МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Шабан Максим Радуйович

УДК 004.056.523:57.087.1(043.3)

МОДЕЛІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЕКСПЕРТИЗ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2021

Дисертацією є рукопис.
Робота виконана в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.

Науковий керівник:	кандидат 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 **Лахно Валерій Анатолійович**, Національний університет біоресурсів і природокористування України, завідувач кафедри комп'ютерних систем і мереж;
	кандидат технічних наук **Петренко Тарас Анатолійович,** Національний університет «Чернігівська політехніка», доцент кафедри кібербезпеки та математичного моделювання.

Захист відбудеться 22 квітня 2021 р. о 13.00 на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті (м. Київ, пр. Любомира Гузара 1, корп.11, ауд.111).

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Любомира Гузара, 1.

Автореферат розісланий «19» березня 2021 р.

Учений секретар
спеціалізованої вченої ради Д 26.062.17
кандидат технічних наук, професор Є.В. Іванченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Згідно вимог Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" для забезпечення безпеки в інформаційних ресурсах, що обробляються в автоматизованій системі (АС), необхідно розробляти комплексну систему захисту інформації (КСЗІ). Базовим етапом її побудови є створення політики безпеки, методологія якої включає в себе: розробку концепції інформаційної безпеки в АС; аналіз ризиків; визначення вимог до заходів, методів і засобів захисту; вибір основних рішень з забезпечення ІБ; організацію виконання відновлювальних робіт та забезпечення безперервного функціонування АС; документальне оформлення політики безпеки.

Значний внесок у розвиток моделей побудови КСЗІ внесли такі вчені О.Г. Корченко, С.В. Казмірчук, В.М. Луценко, С.О. Гнатюк, В.А. Лахно, В. В. Мохор, Т.А. Петренко та ін.

Завершальним етапом впровадження КСЗІ є експертиза КСЗІ АС на відповідність вимогам нормативного документу технічного захисту інформації (НД ТЗІ). В процесі проведення експертизи виникає задача знаходження частково формалізованої моделі політики безпеки при умові гарантій Г-2 - Г-3. Модель будується на підставі знань отриманих на етапі побудови КСЗІ і описані в базовому наборі документів (Технічне завдання, Акт обстеження тощо).

Завданням експерта є отримання знань з базового набору документів, розробка вихідного набору документів і проведення ряду спеціалізованих досліджень, а саме: аналіз функціонального профілю захисту (ФПЗ), ідентифікація функціональних послуг безпеки (ФПБ) та побудова тестового набору для перевірки ФПБ.

Але внаслідок розвитку АС зростає складність аналізу систем, що збільшує час необхідний для проведення державних експертиз КСЗІ. Разом з тим, умова по вчасному виконанню експертиз залишилась. Таким чином, розробка моделей підтримки прийняття для експертиз систем технічного захисту інформації (ТЗІ) *є актуальною науковою задачею.*

Зв'язок роботи з науковими програмами, планами, темами. Результати дисертаційної роботи відображені у звітах про науково-дослідну роботу (НДР) Інституту проблем моделювання в енергетиці ім. Г.Є.Пухова (ІПМЕ): "Исследование и разработка методов повышения безопасности и эффективности распределенных высокопроизводительных информационных технологий при решении задач энергетики" (шифр МОД-Б, реєстраційний номер 0108U010588, 2009-2013 рр.), "Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики" (шифр МОД-Д, реєстраційний номер 0114U002361, 2014-2018 рр.), "Державна експертиза комплексної системи захисту інформації локальної обчислювальної мережі Управління справами Національної академії наук України" (№ 207-16 від 30.06.16 р.), "Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними" (шифр МОД-Е, реєстраційний номер 0118U002371, 2019-2020 рр.), "Проведення первинної державної експертизи комплексної системи захисту інформації автоматизованої інформаційної системи Президії Національної академії наук України" (№ 203-14/03 від 22.07.14 р.), "Комплексна система захисту інформації, що циркулює в Ресурсному центрі Інституту кібернетики ім. В.М.Глушкова НАН України" (№ 208-16 від 30.06.16 р.), "Вдосконалення методики проведення експертизи комплексної системи захисту інформації, що циркулює в українському академічному грід-вузлі Інституту теоретичної фізики НАН України" (№ 201-13 від 14.06.13 р.), "Проведення державної експертизи

комплексної системи захисту інформації в автоматизованій системі управління “Кадри” рівня Укрзалізниці” (№ 202-13 від 30.08.13 р.), “Створення та проведення первинної державної експертизи комплексної системи захисту інформації на об’єкті, що належить Департаменту військово-технічної політики, розвитку озброєння, та військової техніки Міністерства оборони України” (№ 149 від 27.06.18 р.) .

Мета і задачі дослідження. Метою дисертаційної роботи є автоматизація процесу проведення експертизи комплексної системи захисту інформації та виявлення невідповідностей при формуванні функціонального профілю захисту.

Для досягнення поставленої мети **необхідно вирішити такі основні задачі:**

− проаналізувати існуючи методи, моделі та засоби підтримки прийняття рішень. З’ясувати, чи існуючи методи, моделі та засоби задовольняють вимогам щодо системи підтримки прийняття рішень, які мали би змогу використовуватись при проведенні державних експертиз комплексної системи захисту інформації;

− розробити декомпозиційну модель представлення смислових констант та змінних, що дозволить формувати базові шаблони вихідних документів експертиз технічного захисту інформації;

− розробити модель параметрів, що дозволить у формальному вигляді сформувати необхідний набір величин для реалізації процесу ідентифікації функціонального профілю захисту в комп'ютерних системах;

− розробити метод ідентифікації функціонального профілю захисту, що дозволить реалізувати процес генерування функціонального профілю захисту і перевірку його вимог щодо функцій захисту (послуг безпеки) та гарантій;

− розробити структурну модель системи підтримки прийняття рішень, що дозволить автоматизувати процес складання вихідних документів за їх шаблонами;

− розробити алгоритмічне та програмне забезпечення, що дозволить зменшити час необхідний для створення вихідних документів та зменшити кількість помилок при їх складанні;

− провести експериментальне дослідження програмного застосунка, що дозволить підтвердити адекватність розроблених моделей та методу.

Об'єктом дослідження є процес підтримки прийняття рішень для експертиз систем технічного захисту інформації.

Предметом дослідження є моделі, методи та засоби підтримки прийняття рішень для експертиз систем технічного захисту інформації.

Методи дослідження. Проведені дослідження базуються на сучасних методах представлення і обробки знань, прийняття рішень, теорії алгоритмів, об'єктно-орієнтованого програмування.

Наукова новизна одержаних результатів полягає в наступному:

− *вперше* розроблено декомпозиційну модель представлення смислових констант та змінних, яка за рахунок сформованих множин вхідних та вихідних документів р-го проекту, а також множини смислових блоків, смислових констант та змінних р-го проекту дозволяє формувати базові шаблони вихідних документів;

− *вперше* розроблено модель параметрів, яка за рахунок визначення рівнів функціональних послуг безпеки, що реалізовані в комплексній системі захисту інформації об'єкта експертизи, визначення повноти та несуперечності профілю, ідентифікації опису

функціональних послуг безпеки у вихідних документах дозволяє у формальному вигляді сформувати необхідний набір величин для реалізації процесу ідентифікації функціонального профілю захисту в комп'ютерних системах;

– *вперше* розроблено метод ідентифікації функціонального профілю захисту, який за рахунок кроків формування множин первинних та вторинних функціональних послуг безпеки, множин їх об'єднання у функціональному профілі захисту, множин порядку за індексами елементів та множин базового функціонального профілю захисту, дозволяє реалізувати процес генерування функціонального профілю захисту та перевірку його вимог щодо функцій захисту (послуг безпеки) та гарантій;

– *вперше запропоновано* структурну модель системи підтримки прийняття рішень, яка за рахунок взаємопов'язаних баз даних смислових змінних, множини критеріїв, функціональних профілів захисту та шаблонів документів, а також модулів виокремлення смислових змінних, взаємодії з експертом та ідентифікації функціонального профілю захисту дозволяє автоматизувати процес складання вихідних документів з шаблонів документів.

Практичне значення одержаних результатів.

Отримані в дисертаційній роботі результати можуть бути використані для побудови системи підтримки прийняття рішень (СППР) для проведення експертиз систем технічного захисту інформації.

Практична цінність роботи полягає в наступному:

– на основі запропонованого структурного рішення СППР при проведенні державних експертиз КСЗІ було розроблено алгоритмічне забезпечення для реалізації відповідного програмного застосунка;

– на основі запропонованого алгоритму був реалізовано програмний застосунок СППР, що виконує перевірку ФПЗ за трьома формальними ознаками нормативного документу;

– результати дисертаційного дослідження впроваджено у діяльність ТОВ "СОФТЛАЙН ІТ" та Інституту кібернетики ім. В.М. Глушкова, а також використовуються у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету.

