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. Використання інформаційних систем передбачає необхідність забезпечення доступу до них користувачів, які з різних причин можуть потребувати інформацію, що знаходиться в таких системах. Серед користувачів, які звертаються за інформацією до системи, завжди є частка яка не має відповідних повноважень. В цьому випадку виробничі потреби можуть приводить до несанкціонованого звертання таких осіб до відповідних інформаційних систем або в відмові доступу до наявної інформації. Проблема захисту доступу до інформаційних систем досліджується досить широко, але додаткової уваги потребує регулювання рівня доступу до інформаційного ресурсу. У зв'язку з зростанням кількості спроб несанкціонованого доступу до інформаційних систем проблема захисту доступу до них залишається актуальною. Таке зростання, в значній мірі, пояснюється тим, що інформаційні системи досить інтенсивно розвиваються, кількість їх зростає та вони використовуються в багатьох сферах людської діяльності. Це приводить до того, що в інформаційних системах знаходиться інформація, несанкціоноване використання якої може приводити до виникнення несанкціонованих наслідків по відношенню до суб'єктів, яких відповідна інформація стосується.

Практика використання інформаційних систем у різних галузях діяльності людини показує, що спроби несанкціонованого отримання інформації є регулярними, особливо в тих випадках, коли інформаційна система вміщає інформацію, яка може бути використана з корисною метою окремими особами. Особливо актуальною проблемою захисту доступу до інформаційних систем є використання інформаційного ресурсу для розв'язання задач державного характеру.

Такі системи, у більшості випадків, є державними інформаційними системами та інформація яка в них розміщується може бути пов'язана з державними таємницями.

Зв'язок роботи за науковими програмами, планами та темами підтверджується участю Суліми О.А. у виконанні науково-дослідних роботах Інституту проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, наприклад дослідження на тему "Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетиці".

Основний зміст роботи. Рецензована дисертаційна робота є цілісним закінченим дослідженням.

У вступі роботи обґрунтовано актуальність дисертаційної теми, зроблено огляд наукових праць відомих фахівців, що працювали у галузі захисту інформації, показано зв'язок роботи з науковими темами, визначено мету дослідження, сформульовано наукову новизну здобутих результатів та їх практичне значення, наведено відомості що до публікацій, структури та обсягу роботи.

У першому розділі проведено аналіз відомих методів надання повноважень користувачам інформаційних систем та зроблено аналіз відповідних основних систем. Детально розглядаються основні методи реалізації захисту доступу користувачів до системи з метою виявлення спроб здійснення несанкціонованого доступу. Однією з поширених моделей захисту доступу, які аналізуються в роботі є матрична модель доступу в якій описуються повноваження ідентифікованих користувачів до виконання різних операцій в інформаційній системі.

В другому розділі досліджуються методи формального опису параметрів процесів надання повноважень. Також в цьому розділі проводиться аналіз міри конфіденційності даних, яка є одним з важливих критеріїв, що визначає актуальність розробки нових методів захисту доступу. Одним з основних підходів до такої оцінки ґрунтується на використанні уявлень про ризик не забезпечення можливості виявлення несанкціонованих користувачів. Переважно, в сучасних системах доступу величина ризику або рівень захисту доступу декларується, а відповідні декларації ґрунтуються на використанні тих, чи інших методів доступу до інформаційної

системи. У зв'язку з тим що система доступу до даних в інформаційних системах повинна визначати різні рівні конфіденційності даних та досить важливим є дослідження способів визначення різних мір конфіденційності даних, що знаходиться в інформаційній системі. Тому в роботі досліджуються способи оцінки міри конфіденційності даних в залежності від якої система доступу повинна надавати, чи забороняти доступ до відповідних даних. В роботі виявляються та досліджуються фактори, які не тільки впливають на величину міри конфіденційності окремих даних і визначаються параметри, що відображають ті, чи інші загрози, що обумовлюють відповідно міру конфіденційності. Для цього в роботі вводиться цілий ряд визначення параметрів, що характеризують у міру конфіденційності даних та визначаються умови при яких міра конфіденційності даних може змінюватися.

