ВІДГУК

офіційного опонента

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 дисертаційної роботи Суліми О.А. обумовлена важливим завданням щодо забезпечення захисту інформаційних систем від несанкціонованого доступу до даних таких систем, які широко використовуються практично у всіх галузях економіки і соціальної сфери в більшості країн світу.

Інформаційні системи спрямовані, як правило, на взаємодію з користувачами, яка обумовлює здійснення процедури їх автентифікації та ідентифікації. З цією метою в таких системах реалізується низка спеціальних засобів та заходів системи доступу, яка надає або забороняє конкретним користувачам використовувати ресурси інформаційних систем для вирішення різнопланових прикладних задач.

Система доступу забезпечує захист інформаційної системи від несанкціонованого доступу нелегітимних користувачів і фактично є показником загального рівня безпеки інформаційної системи. Поширені на даний час засоби захисту системи доступу є переважно недостатньо досконалими, що обумовлює необхідність дослідження і розроблення більш надійних систем захисту інформаційних систем, насамперед, у сфері державного управління та місцевого самоврядування. Ураховуючи зазначене, дослідження та розроблення Сулімою О.А., нових методів захисту системи доступу до інформаційних систем шляхом застосування багаторівневих моделей є актуальними та ~~і~~ мають значне теоретичне і практичне значення.

Це підтверджується виконаними Сулімою О.А. науково-дослідними роботами в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова

НАН України та роботами з Національним авіаційним університетом у 2014-2017 роках.

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

У вступі дисертації викладено матеріал щодо актуальності теми роботи, сформовано мету, задачі, предмет та об'єкт дослідження, обґрунтовано основні положення наукової новизни, а також наведено дані про апробацію та впровадження практичних результатів, отриманих здобувачем.

У **першому розділі** проаналізовано загальновідомі методи надання повноважень користувачам на використання даних, за якими вони звертаються до інформаційної системи, які підтвердили висновки автора про необхідність проведення подальших досліджень з метою розроблення нових підходів і методів. У роботі проведено аналіз методів оцінки рівня захисту доступу, один з яких визначає величину ризику виникнення успішного несанкціонованого доступу до даних.

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

Оскільки система доступу спрямована на забезпечення неможливості несанкціонованого використання різних даних, то вони повинні мати різні рівні конфіденційності, так як такі дані стосуються різних компонентів деякої предметної області. Дані, що відносяться до тієї чи іншої предметної області можна класифікувати не тільки за типом компонентів, до яких вони відносяться, а й на засадах аналізу безпосередньо предметної області. Захист даних необхідний не тільки щоб виключити їх заміщення або видалення, а для того щоб усунути можливість використання їх для реалізації негативного впливу на предметну область. Цей аспект є головним під час визначення такого параметру, як рівень конфіденційності даних, який є визначальним в питанні надання користувачу доступу.

Крім того, замовлення на використання даних можуть пред'являти прикладні задачі, що представляються користувачем. Здобувач вважає, що не може мати місце ситуація, за якої довільні задачі можуть звертатися за довільними даними. У зв'язку з цим у роботі визначено і досліджено ряд параметрів, що характеризують задачу. На підставі аналізу параметрів прикладної задачі та параметрів даних, за якими звертається задача, система надання повноважень, використовуючи відповідні дані, приймає рішення про надання або не надання повноважень прикладній задачі.

У третьому розділі роботи запропоновано дозволити системі здійснювати надання повноважень не тільки шляхом прийняття бінарних рішень, але й вирішувати який спосіб використання даних прикладною задачею є допустимим в залежності від значення відповідного параметра конфіденційності даних. Прикладом може служити ситуація, коли система надання повноважень здійснює перетворення даних, за якими звернулася задача, власним способом за допомогою перетворень, що не порушують конфіденційність даних. У цьому випадку задача отримує від системи надання повноважень не самі дані, а результати їх перетворень для продовження процесу розв'язання прикладної задачі.

Зважаючи на те, що проблеми захисту системи доступу в запропонованому підході розв'язуються на основі використання даних про предметну область, то в роботі розроблено методи аналізу предметної області на основі використання описів інтерпретації даних та на використанні уведених у роботі критеріїв, що визначають характер змін у предметній області, а також на основі деяких інших чинників. Прикладом таких критеріїв можуть служити критерії прогресивності змін, що відбуваються в предметній області, яку обслуговує відповідна інформаційна система, а також критерій, що визначається усуненням аномалії, що була присутня в предметній області, а за підсумками використання результатів розв'язання чергової задачі була усунута, та деякі інші.

