Отримано
22.05.2024 р.
Голова спеціалізованої
вченої ради
ДФ.26.133.062
д.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

СОКОЛОВА Володимира Юрійовича, кандидата технічних наук, доцента, доцента 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. З іншого боку, кількість пристроїв інтернету речей неуклінно зростає. Ці пристрої часто мають обмежені обчислювальні ресурси і можуть бути розгорнуті в різних, а іноді й ворожих середовищах, що робить їх та методи передавання даних вразливими. Багато пристроїв інтернету речей обробляють конфіденційні дані, такі як особиста інформація, медичні записи та фінансові дані. Захист передачі цих та забезпечення безпеки цих даних має

вирішальне значення для захисту від несанкціонованого доступу, витоку даних і кібератак.

Оскільки кількість і різноманітність пристроїв інтернету речей продовжує зростати, все більше уваги буде приділятися стандартам інтероперабельності. Це включає в себе розробку протоколів і фреймворків, які забезпечують безперебійну комунікацію та інтеграцію між різними пристроями і платформами інтернету речей. Що, в свою чергу, потребує розробки надійних методів шифрування, механізмів автентифікації та безпечних протоколів зв'язку для захисту даних від кіберзагроз і несанкціонованого доступу. Також слід зазначити, що потреби в збільшені часу автономної роботи мереж інтернету речей надаватимуть пріоритет стійкості та енергоефективності. Це включає розробку енергоефективних пристроїв інтернету речей, оптимізацію мережевих протоколів і використання ефективних і надійних джерел енергії для живлення інфраструктури інтернету речей.

Тому вдосконалення захисту інформації, що передається відкритими каналами в інформаційних системах та мережах інтернету речей як критичної інфраструктури, так і комерційного напрямку є вкрай актуальним та своєчасним для побудови систем нового покоління.

2. Наукова новизна результатів дисертації

Новизна результатів дисертаційного дослідження **ЧЕРНЕНКА Романа Миколайовича** зумовлена тим, що вперше розроблено 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. А також були вдосконалені стандартний протокол Shockburst безпроводового інформаційного обміну в мережі та модель загроз для побудови системи захисту інформації з обмеженими обчислювальними ресурсами в мережі інтернету речей.

3. Теоретичне і практичне значення результатів дисертації

Теоретичне значення дисертаційної роботи **ЧЕРНЕНКА Романа Миколайовича** не викликає сумніву, оскільки автор пропонує застосовувати криптографічні перетворення, що забезпечують підвищений рівень конфіденційності, криптостійкості, імітостійкості та високу швидкість шифрування на основі модифікації стандартного криптографічного алгоритму A5/1 через ключові фактори:

– визначення недоліків існуючих криптографічних алгоритмів для пристроїв класу C0, C1 та C2;

– збільшення швидкодії криптографічного алгоритму A5/1 за допомогою його модифікації на 30.7%;

– вдосконалення протокол Shockburst безпроводового інформаційного обміну при формуванні сеансових ключів;

– уточнення моделі загроз системи захисту інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами в мережі інтернету речей;

– оцінка функціонування модифікованого алгоритму шляхом використання набору статистичних тестів;

– зменшення споживання енергії на 3.62% за рахунок використання криптографічного алгоритм A5-128;

– рекомендації, щодо впровадження методу криптографічного захисту інформації, що передається відкритими каналами зв'язку пристроями з обмеженими обчислювальними ресурсами та описаний алгоритм роботи даної моделі.

Таким чином, наукове обґрунтування вдосконалення криптографічних методі та уточнення моделей загроз для забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей, набуває вагомості, оскільки вона гармонізується із сучасним ландшафтом кібербезпеки безпроводових мереж, розв'язує проблеми, пов'язані з використанням сенсорів на підприємствах критичної інфраструктури та еволюцією характеру

кіберзагроз. Цей підхід забезпечує прогнозовану та адаптивну реакцію на виклики, які виникають при захисті конфіденційної та персональної інформації в системах критичної інфраструктури та приватних підприємств.

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: системного аналізу, елементарно-теоретичного та структурно-генетичного аналізу, індукції, абдукції, системно-структурного підходу, теорії ймовірності, математичної статистики тощо. 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). А також результати наукових досліджень прийняті до впровадження в діяльність ТОВ «2Д3Д» (акт від 16.01.2024 р.) та в ТОВ «Технологічні ІТ рішення» (акт від 16.01.2024 р.).

