Отримано 23.05.2024 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

**ВІДГУК**

офіційного опонента ГНАТЮКА Сергія Олександровича,
доктора технічних наук, професора, в.о. проректора з наукової роботи
Національного авіаційного університету на дисертацію ЧЕРНЕНКА Романа
Миколайовича за темою «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**

Інтернет речей (IoT) є однією з найбільш використовуваних технологій станом на сьогодні і беззаперечно має вплив на функціонування суспільства у різних сферах, включаючи соціальні, комерційні та економічні аспекти. Пристрої IoT, орієнтовані на певні цілі з властивою їм природою, розроблені для роботи в обмеженому середовищі. З точки зору автоматизації, продуктивності та комфорту для споживачів у широкому спектрі застосувань,

сучасні та майбутні технології IoT мають суттєвий потенціал для покращення існуючих процесів. Проте кібератаки та загрози значно впливають на функціонування пристроїв мереж IoT. Існує висока ймовірність того, що системи IoT можуть бути заражені шкідливим ПЗ, інформація, що циркулює в них може бути перехоплена, модифікована.

У вбудованих системах часто зустрічаються мікроконтролери з 8-, 16- та 32-бітними процесорами, які можуть працювати неефективно, використовуючи стандартні алгоритми криптографічних перетворень. Пристрої RFID та сенсорні мережі, часто мають обмежену кількість обчислювальних ресурсів доступних для криптографічного захисту, і часто сильно обмежені витратою доступної енергії. Таким чином, стандартні алгоритми шифрування не є належним варіантом для багатьох вбудованих пристроїв.

З іншого боку, IoT зумовлює нову хвилю інновацій завдяки своїй концепції підключати інтелектуальні «речі» у фізичному світі до хмарної інформаційно-технологічної архітектури. Захист даних та конфіденційність в IoT є фундаментальними для розвитку і функціонування технології, і це створює нові виклики щодо безпеки в криптографії, автентифікації та управління ідентифікаторами.

Як наслідок, виникає необхідність в розробці моделей та методів захисту інформації, що передається в мережах IoT пристроями з обмеженими обчислювальними ресурсами за допомогою криптографічних перетворень. Саме це і зумовило вибір дисертантом Р. Черненком важливої та актуальної теми цього дослідження.

**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 факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка

відповідно до теми науково-дослідної роботи «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (реєстраційний номер 0122U200483, термін виконання 2022-2027 рр.)

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

Автор розробив і представив у своїй дисертації наукові положення, висновки та рекомендації, які мають достатню обґрунтованість. Дисертант провів обширний аналіз літературних джерел зарубіжних та вітчизняних учених і приділив увагу дослідженню та можливої адаптації зарубіжного досвіду. У процесі вирішення завдань, поставлених у дисертації, автор критично оцінював досягнення вітчизняних та зарубіжних учених, висловлюючи свою думку та демонструючи високий рівень наукової культури. Висновки та рекомендації, представлені в дисертації, логічні та є результатом всебічного та об'єктивного аналізу досліджуваних явищ з використанням сучасного наукового інструментарію. У ході дослідження було використано загальнонаукові та спеціальні методи пізнання, що дозволило дисертантові обґрунтувати теоретичні, методичні та практичні аспекти підвищення рівня безпеки інформації, що передається незахищеними каналами пристроями з обмеженими обчислювальними ресурсами в мережах IoT, за рахунок розробки й впровадження моделей і методів криптографічного захисту інформації.

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

В рамках дисертаційного дослідження сформульовано та обґрунтовано низку наукових положень, висновків та рекомендацій, що відрізняються наявністю наукової новизни. Ключовим науково новим результатом цього дослідження є концептуальне вирішення нової наукової проблеми щодо

безпечного шифрування даних на пристроях з обмеженими обчислювальними ресурсами.

Найбільш значущі наукові досягнення, які розкривають особистий внесок автора у вирішення проблеми, що вивчається, і відображають новизну дослідження, полягають, на наш погляд, у наступному:

- розроблено метод криптографічного захисту інформації в мережі IoT на основі модифікації алгоритму A5/1 для забезпечення підвищеної стійкості шифрування та імітостійкості;
- побудовано криптографічний протокол інформаційного обміну в мережі для забезпечення безпечного формування сеансових ключів та забезпечення криптографічно захищеної передачі даних від пристрою з обмеженими обчислювальними ресурсами до шлюза;
- побудовано модель загроз для системи захисту інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами в мережі IoT;
- досліджено ефективність методу захисту інформації на пристроях з обмеженими обчислювальними ресурсами із застосуванням модифікованого алгоритму шифрування на пристроях класу C0.

