ВІДГУК

офіційного опонента Гізуна Андрія Івановича

на дисертаційну роботу **Суліми Олександра Андрійовича** «Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей», що представляється на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – «Системи захисту інформації».

Актуальність. Інформаційні системи різного призначення активно використовуються практично у всіх сферах діяльності людини, при цьому в основному вони орієнтовані на роботу з користувачами, що обумовлює необхідність процедури їх ідентифікації та автентифікації. Для таких цілей в інформаційних системах використовують комплекс засобів та заходів, що об'єднані під назвою система доступу. Основною функцією системи доступу є надання або заборона визначеним користувачам користуватися ресурсами інформаційної системи в усіх аспектах: починаючи від перегляду, зміни, видалення баз даних відповідних систем і закінчуючи процесами використання таких ресурсів для вирішення системою конкретних прикладних задач. Таким чином захист інформаційних систем від несанкціонованого доступу неавторизованих нелегітимних користувачів по суті визначає загальний рівень безпеки інформаційної системи. Типові засоби захисту системи доступу, що полягають в автентифікації користувачів в багатьох випадках виявляються недостатніми, і для забезпечення необхідного рівня безпеки у системі доступу доцільно розробляти та досліджувати нові підходи до вирішення задач захисту. Особливо важливою є ця задача для інформаційних систем, що орієнтовані на розв'язання державних та соціальних задач. Особливість соціальних систем полягає у тому, що її користувачами можуть бути широкі маси населення, які не завжди можуть бути в необхідній мірі підготовлені для роботи з інформаційною системою. Крім того суттєвих змін в процесі розвитку інформаційного суспільства та інформаційних технологій зазнали категорії «конфіденційності даних», «конфіденційних даних» і парадигма застосування таких даних як основного ресурсу інформаційної системи. З огляду на зазначене, розробка та дослідження

нових методів захисту системи доступу до інформаційних систем, зокрема застосування багаторівневих моделей, є дуже актуальною, а проведені дослідження Сулими О.А., спрямовані на розв'язання поставлених в роботі задач, мають суттєве теоретичне та прикладне значення.

Зв'язок роботи за науковими програмами, планами підтверджується участю Суліми О.А. у виконанні науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України та у роботах з Національним авіаційним університетом протягом 2014-2017 років. Тематика цих робіт відповідає розв'язанню актуальних задач комп'ютерних наук та актуальним задачам прикладних наук, що вирішуються за допомогою засобів комп'ютерної техніки та програмних засобів.

Структура та обсяг дисертації: дисертація складається зі вступу, чотирьох розділів, висновків, списку літератури, додатків.

Вступ дисертації містить матеріал про актуальність теми, що досліджується, сформовані мета, задачі, предмет і об'єкт дослідження, основні положення наукової новизни, що виносяться до захисту, а також наведені дані щодо апробації та впровадження отриманих здобувачем практичних результатів.

В першому розділі роботи проведено аналіз вибраних типових тем доступу до інформаційних ресурсів, завдяки чому автор показав необхідність проведення подальших досліджень з ціллю розробки нових підходів і методів. Оскільки мова йде про захист та безпеку системи доступу до інформаційного ресурсу, то увага автора була спрямована на визначення рівня захищеності. У зв'язку з цим в роботі проводиться аналіз методів такої оцінки, один з яких полягає у визначенні величини ризику виникнення успішного несанкціонованого доступу до даних.

В другому розділі роботи на основі проведеного аналізу показано основні відмінності між різними методами побудови системи доступу, які забезпечують певний рівень захисту від несанкціонованого доступу.

Оскільки система доступу забезпечує неможливість несанкціонованого використання різних даних, то відповідні дані повинні мати різні рівні конфіденційності, оскільки такі дані стосуються різних компонент деякої

предметної області. Дані в тій чи іншій предметній області можна класифікувати не тільки по типу компонент до яких вони відносяться, а і на основі аналізу самої предметної області. Справа у тому, що захист даних потрібен не тільки для того щоб вони не були заміщені, чи видалені, а для того щоб не було можливості використовувати їх для реалізації негативного впливу на предметну область. Цей аспект є основним при визначенні такого параметра, як рівень конфіденційності даних, який є визначальним в питанні надання користувачу доступу.