Особистий внесок здобувача. Всі основні результати дисертаційної роботи отримані здобувачем самостійно. У роботах, опублікованих із співавторами, здобувачу належить: [2, 3, 10] – проведено аналіз використання COM-технологій при проведенні експертиз на відповідність НД ТЗІ, методик проведення експертизи комплексних систем захисту інформації, а також тестування систем підтримки прийняття рішень орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки; [17, 18, 23-26] – розробка метода та моделей СППР при проведенні експертиз КСЗІ, а також структури українського національного грід з точки зору забезпечення потреб безпеки в грід-середовищі; [13, 14] – проведено аналіз актуальності побудови методик оцінки якісних характеристик тестів, тестування СППР орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки, а також розробка тестів для аналізу інформаційної безпеки національної грід-інфраструктури; [27-29] – алгоритмічна та програмна реалізація перевірки повноти та несуперечності функціонального профілю захисту.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на науково-технічних конференціях, семінарах, серед

яких: науково-технічна конференція молодих вчених та спеціалістів (Київ 2013 р., 2014 р., 2015р., 2016р., 2019р.); VI міжнародна наукова конференція “Моделювання-2018” (Київ 2018р.) ; IX науково-технічна конференція “Безпека інформаційних технологій (“Information Technology Security”, ITSEC-2019”)” (Шарм-ель-Шейх 2019р.); X науково-технічна конференція “Безпека інформаційних технологій (“Information Technology Security”, ITSEC-2020”)” (Шарм-ель-Шейх 2020р.); V міжнародна науково-практична конференція “Актуальні питання забезпечення кібербезпеки та захисту інформації” (Верхнє Студене 2020р.); міжнародна наукова інтернет-конференція “Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення” (Тернопіль 2019р.); науково-практична конференція "Безпека енергетики в епоху цифрової трансформації” (Київ 2019р.).

Публікації. Основні положення дисертації опубліковано у 29 наукових праць, у тому числі 1 патент, 5 статей у наукових журналах, що індексуються в науко-метричних базах, 10 статей у фахових наукових виданнях України та 13 тез доповідей і матеріалів конференцій.

Структура роботи та її обсяг. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 141 сторінку основного тексту, 37 рисунків, 12 таблиць, 42 сторінки додатків. Список літератури містить 116 найменувань і займає 12 сторінок. Загальний обсяг роботи 208 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** представлена загальна характеристика роботи, обґрунтована актуальність, сформульовані мета і задачі досліджень, відображені наукова новизна та практична цінність отриманих результатів, наведено дані про їх апробацію та впровадження.

У **першому розділі** виконано аналіз вітчизняної та зарубіжної літератури за темою дисертаційної роботи.

Таблиця1

Зведені дані

СППР	Характеристики СППР									
	SHA	ON	DOC	PC	AHP	FAP	UKS	BAS	KOCK	PAR	ANU	PCM
ACRS	–	+	–	+	+	–	–	+	–	–	+	+
Criterium Decision	–	–	+	–	+	–	–	+	–	–	+	+
DecisionLens	–	–	–	+	+	–	–	+	–	–	+	+
Expert Choice	–	–	–	+	+	–	–	+	–	–	+	+
MakeItRational	–	–	+	+	+	–	–	+	–	–	+	+
MindDecider	–	–	–	+	+	–	–	+	–	–	+	+
GroupSystems	–	+	–	–	+	–	–	–	+	–	+	+
DSSNeoTron	–	–	–	–	+	–	–	+	–	–	+	–
«Выбор»	–	–	–	+	+	–	–	+	+	–	+	–
«Император»	–	–	+	+	+	–	–	+	+	–	+	+
1000Minds	–	–	–	+	+	–	–	+	–	–	+	–
Aaron K-Pacs	–	–	–	+	+	–	–	+	+	–	+	+
PBL ScoreCard	–	–	–	+	+	–	–	–	–	–	+	+
Blaze Advisor	–	+	–	+	+	–	–	+	–	–	+	+
Host Reporting	–	–	–	+	+	–	–	+	–	–	+	–
LOGICNETS	–	–	–	+	+	–	–	+	+	–	+	–
Analytica Optimizer	–	–	–	+	+	–	–	+	+	–	+	+
StrataJazz	–	–	–	+	+	–	–	+	–	–	+	–

Проведено аналіз наукових основ проведення експертиз грід-засобів на відповідність вимогам НД ТЗІ. Також проведено аналіз моделей та методів проведення експертиз на відповідність вимогам НД ТЗІ. Щодо цього були проаналізовані існуючі моделі, методи, методики проведення державних експертиз, що дасть можливість уніфікувати процес дослідження існуючих підходів до проведення експертиз, а також підвищити ефективність здійснення їх вибору.

Було проведено аналіз методів, моделей та засобів сучасних СППР (табл.1) за наступними характеристиками: SHA визначає модель формування шаблонів документів; ON визначає можливість системи працювати в режимі он-лайн; DOC визначає можливість обробки документів; PC визначає платформу ПК; AHP

(analytic hierarchy process) визначає метод аналізу ієрархій; FPP визначає метод ідентифікації ФПЗ; UKR визначає наявність україномовної версії; HAS (Help system availability) визначає наявність довідкової системи; BOCR (benefit, opportunity, cost, and risk) framework for decision analysis визначає наявність фрэймворк по аналізу рішень; PAR визначає модель параметрів для ідентифікації ФПЗ; AIIU (Availability of interactive einteractions with users) визначає наявність інтерактивної взаємодії з користувачем; PCM (The presence of contextual menu) визначає наявність контекстного меню.

Було з'ясовано, що жодна з них не може використовуватись з метою аналізу документів державних експертиз КСЗІ. Тільки СППР Criterium Decision та MakeitRational мають функціональні можливості по обробці документів.

У зв'язку з неповним виконанням завдань перерахованих систем, які мають місце при організації СППР на відповідність НД ТЗІ, постає необхідність в розробці нових методів та моделей, які б виконували поставлене завдання по автоматизації процесу створення вихідних документів та зменшення кількості помилок при їх складанні.

У другому розділі запропоновані нові моделі декомпозиційного представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ, параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах та метод ідентифікації функціонального профілю захисту.

Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ визначає спосіб формування шаблонів вихідних документів.

Вона складається з базових множин проектів документів експертизи ТЗІ, множин смислових блоків (СБ) вихідних документів та структури взаємозв'язку змісту шаблона з множинами смислових змінних.

Базові множини проектів документів експертизи ТЗІ

Введемо множину всіх можливих документів

$$\mathbf{Doc}=\left\{\bigcup_{p=1}^{m}\mathbf{Doc}_p\right\}=\left\{\mathbf{Doc}_1,\mathbf{Doc}_2,...,\mathbf{Doc}_m\right\}, \quad (1)$$

p-го ($p=\overline{1,m}$) проекту, а *m* – кількість можливих проектів.

Далі, використовуючи (1) визначимо

$$\mathbf{Doc}_p=\left\{\mathbf{Doc}_p^{out},\mathbf{Doc}_p^{in}\right\}, \quad (2)$$

де $\mathbf{Doc}_p^{out}$, $\mathbf{Doc}_p^{in}$ – відповідно множини вихідних та вхідних документів *p*-го проекту підмножини $\mathbf{Doc}_p$.

З урахуванням (2) визначимо

$$\mathbf{Doc}_p^{out}=\left\{\bigcup_{i=1}^{z}\mathbf{Doc}_{p,i}^{out}\right\}=\left\{\mathbf{Doc}_{p,1}^{out},\mathbf{Doc}_{p,2}^{out},...,\mathbf{Doc}_{p,z}^{out}\right\}, \quad (3)$$

де $\mathbf{Doc}_{p,i}^{out}$ – підмножина СБ *i* -го ($i=\overline{1,z}$) вихідного документа *p*-го проекту, а *z* – кількість вихідних документів.

Використовуючи (3) сформуємо множину вхідних документів

$$\mathbf{Doc}_p^{in}=\left\{\bigcup_{l=1}^{v}\mathbf{Doc}_{p,l}^{in}\right\}=\left\{\mathbf{Doc}_{p,1}^{in},\mathbf{Doc}_{p,2}^{in},...,\mathbf{Doc}_{p,v}^{in}\right\}, \quad (4)$$

де $\mathbf{Doc}^{\mathbf{in}}_{\mathbf{p,l}}$ – підмножина СБ l -го ($\mathrm{l}=\overline{1,\mathrm{v}}$) вхідного документа p-го проекту, а v – кількість вхідних документів.

Далі, використовуючи (3) визначимо підмножину СБ i -го ($\mathrm{i}=\overline{1,\mathrm{z}}$) вихідного документу p-го ($p=\overline{1,m}$) проекту

$$\mathbf{Doc}^{\mathbf{out}}_{\mathbf{p,i}}=\left\{\bigcup_{\mathbf{i=1}}^{\mathbf{z}}\left\{\bigcup_{\mathbf{j=1}}^{\mathbf{S_i}}\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,j}}\right\}\right\}=\bigcup_{\mathbf{i=1}}^{\mathbf{z}}\left\{\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,1}},\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,2}},\ldots,\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,S_z}}\right\}=\left\{\left\{\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,1,1}},\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,1,2}},\ldots,\right.\right. \tag{5}$$

$$\left.\left.,\ldots,\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,1,S_1}}\right\},\left\{\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,2,1}},\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,2,2}},\ldots,\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,2,S_2}}\right\},\ldots,\left\{\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,z,1}},\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,z,2}},\ldots,\mathbf{SB}^{\mathbf{out}}_{\mathbf{P,z,S_z}}\right\},\right.$$

де $\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,j}}$ – СБ вихідного документу p-го проекту, S_i – кількість СБ i -го ($\mathrm{i}=\overline{1,\mathrm{z}}$) вихідного документу.

