АНОТАЦІЯ

Тіхонов С.В. Метод крипто-стійкого динамічного кодування і розподілу даних мобільної ad-hoc мережі Інтернету речей. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Національний університет «Одеська політехніка», Міністерство освіти і науки України, Одеса, 2026.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної задачі створення проактивних методів криптостійкого динамічного кодування і розподілу даних для підвищення захисту інформації в системах та мережах Інтернету речей.

У **вступі** наведено обґрунтування актуальності теми дослідження, підкреслено недоліки наявних моделей і методів у сфері кібербезпеки, що робить їх неефективними проти невідомих раніше атак і залишає прогалини в захисті. Показано зв’язок роботи з науковими програмами, планами і темами. Визначено об’єкт, предмет, мету, задачі і методи дослідження. Наведено наукову новизну та практичне значення отриманих результатів. Висвітлено особистий внесок здобувача в наукових публікаціях за темою дисертаційних досліджень. Наведені дані про апробацію, використання і впровадження результатів дисертаційної роботи, про публікації здобувача на тему дисертації, а також наведена інформація про структуру і обсяг дисертації.

У **першому розділі** дисертаційної роботи проведено аналітичний огляд проблеми захисту інформації і управління розподілом даних в комп’ютерних системах та мережах у зв’язку із стрімким впровадженням мобільних мереж Інтернету речей (IoT) у промисловість, оборону і повсякденне життя. На основі системного підходу, досліджено розвиток еталонних моделей Інтернету у контексті інформаційної безпеки та сучасні криптографічні технології Інтернету речей.

Проаналізовано існуючі протоколи і стандарти захисту в безпровідних інтерфейсах WiFi, а також моделі і методи управління цифровими потоками в мобільних ad-hoc мережах Інтернету речей.

Аналіз робіт у сфері захисту інформації і управління розподілом даних в комп'ютерних системах та мережах показав, що на поточний момент створено ефективні еталонні безпекові моделі Інтернету речей від організацій IoT-WF, NIST. Досягнуто високої криптографічної стійкості шифрів і крипто-протоколів (шифр AES, протокол GCMP, автентифікація SAE, стандарт WPA3). Існують швидкі моделі та алгоритми оптимізації потоків даних в мережах ("Push-Relabel"). Потужним інструментом захисту і оптимізації мереж IoT є використання ШІ. Разом з тим, існують невирішені питання та виклики, зокрема, консерватизм застарілих технологій, що стримує втілення нових безпекових рішень поверх наявних, а також реактивний підхід до захисту даних в комп'ютерних мережах (виявлення загроз по факту). Окрім того, є недостатньою швидкодія оптимізації потоків реального часу в мобільних ad-hoc мережах. Залишається можливість додаткового збільшення максимального потоку шляхом динамічної ре-конфігурації каналів зв'язку при швидких змінах структури мережі.

Зроблено висновок, що існуючі рішення недостатні для комплексної підтримки сучасних вимог до кодування, захисту і управління даними в мобільних ad-hoc мережах IoT. Є потреба у пост-криптографічному захисті даних незалежно від існуючої апаратної підтримки, проактивних методах динамічного кодування захисту і розподілу даних, усунення вразливості застарілих операційних технологій, а також зменшення впливу людського фактору у питаннях кібербезпеки.

У зв'язку з цим, поставлено завдання щодо створення методу крипто-стійкого динамічного кодування на основі багаторівневої формальної граматики і побудови недетермінованої прикладної машини Тьюринга, а також комп'ютерних алгоритмів крипто-стійкого динамічного кодування і розподілу даних ad-hoc мережі Інтернету речей.

У **другому розділі** дисертаційної роботи обґрунтовано основні теоретичні положення щодо синтезу моделі і методу крипто-стійкого динамічного кодування даних для підвищення рівня кіберзахисту мобільної ad-hoc мережі Інтернету речей. Сформульовано перші три наукові результати роботи.

Досліджено еволюцію екосистеми робототехніки “Robotics Eco-System”, а також методи і моделі автоматизованого проектування роботизованих мобільних комплексів і платформ. Проаналізовано особливості кодування і структуризації даних у технологіях локальних мереж Ethernet та її бездротового аналогу технології WiFi. Обґрунтовано багаторівнева формальна граматика для гнучкої структуризації фреймів мобільної ad-hoc мережі Інтернету речей.