З іншого боку замовлення на використання даних можуть пред'являти прикладні задачі. Для того щоб можна було співставити зв'язок тих, чи інших даних з відповідними задачами, він має також характеризуватися аналогічними параметрами. Автор виходить з гіпотези, що не може мати місце ситуація при якій довільні задачі, можуть звертатися за довільними даними. Тому в роботі визначено і досліджено ряд параметрів, що характеризують задачу. На основі аналізу параметрів прикладної задачі та параметрів даних, за якими звертається задача, система надання повноважень приймає рішення про надання повноважень прикладної задачі, використовуючи відповідні дані, для того щоб надати, чи не надати відповідні повноваження.

В третьому розділі роботи запропоновано дозволити системі здійснювати надання повноважень не тільки прийняттям бінарних рішень, але й приймати рішення про той чи інший спосіб використання даних прикладною задачею, в залежності від значення відповідних параметрів конфіденційних даних. Прикладом не бінарного рішення про надання повноважень системою може служити ситуація, коли система надання повноважень здійснює перетворення даних, за якими звернулася задача власним способом за допомогою перетворень, які не порушують конфіденційність даних на відміну від перетворень, якими планувала скористатися задача. В цьому випадку задача отримує від системи надання повноважень не самі дані, а результати їх перетворень для продовження процесу розв'язання прикладної задачі.

Оскільки проблеми захисту системи доступу в запропонованому підході розв'язуються на основі використання даних про предметну область, на

обслуговування якої орієнтована інформаційна система, то в роботі розроблено методи аналізу предметної області. Вони полягають на використанні описів інтерпретації даних, на використанні введених в роботі критеріїв, що характеризують характер змін в предметній області та ряду інших чинників. Прикладом таких критеріїв можуть служити критерії прогресивності змін, що відбуваються в предметній області, яку обслуговує відповідна інформаційна система, критерій що визначається усуненням аномалії, що була присутня в предметній області, а в результаті використання результатів розв'язку чергової задачі була усунена та інші.

Важливим чинником, який розглядається в роботі є можливість розв'язку критичних ситуацій, що можуть виникати у відповідній предметній області. У зв'язку з можливими критичними ситуаціями, до яких може призвести використання результатів розв'язку окремих задач, система надання повноважень для задачі, яка генерує запит на використання відповідних даних, може формувати для неї ті чи інші рекомендації, що стосуються модифікації мети задачі, для введення обмежень по використання отриманих результатів.

Також в другому і третьому розділах введені такі параметри, на основі яких формується алгоритм роботи запропонованої системи в наступних розділах, як рівень важливості даних, параметр актуальності задачі, характеристика цілі задачі, рівень обґрунтованості даних та інші.

Автор **в четвертому розділі** роботи не тільки проводить теоретичні дослідження, а і розробляє алгоритми реалізації окремих методів, що запропоновані в процесі виконання роботі. Прикладом таких алгоритмів є алгоритми реалізації процесу надання повноважень задачам, що звертаються до інформаційної системи за відповідними даними. Очевидно, що такі задачі ініціюються в інформаційній системі користувачами, які в результаті розпізнання їх системою доступу одержують права санкціонованих користувачів. Наступним прикладом практичної реалізації розв'язання відповідних наукових задач може служити розроблений алгоритм загальної організації процесу функціонування інформаційно-комунікаційної системи.

Також автором вводяться умови, які дозволяють відокремити чинники, інтерпретація яких характеризує надійність від чинників, що можуть характеризувати небезпеки. Це дозволило в цілому проблему захисту відокремити від проблем, що пов'язані з надійністю інформаційної системи.

У **висновках** стисло і чітко сформовані основні наукові та практичні результати дисертаційної роботи.

