НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

ПОТЕНКО Олександр Сергійович

УДК 004.056.5

МЕТОДИ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИСТУ АВТОМАТИЗОВАНОЇ СИСТЕМИ З УРАХУВАННЯМ ПОТОЧНОГО РІВНЯ ЗАГРОЗ

05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2024

Дисертацією є рукопис.

Робота виконана в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Науковий керівник: доктор технічних наук, старший науковий співробітник
Давиденко Анатолій Миколайович,
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України,
провідний науковий співробітник.

Офіційні опоненти: доктор технічних наук, професор
ФАУРЕ Еміль Віталійович,
Черкаський державний технологічний університет,
проректор з науково-дослідної роботи та міжнародних зв'язків;

кандидат технічних наук, професор
ХОХЛАЧОВА Юлія Євгеніївна,
Національний авіаційний університет,
професор кафедри безпеки інформаційних технологій.

Захист відбудеться «28» серпня 2024 року о 13 годині на засіданні спеціалізованої вченої ради Д 26.185.01 в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: вул. Генерала Наумова, 15, м. Київ, 03164.

З дисертацією можна ознайомитися в бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

Автореферат розіслано « __ » липня 2024 року.

Вчений секретар спеціалізованої
вченої ради Д 26.185.01 В.В. Душеба

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В Україні велика увага приділяється захисту інформації, метою якого є створення повного життєвого циклу (проектування, виробництво, експлуатація) захищених автоматизованих систем (АС), призначених для накопичення, обробки, зберігання та передачі інформації з обмеженим доступом.

На рубежі цього сторіччя була створена нормативна база в вигляді низки нормативних документів технічного захисту інформації (НД ТЗІ) НД ТЗІ, загальною ідеєю яких є визначення функціонального профілю захисту(ФПЗ) шляхом стандартизації послуг безпеки з подальшою оцінкою цього профілю та визначення відповідності наданих послуг в існуючій ситуації. В даний час йде як розвиток правової бази, так і наукове забезпечення цього процесу, прикладом є НДР «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014р.- 2018р.). Дана робота направлена на вирішення актуальної задачі пов’язаної з визначенням численного значення імовірності успішної протидії вибраного профілю поточним загрозам.

Значний внесок у розвиток методів побудови комплексних систем захисту інформації (КСЗІ) внесли такі вчені як: М.В. Трутнев, В.А. Кондратюк, Ю.В. Парамонов, А.А. Баранов, А.М. Фаль, В.І. Скуріхін, В.К Задирака, В.О. Хорошко, М.Є. Шелест, О.Г. Корченко, В.В. Мохор, Kris Kaspersky, І.Д. Горбенко, О.С. Зубрицький, Л.А. Завадська, В.М. Чупрін та ін.

При проведенні експертиз КСЗІ, задачею експерта є аналіз механізмів захисту, реалізованих в системі захисту. Експерт зобов'язаний виявити наявність механізмів захисту, упевнитися в їх працездатності, коректності реалізованого механізму захисту та його достатності для протидії існуючим загрозам. На етапі розробки технічного завдання визначається функціональний профіль захисту на основі розроблених політик безпеки, моделі порушника і моделі загроз. Експерт опиняється в ситуації багатозначності відповідей на поставлене їм питання. З однієї сторони виникає бажання створити максимально можливий профіль захисту, а з іншої сторони максимальний профіль потребує максимальних затрат з фінансів та часу, що може привести до зниження ефективності та прибутковості основної розв'язуваної задачі. В результаті виникає оптимізаційна задача визначення мінімально необхідного профілю захисту. За типових умов кількість можливих варіантів профілів може сягати 15 міліардів, повний перебір яких є дуже витратним і неефективним. Таким чином, розробка методу визначення функціонального профілю захисту є актуальною науковою задачею.

Зв’язок роботи з науковими програмами, планами, темами. Результати дисертаційної роботи відображені у звітах НДР «Дослідження і розробка методів розпізнавання, які базуються на використанні спектральних перетворень, для інформаційного забезпечення безпеки енергетичних об’єктів» № 0105U001296 (2005р. - 2008р.). НДР «Дослідження та розробка методів

підвищення безпеки та ефективності розподілених високопродуктивних інформаційних технологій при забезпеченні завдань забезпечення безпеки » №0108U010588 (2009р. - 2013р.). НДР «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014р. - 2018р.). НДР «Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними» № 0118U002371 (2019р.- теперішній час).

Мета і завдання дослідження. Метою роботи є підвищення рівня ефективності процесу побудови комплексної системи захисту інформації під час проведення експертизи технічного захисту інформації шляхом адаптації функціонального профілю захисту автоматизованих систем до поточного рівня загроз.

Для досягнення вказаної мети були поставлені та вирішені наступні основні наукові **завдання**:

1. Провести аналіз та систематизацію методів за засобів визначення функціонального профілю захисту відповідно до існуючих критеріїв оцінки захисту автоматизованих систем.
2. Сформувати критерії визначення функціонального профілю захисту для різних класів АС (ФПЗ).
3. Розробити комплексний метод визначення функціонального профілю захисту для різних класів АС.
4. Розробити спосіб автоматизованої перевірки збіжності методу визначення функціонального профілю захисту для різних класів АС.
5. Розробити метод визначення функціонального профілю захисту для протидії загрозам.

Об'єкт дослідження – процес визначення функціонального профілю захисту автоматизованих систем відповідно до поточного рівня загроз при проведенні експертизи КСЗІ.

Предмет дослідження – методи та засоби визначення функціонального профілю захисту автоматизованих систем відповідно до поточного рівня загроз при проведенні експертизи КСЗІ.

Методи дослідження. У дисертаційній роботі при розв'язанні поставлених наукових задач комплексно використовувалися методи системного і функціонального аналізу, математичного моделювання, теорії ймовірностей та математичної статистики, теорії ризиків, теорії алгоритмів, теорії баз даних, об'єктно-орієнтованого програмування, методи оптимізації, планування наукового експерименту та обробки його результатів тощо.

Наукова новизна отриманих результатів. Основні наукові результати полягають у наступному:

1. *Вперше* запропоновано критерії визначення функціонального профілю захисту, які за рахунок аналізу цільової функції по Белману та визначення математичного сподівання успішної протидії окремої функціональної послуги безпеки, дозволяють у формальному вигляді

сформувати необхідний набір послуг безпеки для реалізації процесу вибору рівня захисту.

2. *Вдосконалено* метод визначення функціонального профілю захисту для різних класів автоматизованих систем (АС), який за рахунок використання розподілу однорідних ресурсів дозволяє автоматизувати процес генерування функціонального профілю захисту та порівняння його з відповідним рівнем захисту.
3. *Вперше* запропоновано спосіб перевірки збіжності методу визначення функціонального профілю захисту для різних класів АС, який, за рахунок автоматизації процесу адаптації загрозам за підкласами автоматизованих систем, дозволяє зменшити кількість помилок при складанні функціональних профілів захисту.
4. *Вперше* запропоновано метод визначення функціонального профілю захисту для різних класів АС, який, за рахунок окремої оцінки умовного рейтингу та коефіцієнту вагомості, дозволяє зменшити час при складанні функціональних послуг захищеності для різних класів АС.

Практичне значення отриманих результатів.

Найбільша практична цінність дисертаційній роботи полягає в тому, що отримані в ній результати можуть бути використані для визначення функціонального профілю захисту для різних класів АС при побудові комплексної системи захисту інформації(КСЗІ) та при проведенні експертиз систем технічного захисту інформації КСЗІ.