В третьому розділі досліджуються методи моделювання процесу функціонування динамічної системи надання доступу, основні компоненти моделі захисту системи доступу. Одним з важливих результатів дослідження, які проведені в роботі є запропонований розподіл процесу надання повноважень на використання даних, за якими звертається користувач до системи. Такий розподіл полягає у тому, що система надання повноважень на використання даних розділяється на дві окремі підсистеми одна з таких підсистем аналізує дані користувача, що звертаються до інформаційної системи, з метою його ідентифікації та автентифікації. Така система може розширюватися шляхом збільшення кількості та характеру параметрів, на основі аналізу яких, система доступу, не тільки дозволяє користувачу доступ до системи, але і визначає набір повноважень для відповідного користувача на той, чи інший спосіб використання даних.

Очевидно, що користувач потребує ті, чи інші дані, які знаходяться в системі для розв'язку певних задач, які мають свою інтерпретацію у відповідній в предметній області. Тому в роботі запропоновано для даних певних рівнів конфіденційності, визначати окремо повноваження на використання таких даних відповідними задачами. Для цього в роботі запропоновано використовувати окрему компоненту надання повноважень задачам, які відповідний користувач повинен представляти. У зв'язку з цим, в роботі розроблено і досліджено параметри, що

характеризують задачу, які використовуються для визначення можливості надання повноважень задачі. При цьому, на процеси надання повноважень задачі на використання тих, чи інших даних користувач не може впливати. Вплив користувача на надання повноважень такою системою доступу можливий лише шляхом повного виходу з інформаційної системи, модифікації, або переробки задачі з якою користувач планує звернутися до системи та наступним зверненням до системи з проходженням з самого початку процедури ідентифікації та автентифікації користувача.

В четвертому розділі досліджуються процеси надання повноважень та описується реалізація основних компонент системи надання повноважень. Важливим результатом, який отримано в роботі, є встановлення зв'язку між рівнями конфіденційності даних та процесами що реалізуються у системі надання повноважень задачі. Такі залежності формуються у вигляді визначень, в якості прикладу розглянемо наступне. Перший рівень конфіденційності даних, за якими звертаються задачі означає що відповідні дані можуть перетворюватися або аналізуватися тільки алгоритмами, що розміщені у системі надання повноважень задачі. Це означає, що задача не отримає для використання відповідних даних, а отримає тільки результат їх перетворення, що здійснюється в системі. У зв'язку з цим система надання повноважень задачі приводить аналіз фрагменту алгоритму задачі, в якому передбачається перетворювати дані, і вибирає серед своїх алгоритмів той, який є найбільш відповідним до фрагменту алгоритму задачі, що орієнтований на перетворення цих даних. Це означає, що в рамках даного підходу в інформаційна система стає середовищем в якому повинна розв'язуватися відповідна задача. Це, в свою чергу, визначає певні вимоги до підготовки задач, для розвитку яких передбачається використовувати дані відповідно інформаційної системи.

Для забезпечення можливості проведення такого аналізу, в роботі розроблена та досліджено параметри самої задачі, по яких система визначає можливість надання, чи ненадання повноважень задачі на використання відповідних даних.

Прикладом таких параметрів можуть служити параметр значимості задачі, актуальність задачі, кількість конфіденційних даних різних рівнів та інші.

Важливе досягнення в роботі полягає у тому, що автор тісно пов'язує дані, що зберігаються в інформаційній системі з предметною областю, в якій ці дані інтерпретуються. Завдяки цьому, система надання повноважень задачі має можливість використовувати критерії, що характеризують зміни в області інтерпретації результатів, що отримані внаслідок розв'язування задач.

Ступінь обґрунтованості положень висновків та рекомендації, що проведені в роботі, повністю відображаються та підтверджуються отриманими результатами, що приведені в роботі, описами процесу розв'язку задач, які представлені в основному змісті роботи, та обґрунтовуються коректною методикою послідовного та повного висвітлення отриманих у роботі результатів.

Достовірність отриманих нових результатів при розв'язку поставлених задач підтверджується коректним використанням формальних засобів опису основних елементів предмету дослідження, повною узгодженістю задач, що розв'язуються в роботі, з відомими методами розв'язку задач забезпечення безпеки систем доступу. Крім того коректність отриманих результатів підтверджується рядом тверджень, які доводяться в роботі і стосуються досліджених та розв'язаних в роботі задач. Прикладом цього може служити твердження про несуперечність результатів розв'язку задачі, що використовуються в предметній області з фрагментами середовища цієї області, в яких застосовуються відповідні результати.

