ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Черненка Романа Миколайовича на тему «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей», поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дослідження. Технології інтернету речей демонструють найбільший приріст серед всіх інших цифрових пристроїв, що підключаються до мереж, при цьому велика частка таких пристроїв має значно менше обчислювальних ресурсів у порівнянні з класичними комп'ютерами. Зважаючи на те, що пристрої інтернету речей використовуються в різних сферах, в тому числі і на об'єктах критичної інфраструктури, існує необхідність забезпечення безпеки інформаційних ресурсів в мережах інтернету речей.

Деякі стандартні алгоритми криптографічного захисту інформації хоча і можуть бути реалізовані на частині таких пристроїв, проте більшість з них не враховують обмеження пристроїв класу C0 та є неефективними з точки зору продуктивності на таких пристроях. Використання неефективних алгоритмів захисту може призвести до недостатнього рівня захисту інформаційних систем та порушенню їх роботи через брак обчислювальних ресурсів.

Такий стан речей зумовлює необхідність впровадження методів криптографічного захисту інформації, що передається відкритими каналами зв'язку пристроями з обмеженими обчислювальними ресурсами в мережах інтернету речей.

Особистий внесок здобувача полягає у виборі теми дисертації, обґрунтуванні та формулюванні мети, об'єкта, методів досліджень,

визначенні завдань наукового дослідження, проведенні теоретичного обґрунтування та обробленні й аналізі даних, формулюванні висновків. В дослідженні автором:

– проаналізовані поточний стан проблеми захисту інформації, що передається відкритими каналами зв'язку в мережах інтернету речей, а також підходи, методи та сучасні практики захисту інформації в мережах інтернету речей;

– визначені критерії аналізу функціонування алгоритмів криптографічного захисту на пристроях з обмеженими обчислювальними ресурсами в мережі інтернету речей;

– здійснено детальний аналіз сучасних алгоритмів криптографічного захисту інформації та визначено їх ефективність на пристроях класу С0;

– вдосконалена модель загроз безпеки інформації в мережі інтернету речей;

– запропоновано та обґрунтовано метод криптографічного захисту інформації на основі модифікованого алгоритму А5/1, що забезпечує підвищену стійкість шифрування та імітостійкість завдяки застосуванню байтової обробки інформації та застосування вузла накладання шифру на основі змінного латинського квадрату;

– визначені особливості програмної реалізації модифікованого алгоритму з урахуванням обмежених обчислювальних ресурсів пристроїв класу С0;

– запропоновано та обґрунтовано вдосконалений протокол Shockburst безпроводового інформаційного обміну в мережі інтернету речей який враховує надійну ідентифікацію пристроїв, безпечне управління сеансовими ключами та скорочує кількість критичних криптографічних параметрів, що зберігаються на пристроях з обмеженими обчислювальними ресурсами.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії

кібербезпеки України. Дисертація виконана відповідно до планів наукової і науково-технічної діяльності Університету Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (06.22 – 06.27рр.) (реєстраційний номер: 0122U200483).

Мета дослідження полягає в забезпеченні 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.

Завдання дослідження.

– 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 розробки 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.

Об'єкт дослідження. забезпечення кібербезпеки мереж інтернету речей, що побудовані на основі пристроїв з обмеженими обчислювальними ресурсами.

Предмет дослідження. моделі та методи криптографічного захисту інформації, що передається відритими каналами зв'язку на пристроях з обмеженими обчислювальними ресурсами в мережах інтернету речей.

Методи дослідження. Для проведення досліджень в дисертації використовувалися методи системного аналізу, елементарно-теоретичного та структурно-генетичного аналізу, індукція, абдукція, моделювання, системно-структурний підхід, теорії ймовірностей та математичної статистики, моделювання, експеримент.

Експериментальна база дослідження. Достовірність дисертації підтверджується документами про впровадження у діяльність кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка (акт №1 від 15.01.2024), ТОВ «2Д3Д» (довідка від 16.01.2024) та в ТОВ «Технологічні ІТ рішення» (довідка від 16.01.2024), а також опублікованими працями та апробацією результатів наукового дослідження на конференції.

Наукова новизна одержаних результатів полягає у вирішенні актуальних наукових питань теоретичного обґрунтування та розроблення практичних рекомендацій щодо підвищенні рівня безпеки інформації, що передається незахищеними каналами пристроями з обмеженими обчислювальними ресурсами в мережах інтернету речей, за рахунок розробки й впровадження моделей і методів криптографічного захисту інформації в таких мережах. Основні положення і результати дослідження, які виносяться на захист та характеризують наукову новизну й особистий внесок дисертанта, полягають у такому:

1. Вперше запропоновано метод криптографічного захисту інформації в мережі IoT на основі модифікованого алгоритму A5/1, що забезпечує підвищену стійкість шифрування та імітостійкість завдяки застосування байтової обробки інформації та застосування вузла накладання шифру на основі змінного латинського квадрату. Алгоритм має високу швидкодію, яка на 30,70 % більше ніж у відомих алгоритмів для IoT.

2. Вдосконалено стандартний протокол Shockburst безпроводового інформаційного обміну в мережі з метою безпечного формування сеансових ключів та забезпечення криптографічного захисту передачі даних від пристроїв з обмеженими обчислювальними ресурсами до шлюзу.