Практична цінність роботи полягає в наступному:

- на основі запропонованого методу визначення функціонального профілю захисту для різних класів АС за обраним мультикритерієм при проведенні державних експертиз КСЗІ розроблено алгоритмічне забезпечення, що дозволяє створити на його основі відповідний програмний засіб;
- на основі запропонованого алгоритму реалізовано програмний модуль, якій виконує перевірку функціонального профілю захисту для різних класів АС за мультикритерієм «ризик безпеки – гарантія безпеки – вид вид інформаційної діяльності (ІД) - вартість»;
- Результати дисертаційного дослідження впроваджено у діяльність ТОВ “ІНФОРМАЦІЙНА БЕЗПЕКА” та ДП Державний науково-технічний центр з ядерної та радіаційної безпеки (ДНТЦ ЯРБ).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У працях, опублікованих у співавторстві, автору належать наступне: [1] – програмна реалізація системи доступу на основі біометрії з використанням штучного інтелекту; [2] – проведено аналіз використання COM-технологій для візуалізації згенерованих ФПЗ; [4] – проведено аналіз методів обробки та захисту інформації в грід-середовищі; [5] – розробка програмного модуля, якій

виконує перевірку функціонального профілю захисту для різних класів АС; [7] – порівняльний аналіз методів паралельного програмування; [8] – аналіз методів шифрування каналів зв'язку безпілотних літальних апаратів; [9] – аналіз систем підтримки прийняття рішень орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки; [10] – розгляд систем підтримки прийняття рішень орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки; [12] – розробка програмного забезпечення для реалізації методології оцінки суми ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури; [13] – проведено аналіз використання CASE-технології для моделювання ФПЗ; [14] – аналіз методів обробки критичної інформації у високопродуктивних середовищах; [16] – програмна реалізація системи протидії загрозам на основі динамічного програмування «Профіль-1» та проведення обчислювальних експериментів; [19] – огляд засобів захисту веб-ресурсів від зовнішніх атак; [21] – аналіз моделей безпеки в інформаційних системах; [22] – аналіз існуючих механізмів безпеки кіберфізичних систем; [23] – розгляд практичних аспектів роботи CSIRT; [24] – програмна реалізація застосунку вибору складу профілю протидії загрозам на основі аналізу вірогідності їх реалізації; [27] – аналіз способів кодування інформації в кіберфізичних системах; [28] – аналіз сучасних бібліотек розпізнавання образів в сучасних системах захисту інформації; [29] – тестування програмного забезпечення розпізнавання образів в сучасних системах захисту інформації; [32] – розробка та тестування застосунка для вибору складу профілю протидії загрозам в інформаційно-телекомунікаційних системах, проведення обчислювальних експериментів; [33] – програмна реалізація модулю розрахунку агрегованого ризику у разі множини сумісних випадкових подій.

Апробація результатів дисертації. Основні положення і результати дисертаційного дослідження доповідалися та обговорювалися на: XXVII-XXX, XXXVIII, XLI щорічних науково-технічних конференціях молодих учених і спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України (м. Київ, 2008-2011, 2020, 2023 рр.); Науково-практичних конференціях ІПМЕ ім. Г.Є. Пухова НАН України "Кібербезпека енергетики" (м. Київ, 2021, 2023); IX Міжнародній науково-практичній конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Європейський університет, м. Київ, 2023р); Всеукраїнській науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (Національна академія СБУ, м. Київ, 2023р); Науково-практичній конференції ІПМЕ ім. Г.Є. Пухова НАН України «Резильєнтність критичної інфраструктури – 2023» (м.Київ, 2023); XIV Міжнародній науково-практичній конференції «Комп'ютерні системи та мережні технології, CSNT-2023) (Національний авіаційний університет, м. Київ, 2023); IX Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем» (м. Львів, 2023); Міжнародній науково-практичній конференції ІПМЕ ім. Г.Є. Пухова НАН України «Живучість та резильєнтність – 2023» (м. Київ, 2023); V науково-практичній конференції ІПМЕ ім. Г.Є. Пухова НАН України «Безпека енергетики в епоху цифрової трансформації» (м. Київ, 2023).

Публікації. Результати дослідження опубліковано у 33 наукових працях, серед яких: 1 стаття у закордонному науковому періодичному виданні, що індексується наукометричною базою даних Scopus; 11 статей у наукових фахових виданнях України; 20 тез та матеріалів конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, вступу, чотирьох розділів, висновків, 2 додатків, списку використаних джерел, та містить 138 сторінок основного тексту, 35 рисунків, 21 таблицю. Список використаних джерел налічує 101 найменування на 11 сторінках. Загальний обсяг дисертаційної роботи складає 172 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** роботи обґрунтована актуальність обраного напрямку досліджень, вказаний його зв'язок з науковими програмами, планами та темами, сформульовані мета і задачі наукового дослідження, визначено наукову новизну отриманих результатів та їх практичне значення, наведено дані про особистий внесок здобувача та апробацію результатів дисертації.

У **першому розділі** проаналізовано загальновідомі стандарти щодо оцінки захисту АС, такі як Критерії безпеки комп'ютерних систем (Trusted Computer System Evaluation Criteria, DoD 5200.28-STD), Критерії безпеки інформаційних технологій (Information Technology Security Evaluation Criteria), Федеральні критерії безпеки інформаційних технологій (Federal Criteria for Information Technology Security)" "Американського федерального стандарту з обробки інформації (Federal Information Processing Standard), Канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria), Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Проведено порівняння їх структури, та області застосування. Систематизовано існуючі міжнародні критерії оцінки захисту автоматизованих систем та визначити специфіку оцінки захищеності АС кожного з них.

Визначено специфіку кожного стандарту.

Встановлено, що різні критерії мають унікальні сфери застосування, але всі вони тісно пов'язані з кібербезпекою. Схожість предметної сфері визначає подібність їх архітектури. Зазвичай це множина критеріїв (1)

$$МКБ = \{M_{КБ1}, M_{КБ2}, ..., M_{КБN}\}, \quad (1)$$

яка включає кортежи (2)

$$M_{КБi} = \{ФПБ_1, ФПБ_2, ..., ФПБ_{Ki}\}. \quad (2)$$

Кількість N та розмірність K_i відрізняється в різних групах критеріїв.

Проведено порівняльний аналіз методів побудови функціональних профілів захисту (ФПЗ), які представлені в табл. 1.

Таблиця 1 – Порівняльна таблиця методів побудови ФПЗ

Метод побудови ФПЗ	Витрати (рівень)	Використання стандартних ФПЗ	Використання нестандартних ФПЗ	Часові витрати	Кваліфікація експерта	Чисельне вираження ФПБ
Стандартний метод	високий	+	+	високі	середня	-
Метод перевірки несуперечності та повноти	високий	-	+	високі	висока	-
Метод побудови таксономії	високий	-	+	високі	висока	-
Метод парето-оптимальних ФПЗ	високий	-	+	високі	висока	-
Удосконалений метод визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР	невисокі	+	+	середні	середня	-

Отже, у першому розділі на підставі проведеного аналізу обґрунтовані ключові завдання дослідження, вирішення яких є необхідним для досягнення поставленої мети у дисертаційній роботі.

У **другому розділі** було розглянуто задачі оптимізації по Белману, а саме використання детермінованих методів розв'язання для розподілу однорідних ресурсів. Точна математична постановка цих задач необхідна для розуміння пропонованої нами інтерпретації. Особливу увагу було приділено другій зворотній задачі для визначення профілів захисту.

Розроблено метод оцінки та оптимізації інформаційної безпеки АС за мультикритерієм «ризик безпеки – гарантія безпеки – вид ІД - вартість» (рис. 1).

В даному методі для оцінки видів інформації діяльності необхідно оцінювати суперпозицію вектору інформаційної діяльності і технологічної направленості АС. Рівень витрат на безпеку інформації може бути оцінений в загальному вигляді як семантичний вектор, формула якого наведена далі (3):

$$PB = \begin{Bmatrix} MPB \\ ДРВ \\ НРВ \end{Bmatrix} \quad (3)$$

Де *MPB* – мінімальний рівень витрат, *ДРВ* – достатній рівень витрат, *НРВ* – необхідний рівень витрат.

