Отримано
23.05.2024 р.
Голова спеціалізованої
вченої ради
ДФ 26.133.062
к.т.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

РЕЦЕНЗІЯ

ГУЛАКА Геннадія Миколайовича, доктора технічних наук, професора, професора кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка, 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 дисертаційного дослідження

Збільшення кількості атак на критичну інфраструктуру, державні та комерційні інформаційні системи та мережі в умовах повномасштабної війни призводить до гострої необхідності в удосконаленні існуючих та розробці нових методів захисту таких систем. При цьому у багатьох випадках під загрозою опиняються такі важливі характеристики цифрових потоків, як їхня конфіденційність та цілісність. Цифрові комунікаційні системи інтернету речей, які в багатьох випадках є складовою інформаційних систем критичної інфраструктури, мають власні особливості їх убезпечення з точки зору застосованого комунікаційного обладнання. Мікрокомп'ютери та контролери, що є основою інтернету речей, мають суттєві відмінності в аспекті обчислювальних можливостей та доступу до джерел живлення. Як наслідок, це

ускладнює застосування в таких мережах типових рішень та засобів криптографічного захисту інформації.

Хоча деякі з існуючих алгоритмів шифрування можуть бути реалізовані на частині відповідних пристроїв, як свідчить практика, це може призводити до значного уповільнення функціонування систем IoT. Така ситуація спостерігається з багатьма алгоритмами, що були спроєктовані для їх програмної реалізації на достатньо потужних комп'ютерах. Зокрема, їх архітектура часто не враховує обмеження пристроїв так званого класу C0, що мають менше 10 кБ оперативної та менше 100 кБ постійної пам'яті. Окрім цього, стосовно деяких відомих міжнародних стандартів криптографічних алгоритмів у науковців та спеціалістів – практиків існують зауваження щодо прозорості їхнього проєктування, що полягає у недостатності інформації щодо управління криптографічними параметрами та умов їх безпечного застосування.

Тому розробка моделей та методів захисту інформації, що передається відкритими каналами пристроями з обмеженими обчислювальними ресурсами, з метою забезпечення високої швидкодії обробки інформації, підвищеної криптостійкості та імітостійкості є вкрай актуальним та своєчасним завданням для побудови систем інтернету речей нового покоління.

2. Наукова новизна результатів дисертації

Новизна результатів дисертаційного дослідження **ЧЕРНЕНКА Романа Миколайовича** зумовлена тим, що вперше запропоновано швидкісний метод криптографічного захисту інформації в мережах інтернету речей, що реалізований на пристроях з низькими обчислювальними можливостями. Запропонований метод забезпечує підвищену стійкість шифрування та імітостійкість (безпеку щодо підробки даних), а також можливість ефективної програмної реалізації. Також в роботі з метою убезпечення процедур формування криптопараметрів був вдосконалений стандартний протокол безпроводового інформаційного обміну в мережі та уточнена модель загроз безпеки для побудови системи захисту інформації в мережах інтернету речей.

3. Теоретичне і практичне значення результатів дисертації

Наукові положення, висновки та рекомендації дисертаційної роботи **ЧЕРНЕНКА Романа Миколайовича** мають теоретичну цінність і практичну значущість. Отримані результати є певним внеском у розвиток інформаційної та кібернетичної безпеки.

Теоретичне значення дослідження полягає в обґрунтуванні необхідності та дослідженні можливості впровадження методів криптографічного захисту інформації, що передається відкритими каналами зв'язку пристроями з обмеженими обчислювальними ресурсами, в мережах інтернету речей. Це дозволяє підвищити криптостійкість, імітостійкість та забезпечити високу швидкість шифрування на пристроях з обмеженими обчислювальними ресурсами.

Пропозиції та висновки наукових досліджень мають практичне значення та 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).

4. Наукова обґрунтованість результатів дослідження, наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їхня достовірність

Наукова обґрунтованість результатів дослідження зумовлена глибоким опрацюванням теоретичних джерел та їх аналізом. Наукові положення, висновки і результати, які представлено в дисертації **ЧЕРНЕНКА Романа Миколайовича**, є теоретично і емпірично обґрунтованими та достовірними. Вони базуються на використанні загальнонаукових та спеціальних методів дослідження, таких як: системний аналіз, елементарно-теоретичний та структурно-генетичний аналіз, індукція, абдукція, моделювання, системно-структурний підхід, теорія ймовірностей та математична статистика, моделювання, експеримент. Загальні висновки дисертації логічні та переконливі. Вони повністю висвітлюють хід дослідження, поставлені завдання та результати

проведеної роботи.

