ВІДГУК

офіційного опонента на дисертаційну роботу

ПОТЕНКА ОЛЕКСАНДРА СЕРГІЙОВИЧА

«Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз»,

яка подається на здобуття наукового ступеня

кандидата технічних наук за спеціальністю

05.13.21 – системи захисту інформації

1. Актуальність теми дисертаційної роботи

В Україні активно розвивається сфера захисту інформації, зокрема у контексті проектування, виробництва та експлуатації автоматизованих систем (АС), які призначені для обробки, зберігання та передачі інформації з обмеженим доступом. На початку XXI століття була сформована нормативна база у вигляді ряду документів технічного захисту інформації (НД ТЗІ), що мають на меті визначення функціонального профілю захисту (ФПЗ) шляхом стандартизації послуг безпеки, їх оцінки та перевірки відповідності. В даний час триває як розвиток правової бази, так і наукове забезпечення цього. Ця дослідницька робота зосереджена на вирішенні актуальної проблеми — визначенні ймовірності успішного протистояння вибраного профілю наявним загрозам.

У процесі експертизи КСЗІ завданням експерта є детальний аналіз реалізованих в системі механізмів захисту. Експерт повинен виявити ці механізми, перевірити їх працездатність, коректність реалізації та оцінити їх достатність для протидії існуючим загрозам. На етапі розробки технічного завдання здійснюється визначення функціонального профілю захисту на основі розроблених політик безпеки, моделі загроз та моделі порушника.

Експерт стикається з проблемою багатозначності відповіді: з одного боку, існує прагнення створити максимально ефективний профіль захисту, з іншого боку — реалізація такого профілю вимагає значних фінансових та часових витрат, що може негативно вплинути на ефективність і прибутковість основного завдання. Як наслідок, виникає оптимізаційна задача визначення мінімально необхідного профілю безпеки. У звичайних умовах кількість можливих профілів може досягати 15 мільярдів, що робить повний перебір варіантів надмірно витратним та неефективним. Тому розробка методів для визначення функціонального профілю захисту є актуальною науковою задачею.

Головним завданням дисертаційного дослідження О.С. Потенка була розробка методів визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз.

Отже, наукова задача, яку вирішує дисертант, є актуальною.

2. Зв'язок роботи з науковими програмами, планами, темами

Здобувач приймав участь в якості виконавця в таких НДР: «Дослідження і розробка методів розпізнавання, які базуються на використанні спектральних перетворень, для інформаційного забезпечення безпеки енергетичних об'єктів» № 0105U001296 (2005р. - 2008р.). «Дослідження та розробка методів підвищення безпеки та ефективності розподілених високопродуктивних інформаційних технологій при забезпеченні завдань забезпечення безпеки » №0108U010588 (2009р. - 2013р.). «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014р. - 2018р.). «Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними» № 0118U002371 (2019р.-теперішній час).

3. Обґрунтованість наукових положень, висновків і рекомендацій

Дисертаційна робота є комплексним і завершеним науковим дослідженням, яке демонструє цілісний підхід до вирішення поставлених завдань. Усі основні положення та висновки роботи відповідають загальновизнаними науковими принципами або ґрунтуються на отриманих експериментальних результатах. Ці результати пройшли апробацію на ряді локальних та загальнонаціональних наукових конференціях в Україні, що підтверджує їхню наукову значимість та відповідність сучасному рівню знань у відповідній галузі.

Достовірність отриманих результатів також підтверджується позитивним досвідом практичного використання розробленого програмного додатку для визначення функціонального профіля захисту, що підтверджується наданими в дисертації актами впровадження, які свідчать про успішне застосування розробки.

4. Наукова новизна отриманих результатів

– Вперше запропоновано критерії для визначення функціонального профілю захисту. Ці критерії використовують аналіз цільової функції за методом Беллмана, а також оцінку математичного сподівання успішної протидії окремої функціональної послуги безпеки. За допомогою цих критеріїв можна у формальному вигляді визначити необхідний набір послуг безпеки, який потрібен для ефективного вибору рівня захисту.