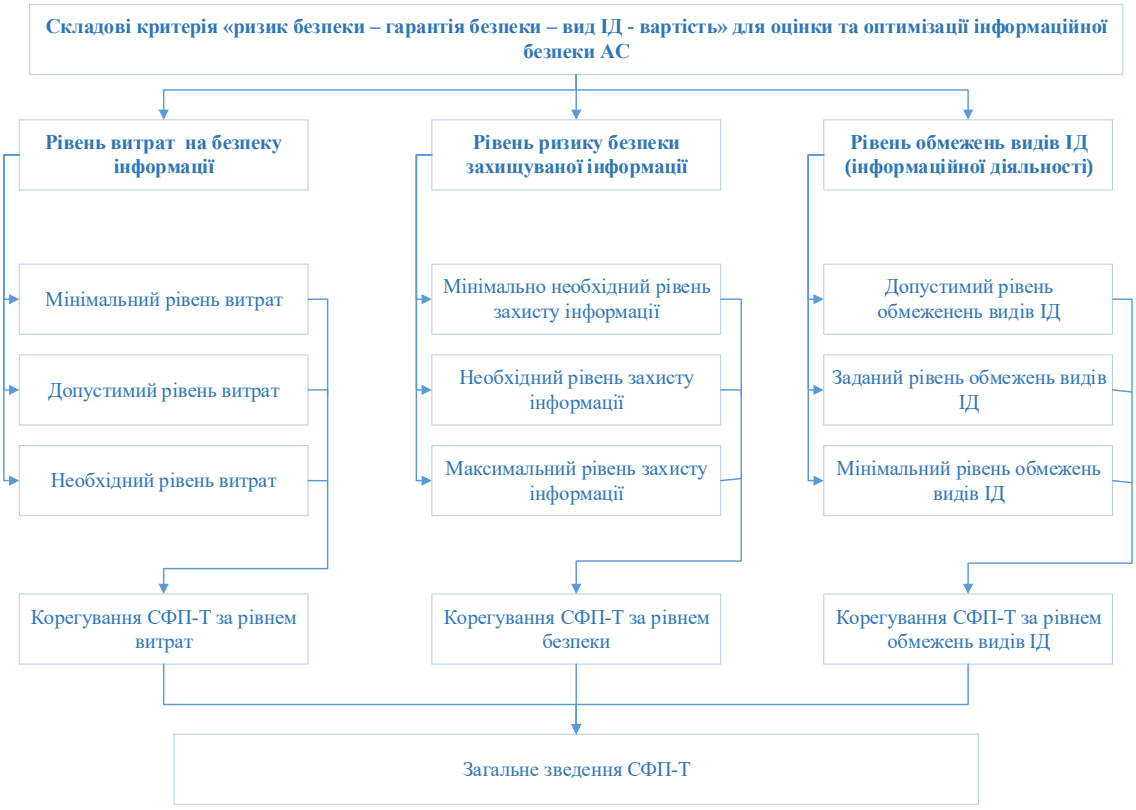

Рисунок 1 – Графічне відображення методу оцінки та оптимізації інформаційної безпеки АС за мультикритерієм «Ризик безпеки – гарантія безпеки – вид ІД - вартість»

Конкретне значення семантичних змінних визначаються із фінансових можливостей проекту та вартості реалізації послуг(4).

$$O_{RV} = \lim_{O_{RV,i} \to \max} \left[\sum_{i=1}^{N} O_{RV,i} \right] \quad (4)$$

В кожному конкретному випадку оцінка $O_{rv,I}$ – оцінка витрат на і-му о'бєкті вироджується в тривіальну розрахункову задачу. Таким чином множина підкритеріїв це рівень витрат на безпеку інформації, рівень ризику безпеки інформації, що захищається, рівень обмежень видів ІД (5).

$$K_{MK} \in \{K_{RVBI}\, K_{RRBZI}\, K_{ROVID}\} \quad (5)$$

Враховуючи вищесказане, було сформульовано метод оцінки та оптимізації інформаційної безпеки АС за мультикритерієм «ризик безпеки – гарантія безпеки – вид ІД – вартість».

Першим кроком є вибір профілю захисту залежно від призначення автоматизованих систем. Відповідно до НД ТЗІ 2.5-005-99 (існує чотири вибори)

На ***другому кроці*** методики здійснюється визначення класу АС та підкласів АС.

На ***третьому кроці*** методики починається оцінка складових критерія «ризик безпеки – гарантія безпеки – вид ІД – вартість» для оцінки та оптимізації інформаційної безпеки АС.

На ***четвертому кроці*** здійснюється обчислення цільової функції.

На ***п'ятому кроці*** здійснюється обчислення максимального значення математичного сподівання втрат на об'єктах АС при оптимальному використанні СФП-Т.

На ***шостому кроці*** в залежності від мети визначається чи досягнуті умови оптимізації і відповідно, якщо умови оптимізації не досягнуто, переходимо до нового обчислення цільової функції з новими умовами, тобто до нового кроку оптимізації – четвертого крок методики. Якщо умови оптимізації досягнуто, переходимо до наступного кроку методики.

На ***сьомому кроці*** перевіряється розподіл ФПБ по складовим АС

На ***восьмому кроці*** здійснюється оцінка фінансових витрат на реалізацію захисту і відповідності витрат наявному бюджету. В разі коли наявний бюджет суттєво перевищує витрати, з'являється можливість покращення рівня захисту що відображається в зміні умов оптимізації та повторенню кроків методики.

На ***дев'ятому кроці*** відбувається загальне зведення ФПЗ.

У **третьому розділі** було запропоновано спосіб перевірки збіжності метода (ПЗМ) та метод визначення функціонального профілю захисту автоматизованої системи (ВФПЗАС).

Для перевірки збіжності обмежимо кількість об'єктів до семи та обмежим математичне сподівання кількості зупинених об'єктів значенням 0.65. Тестовий алгоритм ПЗМ представлений на рис 1. Приклад: Нехай M0 = 0.65, n = 7, значення pi, ai, wi задано в табл. 2.

Результати обчислень наведено в таблицях 3-5.

1. Прийняти N := 1.

2. Обчислити значення Ψi (N) для усіх об'єктів (i = 1, 2, …, 7) по формулі (6) за умови (7) або для зворотної задачі по формулі (9), що теж саме.

$$\Psi_i(x_i) = [1-(1-\gamma)^{xi-ai}] \tag{6}$$

$$x_i \geq a_i, i = 1,2...n \tag{7}$$

3. Знайти n значень функції Mi (N) за допомогою наступного рекурентного співвідношення(8)

$$M_i(N) = \max[\Psi_i(y) + M_{i-1}(N-y)], \quad 0 \leq y \leq N \tag{8}$$

де i = 2, 3,…, 7; M1 (N) = Ψ1 (N).

Для кожного значення *i* фіксувати значення yi (N).

4. Перевірка виконання, для виключення можливих помилок. Порівняти Mn (N) з M0. Якщо Mn (N) ≥ 0,65, то перейти до пункту 6. Якщо ні, то – до пункту 5.

5. Прийняти N := N+1 і перейти до пункту 2.

6. Знайти розподіл атакуючих потенційних загроз по n об'єктам захисту x = {xi} за допомогою таблиці значень функції yi (N)

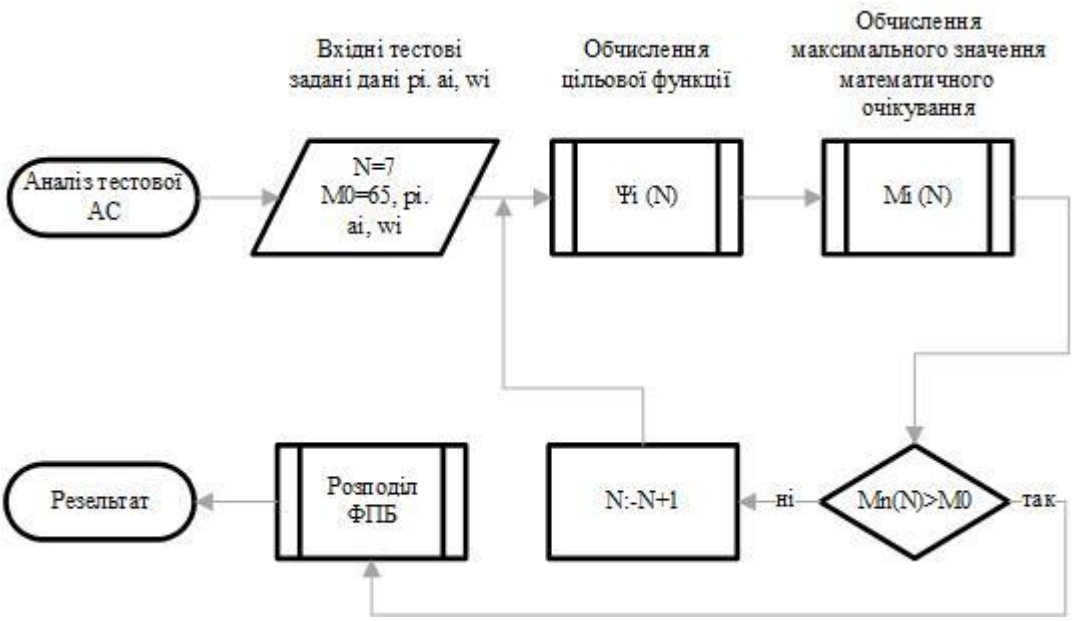

Рисунок 2 – Тестовий алгоритм ПЗМ

Як бачимо з рисунку 2, процес обчислень складається у побудові таблиць трьох функцій - Ψi (N), Mi (N) та yi(N), i = 1, 2, …, n; N = 1, 2, … , при цьому найбільш трудоємким є обчислення для кожного із значень N значень функцій Mi(N) (див. п. 3 алгоритму). По смислу Mi (N) представляє собою максимальне значення математичного сподівання (МОЧ) втрат на перших «i» об'єктах АС-1 при оптимальному використанні N засобів захисту.