Множини СБ вихідних документів.

Визначимо принцип формування змісту СБ. Кожен СБ складається з множини смислових змінних (СЗ) і констант (СК), де СК – це стійка смислова конструкція, час існування якої виходить за межі проведення державної експертизи КСЗІ. В свою чергу, СЗ – це смислова конструкція, час існування якої відбувається протягом державної експертизи КСЗІ.

Тоді, вираз (5) для СБ вихідного документу $\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,j}}$ має вигляд

$$\mathbf{SB}^{\mathbf{out}}_{\mathbf{p,i,j}}=\left\{\bigcup_{\mathbf{i=1}}^{\mathbf{z}}\left\{\bigcup_{\mathbf{j=1}}^{\mathbf{S_i}}\left\{\left\{\bigcup_{\mathbf{a=1}}^{\mathbf{t_{i,j}}}\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,j,a}}\right\},\left\{\bigcup_{\mathbf{b=1}}^{\mathbf{r_{i,j}}}\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,j,b}}\right\}\right\}\right\}\right\}=\bigcup_{\mathbf{i=1}}^{\mathbf{z}}\bigcup_{\mathbf{j=1}}^{\mathbf{S_i}}\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,j,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,j,2}},\ldots,\right.\right.$$

$$\left.\left.,\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,j,t_{i,j}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,j,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,j,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,j,r_{i,j}}}\right\}\right\}=\bigcup_{\mathbf{i=1}}^{\mathbf{z}}\left\{\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,1,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,1,2}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,1t_{i,1}}}\right\},\right.\right.$$

$$\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,1,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,1,2}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,1,t_{i,1}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,1,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,1,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,1r_{i,1}}}\right\}\right\},\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,2,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,2,2}},\ldots,\right.\right.$$

$$\left.\left.,\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,2t_{i,2}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,2,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,2,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,2r_{i,2}}}\right\}\right\},\ldots,\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,S_i,t_{i,1}}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,S_i,t_{i,2}}},\ldots,\right.\right.$$

$$\left.\left.,\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,i,S_i,t_{i,S_i}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,S_i,r_{i,1}}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,S_i,r_{i,2}}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,i,S_i,r_{i,S_i}}}\right\}\right\}=\left\{\left\{\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1,1,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1,1,2}},\ldots,\right.\right.\right.\right.$$

$$\left.\left.\left.\left.,\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1,1t_{1,1}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1,1,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1,1,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1,1r_{1,1}}}\right\}\right\},\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1,2,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1,2,2}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1,2t_{1,2}}}\right\},\right.\right.$$

$$\left.\left.\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1,2,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1,2,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1S_1,r_{1,2}}}\right\}\right\},\ldots,\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1S_1,t_{1,1}}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1S_1,t_{1,2}}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,1S_1,t_{1,S_1}}}\right\},\right.\right. \tag{6}$$

$$\left.\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1S_1,r_{1,1}}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1S_1,r_{1,2}}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,1S_1,r_{1,S_1}}}\right\}\right\},\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2,1,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2,1,2}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2,1t_{2,1}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2,1,1}},\right.\right.$$

$$\left.\left.\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2,1,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2,1r_{2,1}}}\right\}\right\},\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2,2,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2,2,2}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2,2t_{2,2}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2,2,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2,2,2}},\ldots,\right.\right.$$

$$\left.\left.,\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2,2r_{2,2}}}\right\}\right\},\ldots,\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2S_2,t_{2,1}}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2S_2,t_{2,2}}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{p,2S_2,t_{2S_2}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2S_2,r_{2,1}}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2S_2,r_{2,2}}},\ldots,\right.\right.$$

$$\left.\left.,\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,2S_2,r_{2S_2}}}\right\}\right\},\ldots,\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,1,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,1,2}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,1t_{z,1}}}\right\},\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{pz,1,1}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{pz,1,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{pz,1r_{z,1}}}\right\}\right\},$$

$$\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,2,1}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,2,2}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{pz,2r_{z,2}}}\right\}\right\},\ldots,\left\{\left\{\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,S_z,t_{z,1}}},\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,S_z,t_{z,2}}},\ldots,\mathbf{SC}^{\mathbf{out}}_{\mathbf{pz,S_z,t_{z,S_z}}}\right\},\right.\right.$$

$$\left.\left.\left\{\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,z,S_z,r_{z,1}}},\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,z,S_z,r_{z,2}}},\ldots,\mathbf{SV}^{\mathbf{out}}_{\mathbf{p,z,S_z,r_{z,Sz}}}\right\}\right\}\right\}\right\},$$

де $SV_{p i,j,b}^{out}$ – СЗ вихідного документу *p*-го проекту, $SC_{p i,j,a}^{out}$ – СК вихідного документу *p*-го проекту, $t_{i,j}$ – ідентифікатор СК j -го смислового блоку S_i -ої кількості СБ i -го ($i=\overline{1,z}$) вихідного документу p -го проекту, а $r_{i,j}$ – ідентифікатор СЗ j -го смислового блоку S_i -ої кількості СБ i-го ($i=\overline{1,z}$) вихідного документу p -го проекту.

Для вирішення задачі ідентифікації ФПЗ необхідно здійснити: визначення рівнів ФПБ, реалізованих в КСЗІ об'єкта експертизи; визначення повноти та несуперечності профілю; ідентифікацію опису ФПБ у вихідних документах. З урахуванням цього пропонується модель параметрів для ідентифікації ФПЗ в комп'рних системах (КС).

Визначення множини критеріїв

Сформуємо множину усіх критеріїв захищеності інформації

$$\mathbf{МК}=\left\{\bigcup_{q=1}^{w}\mathbf{МК}_{q}\right\}=\{\mathbf{МК}_{1},\ \mathbf{МК}_{2},...,\mathbf{МК}_{w}\}. \tag{7}$$

Визначення елементів множин критеріїв

Далі, на основі (7) визначимо елементи $\mathbf{МК}_q$-ї множини критеріїв

$$\mathbf{МК}_{q}=\left\{\bigcup_{e=1}^{w_q}\mathbf{МК}_{q,e}\right\}=\{\mathbf{МК}_{q,1},\mathbf{МК}_{q,2},...,\mathbf{МК}_{q,w_q}\}. \tag{8}$$

де $\mathbf{МК}_{q,e}\subseteq\mathbf{МК}_{q}$ ($e=\overline{1,w_q}$) – e -й елемент $\mathbf{МК}_q$-ї множини критеріїв, а w_q їх кількість.

Таким чином, (7) з урахуванням (8) представимо в наступному вигляді:

$$\mathbf{МК}=\left\{\bigcup_{q=1}^{w}\mathbf{МК}_{q}\right\}=\left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\mathbf{МК}_{q,e}\right\}\right\}=\{\{\mathbf{МК}_{1,1},\mathbf{МК}_{1,2},...,\mathbf{МК}_{1,w_1}\},\ \{\mathbf{МК}_{2,1},\ \mathbf{МК}_{2,2},...,\mathbf{МК}_{2,w_2}\},...,\ \{\mathbf{МК}_{w,1},\mathbf{МК}_{w,2},...,\mathbf{МК}_{w,w_w}\}\}. \tag{9}$$

Визначення рівнів елементів множин критеріїв

Далі, на основі (9) визначимо рівень кожного $\mathbf{МК}_{q,e}$-го елемента $\mathbf{МК}_q$-ї множини критеріїв

$$\mathbf{МК}_{q,e}=\left\{\bigcup_{y=1}^{w_{q,e}}\mathbf{МК}_{q,e,y}\right\}=\{\mathbf{МК}_{q,e,1},\mathbf{МК}_{q,e,2},...,\mathbf{МК}_{q,e,w_{q,e}}\}, \tag{10}$$

де $\mathbf{МК}_{q,e,y}\subseteq\mathbf{МК}_{q,e}$ ($y=\overline{1,w_{q,e}}$) – y -й рівень $\mathbf{МК}_{q,e}$-го елемента $\mathbf{МК}_q$-ї множини критеріїв, а $w_{q,e}$ їх максимальний рівень.