Розглянуто узагальнену функціональну схему дистанційного управління мобільною платформою Інтернету речей. Розроблено трирівневу структуру інтерфейсів роботизованого мобільного комплексу, а також формальну граматику побудови фреймів в каналі зв’язку з трійковим лінійними сигналами для нестандартного утворення цифрового потоку з окремих незалежних функціональних елементів у довільному порядку і складі. На основі цього, удосконалено модель динамічного кодування даних мобільної ad-hoc мережі Інтернету речей, що дозволяє збільшити ефективність каналу у 1.5÷6.6 разів та ускладнити його злам за рахунок скорочення службової інформації і непередбачуваного формату даних (**перший науковий результат**).

Визначено систему команд і узагальнену формальну граматику для прикладної машини Тьюринга з правилами семантики потокового кодування фреймів. Розроблено недетерміновану машину Тьюринга для структуризації даних в каналі зв’язку, *відмінну тим*, що через випадкові інтервали часу, кодові кортежі команд перемішуються і змінюють свою семантику у порядку відомому лише конкретному адресату. Таким чином, *отримала подальший розвиток* методика застосування теорії автоматів, *що дозволяє* створювати різноманіття алгоритмів криптографічного захисту інформації незалежно від існуючих апаратно-програмних засобів (**другий науковий результат**).

Вперше запропоновано спосіб динамічної синхронізації профільного ключа крипто-стійкого кодування між бортовим контролером мобільного об'єкту та базовою станцією дистанційного управління на основі недетермінованої машини Тьюринга, *відмінний тим*, що на кожну місію мобільного об'єкту генерується і закладається в пам'ять обох сторін унікальна випадкова послідовність профільних ключів, а номер ключа у цій послідовності відіграє роль відкритого ключа для передачі по каналу зв'язку, *що дозволяє* підвищити проактивний кіберзахист мережі, спростити його апаратно-програмну реалізацію і підвищити ефективність каналів зв'язку, а також обмежити людський фактор у питаннях конфіденційності (**третій науковий результат**).

У **третьому розділі** дисертаційної роботи розроблено комп'ютерний алгоритм для крипто-стійкого динамічного кодування в мобільній ad-hoc мережі Інтернету речей (IoT) на основі недетермінованої машини Тьюринга, теоретичні засади якого сформульовані у розділі 2. Побудовано блок-схему алгоритму і програмний модуль TMSend на мові Python. Наведено типові приклади симуляції недетермінованої машини Тьюринга NdTM у середовищі Python/Mac OS. Визначено три базові профіля роботи роботи алгоритму:

а) «гнучка структура» (без крипто-захисту): гнучке формування структури фрейму при відсутності кіберзагроз для зменшення службової інформації та підвищення інформаційної ефективності каналу зв'язку; дає виграш інформаційної ефективності у 1.5÷6.6 рази.

б) «крипто-захист»: динамічне крипто-стійке кодування фрейму змінним ключом що синхронізується між взаємодіючими сторонами; забезпечує еквівалентний до існуючих методів («нормальний») рівень захисту простими засобами незалежно (або на додаток) до традиційних методів шифрування; забезпечує достатню для ad-hoc мережі стійкість до зламу і виграш інформаційної ефективності у 2.5÷9.6 рази (в залежності від розміру даних і типу інкапсуляції).

в) «Пост-шифрування»: додаткове крипто-кодування корисних та службових даних тимчасовим ключем, номер якого передається відкритим параметром і визначає значення ключа в секретному масиві, що наперед випадково згенеровано і завантажено в пам’ять взаємодіючих сторін; даний механізм реалізує підвищений проактивний рівень захисту даних на додаток до відомих методів шифрування і дозволяє підвищити рівень захисту відомих методів; підвищує рівень захисту незалежно і на додаток до існуючих методів.

Досліджено структурно-параметричні характеристики нормалізованого планарного графу ad-hoc мережі (ST-графу). Систематизовано і розширено базові формули комбінаторики з шістьма новими функціями для обчислення параметрів ST-графу за кількістю його вершин.

Розглянуто структуру шляхів ST-графу з точки зору побудови дерева пошуку найкоротших шляхів.