Таблиця 2 – Вхідні тестові дані показників p_i , a_i, w_i ПЗМ

Номер об'єкта i	1	2	3	4	5	6	7
p_i	0.12	0.16	0.08	0.14	0.23	0.10	0.17
a_i	1	2	0	2	3	1	4
w_i	0.60	0.60	0.40	0.80	0.70	0.70	0.85

Таблиця 3 – Значення функції Ψi (N) ПЗМ

N	Значення функції Ψi (N)						
	Номер об'єкта i						
	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0
1	0	0	0.0320	0	0	0	0
2	0.0720	0	0.0512	0	0	0.0700	0
3	0.108	0.0960	0.0627	0.1120	0	0.0910	0
4	0.1123	0.1344	0.0696	0.1344	0.1610	0.0973	0
5	0.1169	0.1498	0.0738	0.1389	0.2093	0.0992	0.1445
6	0.1188	0.1559	0.0763	0.1398	0.2238	0.0998	0.1662
7	0.1195	0.1584	0.0778	0.1400	0.2281	0.0999	0.1694
8	0.1198	0.1593	0.0787	0.1400	0.2294	0.1000	0.1699

Продовження таблиці 3

	1	2	3	4	5	6	7
9	0.1199	0.1597	0.0792	0.1400	0.2298	0.1000	0.1700
10	0.1200	0.1599	0.0795	0.1400	0.2300	0.1000	0.1700
11	0.1200	0.1600	0.0797	0.1400	0.2300	0.1000	0.1700
12	0.1200	0.1600	0.0798	0.1400	0.2300	0.1000	0.1700
13	0.1200	0.1600	0.0799	0.1400	0.2300	0.1000	0.1700
14	0.1200	0.1600	0.0799	0.1400	0.2300	0.1000	0.1700
15	0.1200	0.1600	0.0800	0.1400	0.2300	0.1000	0.1700
16	0.1200	0.1600	0.0800	0.1400	0.2300	0.1000	0.1700
17	1200	0.1600	0.0800	0.1400	0.2300	0.1000	0.1700
18	1200	0.1600	0.0800	0.1400	0.2300	0.1000	0.1700

Таблиця 4 – Значення функції $M_i(N)$ ПЗМ

N	Значення функції $M_i(N)$						
	Номер об’єкта і						
	1	2	3	4	5	6	7
1	0	0	0.0320	0.0320	0.0320	0.0320	0.0320
2	0.0720	0.0720	0.0720	0.0720	0.0720	0.0720	0.0720
3	0.1008	0.1008	0.1040	0.1120	0.1120	0.1120	0.1120
4	0.1123	0.1344	0.1344	0.1440	0.1610	0.1610	0.1610
5	0.1169	0.1680	0.1680	0.1840	0.2093	0.2093	0.2093
6	0.1188	0.2084	0.2084	0.2160	0.2413	0.2413	0.2413
7	0.1195	0.2352	0.2384	0.2464	0.2813	0.2813	0.2813
8	0..1198	0.2506	0.2672	0.2800	0.3213	0.3213	0.3213
9	0.1199	0.2621	0.2864	0.3184	0.3533	0.3533	0.3533
10	0.1200	0.2682	0.3018	0.3504	0.3933	0.3933	0.3933
11	0.1200	0.2728	0.3133	0.3792	0.4253	0.4253	0.4253
12	0.1200	0.2747	0.3248	0.4016	0.4557	0.4633	0.4633
13	0.1200	0.2762	0.3317	0.4208	0.4893	0.4953	0.4953
14	0.1200	0.2781	0.3378	0.4362	0.5277	0.5277	0.5277
15	0.1200	0.2792	0.3424	0.4477	0.5597	0.5597	0.5597
16	0.1200	0.2795	0.3466	0.4592	0.5885	0.5977	0.5977
17	0.1200	0.2795	0.3491	0.4637	0.6109	0.6297	0.6297
18	0.1200	0.2797	0.3510	0.4722	0.6301	0.6585	0.6585

Таблиця 5 – Значення функції y_i (N) ПЗМ

N	Значення функції y_i (N)						
	Номер об’єкту і						
	1	2	3	4	5	6	7
1	1	0	1	0	0	0	0
2	2	0	0	0	0	0	0
3	3	0	1	3	0	0	0

Продовження таблиці 5

	1	2	3	4	5	6	7
4	4	4	0	3	4	0	0
5	5	3	0	3	5	0	0
6	6	4	0	3	5	0	0
7	7	4	1	3	5	0	0
8	8	5	1	3	5	0	0
9	9	5	2	3	5	0	0
10	10	6	2	3	5	0	0
11	11	6	2	3	5	0	0
12	12	6	3	4	5	2	0
13	13	7	4	4	5	2	0
14	14	8	5	4	5	0	0
15	15	8	4	4	5	0	0
16	16	8	5	5	5	2	0
17	17	9	6	5	5	2	0
18	18	10	6	4	5	2	0

Графічне відображення функцій Ψi (N) ПЗМ та M_i(N) ПЗМ показано на рисунках 3 та 4.

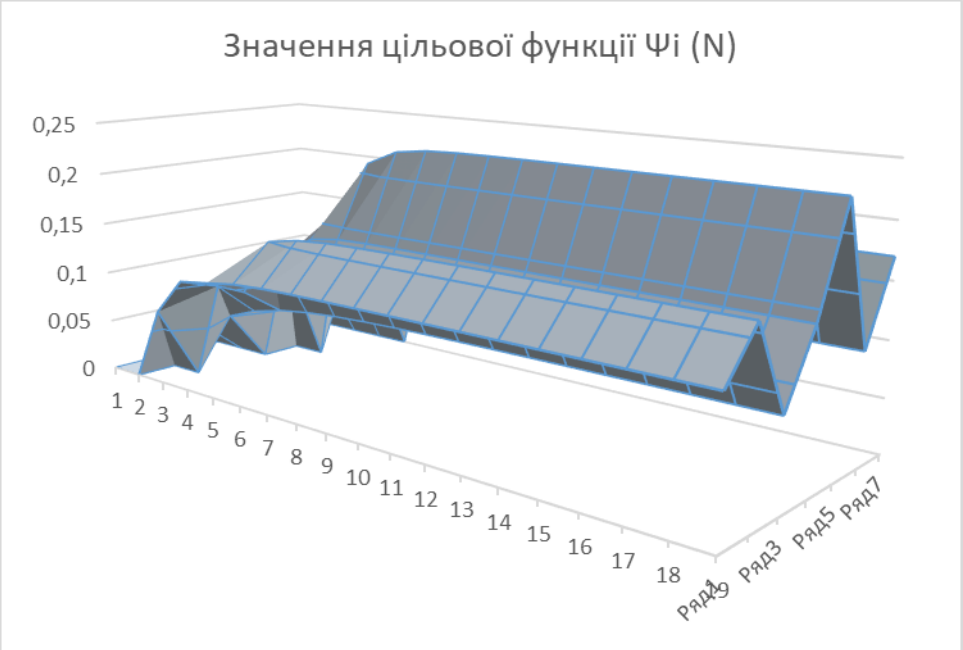

Рисунок 3 – Значення цільової функції Ψ_i (N) ПЗМ

Встановлено що алгоритм дозволяє знаходити цілочислені рішення розподілу функціональних послуг безпеки в АС першого, другого та третього класу за рахунок визначення вектору X (цілочислені значення xi).

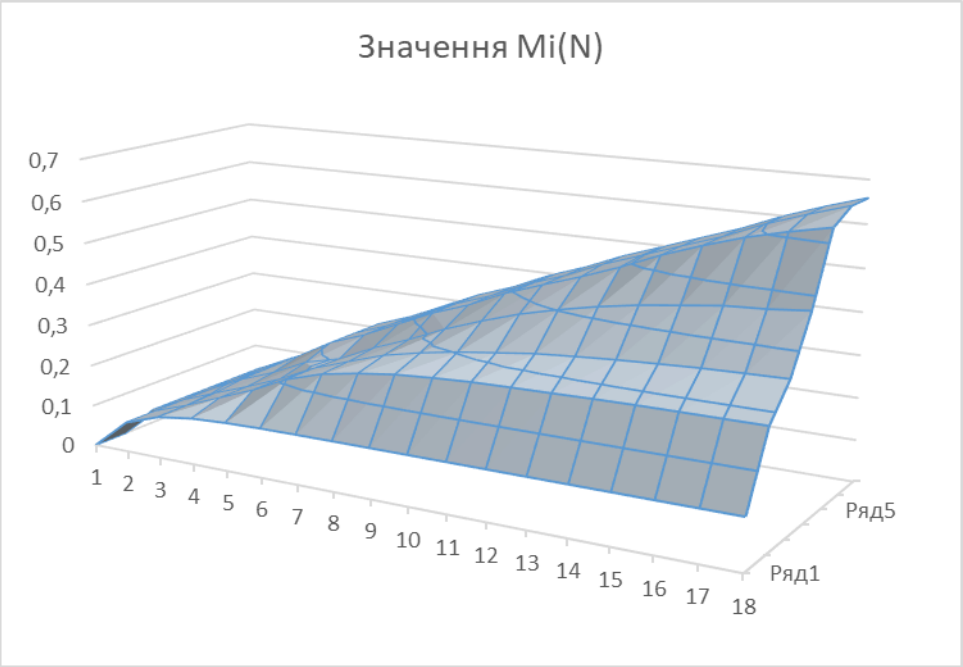

Рисунок 4 – Значення математичного сподівання успішного захисту $M_i(N)$ ПЗМ об'єкту АС

За методом визначення профілю протидії загрозам ВФПЗАС коефіцієнти вагомості (рейтинги) pi, уразливості wi оцінюються експертними методами. Прикладом такого підходу є системи «Інтерфейс СМ», «Профіль» та «Торсіон-3». Крім того змінюється критерії зупинки роботи алгоритму, в наслідок того що змінюється і стратегія пошуку, є сенс зупиняти аналіз після фіксованого числа ітерації.

