УДК 004.056.5 DOI: 10.46972/2076-1546.2022.23.03

Р. В. Нетребко

ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВИЗНАЧЕННЯ РІВНЯ ЗАХИЩЕНОСТІ У ВІЙСЬКОВИХ АВТОМАТИЗОВАНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ВОРОГА

У статті запропоновано та проаналізовано основні етапи застосування програмного забезпечення групової оцінки функціонального профілю та визначення або узгодження рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації військових автоматизованих систем управління від несанкціонованого доступу противника в Україні на основі раніше проведених авторами теоретичних досліджень та розробленого програмного забезпечення. Проаналізовано останні дослідження та публікації провідних науковців у сфері захисту інформації від несанкціонованого доступу. Наведено основні нормативні документи технічного захисту інформації, які регламентують порядок оцінювання та визначення функціонального профілю і рівня гарантій автоматизованих систем від несанкціонованого доступу, що застосовуються для цивільних та державних автоматизованих систем в Україні. Здійснено проєктування функціонування програми за допомогою діаграм та алгоритмів. Протестовано програмне забезпечення та наведено приклади роботи. Виявлено переваги та недоліки програмного забезпечення групового визначення функціонального профілю захищеності та рівня гарантій для перевірки військових автоматизованих систем.

Розроблене програмне забезпечення полегшить роботу експертів щодо визначення захищеності системи від несанкціонованого доступу та пришвидшить удосконалення необхідного комплексу засобів захисту, потрібного для надійного захисту таємної інформації. Окреслено подальші кроки удосконалення для оцінювання рівня захищеності військових автоматизованих систем від несанкціонованого доступу противника.

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

Постановка проблеми в загальному вигляді. У період широкомасштабних змін у міждержавних відносинах першочерговим кроком є захист державної та військової інформації. У сьогоднішній ситуації зі значним розвитком сфери інформатизації потрібен швидкий аналіз розроблених військових систем на захист інформації, яка обробляється в них. Спеціалісти багатьох країн світу намагаються вирішити цю проблему, використовуючи різноманітні засоби та методи. Тому запропоновано методику оцінювання, що ґрунтується на використанні експертних процедур, тобто визначенні групової експертної оцінки. Для характеристики захисту інформації потрібно визначити рівень захищеності. Оскільки цей процес займає багато часу, то постає актуальне питання щодо автоматизації визначення рівня захищеності військових автоматизованих систем (ВАС) від несанкціонованого доступу ворога (НСДВ).

Аналіз останніх досліджень і публікацій показав, що головним завданням методів визначення рівня захищеності ВАС є пошук конкретного функціонального профілю

захищеності (ФПЗ) та підтвердження рівня гарантій. Питання створення, організації та дослідження процесів функціонування й розвитку систем захисту інформації розглянуто в працях багатьох українських науковців, серед яких Корченко О. Г., Лєншин А. В., Паламарчук Н. А., Шевченко В. Л., Шаньгин В. Ф., Юдін О. К., Чунарьов А. В., Бучик С. С. тощо. Вони запропонували основні теоретичні положення із захисту інформації, розробили методологічні та науково-теоретичні основи побудови систем захисту, оцінювання їх ефективності та принципи вибору параметрів для цього. Проаналізувавши відомі дослідження, ми з'ясували, що в роботі [1] розглянуто теоретичні основи визначення стандартних функціональних профілів на основі нормативно-правового забезпечення. У статті [2] проведено теоретичну побудову парето-оптимальних профілів. Автори [3] реалізували метод формування функціональних профілів на основі побудови таблиць для визначення необхідності та рівня послуг. У роботі [4] охарактеризовано стан нормативно-правової бази технічного захисту інформації. У [5] розглянуто питання захисту інформації зі створення альтернативних систем захисту. Автори статті [6] та монографії [7] описали загальну модель формування системи захисту державних інформаційних ресурсів, де основним процесом є вибір профіля захищеності. У праці [8] розроблено методи побудови та перевірки на повноту ФПЗ. Проаналізовані роботи теоретично спрямовані, вони не мають відношення до військової галузі. Звідси постало питання протестувати розроблене програмне забезпечення для оцінювання ВАС.

Формулювання завдання дослідження. Метою статті є проведення тестування програмного забезпечення узгодження експертної групової оцінки визначення ФПЗ та рівня гарантій у засобах захисту інформації ВАС від НСДВ, а також з'ясування напрямків його удосконалення.

