Отримано
28.05.2024 р.
Голова спеціалізованої
вченої ради
ДФ 26.133.062
д.ф.-м.н., проф. Н.В. Коршун

Голові спеціалізованої вченої ради
ДФ 26.133.062
у Київському столичному університеті імені Бориса Грінченка
доктору технічних наук, професору
професору кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка
Коршун Наталії Володимирівні

ВІДГУК

офіційного опонента **СМІРНОВА Олексія Анатолійовича**, доктора технічних наук, професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету на дисертацію **ЧЕРНЕНКА Романа Миколайовича «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей»** подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації

1. Актуальність теми дослідження.

Сьогодні інтернет стає все більш важливим для суспільства як в приватному, так і в професійному напрямку. Різні пристрої, такі як смартфони, сенсори, комп'ютери та інші «розумні» об'єкти, є прикладами речей, якими люди щоденно користуються. Технології пов'язані з інтернетом речей, значно впливають на сучасні інформаційно-комунікаційні технології та функціонування підприємств, зокрема об'єктів критичної інфраструктури. З точки зору інновацій та розвитку економіки, значна увага змістилася на технології, пов'язані з інтернетом речей. Інтернет речей розглядається як основа майбутнього інтернету оскільки він забезпечує функціонування комунікації пристроїв, розумних об'єктів, систем та послуг між різними пристроями та людиною.

Коли мільярди розумних пристроїв, що працюють на різних платформах, підключаються до інтернету, особливо коли переходять від настільних комп'ютерів до малих пристроїв, вони створюють широкий спектр нових і непередбачених загроз для їх власників або користувачів, таких як безпека та конфіденційність, сумісність, наявність оновлень. Крім того, пристрої інтернету речей мають значні вразливості з точки зору кібербезпеки, оскільки вони безпосередньо взаємодіють з контрольованими об’єктами для збору конфіденційних даних або керування змінними фізичного середовища, що

робить їх привабливою мішенню для атак. Усі ці обставини роблять кібербезпеку ключовим аспектом для пристроїв інтернету речей, висуваючи вимоги до конфіденційності, цілісності даних, аутентифікації та авторизації, доступності. У цьому контексті криптографія може бути одним з ефективних заходів для забезпечення кібербезпеки таких пристроїв. Однак сучасні алгоритми криптографічного захисту, не завжди працюють ефективно для більшості пристроїв інтернету речей, включаючи сенсори та мітки RFID, через їх обмежені обчислювальні ресурси.

Таким чином, дослідження і розробка моделей та методів криптографічного захисту інформації які могли б ефективно функціонувати на пристроях з обмеженими обчислювальними ресурсами в мережах інтернету речей є важливою задачею для забезпечення кібербезпеки мереж інтернету речей.

2. Зв'язок теми дисертаційної роботи з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертація виконана на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка відповідно до теми науково-дослідної роботи та індивідуального плану аспіранта Київського столичного університету імені Бориса Грінченка. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КУБГ, м. Київ).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їхня достовірність

Зміст дисертаційної роботи повною мірою розкриває тему наукового дослідження та відповідає визначеним меті, завданням, об'єкту та предмету дослідження. Розроблені автором і викладені у дисертаційній роботі наукові положення, висновки та рекомендації є аргументованими та обґрунтованими, сформульовані чітко, логічно і послідовно.

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості та достовірності, оскільки при її підготовці:

1) опрацьовано значну кількість літературних джерел зарубіжних і вітчизняних вчених, проаналізовано нормативно-правове забезпечення та

приділено значну увагу дослідженню та можливості впровадження іноземного досвіду;

2) використано широкий спектр загальнонаукових і спеціальних методів дослідження – індукції і абдукції, системного аналізу, елементарно-теоретичного та структурно генетичного аналізу, системно-структурного підходу, теорії ймовірностей та математичної статистики; моделювання та експеримент;

3) вміло використано значний масив статистичного і фактологічного матеріалу, який якісно опрацьовано і подано в таблицях;

4) здійснена апробація результатів дослідження, про що свідчить перелік наукових праць здобувача;

5) результати наукових досліджень прийняті до впровадження в діяльність кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка, ТОВ «2Д3Д» та в ТОВ «Технологічні ІТ рішення».

Дисертаційна робота Черненка Р.М. є оригінальною науковою працею, яка виконана на належному теоретичному та методичному рівнях. Робота має послідовну та логічну структуру і є комплексним, завершеним науковим дослідженням. Зміст роботи та багатогранність висвітленої проблеми свідчать про високий рівень наукової компетентності автора.

Викладене вище дає можливість висловити позитивний висновок стосовно наукового рівня, достовірності подання в дисертації матеріалу, теоретичних обґрунтувань і аргументації всіх положень, практичного значення висновків і рекомендацій.

4. Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

У дисертаційному дослідженні Черненка Р.М. сформульовано та обґрунтовано ряд наукових положень, висновків і рекомендацій, які відзначаються наявністю наукової новизни. До положень, що відображають наукову новизну дисертаційного дослідження, можна віднести результати, отримані дисертантом самостійно, а саме:

– запропоновано метод криптографічного захисту інформації в мережі інтернету речей на основі модифікованого алгоритму A5/1, що забезпечує підвищену стійкість шифрування та імітостійкість завдяки застосуванню байтової обробки інформації та застосування вузла накладання шифру на основі змінного латинського квадрату;

– вдосконалено стандартний протокол Shockburst безпроводового інформаційного обміну в мережі, з метою безпечного формування сеансових ключів та забезпечення криптографічно захищеної передачі даних від пристроїв з обмеженими обчислювальними ресурсами до шлюзу;

– подальшого розвитку набула модель загроз для побудови системи захисту інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами в мережі інтернету речей.