Параметри xi, wi, βi, mi визначаються в прикладному робочому алгоритмі ВФПЗАС з урахуванням їх прикладного смислу якій залежить від головної мети - розробки рекомендацій до проектування профілю послуг безпеки:

pi – адаптивний повний рейтинг кожної і-ї профільної функціональної послуги безпеки (об'єкта-послуги) із множини типів функціональних послуг безпеки (МТФПБ) нормується до 1.0 для цієї множини тільки при N = 67;

xi – порядковий номер і-ї профільної функціональної послуги безпеки (об'єкта-послуги) множини із множини їх різних рівнів 67-ми профільних послуг безпеки ПМТФПБ

wi – уразливість і-го об'єкта-послуги від загроз за підкласами АС-1, АС-2, АС-3 - Вона оцінюється ризиком безпеки за правилом wi = 1- pi для кожного підкласу К, Ц, Д, КЦ, КД, ЦД, КЦД;

βi – імовірність протидії і-го об'єкта-послуги від загроз за підкласами АС-1, АС-2, АС-3 множини МТФПБ із упорядкованої за рівнями їх множини ПМТФПБ. Оцінюється адаптивним (довільним) рейтингом і-ї профільної послуги безпеки.

mi – кількість рівнів в обраній множині із упорядкованої за рівнями їх множини ПМТФПБ.

ai – фактор протидії загрозі і-ою профільною послугою безпеки.

У **четвертому розділі** розроблено та протестовано програмний застосунк для перевірки збіжності методу визначення профілю протидії загрозам призначений для допомоги експерту при визначенні рівня захищеності ФПЗ відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

Програмний застосунок (рис. 5 - рис. 7) було реалізовано на мові програмування C# в середовищі розробки VisualStudio 2022. При написанні програмного коду, використовувалась базові бібліотеки мови програмування C#.

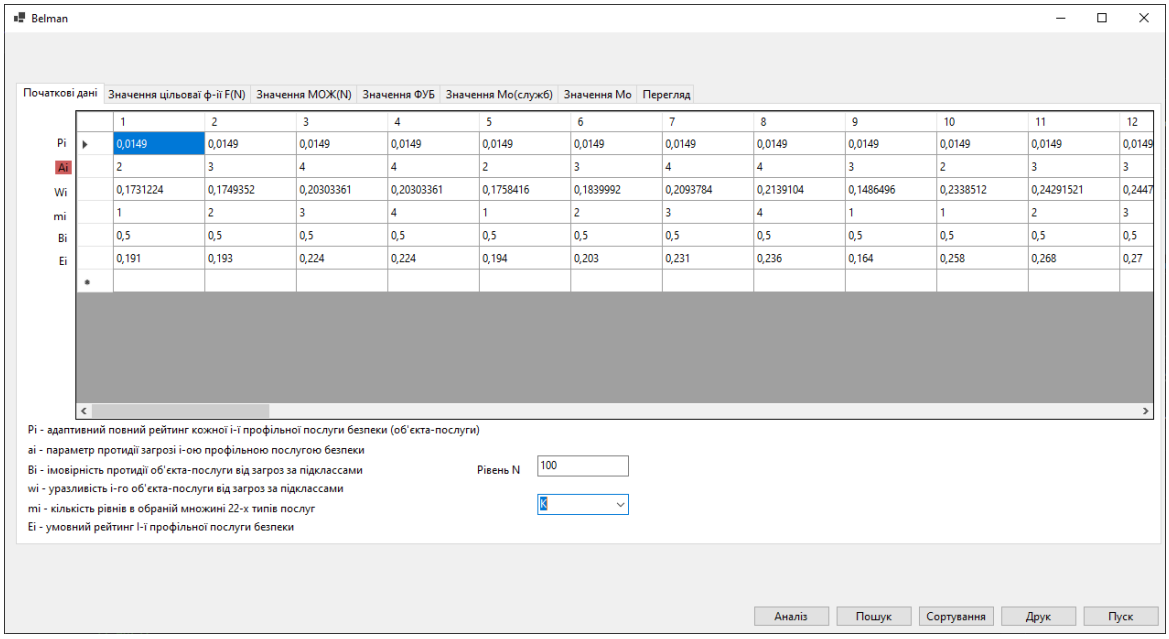

Рисунок 5 – Інтерфейс програми

Інтерфейс програмного застосунку представляє собою віконний додаток, який реалізований у вигляді GUI-програми. Інтерфейс застосунку розділений на такі вкладки:

«Початкові дані» – для введення експертом початкових даних для подальших розрахунків.

«Значення цільової функції F(N)» де проводяться розрахунки Ψi (N)

«Значення МОЖ» де проводяться розрахунки Mi (N)

«Значення ФУБ»

«Значення M0(служб)»

«Значення M0»

«Перегляд» для зручного аналізу експертом окремо взятих функціональних послух безпеки.

А також кнопок «Аналіз» (для пошуку функціонального профілю захисту з заданим рівнем безпеки), «Пошук» (для пошуку значень функціональних послуг безпеки), «Сортування» (для зручного сортування ФПЗ), «Друк» (для експорту даних в Excel), «Пуск» (для запуску процедури розрахунку).

Проведено аналіз розподілу значень Ψi(N) та Mi(N). Для всіх підкласів систем К, Ц, Д, КЦ, КД, ЦД, КЦД розмірністю 1000.

Таблиця 6 – Значення функції Ψi (N) для підсистем класу К

	Значення функції Ψi (N)							
	Номер об’єкта і							
N	1	2	3	4	5	6	…	67
0	0	0	0	0	0	0	…	0
1	0,0026	0	0	0	0,0026	0	…	0
2	0,0047	0,0026	0	0	0,0048	0,0027	…	0,0029
3	0,0065	0,0048	0,003	0,003	0,0066	0,005	…	0,0053
4	0,0079	0,0065	0,0054	0,0054	0,008	0,0068	…	0,0072
5	0,0091	0,008	0,0074	0,0074	0,0092	0,0083	…	0,0089
6	0,0101	0,0092	0,0089	0,0089	0,0102	0,0095	…	0,0102
7	0,011	0,0102	0,0101	0,0101	0,0111	0,0105	…	0,0113
8	0,0116	0,011	0,0111	0,0111	0,0117	0,0113	…	0,0122
9	0,0122	0,0117	0,0119	0,0119	0,0123	0,012	…	0,013
10	0,0127	0,0123	0,0125	0,0125	0,0127	0,0125	…	0,0136
11	0,0131	0,0127	0,013	0,013	0,0131	0,0129	…	0,0141
12	0,0134	0,0131	0,0134	0,0134	0,0134	0,0133	…	0,0146
13	0,0136	0,0134	0,0137	0,0137	0,0137	0,0136	…	0,0149
14	0,0139	0,0137	0,0139	0,0139	0,0139	0,0138	…	0,0152
	…	…	…	…	…	…	…	…
999	0,0149	0,0149	0,0149	0,0149	0,0149	0,0149	…	0,0166

Таблиця 7 – Значення функції $M_i(N)$ для підсистем класу К

	Значення функції Mi(N)							
	Номер об’єкта і							
	1	2	3	4	5	6	….	67
1	0	0	0	0	0	0	….	0
2	0	0	0	0	0,0026	0,0026	….	0,0035
3	0,0026	0,0026	0,0026	0,0026	0,0048	0,0048	….	0,0064
4	0,0047	0,0048	0,0048	0,0048	0,0066	0,0066	….	0,0091
5	0,0065	0,0065	0,0065	0,0065	0,008	0,008	….	0,0118
6	0,0079	0,008	0,008	0,008	0,0096	0,0098	….	0,0144
7	0,0091	0,0095	0,0095	0,0095	0,0114	0,0116	….	0,017
8	0,0101	0,0113	0,0113	0,0113	0,0131	0,0134	….	0,0196
9	0,011	0,013	0,013	0,013	0,0146	0,0149	….	0,0222
10	0,0116	0,0145	0,0145	0,0145	0,0161	0,0164	….	0,0248
11	0,0122	0,0159	0,0159	0,0159	0,0179	0,0182	….	0,0274
12	0,0127	0,0171	0,0171	0,0171	0,0196	0,0199	….	0,03
13	0,0131	0,0183	0,0187	0,0187	0,0211	0,0214	….	0,0326
14	0,0134	0,0193	0,0204	0,0204	0,0225	0,0229	….	0,0352
15	0,0136	0,0203	0,0219	0,0219	0,0239	0,0247	….	0,0377
….	….	….	….	….	….	….	….	….
999	0,0149	0,0298	0,0447	0,0596	0,0745	0,0894	….	0,9355

Значення математичного сподівання успішного захисту Mi(N) об’єкту для підсистем класу К представлено на рисунку 6.

