Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті
03058, м. Київ, пр. Любомира Гузара, 1

ВІДГУК

офіційного опонента доктора технічних наук, професора Лахна В.А.

на дисертацію

Шабана Максима Радуйовича

"Моделі підтримки прийняття рішень для експертиз технічного захисту інформації",

подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – "Системи захисту інформації"

Актуальність. Згідно вимог Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" для забезпечення безпеки в інформаційних ресурсах, що обробляються в автоматизованій системі, необхідно розробляти комплексну систему захисту інформації. Базовим етапом її побудови є створення політики безпеки, методологія побудови якої включає: розробку концепції інформаційної безпеки в автоматизованій системі; аналіз ризиків; визначення вимог до заходів, методів і засобів захисту; вибір основних рішень з забезпечення інформаційної безпеки; організацію виконання відновлювальних робіт та забезпечення безперервного функціонування автоматизованої системи; документальне оформлення політики безпеки. Завершальним етапом впровадження комплексної системи захисту інформації є експертиза інформаційно-телекомунікаційних систем на відповідність вимогам нормативного документу технічного захисту інформації. В процесі проведення експертизи виникає задача перевірки та модифікації частково формалізованої моделі політики безпеки при умові гарантій рівня Г2 — Г3. Модель будується на підставі знань отриманих на етапі побудови комплексної системи захисту інформації 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: аналізу функціонального профілю захисту, ідентифікації функціональних послуг безпеки та побудови тестового набору для перевірки функціональних послуг безпеки.

Внаслідок розвитку інформаційно-телекомунікаційних систем зростає складність аналізу систем, що збільшує час необхідний для проведення державних експертиз комплексних систем захисту інформації. Разом з тим, умова вчасного виконання експертиз залишилась. Все вищезазначене робить актуальним дослідження, які проведені в дисертаційній роботі Шабана Максима Радуйовича "Моделі підтримки прийняття рішень для експертиз технічного захисту інформації".

Структура та обсяг дисертації. Дисертація складається з анотації, переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та трьох додатків. Робота містить 37 рисунків, 12 таблиць. Список використаних джерел складається з 116 найменувань і займає 12 сторінок. Додатки розміщені на 42 сторінках. Загальний обсяг дисертації складає 208 сторінок, основний текст роботи викладено на 141 сторінці.

Основний зміст роботи

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.

Перший розділ присвячено аналізу вітчизняної та зарубіжної літератури за темою дисертаційної роботи. Проведено аналіз наукових основ проведення експертиз грід-засобів, моделей та методів проведення експертиз на відповідність вимогам нормативних документів технічного захисту інформації. Були проаналізовані існуючі моделі, методи, методики проведення державних експертиз, що дає можливість уніфікувати процес дослідження існуючих підходів до проведення експертиз, а також підвищити ефективність здійснення їх вибору. Також було виконано порівняльний аналіз найбільш поширених методів, моделей та засобів сучасних систем підтримки прийняття рішень.

Другий розділ присвячено розробці моделей декомпозиційного представлення смислових констант та змінних для реалізації експертиз у сфері технічного захисту інформації, параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах. На основі моделі параметрів для ідентифікації функціонального профілю захисту було розроблено метод ідентифікації функціонального профілю захисту.

Третій розділ присвячено побудові структурної моделі системи підтримки прийняття рішень та алгоритмам роботи програмного застосунка модуля ідентифікації функціонального профілю захисту. В основі інформаційної системи лежать математичні моделі та метод, які вже були розглянуті раніше в дисертаційній роботі. Для запропонованої структурної моделі було реалізовано алгоритмічне забезпечення функціонування системи підтримки прийняття рішень. Розроблений алгоритм описує взаємодію окремих модулів та баз даних структурної моделі системи підтримки прийняття рішень для реалізації експертиз комплексних систем захисту інформації. Далі, виконана алгоритмічна реалізація метода ідентифікації функціонального профілю захисту для подальшої програмної реалізації.