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

Теоретичне значення результатів дисертації. Результати досліджень представлені у вигляді наукових положень, висновків і рекомендацій. Розроблені автором і викладені у дисертації наукові положення, висновки та пропозиції мають високий рівень обґрунтованості. Опрацьовано значну кількість наукових, публіцистичних та фахових джерел вітчизняних і зарубіжних вчених, здійснено їх аналіз та запропоновано власні підходи, що стосуються підвищення рівня безпеки інформації, що передається незахищеними каналами пристроями з обмеженими обчислювальними ресурсами в мережах інтернету речей.

Дисертація характеризується науковою глибиною та логічністю. Черненко Р.М. володіє ґрунтовними знаннями предмета дослідження, а також методології досліджень. Основні положення, висновки та рекомендації теоретичного та практичного характеру є обґрунтованими та достовірними. Результатом проведеного наукового дослідження є досягнення визначеної мети шляхом виконання поставлених дисертантом завдань, про що свідчать висновки до кожного розділу та дисертації загалом.

Практична значення результатів дисертації полягає в тому, що в дослідженні запропоновано метод криптографічного захисту інформації на основі модифікованого алгоритму A5/1, що передається відкритими каналами зв'язку пристроями з обмеженими обчислювальними ресурсами в мережі інтернету речей. Модифікований алгоритм не вимагає великої кількості обчислювальних ресурсів та може використовуватись на пристроях класу C0. Він є ефективнішим від існуючих рішень по таким показникам: має

на 30,70% вищу швидкість шифрування в порівнянні з існуючими алгоритмами для IoT. При цьому споживає на 3,62% менше енергії, та забезпечує підвищену імітостійкість шифрування.

Слід відзначити розробки дисертанта, які мають практичну цінність та доведені до практичного використання. Розробки та рекомендації мають практичне застосування у діяльності:

- Київського столичного університету імені Бориса Грінченка – впроваджені в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка у робочих програмах навчальних дисциплін спеціальності 125 Кібербезпека за захист інформації першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового) рівнів вищої освіти та впроваджені в програмно-апаратне забезпечення лабораторій безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації (акт від 15.01.2024);
- ТОВ «2Д3Д» – застосовані для удосконалення існуючих механізмів забезпечення кібербезпеки в мереж інтернету речей;
- ТОВ «Технологічні IT рішення» – використані для криптографічного захисту інформації, що передається пристроями з обмеженими обчислювальними ресурсами.

Апробація результатів дисертації. Матеріали дисертаційного дослідження обговорювалися на міжнародній науковій конференції: Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2023.

Публікації. Основні результати дисертації опубліковано у 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. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

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

Наукова стаття, опублікована у періодичному науковому виданні, проіндексована у базі даних Scopus

1. Chernenko R., Anosov A., Kyrychok R., Brzhevska, Z., Spasiteleva S. (2022). Encryption Method for Systems with Limited Computing Resources. CEUR Workshop Proceedings, 3288, pp. 142-148. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85143827975&partnerID=40&md5=fc5b960373acefb92e4755f0a571afb2

Особистий внесок здобувача. Всі наукові результати, що виносяться на захист, одержано здобувачем самостійно.

У статті «Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами» опублікованій у співавторстві, внесок Черненка Р.М. полягає у дослідженні алгоритмів та розробці прототипу системи IoT.

У статті «Encryption Method for Systems with Limited Computing Resources» опублікованій у співавторстві, внесок Черненка Р.М. полягає у імплементації методу шифрування та формуванні криптографічних параметрів.

У статті «Модифікація криптографічного алгоритму a5/1 для забезпечення комунікацій пристроїв IoT» опублікованій у співавторстві, внесок Черненка Р.М. полягає у побудові моделі загроз, модифікації алгоритму та побудові криптографічного протоколу.

У одноосібних статтях всі результати отримані автором самостійно.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел із 121 найменування на 16 сторінках. Загальний обсяг роботи становить 156 сторінок, 30 рисунків, 7 таблиць.

Оцінка мови та стилю дисертації. Дисертація написана науковою українською мовою. Стиль викладу матеріалу логічний, послідовний. Зміст роботи повністю висвітлює результати наукових досліджень. Текст роботи має смислову цілісність, послідовність і завершеність, що забезпечує легкість і доступність сприйняття матеріалу.

Дотримання здобувачем академічної доброчестності в дисертації та наукових публікаціях, в яких висвітлено наукові результати дисертації. На підставі вивченого тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено,

що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації.

Відповідність дисертації вимогам, що представляються до дисертацій на здобуття ступеня доктор філософії. Дисертація Черненка Р.М., на тему «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей» є завершеним науковим дослідженням, в якому отримано нові обґрунтовані результати. Дисертацію виконано на достатньо високому рівні, її результати мають наукову новизну і практичну значимість. Основні положення дисертації опубліковані в наукових фахових виданнях, виданнях, що входять до наукометричної бази Scopus та оприлюднювались на науково-практичних конференціях. Дисертаційне дослідження відповідає обраній темі, розкриває її суть та підтверджує, що автором повністю вирішено поставлені у роботі завдання.

Рішення:

1. Дисертація Черненка Романа Миколайовича на тему «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає п.6-9 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 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023.

2. Дисертація Черненка Романа Миколайовича та наукові публікації, у яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності.

3. Черненко Роман Миколайович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом.

4. Рекомендувати дисертацію Черненка Романа Миколайовича на тему «Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей» до публічного захисту у разовій спеціалізованій вченій раді для присудження Черненку Р.М. ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Головуючий –
кандидат технічних наук, доцент,
завідуючий кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка Павло СКЛАДАННИЙ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС Складанного П. ЗАСВІДЧУЮ
Провід. фах. В.К. Л. Маліченко