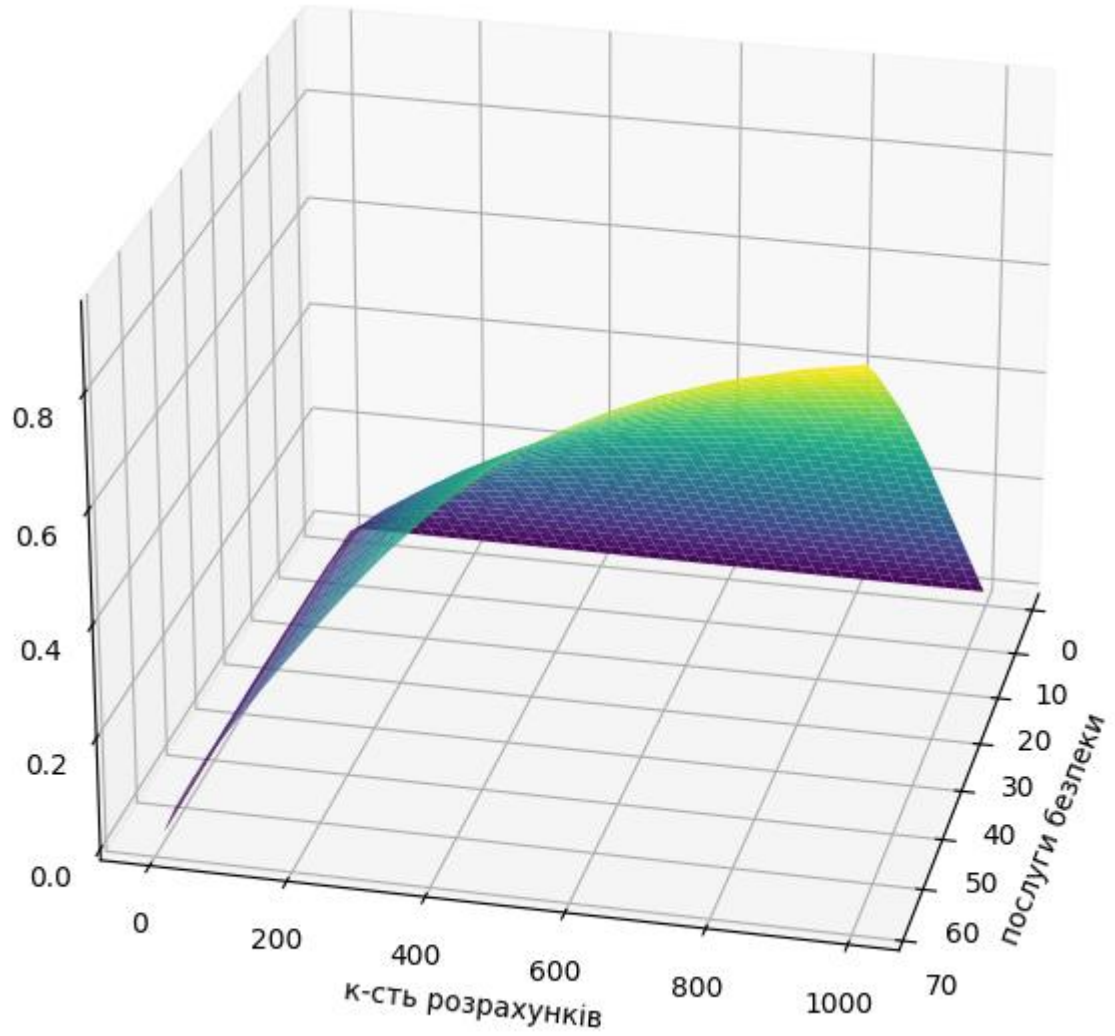

Рисунок 6 – Значення математичного сподівання успішного захисту Mi(N) об’єкту для підсистем класу К

Зведений графік математичного сподівання успішного захисту Mi(N) об’єкту АС для підсистем класу К, Ц, Д, КЦ, КД, ЦД, КЦД представлений на рисунку 7.

Порівняльний аналіз методу ВФПЗАС з іншими методами побудови ФПЗ представлений в таблиці 8.

Загалом, програмний застосунок методу ідентифікації ФПЗ виконав усі задачі, які були визначені при його створені, що підтверджує адекватність отриманих результатів.

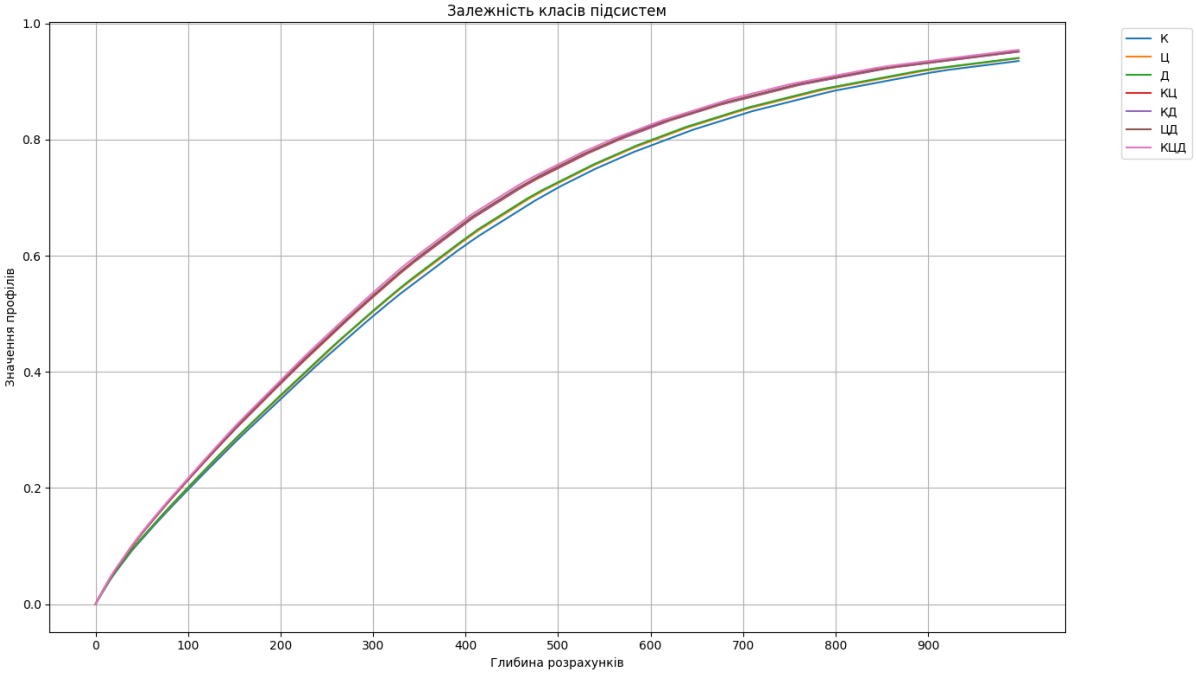

Рисунок 7 – Зведений графік математичного сподівання успішного захисту $M_i(N)$ об’єкту АС для підсистем класу К, Ц, Д, КЦ, КД, ЦД, КЦД

Таблиця 8 – Порівняльна таблиця методів побудови ФПЗ з ВФПЗАС

Метод побудови ФПЗ	Витрати (рівень)	Використання стандартних ФПЗ	Використання нестандартних ФПЗ	Часові витрати	Кваліфікація експерта	Чисельне вираження ФПБ
Стандартний метод	високий	+	+	високі	середня	-
Метод перевірки несуперечності та повноти	високий	-	+	високі	висока	-
Метод побудови таксономії	високий	-	+	високі	висока	-
Метод парето-оптимальних ФПЗ	високий	-	+	високі	висока	-
Удосконалений метод визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР	невисокі	+	+	середні	середня	-
Метод ВФПЗАС	невисокі	+	+	низькі	середня	+

Після проведених експериментальних досліджень, було доведено їх ефективність для визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз.