Удосконалено методи рішення комбінаторних задач на графах *шляхом* обґрунтування рекурсивної побудови дерева пошуку найкоротших шляхів на вільно-орієнтованому графі мережі та комбінаторної формули від числа вершин графу для визначення необхідної кількості ітерацій, *що дозволяє* прискорити алгоритми оптимізації потоків даних в мережах, а також залучити штучний інтелект до реалізації таких алгоритмів (**четвертий науковий результат**).

Розроблено комбінаторну модель оптимізації розподілу даних ad-hoc мережі Інтернету речей з використанням штучного інтелекту, а також комп’ютерний алгоритм динамічного розподілу даних в мережі IoT.

Імплементація цього алгоритму розширює можливості адаптації ad-hoc мережі Інтернету речей до динамічно змінюваних факторів для *максимально ефективного використання наявних ресурсів* (енерго-запаси мобільних об’єктів, канали зв’язку, мережеві інтерфейси тощо).

Це підсилює функціональну стійкість мережі, і зокрема, рівень кіберзахисту, що важливо при організації спеціальних місій для групи автономних мобільних роботизованих платформ, які об’єднуються в ad-hoc мережу змінної топології і метрики.

У висновках зазначено основні результати дисертаційного дослідження.

Сукупність наукових результатів дисертаційного дослідження дозволяє розв'язати актуальну науково-прикладну задачу, що полягає у створенні проактивних методів криптостікого динамічного кодування і розподілу даних для підвищення захисту інформації в системах та мережах Інтернету речей.

Основним науковим результатом дисертаційної роботи є створення методу крипто-стійкого динамічного кодування і розподілу даних мобільної ad-hoc мережі Інтернету речей для підвищення захисту інформації. *На відміну від існуючих*, даний метод застосовує недетерміновану машину Тьюринга зі змінною у часі системою команд для гнучкого формування структури даних в каналі зв'язку, а також комбінаторну модель оптимального розподілу даних для рекурсивної побудови дерева пошуку найкоротших шляхів на вільно-орієнтованому планарному графі з використанням штучного інтелекту, *що дозволяє* підвищити проактивний кіберзахист мережі, спростити його апаратно-програмну реалізацію, підвищити ефективність каналів зв'язку, обмежити людський фактор у питаннях конфіденційності, збільшити швидкодію адаптивної реконфігурації розподілу даних та підсилити функціональну стійкість в умовах динамічно змінних факторів впливу.

У межах основного наукового результату роботи отримано наступне.

1) *Удосконалено* модель динамічного кодування даних мобільної ad-hoc мережі Інтернету речей *шляхом* розробки і застосування трирівневої структури інтерфейсів роботизованого мобільного комплексу та відповідної формальної граматики побудови фреймів в каналі зв'язку з трійковим лінійними сигналами для нестандартного утворення цифрового потоку з окремих незалежних функціональних елементів у довільному порядку і складі, *що дозволяє* збільшити ефективність каналу у 1.5÷6.6 разів та ускладнити його злам за рахунок скорочення службової інформації і непередбачуваного формату даних.

2) *Отримала подальший розвиток* методика застосування теорії автоматів шляхом розробки недетермінованої машини Тьюринга для структуризації даних в каналі зв'язку, *відмінна тим*, що через випадкові інтервали часу, кодові кортежі команд перемішуються і змінюють свою семантику у порядку відомому лише конкретному адресату, *що дозволяє* створювати різноманіття алгоритмів криптозахисту незалежно від існуючих апаратно-програмних засобів.

3) *Вперше запропоновано* спосіб динамічної синхронізації профільного ключа крипто-стійкого кодування між бортовим контролером мобільного об’єкту та базовою станцією дистанційного управління на основі недетермінованої машини Тьюринга, *відмінний тим*, що на кожну місію мобільного об’єкту генерується і закладається в пам’ять обох сторін унікальна випадкова послідовність профільних ключів, а номер ключа у цій послідовності відіграє роль відкритого ключа для передачі по каналу зв’язку, *що дозволяє* підвищити проактивний кіберзахист мережі, спростити його апаратно-програмну реалізацію і підвищити у 2.5÷9.6 разів ефективність каналів зв’язку, а також обмежити людський фактор у питаннях конфіденційності.