Слід підкреслити, що отримані результати розширюють попередні наукові дослідження проблем криптографічного захисту інформації в мережах інтернету речей.

5. Теоретична цінність і практична значущість наукових результатів.

Проведене Черненком Р.М. дослідження має як теоретичне, так і прикладне значення, що є певним внеском дисертанта в кібербезпеку, а саме, в частині проблематики захисту інформації в мережах інтернету речей.

Теоретичне значення розробок визначається в розширенні та уточненні моделей та методів захисту інформації в мережах інтернету речей, систематизації загроз безпеки інформації, що передається відкритими каналами в мережах інтернету речей.

Практична значущість дослідження полягає у розробці методу криптографічного захисту інформації на основі модифікованого алгоритму A5/1, що передається відкритими каналами зв'язку пристроями з обмеженими обчислювальними ресурсами в мережі інтернету речей. Практичні рішення наукових досліджень прийняті до впровадження в діяльність кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка (акт від 15.01.2024), ТОВ «2Д3Д» (довідка від 16.01.2024) та в ТОВ «Технологічні ІТ рішення» (довідка від 16.01.2024 року).

Запропоновані рішення можуть використовуватися для таких галузей як інтернет речей, телеметрія, дистанційне управління інфраструктурними об’єктами, побутові розумні пристрої тощо.

6. Повнота викладення наукових результатів дисертації в опублікованих працях.

Результати дисертаційної роботи, висновки та рекомендації знайшли відображення в іноземних та вітчизняних наукових виданнях.

За темою дослідження опубліковано 5 наукових праць, з них 4 опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України та 1 опублікована у закордонному науковому виданні, що входить до наукометричної бази Scopus.

Слід відзначити належний рівень апробації досліджень та їх представлення на конференції Workshop on Cybersecurity Providing in Information and Telecommunication Systems (Scopus).

Обсяг і зміст опублікованих праць свідчать, що в них висвітлені основні

положення проведеного наукового дослідження, які були апробовані й отримали позитивну оцінку на наукових заходах різних рівнів. У роботах, опублікованих у співавторстві, зазначено особистий внесок здобувача.

7. Відсутність (наявність) порушення академічної доброчесності.

Аналіз тексту дисертації, а також публікації здобувача свідчать про відсутність ознак порушення вимог академічної доброчесності. Зокрема, дисертаційна робота містить посилання на джерела інформації у випадку використання ідей, розробок, тверджень, відомостей; відповідає нормам законодавства про авторське право і суміжні права; відображає прагнення автора надати достовірну інформацію про результати власної наукової діяльності, використані методики досліджень та інформаційні ресурси. Посилання на першоджерела є коректними, навмисних спотворень не виявлено.

8. Дискусійні положення та недоліки дисертаційної роботи.

1. У другому розділі дисертаційної роботи абсолютно вірно визначено загрози та ризики захисту інформації в мережах інтернету речей. Проте не всі з них набули подальшого розвитку та належного обґрунтування в моделі загроз безпеки інформації в мережі інтернету речей.

2. У четвертому розділі автором проведено дослідження платформ для реалізації модифікованого алгоритму та оцінки швидкодії. Обрано пристрої з обмеженими обчислювальними ресурсами, що за своїми характеристиками відносяться до пристроїв класу С0, які були визначені як ті, що потребують впровадження методу криптографічного захисту інформації. Проте дослідження були б більш повними, як що автор провів аналіз роботи модифікованого алгоритму на пристроях з обмеженими обчислювальними ресурсами, що за своїми характеристиками відносяться до пристроїв класу С1.

3. Автором визначено, що напрями подальших досліджень в зазначеній галузі можуть ґрунтуватись на вдосконаленні процедур генерації випадкових параметрів. В той же час доцільно було б розглянути і методи розробки та використання унікальних ідентифікаторів для надійної ідентифікації пристроїв в мережі.

4. В розділі 3 на рисунку 3.1 вказано пристрій шлюз в моделі системи інтернету речей. Доцільно було б зазначити більш конкретні вимоги до обчислювальних ресурсів такого пристрою виходячи з його ролі в системі.

Наведені зауваження і дискусійні моменти вказують на деякі суперечливі аспекти дослідження, проте загалом вони засвідчують складність і багатогранність обраної теми, її практичну важливість та актуальність і суттєво не впливають на якісні характеристики дисертаційної роботи.

9. Загальна оцінка дисертаційної роботи, її відповідність встановленим вимогам.

Дисертаційне дослідження Черненка Романа Миколайовича на тему «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей» є завершеним науковим дослідженням, яке за актуальністю, достовірністю отриманих результатів, їхньою науковою новизною і практичною цінністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а його автор, Черненко Роман Миколайович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент:
доктор технічних наук, професор
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
Олексій СМІРНОВ

Підпис доктора технічних наук, професора, завідувача кафедрою кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету Смірнова Олексія Анатолійовича засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету
кандидат технічних наук, доцент
Андрій ТИХИЙ