Виклад основного матеріалу. З визначенням стандартних ФПЗ та рівнів гарантій пов'язана ціла низка нормативних документів технічного захисту інформації (НД ТЗІ), а саме: НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, НД ТЗІ 2.7-010-09. З чинної нормативно-правової бази випливає, що в документах НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» 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» описано процес оцінювання функціональних послуг безпеки та рівня гарантій коректності їх реалізації. Але досі залишилося не вирішеним питання, яким чином первинно обґрунтувати склад ФПЗ та рівень гарантій. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» встановлює єдиний підхід до визначення ФПЗ шляхом вибору з множини стандартних профілів. Крім того, в ньому описані критерії оцінки рівня гарантій. На основі НД ТЗІ 2.5-004-99 було проведено аналіз методів визначення рівня захищеності автоматизованих систем (АС), одним з яких є стандартний метод. Більш детально НД ТЗІ було проаналізовано в статті [9]. Дані документи надають лише методологічну базу для вибору та реалізації вимог безпеки в АС, але єдиної методики, яка б поєднувала ці документи й надавала зрозумілу та просту інтерпретацію процесу обирання ФПЗ і рівнів гарантій немає, тому на основі НД ТЗІ було реалізоване програмне забезпечення для визначення групової оцінки [10], яке також можливо застосовувати експертам для оцінювання ВАС. Аналіз відомих експертиз показує, що в процесі їх побудови можна виділити послідовність дій, описану в [11].

З метою дослідження ВАС складено таблицю для опитування експертів у вигляді системи запитань, яка задається програмним продуктом ОФПАС 2.0 [12]. До складу комісії обрано 10 експертів. Визначення профілю захищеності та рівня гарантій здійснюється саме програмним продуктом ОФПАС 2.0. Надіслана експертами інформація обробляється програмним продуктом сервера, після чого ухвалюється рішення з урахуванням результатів роботи експертів.

Для обробки експертної інформації обрано один із методів експертної оцінки – ранжування, який полягає в порівнянні досліджуваної системи з деякою стандартною.

Оцінювання ВАС проведено на основі перевірки третього рівня гарантій десятьма експертами. Нижче наведено процедуру роботи одного з експертів. Приклад оцінки потрібного рівня гарантій потребує початково визначити рівень послуги цілісності комплексу засобів захисту (КЗЗ) НЦ-1 (рис. 1), після чого проводиться вибір третього рівня (рис. 2).

