DOI: https://doi.org/10.17721/ISTS.2019.1.11-18
УДК 004.056.5

РЕАЛІЗАЦІЯ ГРУПОВОГО ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ ТА РІВНЯ ГАРАНТІЙ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Бучик Сергій [1]
orcid.org/0000-0003-0892-3494
Юдін Олександр [2]
orcid.org/0000-0002-6417-0768
Нетребко Руслан [3]
orcid.org/0000-0003-3212-5249

[1] м. Київ, Київський національний університет імені Тараса Шевченко, buchyk@knu.ua
[2] м. Київ, Київський національний університет імені Тараса Шевченко, yak333@ukr.net
[3] м. Житомир, Житомирський військовий інституту імені С.П. Корольова, netr_rv@ukr.net

Історія статті:
Надійшла до редакції 28.06.2019
Прийнято 12.07.2019

Ключові слова:
інформаційно-телекомунікаційна система;
автоматизована система;
інформаційна безпека;
функціональний профіль захищеності;
рівень гарантій;
політика безпеки інформації;
правила розмежування доступу;
несанкціонований доступ;
комплекс засобів захисту;
експертна інформація.

Анотація: У статті запропоновано, показано та проаналізовано основні етапи реалізації програмного забезпечення по груповій оцінці функціонального профілю та визначення або узгодження рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації інформаційно-телекомунікаційних систем від несанкціонованого доступу в Україні на основі раніше проведених авторами теоретичних досліджень. Висвітлено необхідні нормативні документи технічного захисту інформації, які регламентують порядок оцінки та визначення рівня гарантій автоматизованих систем від несанкціонованого доступу в Україні. Здійснено проектування роботи програми за допомогою діаграм Data Flow Diagram, а саме: розроблені контекстна діаграма процесу групового визначення та декомпозована діаграма процесу групового визначення функціональних профілів захищеності та рівня гарантій. Побудовані більш детальні блок-схеми роботи програмного забезпечення та алгоритмів, які реалізовані в прототипі програмного забезпечення. Приведено приклади роботи по кожному з основних блоків роботи, які були попередньо спроектовані в діаграмах та блок-схемах алгоритмів. Визначені переваги та недоліки розробленого програмного забезпечення групового визначення функціонального профілю захищеності та рівня гарантій. Розроблена програма дозволяє провести групову оцінку та порівняти результати відправлені на сервер. Даний підхід дозволяє зменшити час, який витрачає адміністратор безпеки для визначення функціональних профілів захищеності та рівнів гарантій оброблюваної 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. За рахунок проведення групової експертизи підвищується достовірність отриманих результатів.

Abstract: The article proposes, shows and analyzes the main stages of implementing software for group assessment of a functional profile and determining or agreeing the level of guarantees for the correct implementation of functional security services in information security tools of information of telecommunication systems from unauthorized access in Ukraine based on theoretical studies previously conducted. The necessary regulatory documents on technical protection of information governing the procedure of evaluating and determining the level of guarantees of automated systems against unauthorized access in Ukraine are covered. The program was designed using the Data Flow Diagram, namely, a contextual diagram of the group definition process and a decomposed diagram of the process of group determination of the functional security profiles and the level of guarantees. More detailed flowcharts of software and algorithms are constructed. A prototype of the software is implemented;

examples of work on each of the main blocks of work that were previously designed in the diagrams and flowcharts of the algorithms are given.
Certain advantages and disadvantages of the developed software for group determination of the functional security profile and the level of guarantees are defined. The developed program allows to carry out group estimation and to compare the results sent to the server. This approach reduces the time spent by the security administrator to determine the security profiles and security levels of the information being processed against unauthorized access and to detect whether a specified functional profile coincides with a standard one (provided this match the user is provided with information about that standard functional profile) or determine another level of warranty. By conducting a group examination, the reliability of the obtained results increases.

1. 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 усе ширше застосування в таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинута 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].

Досліджуючи нормативно-правову базу (НПБ) України в галузі захисту інформаційно-телекомунікаційних систем (ІТС) 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» затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 [2];
- НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24 липня 2009 року № 172 [3].

Саме дані документи стали основою для проведення аналізу та подальшого дослідження.

В розрізі продовження дослідження є актуальним здійснити формалізацію теоретичних основ групового визначення функціонального профілю захищеності та рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу та реалізувати програмно, що дозволить автоматизувати процес визначення та зменшить витрати часу та матеріальних (людських) ресурсів, які витрачаються на такий процес. Також, за рахунок проведення групової експертизи, підвищиться достовірність отриманих даних.