Таким чином, (10) з урахуванням (9) має вигляд:

$$\mathbf{МК}=\left\{\bigcup_{q=1}^{w}\mathbf{МК}_{q}\right\}=\left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\mathbf{МК}_{q,e}\right\}\right\}=\left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\left\{\bigcup_{y=1}^{w_{q,e}}\mathbf{МК}_{q,e,y}\right\}\right\}\right\}=\left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\{\mathbf{МК}_{q,e,1},\mathbf{МК}_{q,e,2},...,\mathbf{МК}_{q,e,w_{q,e}}\}\right\}\right\}=\left\{\bigcup_{q=1}^{w}\{\{\mathbf{МК}_{q,1,1},\mathbf{МК}_{q,1,2},...,\mathbf{МК}_{q,1,w_{q,1}}\}\right\},\ \{\{\{\mathbf{МК}_{1,1,1},$$

$$\begin{aligned}&МК_{1,1,2},...,МК_{1,1,w_{1,1}}\}\},\ \{МК_{1,2,1},\ МК_{1,2,2},...,МК_{1,2,w_{1,2}}\},...,\\&\{МК_{1,w_1,1},\ МК_{1,w_1,2},...,\ МК_{1,w_1,w_{1,w_1}}\}\},\\&\{\{МК_{2,1,1},МК_{2,1,2},...,МК_{2,1,w_{2,1}}\},\ \{МК_{2,2,1},МК_{2,2,2},...,\ МК_{2,2,w_{2,2}}\}\\&\{МК_{2,w_2,1},МК_{2,w_2,2},...,МК_{2,w_2,w_{2,w_2}}\}\},..,\ \{\{МК_{w,1,1},МК_{w,1,2},...,\\&МК_{w,1,w_{w,1}}\},\ \{МК_{w,2,1},МК_{w,2,2},...,МК_{w,2,w_{w,2}}\},...,\ \{МК_{w,w_w,1},\\&МК_{w,w_w,2},...,\ МК_{w,w_w,w_{w,w_w}}\}\}\}.\end{aligned} \quad (11)$$

Для вирішення задачі ідентифікації ФПЗ необхідно здійснити: визначення рівнів ФПБ, реалізованих в КСЗІ об'єкта експертизи; визначення повноти та несуперечності профілю; ідентифікацію опису ФПБ у вихідних документах. Для визначення повноти та несуперечності слід враховувати правила побудови ФПЗ, а автоматизація цього процесу пов'язується з відповідними правилами. Таким чином, є нагальна необхідність в створенні методу, що дозволить автоматизувати процес генерування функціонального профілю захисту і перевірку його вимог щодо функцій захисту (послуг безпеки) та гарантій.

Для вирішення поставленого завдання пропонується метод ідентифікації ФПЗ, який засновується на процедурах, що реалізуються за допомогою п'яти кроків, пов'язаних з формуванням: множин первинних (**МП**) та вторинних (**МВ**) ФПБ; множини об'єднання (**МО**) **МП** і **МВ** в ФПЗ; множини порядку $\mathbf{МО}^{\mathbf{П}}_{\mathbf{р}}$ за індексами елементів $МК_{q,e,z}$; базового функціонального профілю захисту (**БЗ**).

Крок 1. Формування МП ФПБ.

Профіль **БЗ**, з огляду на об'єкт експертизи та вимог щодо безпечного обігу інформації, складається з **МП** та **МВ** ФПБ, де **МП** визначається експертом.

Як відомо, $МК_{q,e,z}$ $(z=\overline{1,w_{q,e}})$ є *z*-й рівень *e*-го елемента *q*-ї **МК**, а $w_{q,e}$ їх максимальний рівень. З урахуванням цього, на основі рішень експерта, визначимо **МП** ФПБ:

$$\mathbf{МП}_{\mathbf{р}}=\left\{\bigcup_{f=1}^{k}МП_{p,f}\right\}=\{МП_{p,1},МП_{p,2},...,МП_{p,k}\}, \quad (12)$$

де *k* – кількість первинних ФПБ *p*-го проекту, $f=\overline{1,k}$.

Крок 2. Формування МВ ФПБ.

Далі, сформуємо **МВ**, що складається з елементів **МК**. Для формування **МВ** введемо табличну функцію похідних елементів від $МП_{p,f}$, тобто **ФПЕ(**$МП_{p,f}$**)** здійснює відображення певних членів множини **МП** в один або більше елементів множини **МК**. Таким чином, **МВ** можна представити, як:

$$\begin{aligned}&\mathbf{МВ}_{\mathbf{р}}=\left\{\bigcup_{f=1}^{k}\mathbf{МВ}_{\mathbf{p,f}}\right\}=\left\{\bigcup_{f=1}^{k}\mathbf{ФПЕ(}\ МП_{p,f}\ \mathbf{)}\right\}=\{\mathbf{МВ}_{\mathbf{p,1}},\mathbf{МВ}_{\mathbf{p,2}},...,\mathbf{МВ}_{\mathbf{p,k}}\}=\\&\{\mathbf{ФПЕ(}\ МП_{p,1}\ \mathbf{)},\mathbf{ФПЕ(}\ МП_{p,2}\ \mathbf{)},...,\mathbf{ФПЕ(}\ МП_{p,k}\ \mathbf{)}\},\end{aligned} \quad (13)$$

де *k* – кількість функції від елементів **МВ** ФПБ *p*-го проекту.

Крок 3. Формування множини об'єднання (МО) ФПЗ в МП і МВ.

Для побудови **БЗ** необхідно сформувати проміжну множину **МО**, що об'єднує **МП** і **МВ** за формулою:

$$\mathbf{МО_р} = \mathbf{МП_р} \cup \mathbf{МВ_р} = \left\{ \bigcup_{f=1}^{k} МП_{p,f} \right\} \cup \left\{ \bigcup_{f=1}^{k} \mathbf{ФПЕ}(МП_{p,f}) \right\} = \{ МП_{p,1}, МП_{p,2}, ..., \quad (14)$$

$$..., МП_{p,k} \} \cup \{ \mathbf{ФПЕ}(МП_{p,1}), \mathbf{ФПЕ}(МП_{p,2}), ..., \mathbf{ФПЕ}(МП_{p,k}) \}.$$

Крок 4. Формування $\mathbf{МО_р^П}$ у вигляді множини порядку за індексами елементів $МК_{q,e,z}$.

Далі, сформуємо множину порядку за індексами:

$$\mathbf{МО_р^П} = \{ \{ МО^П_{1,1,1}, МО^П_{1,1,2}, ..., МО^П_{1,1,4} \}, \{ МО^П_{1,2,1}, МО^П_{1,2,2}, ..., МО^П_{1,2,4} \}, \{ МО^П_{1,3,1}, МО^П_{1,2,2}, ..., МО^П_{1,2,4} \}, \{ МО^П_{1,3,1}, МО^П_{1,3,2}, МО^П_{1,3,3} \}, \{ МО^П_{1,4,1} \}, \{ МО^П_{1,5,1}, МО^П_{1,5,2}, ...,$$
$$..., МО^П_{1,5,4} \}, \{ МО^П_{2,1,1}, МО^П_{2,1,2}, ..., МО^П_{2,1,4} \}, \{ МО^П_{2,2,1}, МО^П_{2,2,2}, ..., МО^П_{2,2,4} \},$$
$$\{ МО^П_{2,3,1}, МО^П_{2,3,2} \}, \{ МО^П_{2,4,1}, МО^П_{2,4,2}, МО^П_{2,4,3} \}, \{ МО^П_{3,1,1}, МО^П_{2,1,2}, МО^П_{3,1,3} \}, \quad (15)$$
$$\{ МО^П_{3,2,1}, МО^П_{2,2,2}, МО^П_{3,2,3} \}, \{ МО^П_{3,3,1}, МО^П_{2,3,2}, МО^П_{3,3,3} \}, \{ МО^П_{3,4,1}, МО^П_{3,4,2}, МО^П_{3,4,3} \},$$
$$\{ МО^П_{4,1,1}, МО^П_{4,1,2}, ..., МО^П_{4,1,5} \}, \{ МО^П_{4,2,1}, МО^П_{4,2,2} \}, \{ МО^П_{4,3,1}, МО^П_{4,3,2} \}, \{ МО^П_{4,4,1},$$
$$МО^П_{4,4,2}, МО^П_{4,4,3} \}, \{ МО^П_{4,5,1}, МО^П_{4,5,2}, МО^П_{4,5,3} \}, \{ МО^П_{4,6,1}, МО^П_{4,6,2}, МО^П_{4,6,3} \},$$
$$\{ МО^П_{4,7,1}, МО^П_{4,7,2}, МО^П_{4,7,3} \}, \{ МО^П_{4,8,1}, МО^П_{4,8,2} \}, \{ МО^П_{4,9,1}, МО^П_{4,9,2} \}, \{ МО^П_{5,1,1},$$
$$МО^П_{5,1,2}, ..., МО^П_{5,1,7} \} \}.$$

Крок 5. Формування БЗ

Цей крок реалізується шляхом мінімізації сформованої **МО** у вигляді множини порядку. Тобто, якщо:

$$\mathbf{МО_р^П} = \left\{ \bigcup_{q=1}^{w^p} \left\{ \bigcup_{e=1}^{w^p_q} \left\{ \bigcup_{z=1}^{w^p_{q,e}} МО^П_{q,e,z} \right\} \right\} \right\}, \quad (16)$$