Наукова новизна результатів дисертації. Наукова новизна, з точки зору опонента, полягає в наступному:

удосконалено:

1. метод формального опису параметрів даних, які за рахунок обчислення їх величин, дозволяють оцінювати їх адекватно по відношенню до необхідних рівнів захисту;

вперше:

2. розроблено метод визначення параметрів прикладних задач та їх оцінок, який на основі використання характеристик конфіденційних даних з інформаційної системи, не залежно від користувача, який представив відповідну задачу, дозволить

приймати рішення системою надання повноважень, при цьому стає можливим уникнути небезпек, які можуть з'явитися під впливом дій користувача;

3. розроблено метод визначення параметрів додаткових компонент засобів доступу в інформаційну систему, який за рахунок аналізу предметної області, що обслуговується інформаційною системою, дозволяє співставити рівень конфіденційності даних з величинами параметрів прикладних задач, що дає змогу встановити залежність між рівнем захисту системи та умовами предметної області по використанню даних;

4. розроблено основні компоненти дворівневої моделі доступу даних, в якій відповідні рівні функціонують незалежно, але перехід з нижчого рівня на вищий рівень реалізується на основі даних нижчого рівня, за рахунок чого з'являється можливість уникнути впливу нижчого рівня на вищий, при розв'язуванні задач доступу до інформаційного ресурсу.

Практична значимість виконаної роботи підтверджуються розробкою алгоритмів реалізації основних отриманих результатів, які представлені в роботі відповідними блок-схемами та документами про використання нових отриманих наукових результатів в проектних роботах, які проводились в інших організаціях.

Дисертаційна робота представляє собою завершену наукову роботу в цілому, яка розв'язує поставлену науково-прикладну задачу в галузі захисту інформації.

Матеріали дисертаційної роботи повністю відображені в публікаціях та були апробовані у відповідному науковому середовищі на науково-технічних конференціях.

Автореферат повністю відображає зміст дисертаційної роботи в рамках вимог, що визначають правила його оформлення.

До роботи слід зробити наступні зауваження.

1. Недостатньо повно в роботі відображається процедури взаємозв'язку системи надання повноважень задачі, що потребує дані кожного рівня конфіденційності з даними про предметну область, на обслуговування якої орієнтована інформаційна система.

2. Автору було б доцільним приділити більше уваги питанням інтерпретації даних різних рівнів конфіденційності.

3. В роботі недостатньо чітко автор описує процедуру відмови від надання повноважень користувачу та задачі, що не дозволяє зрозуміти, чи може отримати користувач обґрунтованість відмови. Якщо такої обґрунтованості буде недостатньо, то користувач може розглядати відмову у обслуговуванні як помилку, або збій в інформаційній системі.

4. Автор в роботі мало уваги приділяє проблемам оцінки рівнів конфіденційності даних.

5. В роботі йде мова про алгоритми перетворень конфіденційних даних, які розміщуються в системі надання повноважень задачам, але автор не наводить даних, чи мова йде про певні бібліотеки програм, чи про якісь інші структури, що використовуються відповідною системою надання повноважень.

6. В тексті дисертаційної роботи є ряд редакційних помилок, наприклад, по тексту трапляються відсутність інтервалів між словами та інші.

Приведені зауваження не впливають на загальну позитивну оцінку роботи.

Висновки.

Дисертаційна робота Олександра Суліми представляє собою завершену наукову роботу, в якій розв'язується важлива науково-прикладна задача, що має велике науково-прикладне значення для галузі захисту інформації, в частині побудови засобів доступу до інформаційних систем. Дисертаційна робота Суліми О.А. на тему «Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей», є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, що в сукупності вирішують важливу науково-технічну задачу побудови інформаційних засобів, для реалізації методів підвищення рівня захисту даних в інформаційних системах на основі використання багаторівневої системи надання повноважень та автоматизації процесу визначення поточного значення рівня конфіденційності даних, оформлена у

відповідності з вимогами “Порядку присудження наукових ступенів”, затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами), що пред’являються до кандидатських дисертаційних робіт, відповідає напрямкам досліджень згідно паспорту спеціальності 05.13.21 – системи захисту інформації, а її автор **Суліма Олександр Андрійович**, заслуговує присудження наукового ступеня кандидата технічних наук за вказаною вище спеціальністю.

Професор кафедри системного
програмування і спеціалізованих
комп'ютерних систем
факультету прикладної математики
Національного технічного університету
України «КПІ імені І. Сікорського»
д.т.н., доц. І.А. Терейковський

Підпис засвідчую:
вчений секретар
університету А.А. Мєлянченко