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

Повнота викладу основних результатів дисертації у наукових публікаціях. 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 яких дві одноосібної): 4 статті у наукових фахових виданнях України, 1 тези доповідей у періодичному науковому виданні, включеному до міжнародної наукометричної бази Scopus. Основні положення, висновки і результати дослідження викладались і у процесі виступів і обговорень на науково-практичній міжнародній конференції. 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 Романа 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 найменувань та трьох додатків. Робота містить 7 таблиць та 30 рисунків. Обсяг основного тексту дисертації складається з 150 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, її зв'язок із науковими програмами, планами, темами, мету і завдання дослідження, сформульовано об'єкт, предмет, 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 розвитку пристроїв інтернету речей типу M2M. Визначено поточний стан і проблеми захисту інформації, що передається відкритими каналами зв'язку в мережах інтернету речей. Проаналізовано підходи до стандартизації передачі інформації засобів перевірки достовірності і управління пристроями передачі інформації. Досліджено існуючі протоколи для передачі даних у мережі з низьким енергоспоживанням та обмеженими обчислювальними ресурсами. Порівняно методики аналізу інформаційних ризиків.

У другому розділі «Аналіз моделей та алгоритмів захисту даних на пристроях з обмеженими обчислювальними ресурсами» здобувачем були визначені критерії аналізу функціонування алгоритмів на пристроях з обмеженими обчислювальними ресурсами в мережі інтернету речей. Проведено дослідне порівняння існуючих алгоритмів захисту даних для пристроїв класу C0. Оцінене функціонування існуючих алгоритмів на пристроях з обмеженими обчислювальними ресурсами. Побудована модель загроз безпеки інформації в мережах інтернету речей.

Третій розділ роботи «Розробка методики криптографічного захисту інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами в мережі інтернету речей» містить розробку методу криптографічного захисту інформації за рахунок модифікації криптографічного алгоритму A5/1 для забезпечення комунікацій пристроїв

інтернету речей. Підсвічує особливості реалізації криптоалгоритму А5-128. Оцінює ймовірнісно-статистичні якості шифруючої послідовності та рівень інформаційного ризику з використанням алгоритму А5-128 в незахищених протоколах.

Четвертий розділ роботи «Аналіз ефективності модифікованого алгоритму А5-128 для захисту інформації в мережах інтернету речей» присвячений вибору апаратно-програмних платформ для проведення експерименту. Побудований експериментальний макет для дослідження захищеного протоколу для забезпечення безпеки даних в мережі інтернету речей. Оцінено ефективність алгоритму А5-128 на пристроях з обмеженими обчислювальними ресурсами.

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 дисертанткою результатів, дозволю собі висловити зауваження і рекомендації до окремих положень дисертації.

1. Наведена в таблиці 1.1 класифікація пристроїв з обмеженими обчислювальними ресурсами не дозволяє однозначно визначити, до якого класу відноситься пристрій, через неточні критерії визначення цих класів.

2. Перелік рівнів (фізичний, мережевий і прикладний) на сторінках 27 і 28 не узгоджуються з рівнями (канальний, мережевий, транспортний і прикладний), зазначеними на рисунку 1.4.

3. Поняття «розшифрування» і «дешифрування» використовуються непослідовно, наприклад, для позначення однієї і тої самої процедури на рисунку 3.2 використані різні поняття.

4. В формулі (3.1) не вистачає групуючих душок.

5. Формула в кінці третього абзацу на сторінці 94 має двозначний характер: замість «! =» має бути знак нерівності.

6. Невірно зазначені одиниці вимірювання («мБ» і «гБ») в останньому абзаці на сторінці 115.

7. Не зрозуміло, чому на рисунках 2.5, 2.7, 2.8 і 4.8 за базовий відлік вибрана одиниця.

8. В першому отриманому результаті в «Висновках» представлена зайва інформація загального характеру. Висновки неточно відповідають поставленим завданням.

9. Також присутні незначні зауваження до розділових знаків і узгодженості словосполучень, вирівнювання тексту тощо. Пункт «1.6. Обґрунтування мети та задач дослідження» в першому розділі є зайвим, бо він частково дублює інформацію наведену у вступі. У вступі відсутня інформація про мету дослідження. Відсутнє посилання на рисунок 2.9 в тексті пояснювальної записки. Схема керування рухом регістрів на рисунку 3.4 має бути в основну тексті. На рисунку 4.7 зайва рамка. В тексті зустрічаються абревіатури (AEAD, LTE, НСД, DDoS тощо), які не використовуються в подальшому. Також на рисунку 2.9 та в назві пункту 1.1 використані скорочення. Таблиця 4.1 розірвана. В списку використаних джерел гіперпосилання оформлені в різний спосіб. Для джерел 18, 60, 83 і 98 замість посилань на джерело приведені посилання на картки робіт у наукометричних базах. Використання великих літер в англійських заголовках носить безсистемний характер.

В цілому, наведені зауваження не знижують наукової та практичної

цінності проведеного **ЧЕРНЕНКОМ Романом Миколайовичем** дослідження та не відбиваються на загальній позитивній оцінці дисертації.

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:

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

Соколов В.Ю.

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
* ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
В. Соколова (ПІБ) ЗАСВІДЧУЄ
Нач. інф.-орг. відд. ВК Лисогор І.В. (посада)