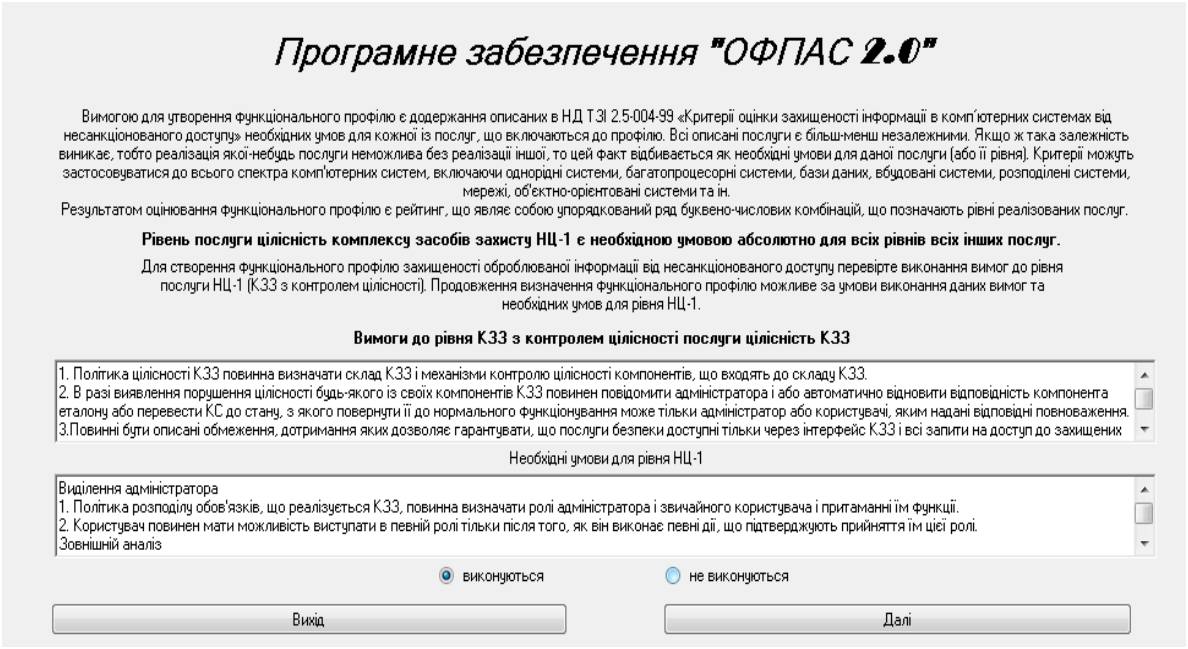

Рис. 1. Підтвердження рівня послуги НЦ-1

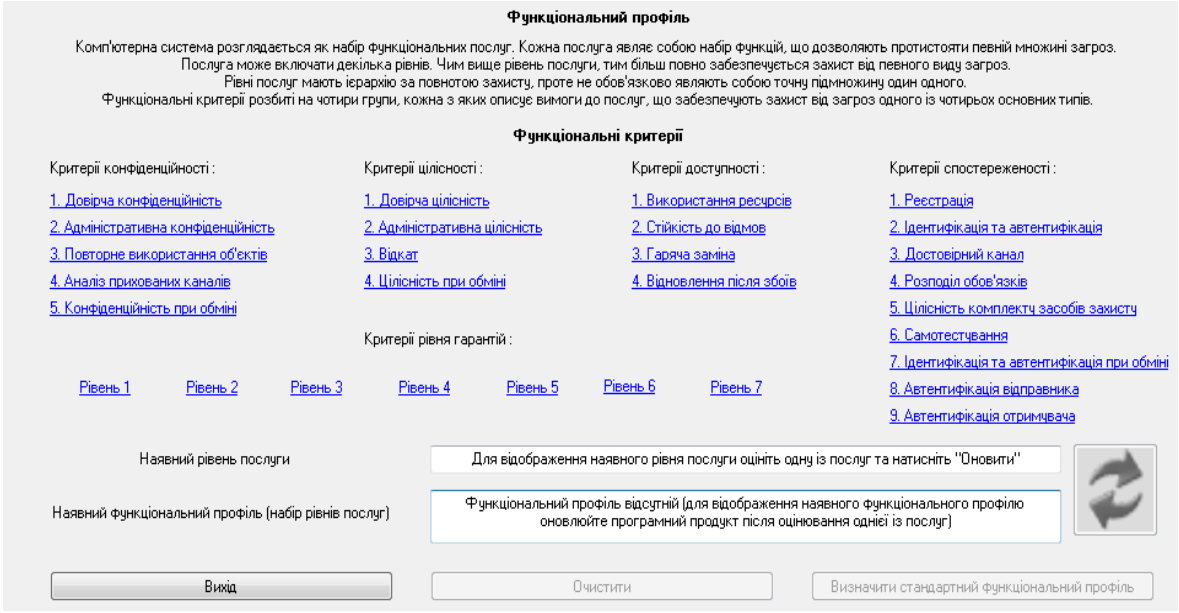

Рис. 2. Вибір третього рівня гарантій

Далі проводиться оцінювання відповідності документів рис. 3 третього рівня гарантій.

