Рішення разової спеціалізованої вченої ради ДФ 26.133.062 про присудження ступеня доктора філософії

Разова спеціалізована вчена рада ДФ 26.133.062 Київського столичного університету імені Бориса Грінченка виконавчого органу Київської міської ради (Київської міської державної адміністрації), місто Київ, прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології на підставі прилюдного захисту дисертації Черненка Романа Миколайовича «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей» за спеціальністю 125 Кібербезпека 12 червня 2024 року.

Черненко Роман Миколайович, 1997 року народження, громадянин України, освіта вища: закінчив у 2019 році магістратуру Київського університету імені Бориса Грінченка за спеціальністю «Кібербезпека».

Тимчасово не працює.

Дисертацію виконано в Університеті Грінченка.

Науковий керівник: Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Здобувач має 5 наукових публікаціях, а саме: 4 наукових виданнях (з них 2 у співавторстві), включених на дату опублікування до переліку наукових фахових видань України, 1 стаття (з них 1 у співавторстві) у періодичному науковому виданні, проіндексованому у базі даних Scopus.

1. Черненко, Р. М., Рябчун, О. П., Ворохоб, М. В., Аносов, А. О., & Козачок, В. А. (2021). Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. Електронне фахове наукове видання

«Кібербезпека: освіта, наука, техніка», 3(11), 124–135. https://doi.org/10.28925/2663-4023.2021.11.124135

2. Корнієць, В., & Черненко, Р. (2023). Модифікація криптографічного алгоритму a5/1 для забезпечення комунікацій пристроїв IoT. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 253–271. https://doi.org/10.28925/2663-4023.2023.20.253271

3. Черненко, Р. (2023). Оцінка продуктивності алгоритмів легкої криптографії на обмежених 8-бітних пристроях. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21). https://doi.org/10.28925/2663-4023.2023.21.273285

4. Черненко, Р. (2023). Генерація псевдовипадкових послідовностей на мікроконтролерах з обмеженими обчислювальними ресурсами, джерела ентропії та тестування статистичних властивостей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 191–203. https://doi.org/10.28925/2663-4023.2023.22.191203

У дискусії взяли участь голова і члени разової спеціалізованої вченої ради:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, зауваження та побажання:

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.

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, зауваження та побажання:

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 основному 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.

Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Механіко-технологічного факультету Центральноукраїнського національного технічного університету, зауваження та побажання:

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.

Гнатюк Сергій Олександрович – доктор технічних наук, професор, в.о. проректора з наукової роботи Національного авіаційного університету, зауваження та побажання:

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.)

Результати відкритого голосування:

«За» – 5 членів ради,

«Проти» – немає,

«Утримались» – немає.

На підставі результатів відкритого голосування разова спеціалізована вчена рада ДФ 26.133.062 присуджує Черненку Роману Миколайовичу ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Голова разової спеціалізованої
вченої ради ДФ 26.133.062 Наталія КОРШУН