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

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи №0122U200483 «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (КСУБГ, м. Київ).

Обрана тема дисертації безпосередньо пов'язана з реалізацією та виконанням доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

6. Рівень виконання поставленого наукового завдання та оволодіння здобувачем методологією наукової діяльності

Визначені в дисертації завдання здобувач виконав на високому рівні. Чітко сформульовано мету дослідження, точно сформульовано завдання та застосовано доцільні методи для її досягнення. Представлений текст дисертаційної роботи демонструє, що **ЧЕРНЕНКО Роман Миколайович** опанував методологію наукової діяльності, уміло застосовує її на практиці, а отже, оволодів необхідними для рівня доктора філософії компетенціями.

7. Апробація результатів дисертації

У наукових публікаціях у повному обсязі висвітлено наукові результати дисертації відповідно до мети та поставлених завдань. Наукові результати дисертації висвітлено у 5 наукових працях (з них 2 одноосібні): 4 статті у наукових фахових виданнях України, 1 тези доповідей у періодичному науковому виданні, включеному до міжнародної наукометричної бази Scopus. В роботах, опублікованих у співавторстві, зазначено особистий внесок здобувача.

8. Структура та зміст дисертації, її самостійність, завершеність, відповідність вимогам щодо оформлення й обсягу

Зміст дисертаційної роботи **ЧЕРНЕНКА Роман Миколайовича** «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей» охоплює основні аспекти теми, відповідає меті та завданням дослідження. Робота містить анотацію, вступ, чотири розділи основної частини з підпунктами, висновки до розділів, загальні висновки, список використаних джерел з 121 найменування та трьох додатків. Робота містить 7 таблиць та 30 рисунків. Обсяг основного тексту дисертації складається з 134 сторінок друкованого тексту. Контекст дисертаційного дослідження вирізняється логічністю, індивідуальним і творчим авторським підходом до задуму дисертації, обізнаністю автора в методологічному інструментарії, підходах, методах, принципах, обґрунтованістю висновків, оригінальному баченні дискусійних проблем.

У вступній частині автором обґрунтовано актуальність теми дослідження, визначено її зв'язок із науковими програмами, планами, темами, сформульовано об'єкт, предмет, мету і завдання дослідження, інформаційну базу, методи дослідження, наукову новизну і практичне значення роботи, особистий внесок автора, дані про апробацію отриманих результатів та публікації за темою дисертації.

У першому розділі «Теоретико-методологічні засади захисту інформації, що передається відкритими каналами зв'язку в мережах інтернету речей» **ЧЕРНЕНКОМ Романом Миколайовичем** було проведено аналіз поточного рівня розробки методів захисту інформації в мережах інтернету речей. Визначено перспективи і необхідність розробки та впровадження методів криптографічного захисту інформації в мережах інтернету речей, що обробляється пристроями з обмеженими обчислювальними ресурсами. Сформульоване актуальне наукове завдання, яке полягає в розробці моделей та методів захисту інформації, що передається відкритими каналами зв'язку пристроями з обмеженими обчислювальними ресурсами в мережах інтернету

речей. Для вирішення цього завдання визначено мету роботи – забезпечення безпеки інформаційних ресурсів в мережах інтернету речей, включаючи їх конфіденційність і цілісність, за рахунок розробки моделей і методів криптографічного захисту інформації, що передається пристроями з обмеженими обчислювальними ресурсами.

У другому розділі «Аналіз моделей та алгоритмів захисту даних на пристроях з обмеженими обчислювальними ресурсами» здобувачем були визначені критерії для аналізу існуючих алгоритмів шифрування які здатні функціонувати на пристроях з обмеженими обчислювальними ресурсами. Проведено дослідження алгоритмів та визначено ступінь їх ефективності з точки зору швидкодії. Визначені вразливості та побудовано модель загроз яка включає найімовірніші загрози стосовно інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами.