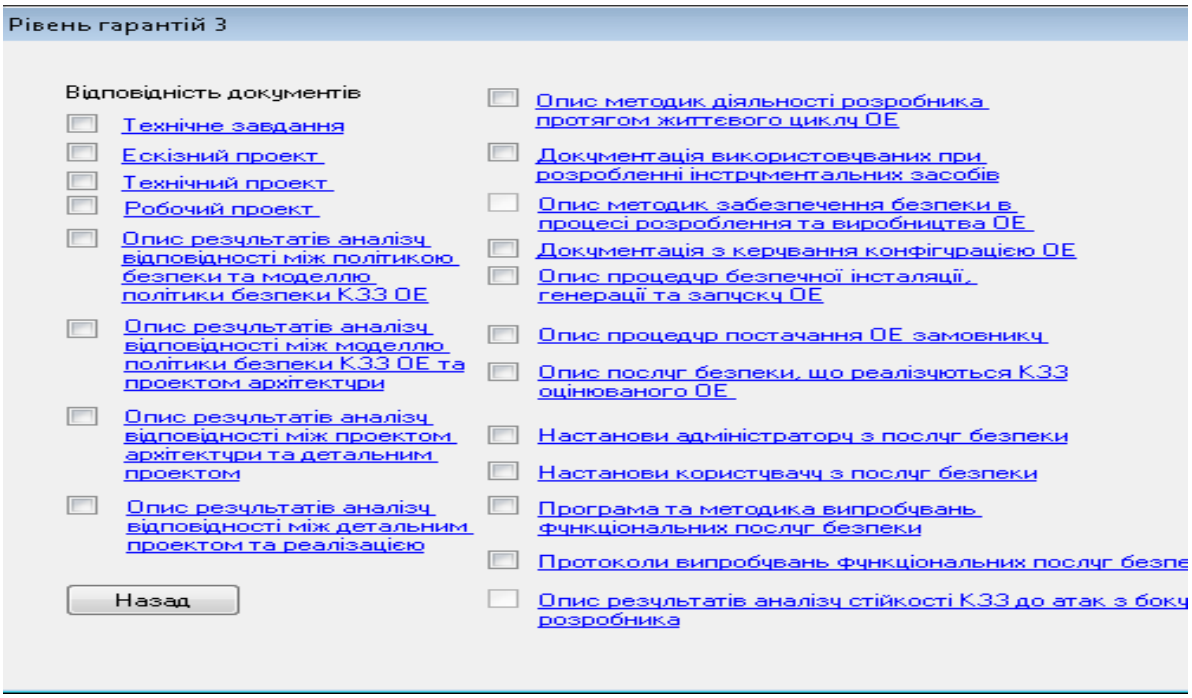

Рис. 3. Оцінка експертами відповідності документів

Наступним кроком роботи експерта є оцінювання критеріїв третього рівня гарантій. Приклад наведено на рис. 4 на основі критерію випробування КЗЗ.