2. 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 багатоьох вітчизняних і закордонних вчених. Так багато праць Баранніка В.В. присвячені захисту відеоінформаційних ресурсів [4,5], Юдіна О.К. та Конаховича Г.Ф. захисту інформації в мережах передачи даних, комп'ютерній стеганографії [6,7], Новікова О.М. безпеці інформаційно-телекомунікаційних систем [8] і т.ін. 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. Також в окремих працях проаналізовано використання методів перевірки несуперечності та повноти профілю захищеності від НСД, побудови таксономії функціональних послуг безпеки від НСД, парето-оптимальних ФПЗ [9,10,11,12]. В роботі [13] проведено системний аналіз профілю захищеності відкритих інформаційних систем, розкрита відома структура критеріїв. Тематиці визначення групової оцінки функціонального профілю та рівня гарантій ІТС від НСД присвячено небагато робіт, що на думку авторів

пов'язано з тим, що процес визначення здійснюється експертною комісією та фактично єдиними документами, які визначають підходи до визначення ФПЗ та гарантій. Дана робота є продовженням роботи реалізація програмного продукту визначення функціональних профілів та рівня гарантій автоматизованих систем від несанкціонованого доступу на основі НПБ [14] та тематики робіт над якими працює група науковців. Тому наразі стоїть питання можливості групової оцінки ФПЗ та запропонованого рівня гарантій автоматизовано на основі НПБ. Раніше авторами було розроблено програмне забезпечення визначення функціональних профілів та рівня гарантій ІТС від несанкціонованого доступу (А.с. 74344 Україна. Комп'ютерна програма. Інформаційна система визначення функціонального профілю захищеності та рівня гарантій автоматизованої системи від несанкціонованого доступу (ОФПАС 2.0)), але дане програмне забезпечення було розраховане на одного експерта. Тому актуальним стоїть питання впровадження групової оцінки.

3. МЕТА СТАТТІ

Здійснити реалізацію теоретичних основ групової оцінки визначення ФПЗ та рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованої системи від несанкціонованого доступу та розробити прототип програмного забезпечення.

4. 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 ІТС.

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, НД ТЗІ 2.5-005-99, НД ТЗІ 2.7-010-09. 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 ІТС, але єдиної методології, яка б поєднувала дані документи та надавала зрозумілу та просту інтерпретацію процесу обирання ФПЗ та рівнів гарантій немає, тому було реалізоване програмне забезпечення для роботи одного експерта. В зв'язку з чим, актуальним є створення системи для визначення групової оцінки, тобто мережевої версії.

У ході дослідження методу авторами було проведено моделювання процесів групового визначення. На рис. 1 наведено головну контекстну діаграму процесу групового визначення ФПЗ та рівня гарантій, на рис. 2 – результат моделювання підпроцесів групового визначення ФПЗ та рівня гарантій проміжного рівня деталізації.