4) *Удосконалено* методи рішення комбінаторних задач на графах *шляхом* обґрунтування рекурсивної побудови дерева пошуку найкоротших шляхів на вільно-орієнтованому графі мережі та відповідної комбінаторної формули від числа вершин графу для визначення необхідної кількості ітерацій, *що дозволяє* прискорити у 1.3÷1.5 рази алгоритми оптимізації потоків даних в мережах, а також залучити штучний інтелект до реалізації таких алгоритмів.

Результати дисертації сприяють підвищенню рівня кіберзахисту систем та мереж Інтернету речей в умовах зростання кіберзагроз та складності атак. Впровадження результатів дисертації дозволить підвищити стійкість та надійність функціонування критично важливих систем та мереж, що є необхідною передумовою сталого розвитку цифрового суспільства.

Практично значущими є наступні результати роботи.

– Для суб’єктів критичної інфраструктури та промислових підприємств, метод крипто-стійкого динамічного кодування та розподілу даних може бути використано для надійного стійкого захисту від атак типу DoS, ін’єкцій шкідливого коду та несанкціонованого доступу. Це дозволить запобігти збою енергосистем типу Smart Grid, промислових IoT-мереж і транспортних систем.

– Для розробників та виробників IoT-пристроїв, алгоритми та протоколи, що використовують штучний інтелект для адаптивного керування кодуванням, можуть бути інтегровані у програмне забезпечення нових пристроїв.

Це забезпечить проактивний захист і можливість автономно протистояти новим, раніше невідомим загрозам без необхідності втручання оператора.

– Для розробників та користувачів мобільних роботизованих об`єктів та ad-hoc мережам. Запропонована методологія забезпечує підвищену стійкість зв'язку та маскування трафіку в умовах активної радіоелектронної боротьби. Динамічний розподіл даних та адаптивне кодування дозволяють протидіяти навмисним перешкодам, запобігати втраті управління та інформації в роях дронів та інших автономних системах, що працюють у ворожому середовищі. Це є критично важливим для безпеки та ефективного виконання бойових, розвідувальних та рятувальних місій.

– Для наукових установ та закладів вищої освіти, розроблена методологічна база слугує теоретичним підґрунтям для подальших наукових досліджень у сфері кібербезпеки децентралізованих систем. Результати роботи можуть бути використані для модернізації навчальних курсів та спеціалізованих дисциплін з інформаційної безпеки та штучного інтелекту.

Окремі результати роботи впроваджено на ТОВ «Радуга-N» для послуг «Розумний дім»» (спосіб динамічної синхронізації поточного профільного ключа між контролером МО і БС, Додаток Б), у навчальні дисципліни ДУІТЗ: «Інформаційні технології кодування і забезпечення завадостійкості систем» (методи теорії автоматів і недетермінованої машини Тьюринга для крипто-стійкого кодування), «Інтернет речей» (контекстно-визначена модель взаємодії відкритих систем для дослідження проблем кібербезпеки IoT), «Методи та системи штучного інтелекту» (алгоритм комбінаторної оптимізації розподілу даних з використанням штучного інтелект (Додаток В), а також у навчальний процес та наукову діяльність Національного університету «Одеська політехніка» (Додатки Г, Д).

Основні результати дисертаційної роботи представлені і обговорені на 7 міжнародних науково-практичних конференціях (НПК) та відображені у 11 наукових публікаціях, у тому числі, 4 статті у наукових фахових виданнях що індексуються у НМБД Scopus (у співавторстві), 7 опублікованих тез доповідей на міжнародних НПК (з них 5 одноосібних).

Дисертаційна робота підготовлена у відповідності до законів України «Про основні засади забезпечення кібербезпеки України» від 27.03.2025, «Про захист інформації в інформаційно-комунікаційних системах» від 20.04.2025, «Про Стратегію кібербезпеки України» (рішення Ради національної безпеки та оборони України від 14.05.2021). Тема роботи корелюється з пунктом 1.2.9.5 («Дослідження та розроблення методів інформаційної безпеки комп'ютерних систем і мереж») положень Національної академії наук України «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2024–2028 роки» No8 від 10.01.2024.