У **додатках** знаходяться акти впровадження результатів дисертаційної роботи.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну задачу, пов’язану з розробкою методу визначення функціонального профілю захисту автоматизованих систем.

При вирішенні цієї задачі отримані такі основні результати:

1. Проведено аналіз та систематизацію методів і засобів визначення функціонального профілю захисту відповідно до існуючих критеріїв оцінки захисту автоматизованих систем. З’ясовано, що дослідженню задач, пов’язаних з вивченням критеріїв захисту інформації та визначенню функціонального профілю захисту присвячується значна частина публікацій як зарубіжних так і вітчизняних вчених. Однак, незважаючи на різноманітні підходи до вирішення цієї задачі, вона залишається актуальною не лише для України, але і для всесвітньої спільноти.

2. Вперше запропоновано мультикритерії «ризик безпеки – гарантія безпеки – вид ІД - вартість», який шляхом послідовної виваженої оцінки гарантії безпеки, виду інформаційної діяльності та вартості дозволяє у формальному вигляді сформувати необхідний набір послуг безпеки для реалізації процесу вибору рівня захисту.

3. Вдосконалено метод визначення функціонального профілю захисту для різних класів АС, який, за рахунок аналізу цільової функції по Р. Белману та виміру математичного сподівання успішної протидії, та завдяки використанню розподілу однорідних ресурсів, дозволяє формалізувати процес генерування функціонального профілю захисту та порівняння його з відповідним рівнем загроз.

4. Вперше запропоновано спосіб перевірки збіжності методу визначення функціонального профілю захисту для різних класів АС, який за рахунок автоматизації процесу адаптації загрозам за підкласами автоматизованих систем дозволяє масштабувати результати розрахунку рівня захисту на обмеженому кортежі ФПЗ на повний простір, що зменшує обсяг розрахунку до 10,45 % від максимального.

5. Вперше розроблено метод визначення функціонального профілю захисту для різних класів АС, який за рахунок окремої оцінки умовного рейтингу та коефіцієнту вагомості дозволяє зменшити час при складанні ФПЗ на 15%.

6. На основі запропонованого методу розроблено програмне забезпечення для визначення функціонального профілю захисту для різних класів АС з використанням розроблених методів. Зазначений програмний застосунок використано при побудові комплексних систем захисту інформації та при проведенні державних експертиз КСЗІ.

7. Експериментальні дослідження програмного забезпечення визначення функціонального профілю захисту для різних класів АС, а також

впровадження та успішне практичне використання зазначених розробок підтвердили достовірність теоретичних гіпотез та практичних розробок і висновків дисертаційної роботи.

Результати дисертаційної роботи було впроваджено у діяльність ТОВ “ІНФОРМАЦІЙНА БЕЗПЕКА” (акт від 03.05.2024р.) та ДП Державний науково-технічний центр з ядерної та радіаційної безпеки (ДНТЦ ЯРБ) (акт від 15.05.2024р.) .

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації.

1. Olena Vysotska, Anatolii Davydenko, Oleksandr Potenko Modeling the mindfulness people's function based on the recognition of biometric parameters by artificial intelligence elements // Radioelectronic and Computer Systems, 2023, no. 3(107), P.136 – 148, doi: 10.32620/reks.2023.3.11. (**Scopus**, ISSN 1814-4225 (print), ISSN 2663-2012 (online))

2. Давиденко А.М. Потенко О.С. Сторчак А.С. Візуалізація елементів моделі загроз за допомогою COM-сервера // Моделювання та інформаційні технології: Зб.наук.праць ІПМЕ НАН України. – Київ, 2008. – Вип. 46 – С.84-89.

3. Потенко О.С. Аналіз моделей безпеки в аспекті експертизи спеціалізованих інформаційних систем // Моделювання та інформаційні технології: Зб.наук.праць ІПМЕ НАН України. – Київ, 2009. – Вип. 52 – С.86-92.

4. Давиденко А.Н. Логачова В.Ю. Марковская М.П. Потенко А.С. Анализ структуры ГРИД-узла кластера ИПМЕ НАНУ с точки зрения информационного взаимодействия открытых систем // Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2009. – Вип. 52. – С.114-121.

5. Шорошев В.В, Давиденко А.Н. Потенко А.С. Оценка профилей противодействия угрозам на основе динамического программирования с использованием принципа Р. Беллмана // Моделювання та інформаційні технології: Зб.наук.праць ІПМЕ НАН України. – Київ, 2010. – Вип. 55 – С.82-87.

6. Потенко А.С. Анализ информационных технологий в современных системах хранения информации // Моделювання та інформаційні технології: Зб.наук.праць ІПМЕ НАН України. – Київ, 2011. – Вип. 62 – С.31-37.

7. С.Д. Винничук, А.Н. Давиденко, С.Я. Гильгурт, А.С. Потенко. Применение ГРИД-системы при исследовании линейных блоковых кодов // Системи обробки інформації. Міністерство оборони України, Харківський університет повітряних сил. – Харків 2013. Вип. 7(114) – С. 61-64. ISSN 1681-7710

8. Давиденко А.Н., Гильгурт С.Я., Потенко А.С., Евдина А.К. Анализ вопросов закрытия информационного канала связи с беспилотным летательным аппаратом // Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2014. –

Вип. 71. – С.70-76., (ISSN 2309-7647)

9. Шабан М.Р., Марковская М.П., Кислов А.Г., Потенко А.С. Использование COM-технологий при проведении экспертизы на соответствие требованиям НД ТЗИ // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2015. – Вип. 75 – С.56–59., (ISSN 2309-7647)

10. Шабан М.Р., Потенко О.С., Попова В.М. Тестування систем підтримки прийняття рішень орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2018. – Вип. 84. – С.73-78., (ISSN 2309-7647)

11. Потенко О.С. Аналіз систем захисту веб-додатків від хакерских атак // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2019. – Вип. 89. – С.166-172. doi:http://doi.org/10.5281/zenodo.3860764, (ISSN 2309-7647)

12. Гончар С., Потенко О. Методологія оцінки суми ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури // Захист інформації, том 25, № 3 2023, С. 159-165, ISSN 2410-7840, DOI: https://doi.org/10.18372/2410-7840.25.17941

Праці апробаційного характеру.

13. А.М. Давиденко, О.С. Потенко, В.В. Шорошев Застосування CASE-технології для моделювання стандартних функціональних профілів безпеки та оцінки ризиків. Зб. тез XXVII науково-технічної конференції «Моделювання», 10-11 січня 2008 р. Київ, 2008. С. 31.

14. А.Н. Давиденко, А.С. Потенко. Анализ методов обработки критической информации в высокопроизводительных средах. Зб. тез XXVIII науково-технічної конференції «Моделювання», 15-16 січня 2009 р. Київ, 2008. С. 34

15. В.В. Шорошев, А.Н. Давиденко, А.С. Потенко, Оценка профилей противодействия угрозам на основе динамического программирования с использованием принципа оптимума Р.Беллмана. Зб. тез XXIX науково-технічної конференції «Моделювання», 12-13 січня 2010 р. Київ, 2010. С. 33.

16. А.Н. Давиденко, В.В. Шорошев, А.С. Потенко, Разработка системы противодействия угрозам на основе динамического программирования «Профиль-1». Зб. тез XXX науково-технічної конференції «Моделювання», 12-13 січня 2011 р. Київ, 2011. С. 11.

17. С.Д. Винничук, А.Н. Давиденко, С.Я. Гильгурт, А.С. Потенко Нижняя оценка максимального кодового расстояния для линейных блокових кодов *(n, k)* над полем *GF(2).*, Киев, 16-18 мая, 2012г. Сборник трудов конференции Моделирование-2012. Институт проблем моделиирования в енергетике им. Г.Е. Пухова С.150-153.

18. Потенко О.С. Захист сайтів від хакерських атак за допомогою Web Application Firewall // Безпека енергетики в епоху цифрової трансформації: матеріали науково-практичної конференції Інституту проблем моделювання в

енергетиці ім. Г.Є. Пухова Національної академії наук України, м. Київ, 20 грудня 2019. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2019. – С.22-23.

19. Потенко А.С., Суліма О.А. Спеціалізовані засоби захисту веб-ресурсів від зовнішніх атак // XXXVIII Щорічна науково-технічна конференція молодих вчених і спеціалістів: Тези доп, м. Київ, 15 травня 2020. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2020. – С.102-103.

20. Потенко О.С. Побудова профілів протидії загрозам за допомогою принципу оптимуму Р. Белмана в АС 1-3 класів // Кібербезпека енергетики: Матеріали наук.-практ. конф. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 28 травня 2021. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2021. – С. 54.