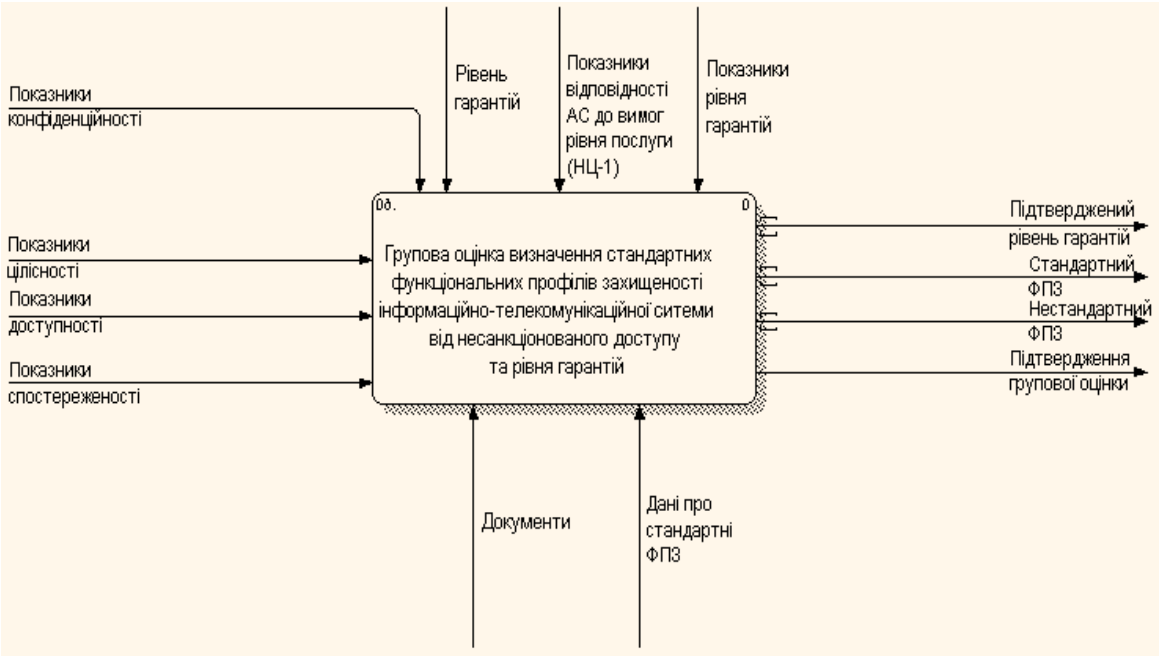

Рис. 1 - Контекстна діаграма процесу групового визначення ФПЗ та рівня гарантій

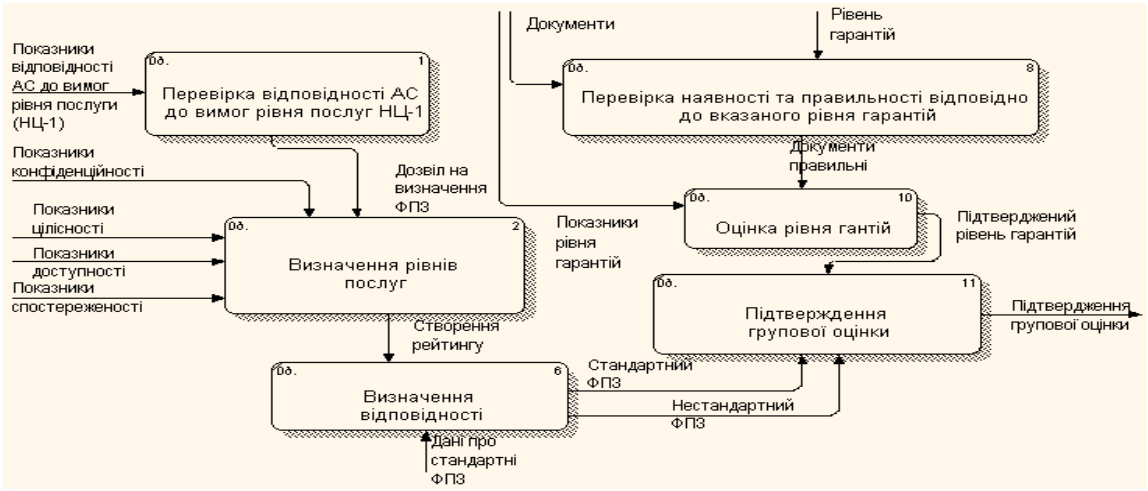

Рис. 2 - Декомпозована діаграма процесу групового визначення ФПЗ та рівня гарантій

Data Flow Diagram (DFD) – стандарт для створення моделі потоків інформації, що циркулює в ІТС. Модель системи визначається, як ієрархія 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 автоматизованої системи до вимог рівня послуги комплексу засобів захисту НЦ-1, блок отримання ФПЗ захищеності ІТС від несанкціонованого доступу, блок перевірки відповідності визначеного профілю захищеності до стандартного ФПЗ, блок визначення відповідності документів та блок оцінки рівня гарантій, блок визначення групової оцінки.

На основі нормативно-правової бази та розроблених діаграм, алгоритмів функціонування [14] було розроблено програмне забезпечення ОФПАС 2.0. Визначення функціонального профілю рис. 3 та вибір рівня гарантій рис. 4. в частині програми критерії гарантій показано на рисунках відповідно та було удосконалено даний програмний продукт визначенням групової оцінки.

Формалізація методу групового аналізу експертних оцінок при визначені рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу показано в тезах доповідей [15].

Приклад групової оцінки приведено на основі оцінки другого рівня гарантій десятьма експертами, тому наступним кроком після вибору потрібного рівня гарантій є оцінка критеріїв рис. 5 та вимог документів рис. 6 обраного рівня гарантій.