Тема дисератційної роботи відповідає науковим планам і тематиці досліджень, а також програмам підготовки студентів Національного університету «Одеська політехніка» у сфері кібербезпеки, інтелектуальних систем та робототехніки. Дисертація є складовою частиною НДР No 199-64 «Моделі, методи розробки та апаратні рішення високочастотних компонентів програмованих мобільних систем» Інституту штучного інтелекту та робототехніки Національного університету «Одеська політехніка» (No держреєстрації 0121U110245).

Ключові слова: комп'ютерні системи та мережі, Інтернет речей, мобільна ad-hoc мережа, кодування, захист інформації, інтерфейс зв'язку, дистанційне управління, робототехніка, формальна граматика, машина Тьюринга, динамічний розподіл даних, нормалізований граф, комбінаторика, штучний інтелект.

Список публікацій здобувача за темою дисертації

1. Тіхонов С.В. Захищене кодування мережевих інтерфейсів у розподілених системах інтернету речей на основі багаторівневих формальних граматик. *Proc. of the VII International Scientific and Practical Conference «Science and Technology: Problems, Prospects and Innovations»* (Osaka, 13-15 April, 2023). С. 174-180. URL: https://sci-conf.com.ua/wp-content/uploads/2023/04/SCIENCE-AND-TECHNOLOGY-PROBLEMS-PROSPECTS-AND-INNOVATIONS-13-15.04.23.pdf.
2. Тіхонов С. Ієрархічний підхід до кодування даних на основі адаптивної формальної граматики. *Proc. of the XIV International Scientific and Practical Conference "Science and Practice: Implementation to Modern Society"* (Manchester, 26-28 April, 2023), № 152. P. 559-563. URL: https://archive.interconf.center/plugins/generic/pdfJsViewer/pdf.js/web/viewer.html.2C1040%2C899%5D.
3. Ситніков В.С., Тіхонов С.В. Принципи захисту інформації у комп'ютерних системах Інтернету речей на основі ієрархічного кодування у формальних граматиках. *Збірник тез 24-ї Міжнародної НПК «Сучасні інформаційні та електронні технології» CIET/MIET-2023* (Одеса, 29-31 травня 2023). С. 31-32. URL: https://old.tkea.com.ua/siet/archive/2023/31.pdf.
4. Тіхонов С.В. Формальна граматика машини Тьюринга для завадостійкого кодування фреймів Ethernet на основі трійкових лінійних сигналів. *Proc. of XII Internetional Scientific and Practical Conference «Innovations and Prospects in Modern Science»* (Stockholm, 20-22 November, 2023). С. 315-325. URL: https://sci-conf.com.ua/wp-content/uploads/2023/11/INNOVATIONS-AND-PROSPECTS-IN-MODERN-SCIENCE-20-22.11.23.pdf.
5. Тіхонов С. Питання кібербезпеки в базових технологіях Інтернету речей. *Proc. of XII International Scientific and Practical Conference "Current Challenges of Science and Education"* (Berlin, 29-31 July, 2024). С. 165-171.

URL: https://sci-conf.com.ua/wp-content/uploads/2024/07/CURRENT-CHALLENGES-OF-SCIENCE-AND-EDUCATION-29-31.07.24.pdf.

