ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

про дисертаційну роботу Стрєлкіної Анастасії Андріївни «Моделі та методи інформаційної технології забезпечення гарантоздатності медичних систем на основі Інтернету речей», представлену на здобуття наукового ступеня доктора філософії за спеціальністю 122 - комп'ютерні науки

Актуальність теми дисертації. Медичні інформаційні системи стають все більш популярними на фоні глобальних проблем, що виникають у сфері охорони здоров'я. Такі системи дозволяють не тільки спрощувати організацію надання допомоги населенню, робити її більш гнучкою і оперативною, але й забезпечувати необхідною інформацією медичні структури, створюючи необхідні банки даних, та підтримуючи процеси прийняття рішень. Особливо значення медичних інформаційних систем зросло з появою Інтернету речей (IoT), що надало можливість значно розширити перелік функцій, які підтримуються даними системами.

В той же час медична IoT система є системою з особливими вимогами до безпеки. Для таких систем характерна велика кількість відмов через динамічність, багатокомпонентність та багаторівневість. Під час використання мережевих медичних пристроїв, які працюють, як правило, у хмарному середовищі та під впливом кібератак, виникають проблеми, пов'язані із оцінюванням та забезпеченням гарантоздатності медичних IoT систем, що є само по собі вкрай трудомістким процесом. Існуючі моделі і методи проведення такого оцінювання недостатньо формалізовані, не відповідають сучасним підходам до забезпечення гарантоздатності, не мають відповідних інструментальних засобів підтримки.

У зв'язку з цим існує необхідність удосконалення інформаційних технологій оцінювання і забезпечення гарантоздатності медичних систем (МС) на основі Інтернету речей з урахуванням атак на вразливості і дефектів програмних та апаратних компонент, процедур функціонування медичних пристроїв, що визначає актуальність теми дисертаційної роботи.

Визначальним з точки зору актуальності є також те, що дане дисертаційне дослідження відповідає пріоритетному напряму розвитку науки і техніки

України «Інтелектуальні інформаційні та інформаційно-аналітичні технології» та збігається з основними науковими напрямами та найважливішими проблемами фундаментальних досліджень в галузі інформатики, а саме розробкою і застосуванням методів та засобів підвищення живучості складних комп'ютерних систем. Робота виконувалася у відповідності до державних планів НДР, проєктів Європейського союзу за програмами TEMPUS і ERASMUS+.

Обгрунтованість наукових положень, висновків і рекомендацій. Теоретичні й практичні добутки, отримані автором під час проведення дослідження, базуються на сучасних досягненнях у галузі системного аналізу, теорії множин, теорії ймовірностей, математичного апарату марковських процесів, методів розв'язання лінійних систем диференційних рівнянь, сучасних методів математичного моделювання поведінки складних систем, теорії ігор, методів об'єктно-орієнтованого та функціонального аналізу. Достовірність отриманих результатів забезпечується коректною постановкою задач, коректним використанням математичного апарату. Висунуті положення перевірені шляхом порівняння результатів модельних експериментів з відомими статистичними даними. Зроблені висновки та надані рекомендації знайшли своє втілення в розроблених моделях, методах, методиках і програмних засобах.

Наукова новизна та теоретична цінність результатів дисертаційної полягає в наступному:

– удосконалено комплекс моделей оцінювання гарантоздатності медичних систем на основі Інтернету речей шляхом врахування різних функціональних станів, типів відмов та кібератак, що дає змогу розраховувати показники готовності, функціональної безпеки, кібербезпеки, визначати їх залежність від параметрів медичних мобільних пристроїв та хмарного середовища;

– вперше одержано модель функціональної поведінки медичного пристрою, яка, на відміну від відомих, враховує різні закони розподілу часу між заявками на обслуговування, а також різні типи відмов за рівнем критичності, що дозволяє визначити вплив показників медичного пристрою на готовність та гарантоздатність медичної IoT системи в цілому;

– набув подальшого розвитку метод забезпечення кібербезпеки медичних систем на основі Інтернету речей шляхом вибору контрзаходів з використанням

теорії матричних ігор, що дозволяє вибирати за максімінним критерієм множину засобів захисту;

– удосконалено метод кейс-орієнтованої оцінки кібербезпеки медичних систем на основі Інтернету речей за рахунок формування профільоутворюючої бази стандартів та функціональних вимог, а також процедури вибору інструментів оцінювання, що дозволяє підвищити повноту оцінювання.

Практичне значення отриманих результатів полягає у доведенні теоретичних положень дисертації до рівня нової інформаційної технлогії, конкретних методик та інструментальних засобів, які безпосередньо використанні на профільному підприємстві ТОВ «ХАІ-МЕДИКА», що займається розробленням та впровадженням медичного обладнання, у навчальному процесі закладу вищої освіти, при виконання держбюджетних тем досліджень гарантоздатності систем критичного застосування, в міжнародних наукових та освітніх проектах за програмами TEMPUS і ERASMUS+ «SEREIN» та «ALIOT». Практичним втіленням отриманих накових результатів стали розроблені інструментальні засоби «IoHTStandard» і «GTC», які забезпечують підтримку процесів оцінювання гарантоздатності медичних IoT систем, а використання запропонованого методу забезпечення кібербезпеки призводить до зменшення неготовності медичної IoT системи в 2 рази.