Ступінь обґрунтованості наукових досліджень висновків та рекомендацій. Високий рівень обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації обумовлюється строгістю використання математичного апарату та коректністю застосування методів дослідження. Достовірність окремих результатів перевірені експериментально за допомогою розроблених програмних засобів.

Публікації та апробація. Публікація отриманих автором результатів у фахових виданнях, повно відображає матеріали, представлені у дисертаційній роботі і є додатковим свідченням про їх новизну, а відповідні практичні результати пройшли необхідні апробаційні процедури.

Значення результатів для науки та практична корисність роботи. Цінність дисертації полягає в тому, що в ній запропоновано рішення важливої науково-технічної задачі розширення можливостей систем управління доступом до інформаційних ресурсів і систем. Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє проектувати більш досконалі, порівняно з відомими, програмні та програмно-апаратні засоби.

Відповідність теми та змісту дисертації паспорту спеціальності, за якою вона подана на захист.

Тема дисертації та її зміст відповідають формулі й галузі досліджень паспорта спеціальності 05.13.21 – «Системи захисту інформації», оформлена відповідно до вимог значних стандартів.

Автореферат повністю ідентичний дисертаційній роботі і відображає основні положення та отримані в роботі наукові результати.

Зауваження:

1. Було б доцільно розглянути у роботі можливість більш детального визначення величини рівня конфіденційності шляхом введення інструментарію її вимірювання. Крім того, вважаю, що рівень конфіденційності даних має визначатися не тільки кількістю користувачів, а й іншими характеристиками, зокрема такими як галузь, потенційні збитки від розголошення тощо.

2. Недостатньо уваги в роботі автор приділяє дослідженню зв'язку між предметною областю та відповідною інтерпретаційною системою. Було б корисно розширити дисертаційну роботу описом використання отриманих результатів на прикладі обраної предметної області.

3. Мало уваги автор приділяє в роботі питанням, що пов'язані з використанням компоненти прийняття рішень, яка входить до системи надання повноважень прикладним задачам.

4. Для визначення дублювання та повторення задач автором пропонується порівнювати мету кожної задачі. Однак в роботі не описано в якій формі зберігаються і обробляються в системі мета задачі або інформація про мету задачі, а також не визначено механізм їх порівняння.

5. Також в роботі не повністю розкритий семантичний механізм, що застосовується для визначення рівня обґрунтованості.

6. В четвертому розділі дисертаційного дослідження описані розроблений програмний засіб, що реалізує один з запропонованих методів, і експериментальне дослідження, однак методика проведення експерименту в явному вигляді відсутня.

7. В дисертації зустрічаються не значні технічні помилки, її розуміння ускладнене великою кількістю формул, крім того автор не завжди використовує термінологію, яка є загальноприйнятою для даної галузі.

ВИСНОВКИ

Дисертація Суліми О.А. «Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей», є завершеним науковим дослідженням та присвячена побудові спеціальних засобів

для реалізації методів підвищення рівня захисту даних в інформаційних системах на засадах використання багаторівневої системи надання повноважень.

Робота виконана самостійно у вигляді підготовленого рукопису, характеризується єдністю змісту, та говорить про особистий внесок здобувача в науку. Результати дисертації в повній мірі викладені в авторефераті і публікаціях та в сукупності вирішують важливу науково-технічну задачу побудови захищених систем доступу до інформаційних систем та ресурсів.

За актуальністю тематики, рівнем виконання, новизною результатів та їх науковим та практичним значенням дисертаційна робота «Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей», в цілому відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами), що пред'являються до кандидатських дисертаційних робіт, а її автор **Суліма Олександр Андрійович заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».**

Офіційний опонент
доцент кафедри безпеки інформаційних технологій
Національного авіаційного університету,
кандидат технічних наук 15.11.17 А.І. Гізун

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ * Ідентифікаційний код 01132330 * М. КИЇВ

підпис гр. Гізуна А.І.
засвідчую
Вчений секретар
Національного авіаційного університету
Г. Єлчева