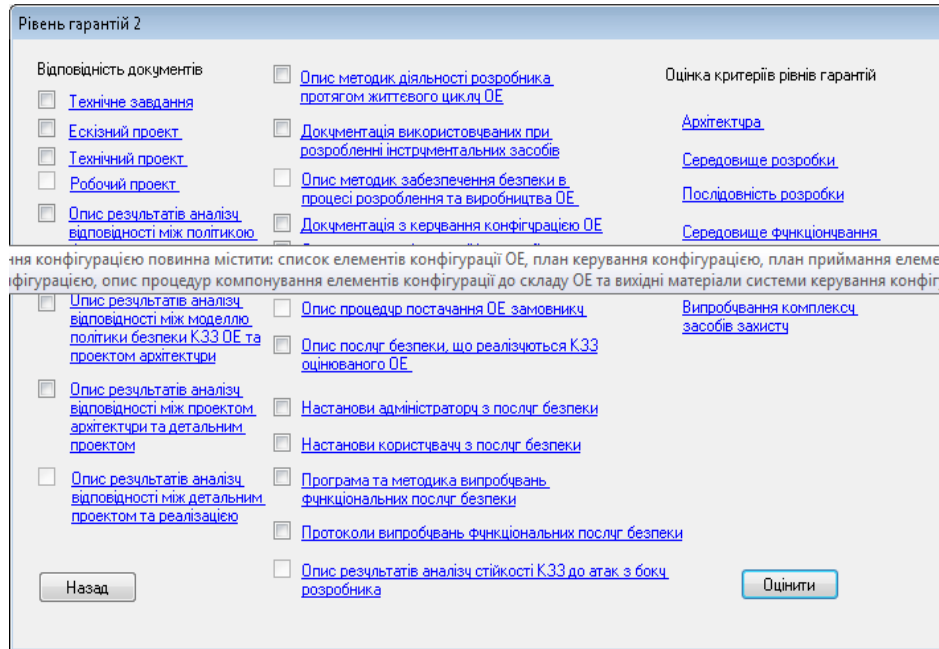


Рис. 7. Панель оцінки документації та критеріїв

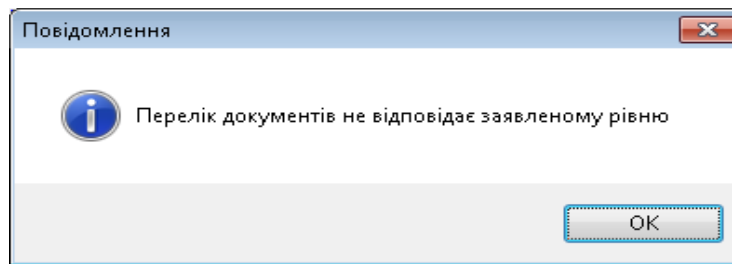


Рис. 8. Повідомлення про невідповідність документації

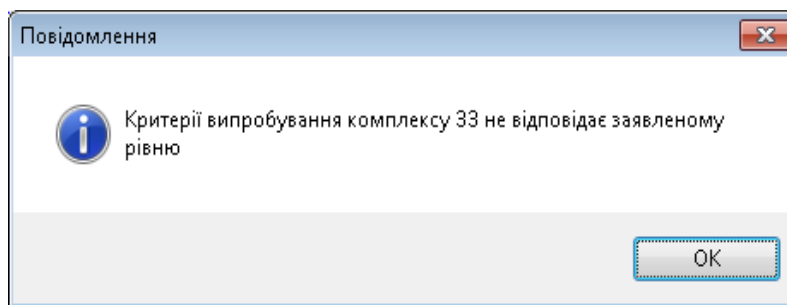


Рис. 9. Повідомлення про невідповідність критерію

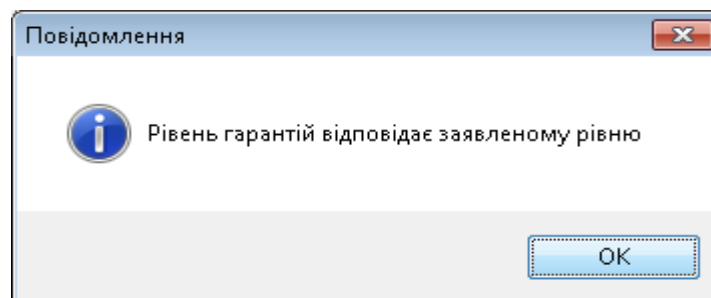


Рис. 10. Повідомлення про підтвердження заявленого рівня

Розроблена програма дозволяє зменшити час, який витрачає адміністратор безпеки (системний адміністратор) для визначення функціональних профілів захищеності та рівнів гарантій обробленої інформації від несанкціонованого доступу, та виявити наявність співпадіння визначеного функціонального профілю із стандартним (за умови виконання даного співпадіння користувачу надається інформація про даний стандартний функціональний профіль) та підтвердити або визначити інший рівень гарантій.