## 5. Теоретична цінність і практична значущість наукових результатів

Результати аналізу дисертаційної роботи та опублікованих праць свідчать про важливість отриманих результатів проведеного дослідження. Основним досягненням є можливість сформувати теоретико-методичний підхід до підвищення рівня безпеки інформації, що передається незахищеними каналами пристроями з обмеженими обчислювальними ресурсами в мережах IoT завдяки розробці та впровадженню моделей і методів криптографічного захисту інформації.

Зазначені теоретичні положення становлять основу для створення системного та уніфікованого підходу до захисту інформації в мережах IoT, що підтверджує вагомість проведеної роботи.

Висновки та пропозиції дисертаційного дослідження мають практичне значення і прийняті до впровадження в діяльність кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка (акт №1 від 15.01.2024 року), ТОВ «2Д3Д» (довідка від 16.01.2024 року) та в ТОВ «Технологічні ІТ рішення» (довідка від 16.01.2024 року).

**6. Повнота викладення наукових результатів дисертації в опублікованих працях**

За темою дослідження опубліковано 5 наукових праць, із них: у фахових виданнях МОН України – 4; у Scopus – 1 (має підтверджений ISSN-номер). За матеріалами виступів на науково-технічній конференції опубліковано тези доповідей.

У публікаціях розкрито ключові результати проведеного дослідження та його наукову новизну, що дозволяє стверджувати, що висновки та пропозиції, викладені у дисертаційному дослідженні, є апробованими.

**7. Відсутність (наявність) порушення академічної доброчесності**

За результатами перевірки дисертаційної роботи Черненка Р.М. на наявність ознак академічного плагіату встановлено коректність посилань на першоджерела для текстових та ілюстративних запозичень; навмисних спотворень не виявлено. З огляду на це, можна зробити висновок про відсутність порушень академічної доброчесності.

**8. Дискусійні положення та зауваження до дисертації**

Відзначаючи позитивні сторони роботи Черненка Р.М., слід звернути увагу на певні зауваження та дискусійні положення, які потребують додаткової аргументації, зокрема:

1. У загальних рекомендаціях щодо впровадження методу криптографічного захисту інформації, що передається відкритими каналами

зв'язку в мережах IoT, автором запропоновано передбачити додаткові джерела для формування ключа та синхромаркера для усунення наслідків фізичного впливу на АЦП, проте у самому дослідженні не представлено які саме додаткові джерела для формування ключа та синхромаркера можна використовувати.

2. У розділі 1 дисертантом здійснена спроба розгляду теоретико-методологічних засад захисту інформації, яка передається відкритими каналами зв'язку в мережах IoT, що деякою мірою перевантажила роботу фактичним матеріалом. Було б доцільніше у рамках проблеми дослідження висвітлити глибше саме питання дослідження протоколів для передачі даних у мережі з низьким енергоспоживанням та обмеженими обчислювальними ресурсами, порівняти їх за певними критеріями.

3. У табл.2.2, в якій відображена модель загроз інформації в системах IoT, вказані загрози для нейтралізації яких необхідні некриптографічні методи захисту. Доцільно було б більш детально описати шляхи нейтралізації вказаних загроз.

4. Автором проведений аналіз переваг та недоліків впровадження для модифікації алгоритму шифрування A5/1. Водночас дослідження набуло б більшого науково-практичного значення, якби дисертант узагальнив отримані результати в частині порівняння алгоритму шифрування A5/1, наприклад, з алгоритмом шифрування A5/3 який побудовано на блочному шифрі KASUMI.

5. Здобувач обмежився дослідженням статистичних характеристик модифікованого криптоалгоритму A5/1, проте варто було б також дослідити стійкість алгоритму до деяких відомих методів криптоаналізу (лінійний, диференціальний, алгебраїчний, квантовий).

6. Не всі абревіатури і скорочення винесені дисертантом у відповідний розділ на стор. 15 (НДТЗІ, КЗІ, SCADA, SMS та ін.).

Проте, зазначені недоліки не знижують ступінь наукової новизни та практичного значення одержаних в дисертації наукових результатів і, відповідно, позитивну оцінку роботи у цілому.

**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
в.о. проректора з наукової роботи
Національного авіаційного університету Сергій ГНАТЮК