– Вдосконалено метод визначення функціонального профілю захисту для різних класів автоматизованих систем, що дозволяє автоматизувати процес створення функціонального профілю захисту та його порівняння з відповідним рівнем захисту за рахунок використання розподілу однорідних ресурсів.

– Вперше запропоновано спосіб перевірки збіжності для методу визначення функціонального профілю захисту різних класів, який передбачає автоматизацію процесу адаптації до загроз, які виникають у підкласах АС. Це

допомагає знизити кількість помилок під час створення функціональних профілів захисту, забезпечуючи більш точну і ефективну оцінку захисту для кожного класу систем.

– Вперше запропоновано метод, який дозволяє визначити функціональний профіль захисту для різних класів автоматизованих систем. Цей метод включає окрему оцінку умовного рейтингу та коефіцієнта вагомості, що, у свою чергу, забезпечує зменшення часу, необхідного для складання функціональних послуг захищеності.

5. Повнота викладу основних результатів

Основні результати дисертації достатньо повно відображено в 33 наукових працях, серед яких: 1 стаття у науковому періодичному виданні, що індексується наукометричною базою даних Scopus, 11 статей у наукових фахових виданнях України, 20 тез та матеріалів конференцій та 1 свідоцтво про реєстрацію авторського права на твір.

За результатами аналізу списку праць, можна вважати, що дисертаційна робота пройшла достатню апробацію. Кількість публікацій, а також їх рівень, дозволяють вважати, що за цими показниками, представлена до захисту робота, відповідає вимогам до кандидатських дисертацій.

У тексті дисертації є посилання на всі праці інших авторів. При цьому випадків плагіату не виявлено.

6. Оцінка змісту дисертації, її завершеності й оформлення

Структура дисертації відповідає прийнятим для наукового дослідження вимогам. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, списку використаних джерел та додатків.

У вступі представлено загальну характеристику дисертаційної роботи, обґрунтовано актуальність і значення теми дослідження, визначено його мету, завдання, об'єкт і предмет. Зазначено наукову новизну і практичну цінність

роботи, а також інформацію про апробацію та впровадження результатів і про структуру дисертації.

Перший розділ присвячений дослідженню і аналізу небезпек, що виникають у сфері інформаційного забезпечення кібероб'єктів, які підтримують технологічні процеси. Розглядаються міжнародні критерії безпеки комп'ютерних систем. Проводиться детальний аналіз, систематизація існуючих критеріїв і їх формалізація для створення єдиного підходу до оцінки безпеки комп'ютерних систем. Також проводиться аналіз вітчизняних критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, відповідно до НД ТЗІ 2.5-004-99. Вивчаються особливості і вимоги, що застосовуються в Україні, для оцінки рівня захищеності інформаційних систем від потенційних загроз. Перший розділ також містить порівняльний аналіз методів визначення функціональних профілів захисту автоматизованих систем від несанкціонованого доступу. У цій частині розглядаються різні методи та підходи, їхні переваги і недоліки, а також проводиться порівняння їх ефективності у забезпеченні захисту систем.

Другий розділ присвячено формуванню профілів протидії загрозам за допомогою динамічного програмування з використанням оптимального принципу Р. Беллмана. Автор розглядає теоретичні основи динамічного програмування. Проводиться загальновідомих аналіз задач оптимізації за Беллманом, зокрема застосування детермінованих методів для розподілу однорідних ресурсів, при цьому точне математичне формулювання цих задач є важливим для повного розуміння запропонованої інтерпретації. Також в другому розділі автор роботи розробляє новий метод оцінки та оптимізації інформаційної безпеки автоматизованих систем за мультикритерієм «ризик безпеки – гарантія безпеки – вид ІД – вартість». В кінці розділу описуються вимоги до алгоритмічної реалізації визначення профілю протидії загрозам.