Важливою задачею, яка розглядається в роботі, є задача надання можливості усунення критичних ситуацій, що можуть виникати у відповідній предметній області. У зв'язку з такими, можливими критичними ситуаціями, які можуть виникати, при використанні результатів розв'язання окремих задач, система надання повноважень задачі, яка генерує запит на використання певних даних, може формувати для неї відповідні рекомендації, що приводять до модифікації мети задачі, що, в свою чергу, наприклад, може приводити до зміни даних, які будуть використовуватися в предметній області.

В другому і третьому розділах уведено параметри, на основі використання яких формуються алгоритми функціонування запропонованої системи. Прикладами таких параметрів можуть служити: рівень важливості даних, параметр актуальності задачі, характеристика цілі задачі, рівень обґрунтованості даних та інші.

В **четвертому розділі** роботи автор проводить теоретичні дослідження окремих аспектів досліджуваної задачі та розробляє алгоритми реалізації окремих методів, що запропоновані в роботі. Прикладом цих алгоритмів можуть служити алгоритми реалізації процесу надання повноважень задачам, що звертаються до інформаційної системи за відповідними даними. Очевидно, що прикладні задачі передаються в інформаційну систему користувачами, які в результаті ідентифікації їх системою доступу одержують права санкціонованих користувачів. Наступним прикладом практичної реалізації результатів, отриманих в дослідженнях, що проведені в роботі, може служити розроблений алгоритм загальної організації процесу функціонування інформаційної системи.

Автор вводить умови, які дозволяють відокремити фактори, інтерпретація яких характеризує надійність від факторів, що можуть характеризувати небезпеки. Це дозволило 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 коректним використанням математичного апарату та обґрунтованістю застосування методів дослідження. Достовірність окремих результатів перевірено при проведенні експериментів, які реалізовані на основі використання розроблених програмних засобів.

Публікації та апробація. Публікація отриманих автором результатів у фахових виданнях повною мірою відображає матеріали, які представлені у дисертації, що є свідченням їх новизни, а відповідні практичні результати пройшли апробацію.

Значення результатів для науки та практична корисність роботи.

Цінність дисертації роботи полягає в тому, що в ній запропоновано розв'язання важливої науково-технічної задачі розширення можливостей систем управління доступом до інформаційних ресурсів і системи, на основі запропонованої дворівневої моделі захисту даних розроблено алгоритм, який реалізує процес надання повноважень задачам, на основі запропонованих та розроблених елементів засобів доступу до інформаційної системи, побудовано алгоритм загальної організації роботи дворівневої системи доступу до даних, що забезпечує елімінацію суб'єктивних факторів користувача, які могли б впливати на можливість доступу до конфіденційних даних.

Використання запропонованих в роботі формальних методів і конкретних рішень дозволяє проектувати більш досконалі, порівняно з відомими, програмні та програмно-апаратні засоби захисту доступу до даних, тим самим обумовлюється практична корисність роботи.

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

Тема дисертації та її зміст відповідають формулі й галузі досліджень, що приведені у паспорті спеціальності 05.13.21 – «Системи захисту інформації», дисертаційна робота оформлена відповідно до вимог відповідних стандартів.

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

Зауваження:

1. У роботі мало уваги приділяється опису предметної області, яку обслуговує задача, хоча дані про предметну область використовуються при формуванні рішень про надання повноважень.
2. Доцільно було би більш повно обґрунтувати використання трьох рівнів конфіденційності у випадку надання повноважень задачам на використання даних високого рівня конфіденційності даних.
3. В роботі не достатньо повно описуються ситуації, в яких задача не отримує даних, за якими звертається до інформаційної системи, та не приводиться діагностика відмов в обслуговуванні, що утруднює розуміння ситуацій пов'язаних з негативними рішеннями системи надання повноважень.
4. Мало уваги в роботі присвячується проблемі можливої співпраці інформаційної системи з системними адміністраторами, що обслуговують відповідну систему.
5. Автор недостатньо уваги приділяє питанням обґрунтуванням визначення того, або іншого рівня конфіденційності даних, які обслуговують задачу та не достатньо повно описують можливості користувача по отриманню даних високого рівня конфіденційності.
6. У тексті роботи трапляється використання термінів без достатнього обґрунтування необхідності їх використання.

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 основі використання багаторівневої системи надання повноважень.

Робота виконана самостійно і представлена у вигляді підготовленого рукопису, характеризується єдністю змісту, що свідчить про значний особистий внесок здобувача в науку. Наукові результати, що отримані в дисертаційній роботі в повному обсязі викладені в авторефераті і публікаціях та в сукупності вирішують важливу науково-технічну задачу побудови захищених систем доступу до інформаційних систем та їх ресурсів.

За актуальністю тематики, рівнем виконання, новизною результатів 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 – к.т.н., асистент
кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій
Київського національного університету
імені Тараса Шевченка А.О. Фесенко

Підпис засвідчую
Вчений секретар
Національного університету
27.11.2020