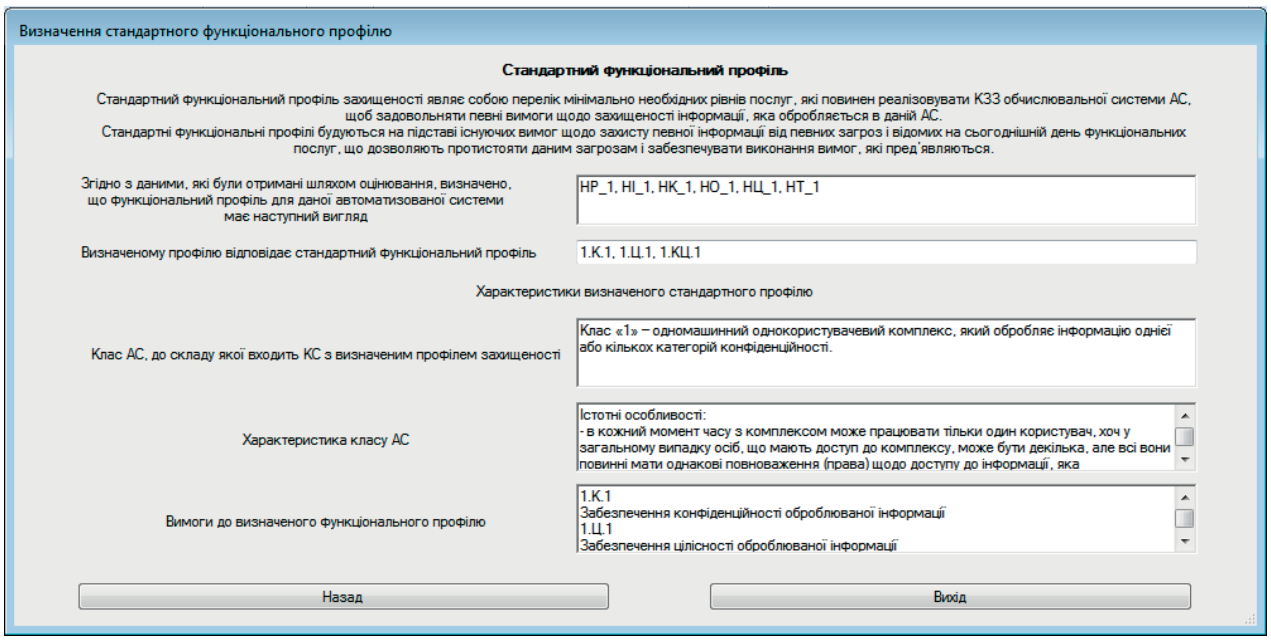

Рис. 3 - Визначення ФПЗ

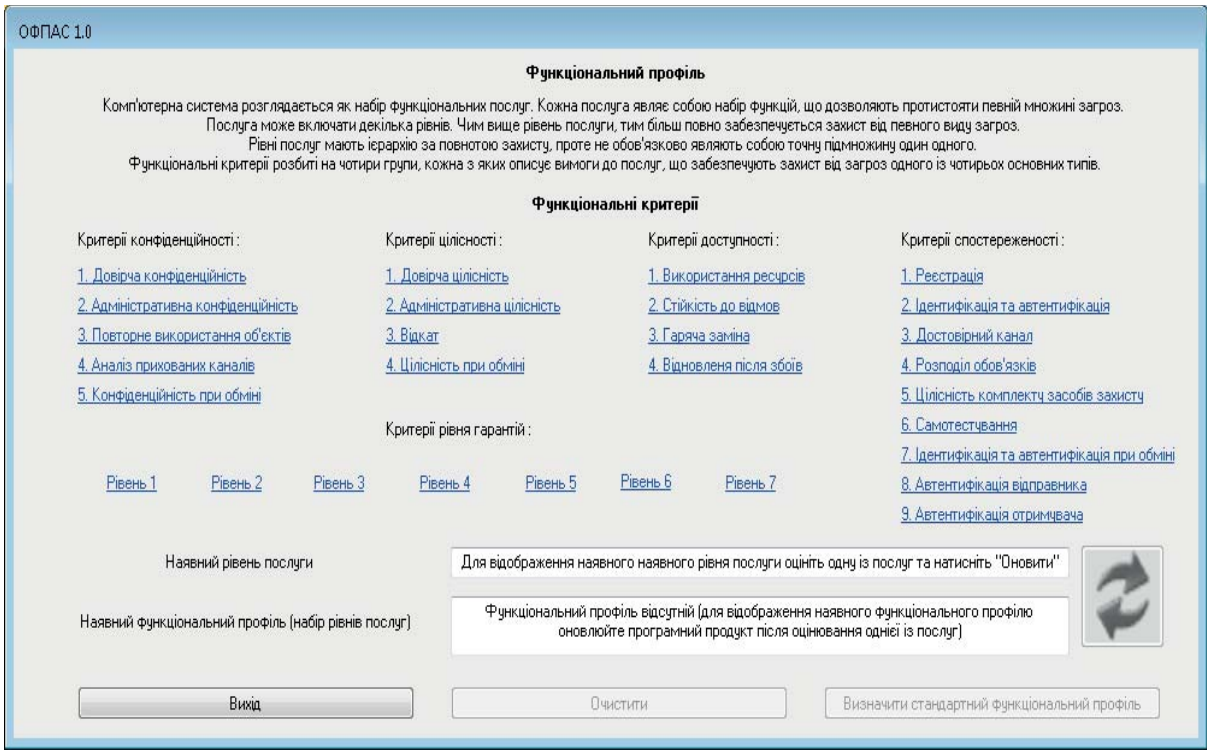

Рис. 4 - Вибір рівня гарантій

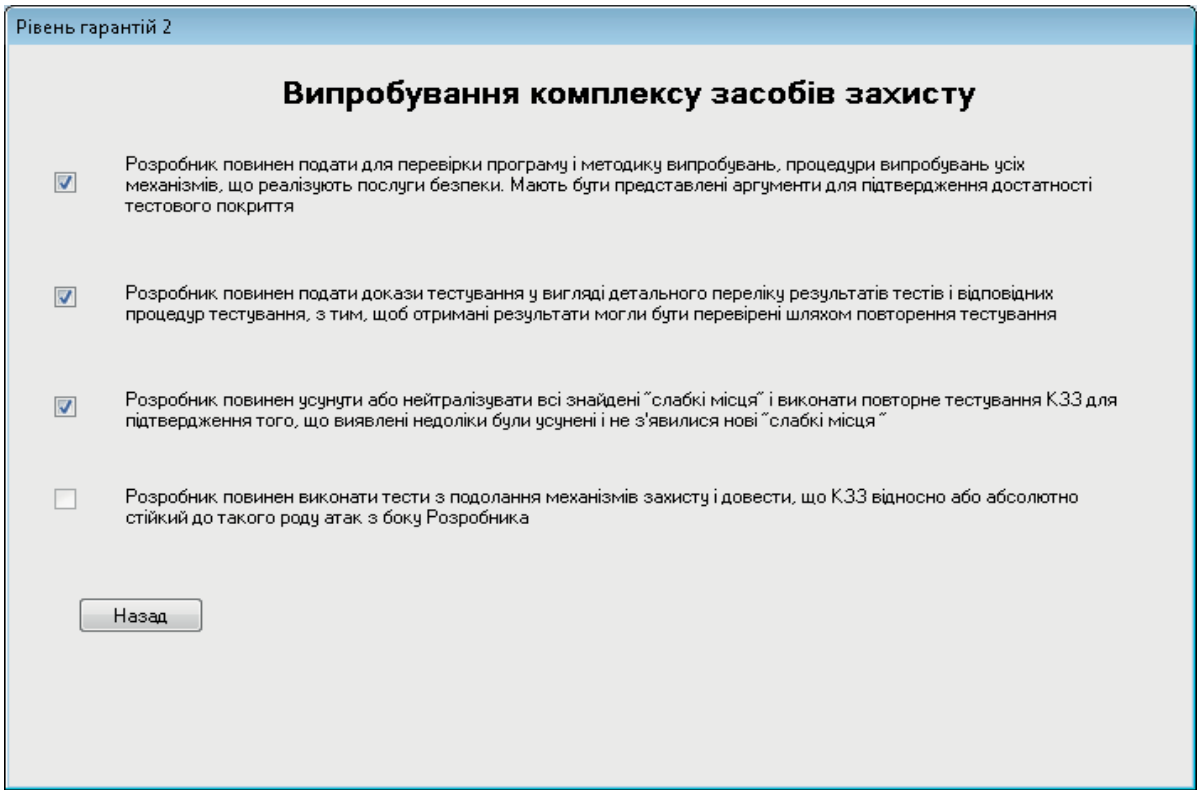

Рис. 5 - Приклад оцінки критерію