Висновки

Таким чином, у статті показано поетапно процес розробки програмного забезпечення 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, розроблено DFD-діаграму та блок-схеми алгоритмів визначення (узгодження) рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації АС від НСД. Розроблений програмний продукт полегшить 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 в подальшому дослідити програмне забезпечення групою експертів.

Перспективи подальших досліджень

Основними результатами автори вважають здійснення реалізацію програмного забезпечення визначення рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу. Запропоноване авторами програмне забезпечення дає можливість в подальшому дослідити експертну систему групою експертів для оцінки АС.

ЛІТЕРАТУРА

Бучик С. С., Нетребко Р. В.

РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ТА РІВНЯ ГАРАНТІЙ АВТОМАТИЗОВАНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

В статті показано основні етапи реалізації програмного забезпечення визначення або узгодження рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу в Україні на основі раніше проведених авторами теоретичних досліджень визначення або узгодження рівня гарантій. Здійснено проектування роботи програми за допомогою діаграм Data a Flow Diagram. Побудовано більш детальні блок-схеми роботи програмного забезпечення та ал-

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 / Бучик С. С., Мельник С. В. (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.

7. **Бучик С. С.** Теоретичні основи визначення рівня гарантій автоматизованих систем від несанкціонованого доступу / С. С. Бучик, О. К. Юдін, Р. В. Нетребко // Наукоємні технології № 2 (34), 2017. — С. 119–124. DOI: 10.18372/2310-5461.34.11609

8. Бучик С. С. Реалізація програмного забезпечення визначення функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу / С. С. Бучик, О. К. Юдін, Р. В. Нетребко // Вісник інженерної академії України №1, 2017. — С. 54–60 [Електронний ресурс]. — Режим доступу: <http://jrn1.nau.edu.ua/index.php/SBT/article/download/11609/15483>.

горитмів. Реалізовано прототип програмного забезпечення та наведено приклади роботи по кожному з основних блоків роботи, які були попередньо спроектовані в діаграмах та блок-схемах алгоритмів.

Визначено переваги та недоліки розробленого програмного забезпечення визначення функціонального профілю захищеності та рівня гарантій. Вказано подальші кроки продовження дослідження у даному напрямку.

Ключові слова: автоматизована система, захист інформації, несанкціонований доступ, комплекс засобів захисту, функціональний профіль захищеності, рівень гарантій.

Бучик С. С., Нетребко Р. В.

РЕАЛИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОПРЕДЕЛЕНИЯ ФУНКЦИОНАЛЬНЫХ ПРОФИЛЕЙ И УРОВНЯ ГАРАНТИЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В статье показаны основные этапы реализации программного обеспечения определения или согласования уровня гарантий корректности реализации функциональных услуг безопасности в средствах защиты информации автоматизированных систем от несанкционированного доступа в Украине на основе ранее проведенных авторами теоретических исследований определения или согласования уровня гарантий. Осуществлено проектирование работы программы с помощью диаграмм Data Flow Diagram. Построены более детальные блок-схемы работы программного обеспечения и алгоритмов. Реализован прототип программного обеспечения и приведены примеры работы по каждому из основных блоков работы, которые были предварительно спроектированы в диаграммах и блок-схемах алгоритмов. Определены преимущества и недостатки разработанного программного обеспечения определения функционального профиля защищенности и уровня гарантий. Указаны дальнейшие шаги продолжения исследования в данном направлении.

Ключевые слова: автоматизированная система, защита информации, несанкционированный доступ, комплекс средств защиты, функциональный профиль защищенности, уровень гарантий.

Buchyk S., Netrebko R.

REALIZATION SOFTWARE OF DETERMINATION OF FUNCTIONAL PROFILES AND LEVEL OF GUARANTEES OF AUTOMATED SYSTEMS FROM AN UNAUTHORIZED ACCESS

In the article basic stages of implementation of software of determination or concordance of level of guarantees of correctness of realization of functional services of safety phases in facilities of security of information of automated systems from an unauthorized access in Ukraine on the basis of undertaken by authors earlier theoretical studies of determination or concordance of level of guarantees are shown. Planning of work of the program is carried out by means of diagrams of Data Flow Diagram. More detailed flow-charts of work of software and algorithms are built. The prototype of software is realized and examples of work on each of basic blocks of work, that were preliminary projected in diagrams and flow-charts of algorithms are made. Certain advantages and drawbacks of the worked out software of functional profile of security and of level of guarantees are determined. The further steps of continuation of research in this direction are indicated.

Keywords: automated systems, security of information, unauthorized access, complex of security facilities, functional profile of security, level of guarantees.

Стаття надійшла до редакції 20.11.2017 р.

Прийнято до друку 25.11.2017 р.

Рецензент — д-р техн. наук, Корнієнко Б. Я.