де w^p, w^p_q і $w^p_{q,e}$, за аналогією з **МК**, є відповідно число елементів $\mathbf{МО_р^П}$ *p*-го проекту ($\overline{q=1,w^p}$), число елементів $\mathbf{МО_q^П}$-ї підмножини критеріїв *p*-го проекту ($\overline{e=1,w^p_q}$) і максимальний рівень $\mathbf{МО_{q,e}^П}$-го елемента $\mathbf{МО_q^П}$-ї множини критеріїв р-го проекту ($\overline{z=1,w^p_{q,e}}$), то

$$\mathbf{БЗ_р} = \mathbf{МО_р^{Пmin}} = \left\{ \bigcup_{q=1}^{w^p} \left\{ \bigcup_{e=1}^{w^p_q} \left\{ \bigvee_{z=1}^{w^p_{q,e}} МО^{Пmin}_{q,e,z} \right\} \right\} \right\} = \left\{ \bigcup_{q=1}^{w^p} \left\{ \bigcup_{e=1}^{w^p_q} МО^{Пmin}_{q,e,1} \vee, МО^{Пmin}_{q,e,2} \vee, ..., \right. \right.$$
$$\left. \left. ..., \vee МО^{Пmin}_{q,e,w^p_{q,e}} \right\} \right\} = \left\{ \bigcup_{q=1}^{w^p} \left\{ \left\{ МО^{Пmin}_{q,1,1} \vee, МО^{Пmin}_{q,1,2} \vee, ..., \vee МО^{Пmin}_{q,1,w^p_{q,1}} \right\} \right\}, \{ МО^{Пmin}_{q,2,1} \vee,$$

$$\left\{ MO^{\Pi\min}_{q,2,2} \vee,...,\vee MO^{\Pi\min}_{q,2,w^{p}_{q,2}} \right\},...,\left\{ MO^{\Pi\min}_{q,w^{p}_{q},1} \vee, MO^{\Pi\min}_{q,w^{p}_{q},2} \vee,...,\vee MO^{\Pi\min}_{q,w^{p}_{q},w^{p}_{q,w^{p}_{q}}} \right\}\Bigg\}\Bigg\}\Bigg\}=$$

$$\left\{\left\{\left\{ MO^{\Pi\min}_{1,1,1} \vee, MO^{\Pi\min}_{1,1,2} \vee,...,\vee MO^{\Pi\min}_{1,1,w^{p}_{1,1}} \right\}, \left\{ MO^{\Pi\min}_{1,2,1} \vee, MO^{\Pi\min}_{1,2,2} \vee,...,\vee MO^{\Pi\min}_{1,2,w^{p}_{1,2}} \right\},...,\right.\right.$$

$$\left.\left\{ MO^{\Pi\min}_{1,w^{p}_{1},1} \vee, MO^{\Pi\min}_{1,w^{p}_{1},2} \vee,...,\vee MO^{\Pi\min}_{1,w^{p}_{1},w^{p}_{1,w^{p}_{1}}} \right\}\right\}, \left\{ MO^{\Pi\min}_{2,1,1} \vee, MO^{\Pi\min}_{2,1,2} \vee,... \right. \quad (17)$$

$$\left.,...,\vee MO^{\Pi\min}_{2,1,w^{p}_{2,2}} \right\}, \left\{ MO^{\Pi\min}_{2,2,1} \vee, MO^{\Pi\min}_{2,2,2} \vee,...,\vee MO^{\Pi\min}_{2,2,w^{p}_{2,2}} \right\},...,$$

$$\left\{ MO^{\Pi\min}_{2,w^{p}_{2},1} \vee, MO^{\Pi\min}_{2,w^{p}_{2},2} \vee,...,\vee MO^{\Pi\min}_{2,w^{p}_{2},w^{p}_{2,w^{p}_{2}}} \right\}\Bigg\},...,$$

$$\left\{\left\{ MO^{\Pi\min}_{w^{p},1,1} \vee, MO^{\Pi\min}_{w^{p},1,2} \vee,...,\vee MO^{\Pi\min}_{w^{p},1,w^{p}_{w^{p},1}} \right\},\right.$$

$$\left\{ MO^{\Pi\min}_{w^{p},2,1} \vee, MO^{\Pi\min}_{w^{p},2,2} \vee,...,\vee MO^{\Pi\min}_{w^{p},2,w^{p}_{w^{p},2}} \right\},.., \left\{ MO^{\Pi\min}_{w^{p},w^{p},w^{p}_{w^{p},1}} \vee, MO^{\Pi\min}_{w^{p},w^{p},w^{p}_{w^{p},2}} \vee,.., \right.$$

$$\left.\left.\left.,...,\vee MO^{\Pi\min}_{w^{p},w^{p}_{w^{p}},w^{p}_{w^{p},w^{p}}} \right\}\right\}\right\}.$$

Розробка наведених моделей та методу забезпечила можливість створення алгоритмічного забезпечення для реалізації відповідного програмного застосунка.

У третьому розділі була запропонована структурна модель СППР та алгоритми роботи програмного застосунка модуля ідентифікації функціонального профілю захисту (МІФПЗ).

Розробимо структурну модель (див. рис. 1), яка складається з модулей: МІФПЗ; виокремлення смислових змінних (МВСЗ); взаємодії з експертом (МВЕ). Також, до складу СППР входять бази даних (БД): смислових змінних (БДСЗ); множини критеріїв (БДМК); шаблонів вихідних документів (БДШВД) та функціонального профілю захисту (БДФПЗ).

Модуль МІФПЗ, за рахунок проведеного аналізу $\mathbf{МК}_{\mathbf{q,e,z}}$ з $\mathbf{Doc}_{\mathbf{p}}$, реалізує процес ідентифікації ФПЗ $\mathbf{БЗ}_{\mathbf{p}}$ шляхом формування за допомогою п'яти кроків: 1) $\mathbf{МП}_{\mathbf{p}}$ ФПБ; 2) $\mathbf{МВ}_{\mathbf{p}}$ ФПБ; 3) **МО** ФПЗ в $\mathbf{МП}_{\mathbf{p}}$ і $\mathbf{МВ}_{\mathbf{p}}$; 4) $\mathbf{МО}^{\mathbf{П}}_{\mathbf{p}}$ у вигляді множини порядку за індексами елементів $\mathbf{МК}_{\mathbf{q,e,z}}(z=\overline{1,w_{q,e}})$; 5) $\mathbf{БЗ}_{\mathbf{p}}$.

Модуль МВСЗ призначення для визначення $SV^{in}_{p,i,j,b}$ p-го ($p=\overline{1,m}$, m – кількість можливих проектів) проекту з $\mathbf{Doc}^{\mathbf{in}}_{\mathbf{p}}$. Визначення $SV^{in}_{p,i,j,b}$ відбувається шляхом взаємодії експерта з інтерфейсом СППР за допомогою підказок.

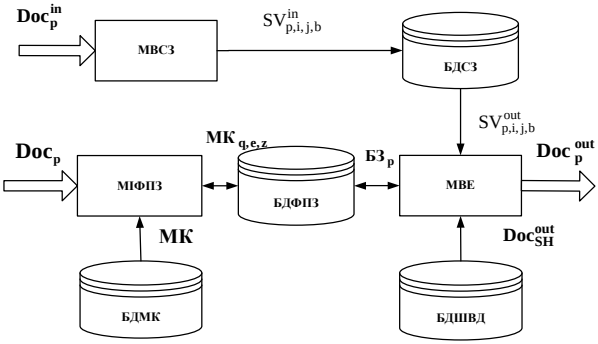

Рис.1. Структурна модель СППР для реалізації експертиз КСЗІ.

Модуль МВЕ призначений для заповнення $\mathbf{Doc}_{SH}^{out}$ за участю експерта, який керує процесом генерування вихідних документів $\mathbf{Doc}_p^{out}$ з $\mathbf{Doc}_{SH}^{out}$ за допомогою відповідного інтерфейсу програми, аналізує $\mathbf{МК}_{q,e,z}$ з $\mathbf{Doc}_p$, приймає участь у наповненні шаблонів $\mathbf{Doc}_{SH}^{out}$ смисловими змінними $SV_{p,i,j,b}^{out}$.

База БДСЗ містить множину смислових змінних $SV_{p,i,j,b}^{out}$, що були сформовані у процесі роботи модуля МВСЗ по виокремленню $SV_{p,i,j,b}^{in}$.

До складу БДМК входять елементи множини усіх критеріїв захищеності інформації $\mathbf{МК}_{q,e,y}$, де $\mathbf{МК}_{q,e,y} \subseteq \mathbf{МК}_{q,e}$ $(y = \overline{1, w_{q,e}})$ – *y*-й рівень $\mathbf{МК}_{q,e}$-го елемента $\mathbf{МК}_q$-ї множини критеріїв, а $w_{q,e}$ їх максимальний рівень, який аналізує модуль МІФПЗ на предмет відповідності ФПЗ.