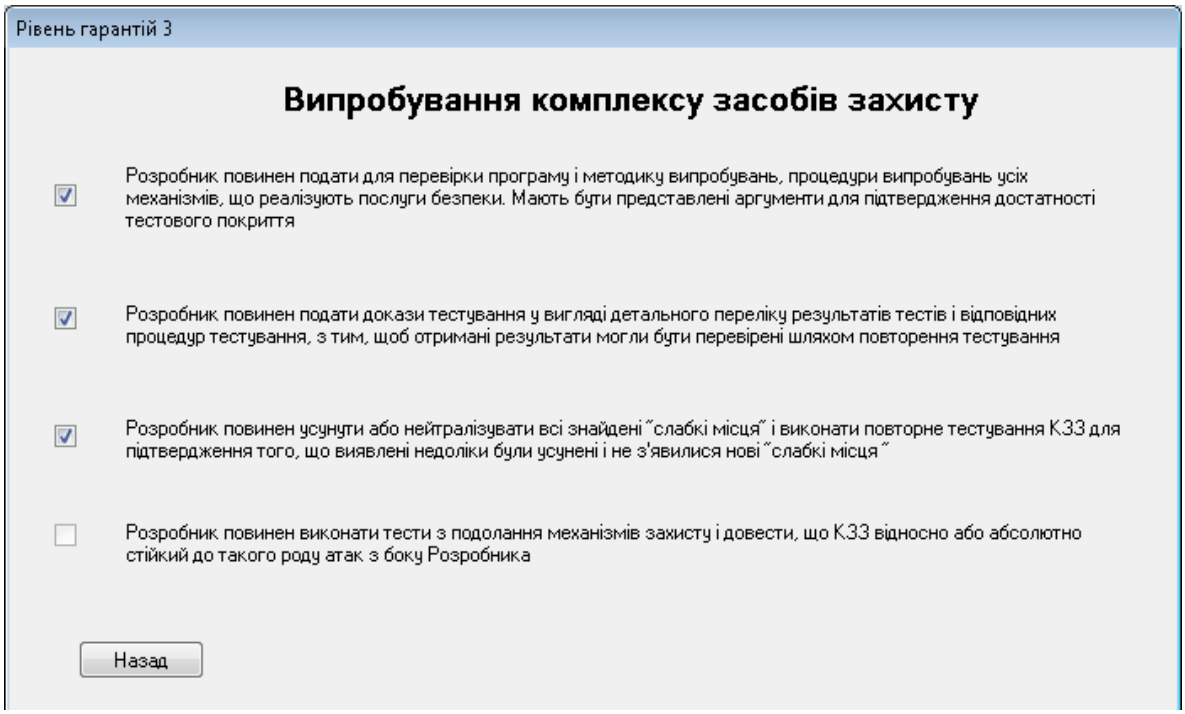

Рис. 4. Приклад оцінки критерію

Після того, як експерт оцінить усі пункти, він повинен підтвердити рівень, натиснувши на кнопку «Оцінити». У підсумку перед ним з'явиться повідомлення про відповідність третьому рівню гарантій (рис. 5).

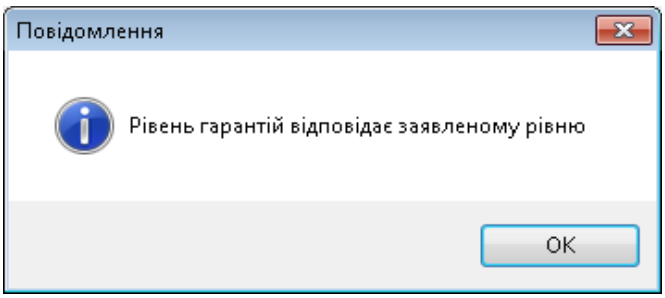

Рис. 5. Приклад оцінки рівня гарантій

Після підтвердження третього рівня у вікні стає доступною функція «Відправити» для передачі отриманого результату на сервер з метою аналізу групового результату роботи десятьох екпертів. Програма на сервері аналізує результати роботи експертів. Приклад аналізу показано на рис. 6.