Третій розділ зосереджений на алгоритмічній реалізації методів для визначення функціонального профілю захисту. Автором розроблено алгоритм, що забезпечує ефективну перевірку збіжності методу (ПЗМ) при створенні

адаптивних профілів для підкласів автоматизованих систем. Проведені тестові розрахунки для перевірки правильності реалізації алгоритму, а результати цих розрахунків будуть використані в четвертому розділі. Також в розділі перевірено працездатність методу з урахуванням заданих обмежень. Розроблено алгоритм для визначення функціонального профілю захисту автоматизованої системи ВФПЗАС, який враховує рівень загроз для підкласів К, Ц, Д, КЦ, КД, ЦД, КЦД. В розділі також визначені вимоги до програмної реалізації програмного забезпечення.

У четвертому розділі розглядається програмна реалізація методів для визначення функціонального профілю захисту. Описано як програмну реалізацію тестового алгоритму, призначеного для перевірки збіжності методу (ПЗМ), так і розроблену автором програмну реалізацію методу визначення функціонального профілю захисту автоматизованих систем ВФПЗАС. Представлені результати тестування програмного модуля для перевірки збіжності методу визначення профілю захисту. Окрім того, проведено порівняльний аналіз запропонованого методу ВФПЗАС з іншими методами створення профілів захисту. В розділі також надано приклади державних експертиз КСЗІ, в яких були використані розробки автора цієї дисертаційної роботи.

7. Значущість висновків здобувача для науки і практики

Наукова значущість проведеного дослідження полягає в тому, що в ньому запропоновано нові методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз.

Практичну цінність виконаної роботи складає доведення отриманих результатів до розробки програмного модуля для генерації функціональних профілів безпеки з заданим рівнем загроз та визначення рівня захищеності профілю безпеки за його складом.

8. Відповідність змісту автореферату тексту дисертації.

Зміст автореферату відповідає тексту дисертації. Особистий внесок автора однаково задекларовано як у тексті автореферату, так і в тексті дисертації. Список публікацій, що стосуються теми дисертації і наведений у рефераті, збігається з переліком, зазначеним в анотації дисертації та додатках до неї.

9. Зауваження до дисертаційної роботи

1. У вступі перераховуються вчені, які зробили внесок у розвиток методів побудови комплексних систем захисту інформації (КСЗІ), але не описано, що саме зробив кожен з них.

2. На сторінці 30 невдало підібрана розподільна здатність рисунку 1.1, це повторюється також в деяких інших рисунках, зокрема в першому розділі, що негативно впливає на їх сприйняття самих.

3. Висновки до першого розділу невдало сформульовані: доцільно було б перерахувати в висновках, про які саме методи йдеться мова, як це зроблено в таблиці 1.1.

4. В другому розділі (с.68, задача 4б) вказані умови (13) та (15), проте далі по тексту не зрозуміло, про що саме йде мова.

5. В роботі для визначення функціонального профілю безпеки та розрахунку математичного очікування його протидії загрозам використовується рівняння Беллмана. Доцільно було б вказати, чому саме вибрано це рівняння, а не інші підходи.

6. В тексті роботи присутні деякі скорочення, зокрема СФПЗ та СФП, які відсутні в переліку умовних скорочень.

7. У тексті дисертації присутні граматичні та стилістичні помилки.

Однак зазначені зауваження не мають істотного впливу на наукову і практичну цінність дисертаційної роботи.

10. Загальний висновок по дисертаційній роботі:

Вважаю, що дисертаційна робота Потенка Олександра Сергійовича на тему «Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз» є завершеною науковою працею, що містить нові науково обґрунтовані результати, які дозволили автору досягти мети: розробки методів визначення функціонального профілю захисту. Обсяг та науковий рівень дисертації є достатнім.

Представлена дисертація відповідає вимогам спеціальності 05.13.21 – системи захисту інформації. Виявлені зауваження не ставлять під сумнів достовірність результатів і не є критичними для загальної позитивної оцінки.

Дисертаційна робота відповідає вимогам Порядку присудження наукових ступенів, а її автор, Потенко Олександр Сергійович, заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
к.т.н., професор
кафедри інженерії програмного
забезпечення та кібербезпеки
Державного торговельно-економічного
університету Юлія ХОХЛАЧОВА

Підпис Юлії Хохлачової засвідчую
Начальник відділу кадрів
Ідентифікаційний код 44470624