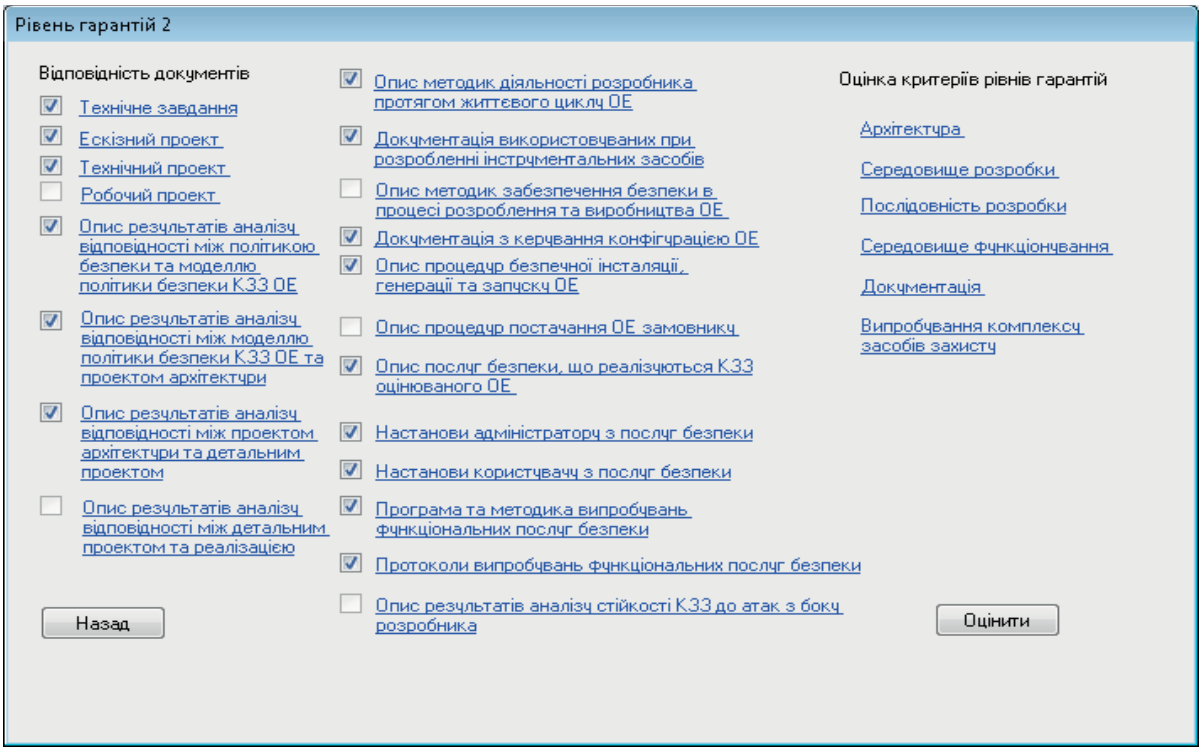

Рис. 6 - Приклад оцінки відповідності документів

Опрацювавши всі пункти експерт оцінює рівень натиснувши на кнопку «Оцінити» і перед експертом з'являється повідомлення про відповідність або не відповідність рівню гарантій. Після чого у вікні стає доступною клавіша «Відправити» для передачі отриманого результату на сервер для визначення загального результату роботи десятьох експертів рис. 7.