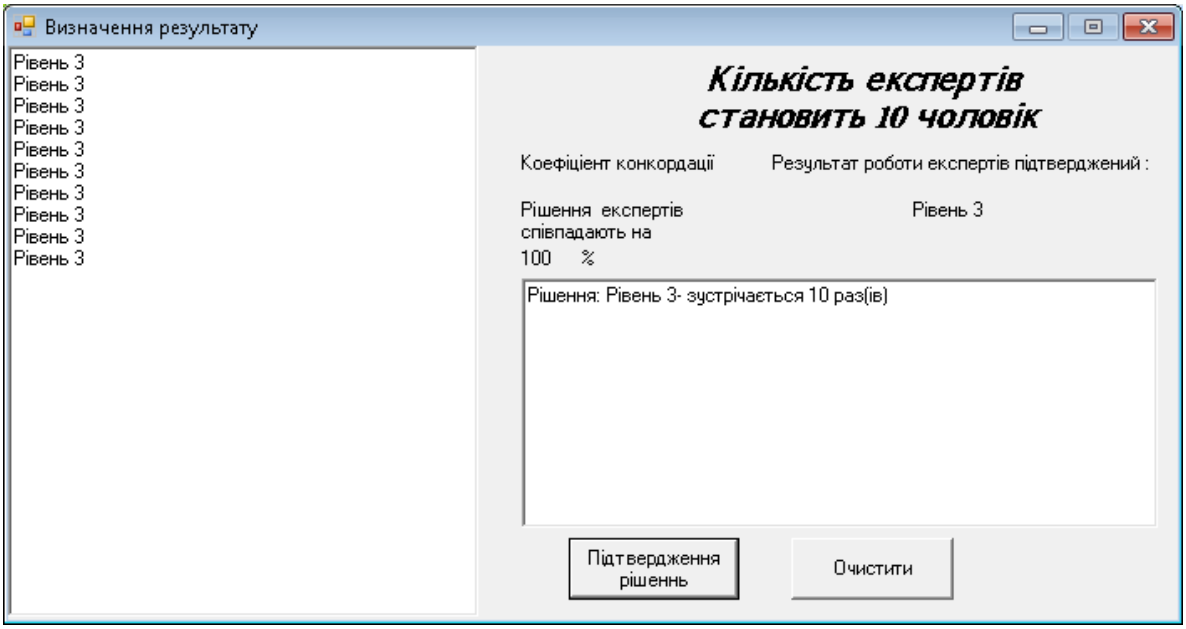

Рис. 6. Визначення групової оцінки

Програмне забезпечення на сервері отримує результати експертів у вигляді підтвердженого або не підтвердженого рівнів гарантій та відповідних набраних балів під час оцінювання системи. Після чого отримані результати обробляються та вираховується коефіцієнт конкордації, він може мати значення від 0 до 1. У разі величини даного коефіцієнта менше 0,3, думки експертів вважаються неузгодженими, за його значень у діапазоні від 0,3 до 0,7, узгодженість вважається середньою. За величини більше 0,7, узгодженість вважається високою. Чим вище даний коефіцієнт, тим краще захищена система від витоку інформації, оскільки вона відповідає заявленому рівню гарантій або ФПЗ. У програмі коефіцієнт переведений у відсотки від 0% до 100%. За результатами роботи експертів щодо оцінювання третього рівня гарантій бачимо коефіцієнт конкордації 1 або 100%, тому робимо висновок, що ВАС відповідає заявленому рівню.

Програмне забезпечення є цілком робочим прототипом для оцінювання цивільних та державних АС і простих ВАС, які описані в нормативно-правових документах

і є перевагою програмного забезпечення, а для застосування до таємних ВАС потрібно доопрацювати критерії їх оцінювання та внести корективи у програмне забезпечення.

Висновки. Програмне забезпечення надається експертам, щоб автоматизовано визначати ФПЗ та рівні гарантій. Після збору усіх результатів їх роботи програмно буде підтверджено ФПЗ або рівень гарантій системи. У разі незбігу результатів у експертів буде сформовано висновок, що система не містить запропонованого ФПЗ або рівня гарантій. І в умовах війни, і в мирний час запропоноване програмне забезпечення дозволить пришвидшити визначення вразливих місць інформаційно-телекомунікаційних систем та оперативно їх усувати. Воно може бути використане для оцінювання більш простих ВАС, а для більш складних та таємних потребує удосконалення, оскільки ці системи мають більш специфічний та засекречений режим роботи. Тому подальші кроки дослідження будуть спрямовані на вивчення документації із забезпечення захисту таємних ВАС та удосконалення програмного продукту.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

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

2. Берестов Д. С., Гульков М. О., Козачок В. А. Побудова парето-оптимальних функціональних профілів захищеності // Збірник наукових праць НУОУ. Київ : ЦВСД НУОУ, 2009. Вип. 1 (39). С. 89–94. URL: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/ Znpcvsd/2009_1/12.pdf (дата звернення: 01.11.2022).

3. Лєншин А. В., Буслов П. В. Метод формування функціональних профілів захищеності від несанкціонованого доступу // Радіоелектронні і комп'ютерні системи : наук.-техніч. журнал. Харків : ХАІ, 2010. Т. 7. С. 77–81. URL: http://nbuv.gov.ua/ UJRN/recs_2010_7_15 (дата звернення: 07.11.2022).

4. Паламарчук Н. А., Хлапонін Ю. І., Овсянніков В. В. Сучасний стан нормативно-правової бази в галузі технічного захисту інформації // Зб. наук. праць ВІТІ НТУУ "КПІ". Київ : ВІТІ НТУУ "КПІ", 2011. № 3. С. 78–82. URL: http://viti.edu.ua/ files/ zbk/ 2011/11_3_2011.pdf (дата звернення: 21.11.2022).

5. Шевченко В. Л., Берестов Д. С. Метод пошуку проєктних альтернатив системи захисту інформації // Сучасний захист інформації. Київ : ДУТ, 2015. № 3. С. 22–27. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/viewFile/386/358 (дата звернення: 01.11.2022).

6. Юдін О. К., Бучик С. С., Фролов О. В. Загальна модель формування системи захисту державних інформаційних ресурсів // Наукоємні технології. 2015. № 4 (28). С. 332–337. doi.org/10.18372/2310-5461.28.9678

7. Юдін О. К., Бучик С. С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія. Київ : НАУ, 2015. 214 с.