Четвертий розділ присвячено оцінюванню часу проведення експертизи, результатам моделювання та аналізу адекватності отриманих результатів. Державна експертиза триває шість місяців, з яких можливе скорочення часу тільки на одному з етапів, а саме, на етапі розробки вихідних документів. На основі методу ідентифікації функціонального профілю захисту було розроблено програмний застосунок, який призначений для допомоги експерту при визначенні функціональних профілів захисту в документах Microsoft Word та при аналізі функціонального профілю захисту на відповідність умовам заданим в нормативному документі технічного захисту інформації, а саме: визначення контролю цілісності; поглинання старшими функціональними послугами безпеки молодших; перевірки взаємопов'язаності функціональних послуг безпеки. Після чого було проведено перевірку адекватності роботи програмного модуля. З цією метою були проаналізовані типові функціональні профілі захисту з набору функціональних профілів захисту нормативного документу технічного захисту

інформації. Результати експериментальних досліджень підтверджують коректність розроблених в дисертаційній роботі моделей та методу.

У додатках містяться акти впровадження результатів дисертаційної роботи і лістинги (коди) програмного забезпечення.

Основною **науковою новизною** дисертаційного дослідження є те, що:

1. 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.
2. 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.

Головне **практичне значення одержаних результатів** полягає в тому, що створений в роботі програмний застосунок, на основі розробленого методу ідентифікації функціонального профілю захисту, може використовуватися на предмет аналізу функціональних профілів захисту при проведенні експертиз систем технічного захисту інформації і виявлення помилок при їх складанні.

Основні результати дисертаційної роботи достатньо повно викладені у 29 наукових працях, 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.

Результати дисертаційного дослідження впроваджені в наступних організаціях: ТОВ "СОФТЛАЙН ІТ", Інститут кібернетики ім. В.М. Глушкова, а також використовуються у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету.

Результати дисертаційної роботи є науково обґрунтовані і підтверджені результатами проведених в роботі експериментів. При виконанні роботи використано комп'ютерне моделювання, теорія алгоритмів, теорія множин, лінійна

алгебра, методи емпіричних та теоретичних досліджень, об'єктно-орієнтовані інформаційні технології.

Зауваження до дисертації:

1. В дисертації не достатньо чітко обґрунтовано необхідність розробки систем підтримки прийняття рішень для експертиз систем технічного захисту інформації.

2. В дисертаційній роботі, при розгляді множин смислових блоків вихідних документів, автор розглядає смисловий блок як множину смислових констант та змінних. Разом з тим, автор не пояснює необхідність такого поділу.

3. В запропонованому методі ідентифікації функціонального профілю захисту досить складно сприймати стиль викладення опису методу.

4. В дисертаційній роботі в формулі 2.27 не наведено визначення множини $\mathbf{МО}_{\mathbf{р}}^{\mathbf{Пmin}}$, що ускладнює сприйняття матеріалу.

5. В роботі присутні стилістичні та орфографічні помилки, котрі, в цілому не впливають на сприйняття роботи.

Загальний висновок по роботі

Робота виконана за актуальною темою. Отримано нові наукові і практичні результати, що полягають у розробці ефективних моделей підтримки прийняття рішень для експертиз систем технічного захисту інформації за рахунок розробки нових моделей та методу, які використовуються для автоматизації процесу проведення експертизи комплексної системи захисту інформації та виявлення невідповідностей при формуванні функціонального профілю захисту. Дисертація Шабана М.Р. є завершеною науковою працею. Автореферат та опубліковані роботи в повній мірі відображають отримані результати та зміст дисертації, яка відповідає паспорту спеціальності 05.13.21 – "Системи захисту інформації" (в першу чергу п. 1). Результати роботи, які впроваджені на підприємствах та в вищому навчальному закладі, безумовно мають наукове і практичне значення. Зазначені вище зауваження не зменшують наукової цінності дисертаційної роботи.

Дисертація відповідає вимогам пп. 11, 13 та 14 "Порядку присудження наукових ступенів ", затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. №567 (із змінами, внесеними згідно з Постановами Кабінету

Міністрів України №656 від 19.08.2015 р., №1159 від 30.12.2015 р., №567 від 27.07.2016 р.), які висуваються ВАК України до кандидатських дисертацій, а її автор Шабан М.Р. заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – "Системи захисту інформації".

Офіційний опонент
Завідувач кафедри комп'ютерних систем і мереж
Національного університету біоресурсів
і природокористування України,
доктор технічних наук, професор В. Лахно

ЗАСВІДЧУЮ
Начальник відділу кадрів
І.В. Михайліченко
2020 р.