База БДШВД містить шаблони вихідних документів $\mathbf{Doc}_{SH}^{out}$, які мають у своєму складі смислові константи $SC_{p,i,j,a}^{out}$, а також низку елементів, що становлять основу документа: графіка, разом з призначеними атрибутами формату; параметри друкованої сторінки; список доступних стилів; макроси; елементи автотексту для вставки текстових або графічних фрагментів; панелі інструментів користувача; меню поєднання клавіш.

База БДФПЗ містить множину критеріїв $\mathbf{МК}_{q,e,z}$ для кожного проекту, які виокремлюються з множини документів $\mathbf{Doc}_p$. Далі, за допомогою експерта та МІФПЗ, відбувається перевірка $\mathbf{МК}_{q,e,z}$ вимогам та складання $\mathbf{БЗ}_p$.

Проведення державних експертиз КСЗІ, відповідно до алгоритму функціонування СППР (див. рис.2), здійснюється за допомогою трьох процедур: виокремлення та запис смислових змінних $SV_{p,i,j,b}^{in}$ до БДСЗ; формування контенту на основі смислових змінних і шаблонів $\mathbf{Doc}_{SH}^{out}$; ідентифікація функціонального профілю захисту.

Процес роботи починається з аналізу вхідних документів *p*-го проекту $\mathbf{Doc}_{\mathbf{p}}^{\mathbf{in}}$ на предмет наявності в них $SV_{p,i,j,b}^{in}$ (див. рис. 2, вершини 2-3)**.** Якщо вони є, то відбувається відкриття БДСЗ та запис відповідних $SV_{p,i,j,b}^{in}$ у БД (див. рис. 2, вершини 4-5).

Далі, відбувається відкриття шаблонів вихідних документів (див. рис. 2, вершини 6-7) для формування контенту на основі відповідних смислових змінних (див. рис. 2, вершини 8-9). У результаті наповнення шаблонів отримаємо вихідний документ *p*-го проекту $\mathbf{Doc}_{\mathbf{p}}^{\mathbf{out}}$ (див. рис. 2, вершина 10).

Далі, здійснюємо аналіз ФПЗ на предмет відповідності його формальним ознакам НД ТЗІ та аналіз вихідного документа *p*-го проекту $\mathbf{Doc}_{\mathbf{p}}^{\mathbf{out}}$ на предмет наявності ФПЗ (див. рис. 2, вершини 11-13). Таким чином, за участю експерта формується $\mathbf{МП_p}$ для *p*-го проекту (див. рис. 2, вершина 14).

Після створення групи ФПБ перевіряється наявність похідних від цих ФПБ (див. рис.2, вершина16). Якщо експертом прийнято рішення у сформованій **МВ** підвищити окремі рівні ФПБ (див. рис. 2, вершини 16-17), то з **МВ** вилучаються відповідні рівні елементів **МК** та об'єднуються з множиною значень табличної функції **ФПЕ** від кожного з вилучених елементів.

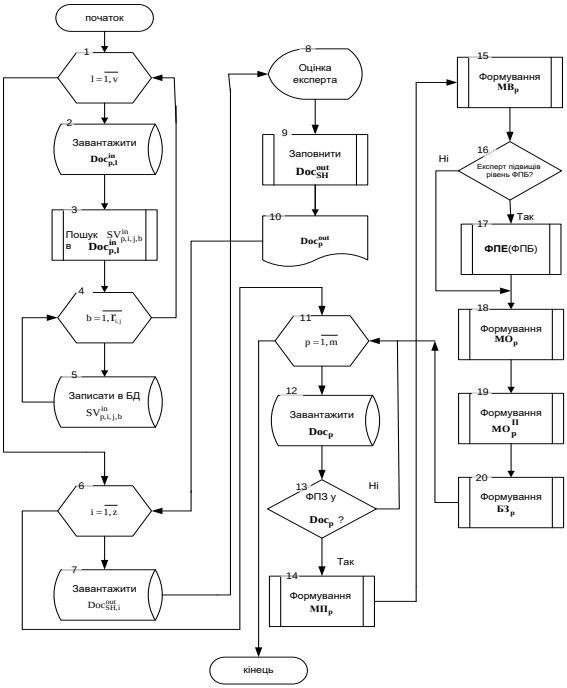

Рис.2. Алгоритм роботи СППР при проведенні державних експертиз КСЗІ.

Далі, формується проміжна множина **МО**, що об'єднує **МП** і **МВ** (див. рис. 2, вершина 18), яка упорядковується за індексами $\mathbf{МО}_{\mathbf{p}}^{\mathbf{П}}$ (див. рис. 2, вершина 19) та мінімізується (див. рис. 2, вершина 20).

Для реалізації МІФПЗ розробимо алгоритмічне забезпечення, яке (відповідно до запропонованої структурної моделі СППР) можна застосовувати в процесі проведення державних експертиз КСЗІ (див. рис. 3). Основою МІФПЗ є модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах. В основу алгоритма реалізації МІФПЗ закладено базовий клас DocumentEngine, що поєднує низку наступних зумовлених процесів (методів класу):

RegularExpressionFind (Пошук $\mathbf{БЗ}_{\mathbf{p}}$ $(p=\overline{1,m})$ та виклик FindNS, FindDuplicate, FindLinks);

FindNS (Ініціалізація МП ФПБ для НЦ рівня визначеного експертом. Відповідно до НД ТЗІ повинен містити ФПБ НЦ рівня 1);

FindDuplicate (Перевірка наявності в ФПЗ ФПБ, які повторюються). Реалізується шляхом мінімізації сформованої МО у вигляді множини порядку);

FindLinks (Формування МВ) та перевірка наявності похідних елементів від $МП_{p,f}$).

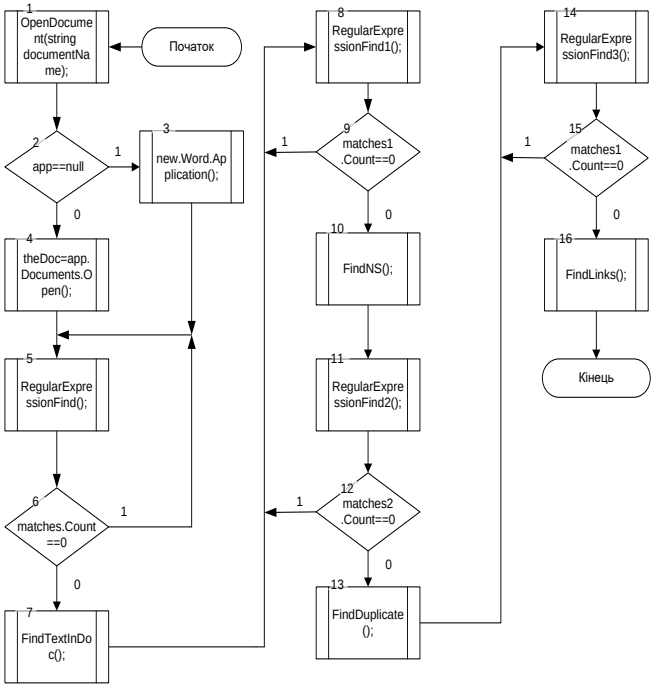

Рис.3 Алгоритм реалізації МІФПЗ СППР

Таким чином, була запропонована структурна модель, алгоритми роботи СППР та реалізації МІФПЗ, що дало можливість автоматизувати процес проведення експертизи та виявлення невідповідностей при формуванні ФПЗ.

Четвертий розділ присвячений оцінюванню часу проведення експертизи, результатам моделювання та аналізу адекватності отриманих результатів.

Державна експертиза КСЗІ триває шість місяців та передбачає виконання таких етапів експертних робіт:

– первинна обробка запиту на проведення експертизи, вибір та узгодження експерта ($\mathbf{T_1}$ = 2 тижні);

– оформлення договору на проведення експертизи та передача первинної документації ($\mathbf{T_2}$ = 2 тижні);

– аналіз первинної документації та розробка програми та методики проведення експертизи ($\mathbf{T_3}$ = 2 місяці);

– затвердження документу «Програма та методика» та розробка тестів ($\mathbf{T_4}$ = 2 тижня);

– проведення випробувань ($\mathbf{T_5}$ = 1 місяць);

– розробка вихідних документів ($\mathbf{T_6}$ = 1 місяць).

– затвердження вихідних документів ($\mathbf{T_7}$ = 2 тижні).

Дамо визначення для часу проведення державної експертизи

$$\mathbf{T_{ДЕ}} = \left\{ \bigcup_{t=1}^{m} \mathbf{T_t} \right\} = \{\mathbf{T_1}, \mathbf{T_2}, ..., \mathbf{T_m}\},$$

де $\mathbf{T_{ДЕ}}$ – загальний час проведення державної експертизи КСЗІ, m – кількість часових відрізків проведення дежавної експертизи КСЗІ.

Таким чином, з загального часу проведення державної експертизи КСЗІ, є можливість по скороченню часу тільки одного з етапів, а саме $\mathbf{T_6}$ – розробка вихідних документів.

За результатами роботи формується група документів – програма та методика проведення експертизи КСЗІ; перелік тестів; особлива думка експерта; протокол випробувань; атестат відповідності та експертний висновок.