8. Потій О. В., Лєншин А. В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу // Прикладная

радиоэлектроника : науч.-технич. журнал. Харків, 2010. Т. 9, № 3. С. 479–488. URL: http://openarchive.nure.ua/handle/document/410 (дата звернення: 01.10.2022).
9. Нетребко Р. В. Аналіз нормативно-правового забезпечення та методів визначення рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2017. Вип. 14. С. 79–85.
10. Бучик С. С., Нетребко Р. В. Реалізація програмного забезпечення визначення функціональних профілів та рівня гарантій автоматизованих систем від несанкціонованого доступу // Наукоємні технології. 2017. № 4 (36). С. 309–315. DOI: 10.18372/2310-5461.36.12228
11. Бучик С. С., Нетребко Р. В. Формалізація методу групового аналізу експертних оцінок при визначенні рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу // Тези доповідей III Міжнар. наук.-практ. конф. «Інформаційна безпека та комп'ютерні технології», (19–20 квітня 2018 р., м. Кропивницький): Кропивницький : ЦНТУ, 2018. С. 40–41.
12. А. с. 74344 Україна. Комп’ютерна програма. Інформаційна система визначення функціонального профілю захищеності та рівня гарантій автоматизованої системи від несанкціонованого доступу (ОФПАС 2.0) / С. С. Бучик, Р. В. Нетребко (Україна). № 74344; заявл. 23.10.2017; опубл. 26.01.2018, Бюл. 47. С. 142–143.

Стаття надійшла до редакції 01.12.2022.

REFERENCES

1. Yudin, O. K., Buchyk, S. S., & Melnyk, S. V. (2016). Teoretychni osnovy vyznachennia standartnykh funktsionalnykh profiliv zakhyshchenosti avtomatyzovanoi systemy vid nesanktsionovanoho dostupu [Theoretical basis of definition of standard functional profiles of security of automated system against unauthorized access]. *Naukoiemni tekhnolohii [Scientific journal "Science-Based Technologies"], 2* (30), 195–205. https://doi.org/10.18372/2310-5461.30.10564 [in Ukrainian].
2. Berestov, D. S., Hulkov, M. O., & Kozachok, V. A. (2009). Pobudova pareto-optymalnykh funktsionalnykh profiliv zakhyshchenosti [Construction of Pareto-optimal functional security profiles]. *Zbirnyk naukovykh prats NUOU [Collection of research papers NUD of Ukraine], 1* (39), 89–94. Retrieved from http://www.nbuv.gov.ua/old_jrn/Soc_Gum/ Znpcvsd/2009_1/12.pdf [in Ukrainian].
3. Lienshyn, A. V., & Buslov, P. V. (2010). Metod formuvannia funktsionalnykh profiliv zakhyshchenosti vid nesanktsionovanoho dostupu [The method of forming functional profiles of protection against unauthorized access]. *Radioelektronni i komp’iuterni systemy : nauk.-tekhnich. zhurnal [Radioelectronic and computer systems: science and technology magazine], 7,* 77–81. Retrieved from http://nbuv.gov.ua/ UJRN/recs_2010_7_15 [in Ukrainian].
4. Palamarchuk, N. A., Khlaponin, Yu. I., & Ovsiannikov, V. V. (2011). Suchasnyi stan normatyvno-pravovoi bazy v haluzi tekhnichnoho zakhystu informatsii [The current state of the regulatory framework in the field of technical information protection]. *Zb. nauk. prats VITI NTUU “KPI” [Collection of Sciences. Proceedings of Military Institute of Telecommunications*

and Information Technologies named after HeroivKrut], 3, 78–82. Retrieved from http://viti.edu.ua/ files/ zbk/ 2011/11_3_2011.pdf [in Ukrainian].

5. Shevchenko, V. L., & Berestov, D. S. (2015). Metod poshuku proiektnykh alternatyv systemy zakhystu informatsii [The method of finding project alternatives of the information protection system]. *Suchasnyi zakhyst informatsii [Modern information protection], 3,* 22–27. Retrieved from http://journals.dut.edu.ua/index.php/dataprotect/article/viewFile/386/358 [in Ukrainian].

6. Yudin, O. K., Buchyk, S. S., & Frolov, O. V. (2015). Zahalna model formuvannia systemy zakhystu derzhavnykh informatsiinykh resursiv [General Model of Forming of System of Defence State Informative Resources]. *Naukoiemni tekhnolohii [Scientific journal "Science-Based Technologies"], 4* (28), 332–337. https://doi.org/10.18372/2310-5461.28.9678 [in Ukrainian].

7. Yudin, O. K., & Buchyk, S. S. (2015). *Derzhavni informatsiini resursy. Metodolohiia pobudovy klasyfikatora zahroz [State information resources. Methodology for building a threat classifier]*. Kyiv [in Ukrainian].