У третьому розділ роботи «Розробка методики криптографічного захисту інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами в мережі інтернету речей» розроблено метод криптографічного захисту інформації, що ґрунтується на модифікації криптографічного алгоритму A5/1 для забезпечення комунікації пристроїв інтернету речей. Математично обґрунтовано основні модифікації, та досліджено статистичні якості шифруючої послідовності. З урахуванням результатів визначено необхідність побудови криптографічного протоколу для ідентифікації пристроїв та управління криптографічними параметрами.

У четвертому розділі «Аналіз ефективності модифікованого алгоритму A5-128 для захисту інформації в мережах інтернету речей» здійснено дослідження платформ для реалізації запропонованого методу. Вдосконалено стандартний протокол безпроводового інформаційного обміну. Практично реалізовано систему інтернету речей з впровадженням модифікованого алгоритму та проведено аналіз та оцінка ефективності методу криптографічного захист інформації.

9. Дотримання академічної доброчесності у дисертації та наукових публікаціях. Відсутність (наявність) академічного плагіату, фабрикації, фальсифікації

Аналіз тексту дисертаційного дослідження та публікацій дозволяє стверджувати, що **ЧЕРНЕНКО Роман Миколайович** дотримувався правил академічної доброчесності, в тексті не знайдено некоректного цитування, ознак плагіату, фабрикації чи фальсифікації. Дисертаційна робота є оригінальним завершеним науковим дослідженням, що відповідає вимогам, які висуваються Міністерством освіти і науки України до оформлення дисертацій на здобуття наукового ступеня доктора філософії.

10. Дискусійні положення, недоліки та зауваження до дисертації

Принципових зауважень щодо структури, основних положень та концепції дисертації **ЧЕРНЕНКА Романа Миколайовича** немає. Оцінюючи загалом позитивно наукове і практичне значення отриманих дисертантом результатів, дозволю собі висловити зауваження і рекомендації до окремих положень дисертації.

1. Обґрунтування в 1 розділі напряму досліджень уявляється дещо скороченим, деякі положення щодо наукових публікацій про криптографічні дослідження алгоритму A5/1 було б доцільно перемістити з 3-го до 1-го розділу.

2. В розділі 2.2 для опису існуючих стандартних алгоритмів захисту подекуди використовуються оператори мов програмування без детального пояснення їх суті.

3. Після таблиці 2.1 порівняння алгоритмів було б доцільно зробити відповідні висновки.

4. Для посилань на джерело інформації поряд з формою *[номер]* використовується форма *[номер, сторінка]*. Було б доцільно використовувати уніфіковане посилання.

5. Після таблиці 2.2 було б доцільним надати розширений коментар щодо можливих наслідків реалізації визначених загроз для безпеки IoT.

6. На с. 94 у третьому абзаці для позначення нерівності бітів замість

звичайного математичного символу «≠» використано елемент програмного коду «!=».

7. В формулі 3.10 записано $S_{abs}/\sqrt{2}$ що не відповідає вірному текстовому коментарю, а також замість поняття інтеграл Лапласа використано комп'ютерний термін для відповідної функції.

8. Для запропонованого криптографічного рішення було б доцільно визначити його клас безпеки згідно державної класифікації (джерело [99]).

9. В тексті роботи присутні окремі семантичні, синтаксичні та граматичні помилки.

10. У списку використаних джерел присутні окремі посилання, що оформлені не за стандартними вимогами.

11. Загальний висновок про рівень набуття здобувачем теоретичних знань, відповідних умінь, навичок та компетентностей

ЧЕРНЕНКО Роман Миколайович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом дослідження та має достатній досвід для проведення самостійних дослідницьких робіт.

12. Загальна оцінка дисертації і наукових публікацій щодо їхнього наукового рівня з урахуванням дотримання академічної доброчесності та щодо відповідності вимогам

Дисертаційна робота 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 її автор, Черненко Роман Миколайович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації.

Рецензент:

доктор технічних наук, професор,
професор кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка

Геннадій ГУЛАК

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Г. Гулака (ПІБ) ЗАСВІДЧУЄ
Пров. фах. ВК Деканат і.В (посада)