Реалізація програмного застосунка МІФПЗ призначена для допомоги експерту при визначенні ФПЗ в документах Microsoft Word, а також допомогає експерту при аналізі ФПЗ на відповідність умовам заданим в нормативному документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», а саме: визначення контролю цілісності; поглинання старшими ФПЗ молодших; перевірки взаємопов'язаності ФПБ.

Програмний застосунок (див. рис. 4) було реалізовано на мові програмування C# в середовищі розробки VisualStudio 2005. При написанні програмного коду, використовувалась технологія MSOffice's COMInterop, а саме бібліотека Microsoft. Office. Interop. Word та базові бібліотеки мови програмування C#.

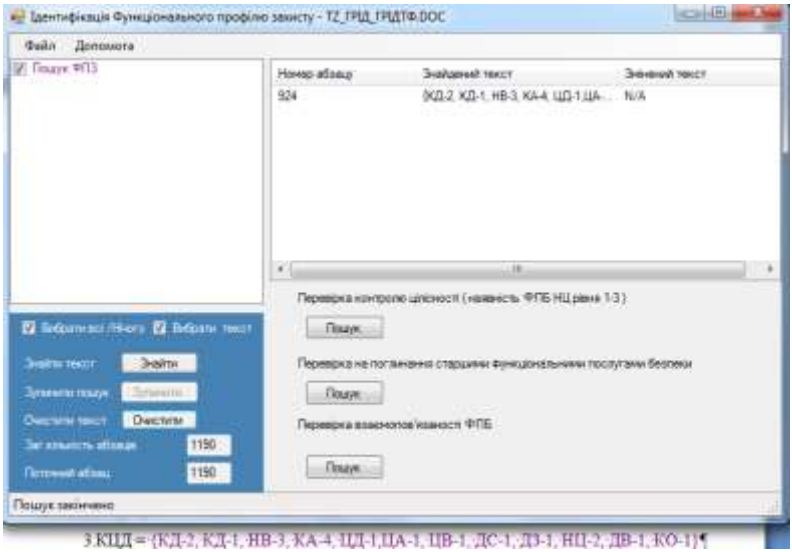

Рис.4 – Інтерфейс програми

Інтерфейс програмного застосунку представляє собою віконний додаток, який реалізований у вигляді GUI-програми. В ньому є такі елементи управління: віконне поле типу «Listbox» пошуку функціонального профілю захисту; кнопок: «Знайти», «Зупинити», «Очистити»; права частина екрану має віконне поле типу «ListView», в якому відображається номер абзацу, де було знайдено ФПЗ; три кнопки пошуку відповідності ФПЗ умовам нормативного документу НД ТЗІ 2.5-004-99; два віконних поля типу «TextBox», в одному з яких відображається загальна кількість абзаців документу, а в іншому полі — поточний абзац при обробці документа; віконне поле типу «statusStrip» має три положення: «Очікую», «Пошук розпочато», «Пошук закінчено»; два віконних поля типу «CheckedBox», в одному з яких є можливість зняти або обрати пошук ФПЗ, а в іншому полі — можливість переходу до заданої частини тексту пошуку ФПЗ; у віконному полі типу «menuStrip» розміщені дві вкладки: «Файл» та «Допомога».

Проведемо перевірку адекватності роботи програмного модуля методу ідентифікації функціональних послуг безпеки. З цією метою проаналізуємо типові ФПЗ з набору ФПЗ НД ТЗИ (див. рис. 5).

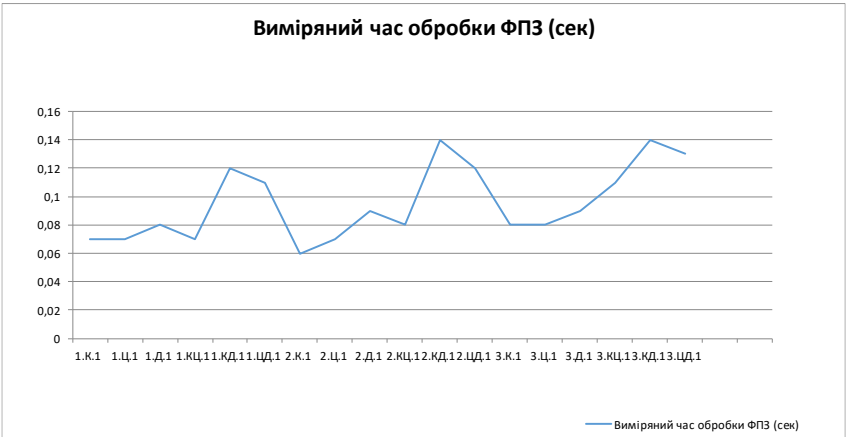

Рис.5. Час обробки ФПЗ.

Час обробки ФПЗ програмним застосунком виявило, що швидкість обробки залежить від кількості ФПБ в ФПЗ, а значення знаходяться в межах від 0.07 до 0.14 сек.

Проведений аналіз ФПЗ (див. рис.6), щодо усунення помилок трьох видів, показав, що найшвидше програма аналізує та усуває помилки другого виду.

Рис.6. Виміряний час обробки ФПЗ з помилками першого, другого та третього виду

Було з'ясовано, що програмний застосунок виявив усі помилки першого, другого та третього виду. Час, що знадобився програмному застосунку для аналізу та коректування ФПЗ за допомогою експерта, склав в межах від 0.15 до 4.12 сек. Усунення помилок першого та третього виду потребує втручання експерта. В свою чергу, помилки другого виду усуваються з ФПЗ автоматично. Час, який необхідний експерту для усунення помилок, у випадку з помилками третього виду, займає найбільший інтервал. Це можна спостерігати на графіку. Час, за який потрібно усунути помилки другого виду не набагато більший, ніж час за який були

проаналізовані ФПЗ, що не мають помилок. Для помилок третього виду було з'ясовано, що програмному застосунку необхідно більше часу для аналізу ФПЗ, так як усунення помилок відбувається за допомогою експерта. Час аналізу ФПЗ залежить від довжини ФПЗ, тобто від кількості ФПБ.

Таким чином, аналіз ФПЗ, щодо усунення помилок трьох видів, показав, що найшвидше програма аналізує та усуває помилки другого виду. Для помилок третього виду було з'ясовано, що програмі потрібно більше часу для аналізу та коректування ФПЗ за допомогою експерта. Час аналізу ФПЗ залежить від довжини ФПЗ, тобто від кількості ФПБ.

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

У додатках знаходяться акти впровадження результатів дисертаційної роботи і лістинги (коди) ПЗ.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв'язання актуальної науково-практичної задачі автоматизації процесу проведення експертиз комплексних систем захисту інформації та виявлення невідповідностей при формуванні функціональних профілів захисту.

У процесі виконання дисертаційної роботи отримані такі вагомі результати:

1. Проведено аналіз існуючих моделей, методів та засобів підтримки прийняття рішень. Було з'ясовано, що існуючи моделі, методи та засоби не задовольняють вимогам щодо систем підтримки прийняття рішень, які мали б змогу використовуватись при проведенні державних експертиз комплексних систем захисту інформації.

2. Вперше розроблено декомпозиційну модель представлення смислових констант та змінних, що дозволило формувати базові шаблони вихідних документів.

3. Вперше розроблено модель параметрів, що дозволило у формальному вигляді сформувати необхідний набір величин для реалізації процесу ідентифікації функціонального профілю захисту в комп'ютерних системах.

4. Вперше розроблено метод ідентифікації функціонального профілю захисту, що дозволило реалізувати процес генерування функціонального профілю захисту і перевірку його вимог щодо функцій захисту (послуг безпеки) та гарантій.

5. Вперше запропоновано структурну модель системи підтримки прийняття рішень, що дозволила автоматизувати процес складання вихідних документів за їх шаблонами.

6. Вперше розроблено алгоритмічне та програмне забезпечення, що дозволило автоматизувати процес проведення експертизи комплексної системи захисту інформації та виявлення невідповідностей при формуванні функціонального профілю захисту.

7. Проведені експериментальні дослідження програмного застосунку, впровадження та успішне практичне використання зазначених розробок підтвердили достовірність теоретичних гіпотез і висновків дисертаційної роботи.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. М. Шабан, «Аналіз існуючих методів захисту інформації в Grid-системах», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.69, С.140-144, 2013.

2.М. Шабан, А.Давиденко, «Разработка методики проведения экспертизы комплексных систем защиты информации», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.73, С.114-121, 2014.

3. М. Шабан, М.Марковская, А.Кислов, О.Потенко, «Использование COM-технологий при проведении экспертизы на соответствие требованиям НД ТЗИ», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 75, С.56-59, 2015.

4. М. Шабан, «Актуальность построения методик оценки качественных характеристик тестов, разрабатываемых в процессе экспертизы функциональных услуг безопасности обработки информации грид-сайта», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 74.– С.69-73, 2015.

5. М. Шабан, «Структура украинского национального грида с точки зрения обеспечения требований безопасности в грид-среде», Безпека інформації, Том 22, №1, С. 20-25, 2016.