8. Potii, O. V., & Lienshyn, A. V. (2010). Metody pobudovy ta veryfikatsii nesuperechnosti i povnoty funktsionalnykh profiliv zakhyshchenosti vid nesanktsionovanoho dostupu [Methods of construction and verification of consistency and completeness of functional profiles for protection against unauthorized access]. *Prikladnaia radioelektronika : nauch.-tekhnich. zhurnal [Applied radioelectronics: scientific and technical magazine], Vol. 9,* № 3, 479–488. Retrieved from http://openarchive.nure.ua/handle/document/410 [in Ukrainian].

9. Netrebko, R. V. (2017). Analiz normatyvno-pravovoho zabezpechennia ta metodiv vyznachennia rivnia zakhyshchenosti informatsiino-telekomunikatsiinoi systemy vid nesanktsionovanoho dostupu [Analysis of regulatory and legal support and methods of determining the level of security of the information and telecommunications system against unauthorized access]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system : zb. nauk. prats [Problems of construction, testing, application and operation of complex information systems: Scientific journal of Korolov Zhytomyr Military Institute], 14,* 79–85 [in Ukrainian].

10. Buchyk, S. S., & Netrebko, R. V. (2017). Realizatsiia prohramnoho zabezpechennia vyznachennia funktsionalnykh profiliv ta rivnia harantii avtomatyzovanykh system vid nesanktsionovanoho dostupu [Realization Software of Determination of Functional Profiles and Level of Guarantees of Automated Systems from an Unauthorized Access]. *Naukoiemni tekhnolohii [Scientific journal "Science-Based Technologies"], 4* (36), 309–315. https://doi.org/10.18372/2310-5461.36.12228 [in Ukrainian].

11. Buchyk, S. S., & Netrebko, R. V. (2018). Formalizatsiia metodu hrupovoho analizu ekspertnykh otsinok pry vyznachenni rivnia zakhyshchenosti informatsiino-telekomunikatsiinoi systemy vid nesanktsionovanoho dostupu [Formalization of the method of group analysis of expert evaluations when determining the level of protection of the information and telecommunications system against unauthorized access]. In *Tezy dopovidei III Mizhnar. nauk.-prakt. konf. «Informatsiina bezpeka ta kompiuterni tekhnolohii» [Abstracts of reports III International science and practice conf. "Information security and computer technologies"]*. Kropyvnytskyi, April 19–20, 2018. (pp. 40–41). Kropyvnytskyi [in Ukrainian].

12. Buchyk, S. S., & Netrebko, R. V. (2018). Author's certificate 74344 Ukraine. *Komp'iuterna prohrama. Informatsiina systema vyznachennia funktsionalnoho profiliu zakhyshchenosti ta*

rivnia harantii avtomatyzovanoi systemy vid nesanktsionovanoho dostupu (OFPAS 2.0) [Computer program. Information system for determining the functional security profile and the level of guarantees of the automated system against unauthorized access (OFPAS 2.0)], *Bulletin 47,* 142–143 [in Ukrainian].

R. V. Netrebko

TESTING SOFTWARE DETERMINING THE LEVEL OF PROTECTION IN MILITARY AUTOMATED SYSTEMS AGAINST UNAUTHORIZED ACCESS BY THE ENEMY

The article proposes and analyzes the main stages of the application of software for group assessment of the functional profile and determination or agreement of the level of guarantees of the correctness of the implementation of functional security services in the means of information protection of military automated control systems against unauthorized access by the enemy in Ukraine on the basis of previously conducted theoretical studies by the authors and developed software . The latest research and publications of leading scientists in the field of information protection against unauthorized access are analyzed. The main normative documents of technical information protection are presented, which regulate the procedure for evaluating and determining the functional profile and level of guarantees of automated systems against unauthorized access, which are used for civil and state automated systems in Ukraine. The design of the program's functioning was carried out using diagrams and algorithms. The software is tested and work examples are provided. The advantages and disadvantages of the software for the group determination of the functional profile of security and the level of guarantees for the verification of military automated systems are revealed.

The developed software will facilitate the work of experts in determining the security of the system against unauthorized access and will speed up the improvement of the necessary set of protection tools required for reliable protection of confidential information. Further improvement steps for assessing the level of security of military automated systems against unauthorized access by the enemy are outlined.

Keywords: *military automated system; information security; information security policy; rules of access demarcation; unauthorized access; complex of protection means; security profile.*