21. Потенко О.С., Корченко А.О. Порівняльний аналіз моделей безпеки в інформаційних системах // Зб. тез наук. доп. XIII Всеукр. наук.-практич. конф. «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2021)», с. Коблеве Миколаївської обл., Україна, 23 – 26 червня 2021. – Миколаїв: 2021. – С.31–34.

22. Давиденко А.М., Гільгурт С.Я., Потенко О.С., Кіслов О.Г. Підхід до забезпечення цілісності інформації в кіберфізичних системах // XL Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції (11 травня 2022 р.). – Київ, 2022. – С. 57-58.

23. Потенко О.С., Суліма О.А. Аналіз динаміки надходжень попереджень від CSIRT // Безпека енергетики в епоху цифрової трансформації, IV науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України: Матеріали (Київ, 24 листопада 2022 р.). Київ: ІПМЕ ім. Г.Є. Пухова НАН України, 2022. С. 86-89.

24. Потенко О.С., Давиденко А.М. Розробка програмного застосунку вибору складу профілю протидії загрозам на основі аналізу вірогідності їх реалізації // XIV Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави», (Київ, 30 березня 2023 року), Нац. акад. СБУ, 2023, С. 398-400.

25. Потенко О.С. Розробка методики вибору складу профілю протидії загрозам на основі аналізу вірогідності їх реалізації // XIV Міжнародна науковопрактична конференція «Комп'ютерні системи та мережні технології» (CSNT-2023), 13–14 квітня 2023 р, Національний авіаційний університет. – К.: НАУ, 2023. – С.133–134.

26. Потенко О.С. Аналіз сучасних баз даних вразливостей інформаційної безпеки // XLI Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції (17 травня 2023 р). – Київ, 2023. – С. 34.

27. Давиденко А.М., Гільгурт С.Я., Потенко О.С., Кіслов О.Г. Поводження з породжувальними матрицями завадостійкого кодування інформації в кіберфізичних системах // XLI Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці

ім. Г.Є. Пухова НАН України. Збірник тез конференції (17 травня 2023 р). – Київ, 2023. – С. 66-68.

28. Anatolii DAVYDENKO, Olena VYSOTSKA, Oleksandr POTENKO Developing a software application for the protection of information systems based on the analysis of graphic images// Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф. – Львів : Видавництво Львівської політехніки, 2023. – Режим доступу: https://drive.google.com/drive/folders/1z5BLogqaxwh4xg Gk2eMLI8WcVNOXCFX6, ISBN 978-966-941-829-6 , С. 122-123.

29. Давиденко А.М., Висоцька О.О., Потенко О.С. Захист інформаційних систем на основі аналізу графічних зображень // Кібербезпека енергетики: Матеріали наук.-практ. конф. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 31 травня 2023. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2023. – С. 74-77.

30. O.S. Potenko Analysis of actual information security vulnerability databases // Науково-практична конференція «Резильєнтність критичної інфраструктури – 2023» Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції (21 червня 2023 р.). – Київ, 2023. – С. 22-23.

31. О.С. Потенко Розробка методики оцінки профілів функціональних послуг захисту на базі оптимізаційних підходів // Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023» Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції (19 жовтня 2023 р.). – Київ, 2023. – С. 101. ISBN 978-617-7903-13-09

32. О.С.Потенко, А.М.Давиденко Програмний застосунок для вибору складу профілю протидії загрозам в інформаційно-телекомунікаційних системах // V науково-практична конференція «Безпека енергетики в епоху цифрової трансформації» , Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 22 листопада 2023 р.). Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2023. С. 95-96

Праці, які додатково відображають наукові результати дисертації.

33. Свідоцтво про реєстрацію авторського права на твір №116311, 08.02.2023р. Комп'ютерна програма «Модуль розрахунку агрегованого ризику у разі множини сумісних випадкових подій» / Мохор В.В., Гончар С.Ф., Потенко О.С., Бакалинський О.О., Чьочь В.В. – опубл. 31.03.2023, Бюл. № 74.

АНОТАЦІЯ

Потенко О.С. Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2024.

Дисертаційна робота присвячена підвищенню рівня ефективності процесу побудови комплексної системи захисту інформації при проведенні експертизи технічного захисту інформації шляхом адаптації функціонального профілю захисту автоматизованих систем до поточного рівня загроз.

Проаналізовано, систематизовано та формалізовано основні світові та вітчизняні критерії оцінки захисту автоматизованих систем за такими шаблонами як: призначення критеріїв, область застосування, методи оцінки, ефективність, актуальність. Показано, що задача розроблення методів адаптації функціонального профілю захисту автоматизованих систем відповідно до поточного рівня загроз є актуальною, що підтверджується, зокрема, відсутністю аналогічних українських та закордонних рішень.

Удосконалено критерії визначення функціонального профілю захисту, які, за рахунок аналізу цільової функції по Беллману та виміру математичного сподівання успішної протидії окремої функціональної послуги безпеки, дозволяють у формальному вигляді сформувати необхідний набір величин для реалізації процесу вибору рівня захисту.

Було розроблено метод визначення інформаційної безпеки АС за мультикритерієм «ризик безпеки – гарантія безпеки – вид ІД - вартість». який, за рахунок використання розподілу однорідних ресурсів, дозволяє автоматизувати процес генерування функціонального профілю захисту та порівняння його з відповідним рівнем захисту. Сформовано множини критеріїв цього методу.

Розроблено алгоритм, який дозволяє ефективно перевіряти збіжність методу для проектування профілів, адаптивних до різних загроз для підкласів автоматизованих систем. Після розробки алгоритму було проведено детальний тестовий розрахунок, який використовується для перевірки коректності реалізації алгоритму в четвертому розділі нашої роботи. Крім того, була проведена перевірка працездатності методу з урахуванням прийнятих обмежень, що підтверджує його ефективність та придатність для використання в практичних умовах.

Розроблено робочий алгоритм визначення функціонального профілю захисту автоматизованої системи ВФПЗАС для профілю захисту автоматизованої системи з урахуванням поточного рівня загроз для підкласів К, Ц, Д, КЦ, КД, ЦД, КЦД, на основі якого розроблено програмний модуль для визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз, який дозволяє генерувати функціональні профілі захисту для всіх 67-ми функціональних послуг безпеки

Ключові слова: захист інформації, комп'ютерна система, мережа, кібербезпека, критерій інформаційної безпеки, інформаційна система, об'єкт критичної інфраструктури, захист інформації, системи підтримки прийняття рішень, функціональний профіль захисту, функціональні послуги безпеки.

ABSTRACT

Potenko O. Methods of determining the functional profile of protection of an automated system taking into account the current level of threats. – As the manuscript.

Dissertation for obtaining the scientific degree of candidate of technical sciences in the specialty 05.13.21 – information security systems. – G.E. Pukhov Institute for Modelling in Energy Engineering of the National Academy of Sciences of Ukraine, Kyiv, 2024.

The dissertation work is devoted to increasing the level of effectiveness of the process of building a complex information protection system when conducting an examination of technical information protection by adapting the functional profile of the protection of automated systems to the current level of threats

The main global and domestic criteria for evaluating the protection of automated systems have been analyzed, systematized and formalized according to such templates as: designation of criteria, scope of application, evaluation methods, effectiveness, relevance. It is shown that the task of developing methods for adapting the functional profile of the protection of automated systems in accordance with the current level of threats is urgent, which is confirmed, in particular, by the absence of similar Ukrainian and foreign solutions.

The criteria for evaluating the functional profile of protection have been improved, which, due to the analysis of the objective function according to Bellman and the measurement of the mathematical expectation of successful countermeasures of a separate functional security service, make it possible to formally form the necessary set of values for the implementation of the process of choosing the level of protection.

A method was developed to determine the information security of the AC based on the multi-criteria "security risk - security guarantee - type of ID - cost". which, due to the use of distribution of homogeneous resources, allows to automate the process of generating a functional protection profile and comparing it with the corresponding level of protection. A set of criteria for this method has been formed.

An algorithm has been developed that allows you to effectively check the convergence of the method (PZM) for designing profiles that are adaptive to various threats for subclasses of automated systems. After developing the algorithm, a detailed test calculation was carried out, which is used to check the correctness of the algorithm implementation in the fourth section of our work. In addition, the test of the efficiency of the method was carried out taking into account the accepted limitations, which confirms its effectiveness and suitability for use in practical conditions.

A working algorithm for determining the functional profile of the protection of the automated system of VFPZAS has been developed for the protection profile of the automated system taking into account the current level of threats for subclasses K, C, D, KC, KD, CD, KCD, based on which a software module has been developed to determine the functional profile of the automated system protection with taking into account the current level of threats, which allows the generation of functional security profiles (FSP) for all 67 functional security services

Keywords: information security, computer system, network, cyber security, information security criterion, information system, critical infrastructure object, information protection, decision support systems, functional protection profile, functional security services.