6. М. Шабан, «Використання апарату регулярних виразів для аналізу функціонального профілю захисту», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.81, С.85-90, 2017.

7. М. Шабан, «Формалізація правил перевірки повноти та несуперечності функціонального профілю захисту», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.76, С.89-94, 2016.

8. М. Шабан, «Предварительная оценка энтропии электронных документов при проведении государственной экспертизы автоматизированной системы», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.77, С.141-144, 2016.

9. М. Шабан, «Програмна реалізація перевірки повноти та несуперечності функціонального профілю захисту», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.78, С.74-78, 2017.

10. М. Шабан, О.Потенко, В.Попова, «Тестування систем підтримки прийняття рішень орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.84, С.73-78, 2018.

11. М. Шабан, «Алгоритмічна реалізація перевірки повноти та несуперечності функціонального профілю захисту», Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є. Пухова, Вип.85, С.116-121, 2018.

12. М. Шабан, «Анализ современного состояния средств и методов защиты информации в Grid на базе Globus Toolkit», Моделювання: XXII Науково-технічна конференція молодих вчених та спеціалістів, Київ, 2013, С.21.

13. М. Шабан, А.Давиденко, «Разработка тестов для анализа информационной безопасности Национальной грид-инфраструктуры», Моделювання: XXXIII Науково-технічна конференція молодих вчених та спеціалістів, Київ, 2014, С.11.

14. М. Шабан, А.Давиденко, «Актуальность построения методик оценки качественных характеристик тестов разрабатываемых в процессе экспертизы

функциональных услуг безопасности грид-сайта», Моделювання: XXXIV Науково-технічна конференція молодих вчених та спеціалістів, Київ, 2015, С.10.

15. М. Шабан, «Особенности проведения предварительных испытаний комплексной системы защиты информации на примере типового ресурсного центра», Моделювання: XXXV Науково-технічна конференція молодих вчених та спеціалістів, Київ, 2016, С.36.

16. М.Шабан, «Реалізація програмного модуля підтримки прийняття рішень при проведенні експертизи грід-засобів на відповідність вимогам НД ТЗІ», Збірка праць конференції «Моделювання 2018», Київ, 2018, С. 259-262.

17. М. Шабан, О.Корченко, А.Давиденко, «Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ», Захист інформації, Том 21, №2, С. 88-96, 2019.

18. М. Шабан, О.Корченко, А.Давиденко, «Модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах», Безпека інформації, Том 25, №2, С. 122-126, 2019.

19. М. Шабан, «Ієрархія моделі декомпозиції вихідних документів», Моделювання: XXXVII Науково-технічна конференція молодих вчених та спеціалістів, Київ, 2019, С.48-51.

20. М. Шабан, «Застосування апарату регулярних виразів для аналізу функціонального профілю захисту», Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення», Вип. 36, Тернопіль, 2019, С.18.

21. М. Шабан, «Використання апарату регулярних виразів для аналізу функціонального профілю захисту», ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, Київ, 2019, С. 53-55.

22. М. Шабан «Алоритмічна реалізація перевірки повноти та несуперечності функціонального профілю захисту», V международная научно-практическая конференция "Актуальные вопросы обеспечения кибербезопасности и защиты информации", Киев, 2019, С. 74.

23. М. Шабан, «Модель параметрів функціонального профілю захисту в комп'ютерних системах», Науково-практична конференція "Безпека енергетики в епоху цифрової трансформації",Київ, 2019, С. 24.

24. М. Шабан, О.Корченко, А.Давиденко, І.Іванченко, «Метод ідентифікації функціонального профілю захисту», Захист інформації,Том 21, №4, С. 251-258, 2019.

25. М. Шабан, Ю.Гончаренко, О.Чолишкіна, «Модель смислових констант та змінних для експертиз ТЗІ», ITSec: Безпека інформаційних технологій: X міжнародна науково-технічна конференція, Київ, 2020, С. 37.

26. М. Шабан, А.Давиденко, О.Корченко, «Формування критеріїв для функціонального профілю захисту», ITSec: Безпека інформаційних технологій: X міжнародна науково-технічна конференція, Київ, 2020, С. 35.

27. М. Шабан, М.Карпінський, О.Корченко, А.Давиденко, «Розробка методу ідентифікації функціональних профілей захисту», VI міжнародна науково-практична конференція "Актуальні питання забезпечення кібербезпеки та захисту інформації", Київ, 2020,С. 113.

28. М. Шабан, А.Корченко, А.Давиденко, С.Казмірчук, «Структурна модель СППР при проведенні державних експертиз КСЗІ», Безпека інформації, Том 26, №1, С. 14-27, 2020.

29. М. Шабан, А.Давиденко, С.Гільгурт, «Апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації», Патент UA 139730 U; G06F17/27. Патент опубліковано 10.01.2020, бюл. № 1.

АНОТАЦІЯ

Шабан М.Р. Моделі підтримки прийняття рішень для проведення експертиз систем технічного захисту інформації. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – "Системи захисту інформації". – Національний авіаційний університет, Київ, 2021.

У роботі вирішено актуальну науково-прикладну задачу автоматизації процесу проведення експертиз комплексних систем захисту інформації та виявлення невідповідностей при формуванні функціональних профілів захисту. У дисертаційній роботі проведено аналіз існуючих моделей, методів та засобів підтримки прийняття рішень. Було з'ясовано, що існуючи моделі, методи та засоби не задовольняють вимогам щодо СППР, які мали б змогу використовуватись при проведенні державних експертиз КСЗІ. Розроблено декомпозиційну модель представлення смислових констант та змінних, що дозволило формувати базові шаблони вихідних документів. модель параметрів, що дозволило у формальному вигляді сформувати необхідний набір величин для реалізації процесу ідентифікації функціонального профілю захисту в комп'ютерних системах. метод ідентифікації функціонального профілю захисту, що дозволило реалізувати процес генерування функціонального профілю захисту і перевірку його вимог щодо функцій захисту (послуг безпеки) та гарантій. Запропоновано структурну модель системи підтримки прийняття рішень, що дозволила автоматизувати процес складання вихідних документів за їх шаблонами. Розроблено алгоритмічне та програмне забезпечення, що дозволило автоматизувати процес проведення експертизи комплексної системи захисту інформації та виявлення невідповідностей при формуванні функціонального профілю захисту. Проведені експериментальні дослідження програмного застосунка, впровадження та успішне практичне використання зазначених розробок підтвердили достовірність теоретичних гіпотез і висновків дисертаційної роботи.

Ключові слова: захист інформації, системи підтримки прийняття рішень, функціональний профіль захисту, функціональні послуги безпеки, грід-системи, державна експертиза КСЗІ.

ABSTRACT

Shaban M.R. Decision support models for expertise of information security systems. - Manuscript.

Thesis for scientific degree of candidate of technical sciences 05.13.21 - "Information Security Systems". - National Aviation University, Kyiv, 2021.

The dissertation is devoted to the decision of an actual scientific and applied problem of creation of models of decision support for examinations of systems of technical protection of the

information which will provide reduction of time and errors at drawing up of documents of the state examination of complex information protection system.

In accordance with the requirements of the legislation of Ukraine to ensure the confidentiality, accessibility, integrity and observability of this information in each automated system must create a comprehensive system of information protection

The state examination of the complex information protection system in information and telecommunication systems is carried out in order to determine the compliance of the integrated information protection system with the technical tasks, requirements of normative documents on information protection, to determine the possibility of putting the integrated information protection system into operation. Based on the results of the work, a group of documents is formed which is the program and methods of examination of the complex information protection system; list of tests; special opinion of the expert; test report; certificate of conformity and expert opinion.

The paper analyzes the existing decision support systems. The models have been analized which has allowed automating the process of identification of the functional protection profile. The developed model of parameters for identification of functional protection profiles in computer systems which due to theoretical and multiple representation of certain sets of criteria of information security, their elements and corresponding levels will formally form the necessary set of values for realization of process of functional protection profiles identification in computer systems.

The actual scientific and applied problem of automation of the process of examinations of complex information protection systems and detection of discrepancies in the formation of functional protection profiles is solved in the work. In the dissertation work the analysis of existing models, methods and means of decision support is carried out. It was found that the existing models, methods and tools do not meet the requirements for decision support systems that could be used in conducting state examinations of integrated information security systems. A decomposition model of representation of semantic constants and variables was developed which allowed to form basic templates of source documents. model of parameters which allowed to formally form the necessary set of values for the implementation of the process of identification of the functional profile of protection in computer systems. The method of identification of the functional protection profile, which allowed to implement the process of generating the functional protection profile and verification of its requirements for protection functions (security services) and guarantees. A structural model of the decision support system is proposed which allowed to automate the process of compiling source documents according to their templates. Algorithmic and software have been developed which allowed to automate the process of examination of the complex system of information protection and detection of inconsistencies in the formation of the functional profile of protection. The conducted experimental researches of software application, introduction and successful practical use of the specified developments have confirmed reliability of theoretical hypotheses and conclusions of dissertation work.

Keywords: information protection, decision support systems, functional security profile, functional security services, grid systems, state expertise of CSIS.