Рекомендації щодо використання результатів. Отримані здобувачем доцільно спрямувати подальше впровадження їх на підприємствах та в організаціях, які займаються проектуванням та розробкою інформаційних систем критичного призначення на основі Інтернету речей, і особливо в медичній галузі, що дозволить, спираючись на отриману інформацію, приймати обґрунтовані рішення щодо підвищення рівня їх гарантоздатності.

Повнота викладу результатів роботи в опублікованих працях. Основні результати повно відображено у 17 друкованих працях (з них 5-ть відповідають вимогам щодо публікацій), а саме: 2 глави в колективних англомовних монографіях видавництв Springer та River Publishers, які включено до бази даних Scopus, 4 статті у наукових фахових виданнях України, 1 стаття, яка опублікована у періодичному науковому виданні іншої держави, що входить до Європейського Союзу, 6 англомовних публікацій в матеріалах міжнародних наукових конференцій, які включено до баз даних Scopus і Web of Science, 4

публікації тез доповідей у матеріалах наукових конференцій. Аналіз внеску здобувачки у публікаціях у співаторстві по питаннях, висвітлених в дисертації, показав на самостійність отриманих результатів.

В тексті дисертаційної роботи та публікаціях автора відсутні порушення академічної доброчесності. Дисертація оформлена згідно існуючих вимог.

Зауваження щодо змісту дисертації:

1. В назві дисертації присутнє тільки забезпечення гарантоздатності, в той час як основні результати стосуються як її оцінки, так і забезпечення.

2. Наведеним в розділі 2.1 марковським моделям бракує опису станів, що розглядаються, та позначення цих станів розходяться з позначеннями в теоретико-множинній моделі, де вони враховуються. До того ж потужності множин F, V, RI, RD в даній моделі мають однакове позначення з самими множинами. Також слід зазначити вільне (без пояснень) використання позначень і індексів, наприклад, μ_r, t_r (п. 2.2) та інших.

3. Для моделі симуляції в п.2.3.3. доречно було провести перевірку адекватності шляхом порівняння з відомими статистичними даними, на які є посилання в роботі, з обчисленням певних характеристик замість простої констатації, що результати підтверджуються.

4. В методі забезпечення кібербезпеки, описаному в п.3.2, ігрова ситуація описується як матрична гра з природою, в той час, як вона є антагоністичною матричною грою, оскільки вважається, що атакуючий має на меті завдати якомога більшої шкоди медичній IoT системі, тож не є байдужим до результатів гри.

5. Не роз'яснено, яким чином за результатами симуляції моделі готовності медичної IoT системи, яка враховує атаки на компоненти, можуть бути отримані як експертні оцінки ймовірності кібератак на 4-му етапі запропонованого метода забезпечення кібербезпеки.

6. У тексті дисертації зустрічаються не роз'яснені терміни, наприклад, «повнота оцінювання гарантоздатності» (стор. 3), віктимізація (стор. 41), некоректні висловлювання, наприклад, «прикладна інформаційна технологія» (стор. 19), «функції готовності моделей кібератак» (стор. 74) та зустрічаються орфографічні помилки.

Висновки. Вказані зауваження суттєво не зменшують загальну позитивну оцінку роботи. Автор досягла поставленої мети з підвищення гарантоздатності медичних систем на основі Інтернету речей, базуючись на розробці та практичному застосуванні моделей та методів запропонованої інформаційної технології.

Дисертація є завершеним самостійним дослідженням, у якому розв'язується наукове завдання з розроблення моделей та методів інформаційної технології забезпечення гарантоздатності медичних систем на основі Інтернету речей з урахуванням атак на вразливості і дефекти програмних та апаратних компонентів, а також процедур функціонування медичного пристрою, що має істотне значення для галузі інформаційних технологій.

За актуальністю обраної теми, обґрунтованістю наукових положень, сформульованих висновків і рекомендацій, їх новизною, повнотою викладення в наукових публікаціях та відсутністю порушень академічної доброчесності дисертаційна робота відповідає вимогам пунктів 9-12 Порядку проведення експерименту з присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 06 березня 2019 року № 167, а її автор – Стрєлкіна Анастасія Андріївна заслуговує на присудження їй наукового ступеня доктора філософії за спеціальністю 122 - комп'ютерні науки.

Професор кафедри інформаційних та комп'ютерних систем
Чернігівського національного технологічного університету,
лауреат Державної премії України у галузі науки і техніки,
лауреат Державної премії України у галузі освіти,
доктор технічних наук, професор В. В. Казимир

«15» квітня 2020 р.

Підпис Казимира В.В. завіряю.
Вчений секретар ЧНТУ І.М. Олійченко