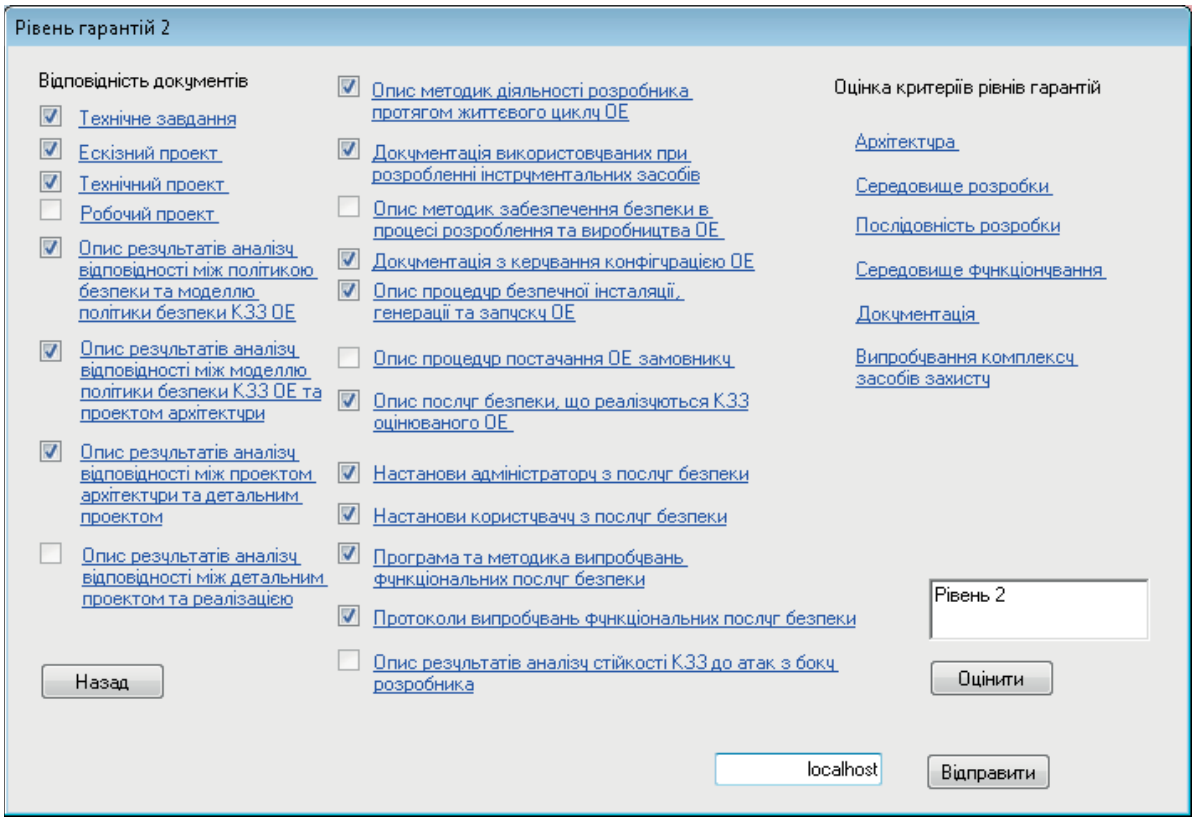

Рис. 7 - Приклад передачі результатів на сервер

Також було проаналізовано суть групової експертизи, визначено за допомогою яких методів проводиться експертиза, кількість експертів, обрано метод обробки експертної інформації [15]. Реалізацію даного методу показано на рис. 8.

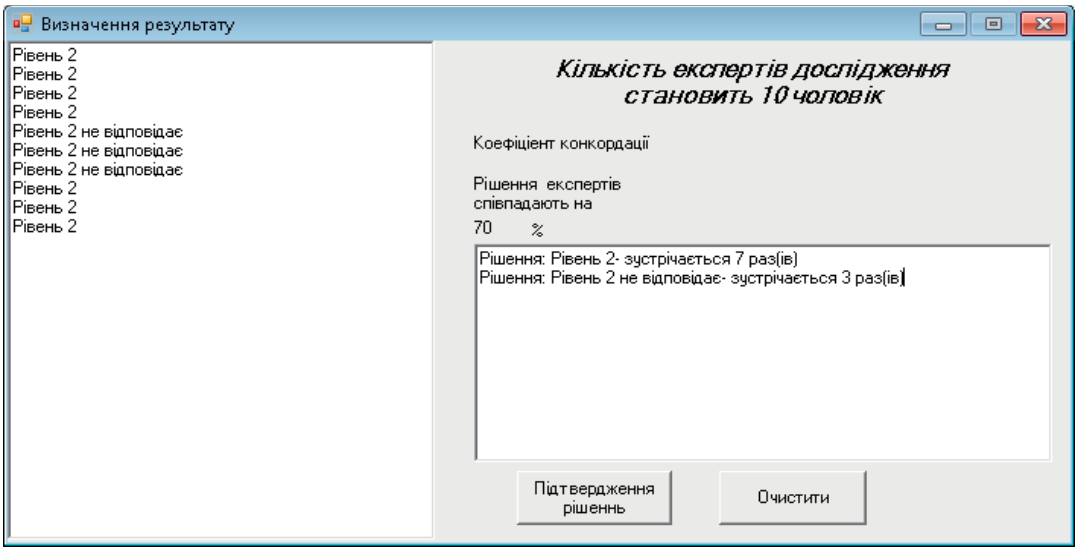

Рис. 8 - Визначення групової оцінки

5. ВИСНОВКИ

Розроблена програма дозволяє провести групову оцінку та порівняти результати відправлені на сервер. Даний підхід дозволяє зменшити час, який витрачає адміністратор безпеки для визначення функціональних профілів захищеності та рівнів гарантій оброблюваної 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. За рахунок проведення групової експертизи підвищується достовірність отриманих результатів.

6. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Основними результатами автори вважають здійснення реалізації групового визначення ФПЗ та рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації автоматизованих систем від несанкціонованого доступу, яка допоможе експертній комісії швидше оцінити систему. Реалізований прототип програми дає можливість в подальшому удосконалити клієнт-серверний зв'язок програми.

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Юдін О. К. Державні інформаційні ресурси. Методологія побудови та захисту українського сегмента дерева ідентифікаторів / О. К. Юдін, С. С. Бучик. – К.: НАУ, 2018. – 319 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] Alimpiev, A.N., Barannik, V.V., and Sidchenko, S.A. (2017), The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. Telecommunications and Radio Engineering. 2017. Vol. 76. No 6. pp. 521-534. DOI: 10.1615/TelecomRadEng.v76.i6.60.

[5] Barannik, V. and Shulgin, S., (2016), The method of increasing accessibility of the dynamic video information resource. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET): 13th Intern. conf., (Lviv-Slavske, Ukraine, febr. 23–26, 2016). Lviv-Slavske: 2016. pp. 621-623. DOI: 10.1109/TCSET.2016.7452133.

[6] Юдін О.К. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О.К. Юдін, Р.В. Зюбіна, О.В. Фролов // Радиоэлектроника и информатика. – 2015.– № 3. – С. 13 - 21.

[7] Юдін О. К. Захист інформації в мережах передачі даних: підручник / О. К. Юдін, О.

Г. Корченко, Г. Ф. Конахович. – К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 716 с.

[8] Грайворонський М. В. Безпека інформаційно-телекомунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

[9] Потій О. В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу /О. В. Потій, А. В. Лєншин //Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2010. – Том 9. – №3. – С.479 – 488. – Режим доступу: http://openarchive.nure.ua/handle/document/410.

[10] 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://nbuv.gov.ua/UJRN/recs_2010_7_15.

[11] Берестов Д. С. Побудова парето-оптимальних функціональних профілів захищеності / Д. С. Берестов, М. О. Гульков, В. А. Козачок // Збірник наукових праць. Вип. 1(39) / Редкол. Шевченко В. Л. (голова) та ін. – К.: ЦВСД НУОУ, 2009. – С. 89 – 94. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Znpcvsd/2009_1/12.pdf.

[12] Лєншин А. В. Морфологічний метод побудови таксономії функціональних послуг захисту від несанкціонованого доступу / А. В. Лєншин // Матеріали другої міжнар. наук.-пр. конф. молодих вчених – Ч.2. – Одеса, ОНАЗ, 2012. – 133–136 с. – Режим доступу: https://onat.edu.ua/dif_files/sborniki/Zbirnyk2012_2.doc.

[13] Проценко А. А. Системный анализ профиля защищённости открытых информационных систем // А.А. Проценко, А.В. Блюма, А.Д. Кожуховский // Системи обробки інформації". – Х., 2015, 7(132) – С.128 – 131. – Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/12373/soi_2015_7_29.pdf.

[14] Бучик С.С. Формалізація методу групового аналізу експертних оцінок при визначені рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу / Бучик С.С., етребко Р.В. // Інформаційна безпека та комп'ютерні технології (INFOSEC & COMPTECH) : III міжнародна науково-практична конференція, 19 – 20 квітня 2018 року : тези доп. – Кропивницький: ЦНТУ, 2018. – С. 40-41.

[15] Бучик С.С. Реалізація програмного забезпечення визначення функціональних профілів та рівня гарантій автоматизованих систем від несанкціонованого доступу / С.С. Бучик, Р.В. Нетребко // Наукоємні технології. – 2017.– № 4 (36). – С. 309 - 315, DOI: 10.18372/2310-5461.36.12228.

Бучик Сергій Степанович, доктор технічних наук, доцент, *Зараз працює професором кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології, теорія прийняття рішень.*

Юдін Олександр Костянтинович, доктор технічних наук, професор, *Зараз працює професором кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології, теорія кодування.*

Нетребко Руслан Васильович*, закінчив Житомирський військовий інститут ім. С. П. Корольова Національного авіаційного університету, отримав освіту за спеціальністю «Системи управління та автоматики», здобув кваліфікацію інженера з керування та обслуговування систем. Наукові інтереси інформаційні технології, інформаційна безпека, кібербезпека.*