6. Тіхонов В., Тіхонов С., Яворська О. Дослідження комбінаторних потокових задач на планарному графі комп'ютерної мережі. *Proc. of XI International Scientific and Practical Conf. "Science in the Modern World: Innovations and Challenges"* (Toronto, 10-12 July 2025). С. 45-52. URL: https://sci-conf.com.ua/wp-content/uploads/2025/07/SCIENCE-IN-THE-MODERN-WORLD-INNOVATIONS-AND-CHALLENGES-12-14.06.2025.pdf.
7. Тіхонов С.В. Підвищення стійкості ad-hoc мережі IoT на основі швидкого алгоритму розподілу даних з використанням ШІ. *Proc. of V International Scientific and Practical Conference "International Experience in Scientific Rresearch"* (Chicago, 18-20 December 2025). P. 300-308. URL: https://sci-conf.com.ua/wp-content/uploads/2025/12/INTERNATIONAL-EXPERIENCE-IN-SCIENTIFIC-RESEARCH-18-20.12.25.pdf.
8. Тіхонов В., Тахер А., Тіхонов С., Шулакова К., Глущенко В., Чайка А. Розробка машини Тюрінга для високозахищеного кодування даних на канальному рівні Інтернету речей. *Hochschule Anhalt Edition "Applied Innovations in Information and Communication Technology" (ICAIIT)*. 2024. V. 12, № 1. P. 1-10. ISSN 2199-8876. DOI: http://dx.doi.org/10.25673/115635.
9. Тіхонов В., Сіменс Е., Васіліу Є., Ситніков В., Тахер А., Тихонова О., Шулакова К., Тіхонов С. Контекстно-визначена модель взаємодії відкритих систем для дослідження проблем кібербезпеки Інтернету речей. *Hochschule Anhalt Edition "Proceedings of the International Conference on Applied Innovations in IT" (ICAIIT).* 2024. V. 12, № 2, P. 35-44. ISSN 2199-8876. DOI: http://dx.doi.org/10.25673/118112.
10. Тіхонов В., Тахер А., Шулакова К., Тіхонов С., Демченко О. Розробка машини Тюрінга для високозахищеного дистанційного керування мобільною платформою IoT. *Springer Nature Link, Lecture Notes in Networks and Systems, ICAIIT- 2024*. 2025. V. 1338. P. 61–80. ISSN 2367-3370, 2367-3389 (electronic). DOI: https://doi.org/10.1007/978-3-031-89296-7_5.

Тіхонов В., Ситніков В., Тіхонов С. Удосконалений алгоритм оптимізації потоків даних на нормалізованому біполярному планарному вільноорієнтованому мережевому графі з використанням штучного інтелекту. *Hochschule Anhalt Edition "Proceedings of the International Conference on Applied Innovations in IT" (ICAIIT)*. 2025. V. 13, № 5. P. 7–14. ISSN 2199-8876. DOI: http://dx.doi.org/10.25673/122800.

ABSTRACT

Tikhonov S.V. Method of crypto-resistant dynamic coding and data distribution in mobile ad-hoc network of the Internet of Things. – Qualification scientific paper as a manuscript.

Thesis for the PhD degree in specialty 123 – Computer engineering. – Odesa Polytechnic National University, Ministry of Education and Science of Ukraine, Odesa, 2026.

The dissertation is dedicated to solving the actual scientific and applied task of creating proactive methods of crypto-resistant dynamic data encoding and distribution to increase information protection in the Internet of Things systems and networks.

The **introduction** justifies the relevance of the research topic, and emphasizes the shortcomings of existing models and methods in the cybersecurity area, which makes them ineffective against previously unknown attacks and leaves gaps in protection. The study aligns with institutional research programs, plans, and projects. The object, subject, aim, objectives, and methods of the research are defined. The scientific novelty and practical significance of the results are presented. The section highlights the author's personal contribution to the co-authored scientific publications on the research topic. The applicant personal contribution is highlighted in the scientific publications on the dissertation research. The data of dissertation results presentation, application, and implementation is given along with the applicant's publications on dissertation topic and the info of the dissertation structure and scope.

In the **first chapter**, an analytical review was conducted regarding the issue of information protection and data distribution control in computer systems and networks amid the rapid implementation of mobile Internet of Things (IoT) networks into industry, defence, and everyday life. Development of the IoT reference models was investigated by the systems approach in the context of information security and modern cryptographic technologies of the Internet of Things. Existing protocols and security standards in WiFi wireless interfaces were analysed, as well as models and methods for digital flows control in mobile ad-hoc Internet of Things networks.

An analysis of the information protection and data distribution in computer systems and networks realm studies revealed that currently effective reference security models for the Internet of Things have been developed by the IoT-WF and NIST. High cryptography resistance of ciphers and crypto protocols has been achieved (AES cipher, GCMP protocol, SAE authentication, WPA3 standard). There are fast models and algorithms for data flows optimizing in networks ("Push-Relabel").

A powerful tool for protecting and optimizing IoT networks is the use of AI. However, there are unresolved issues and challenges, in particular, the conservatism of legacy technologies, which hinders the implementation of new security solutions on the top of existing ones, as well as a reactive approach to data protection in computer networks (detection threats de-facto). In addition, the speed of real-time flows optimization in mobile ad-hoc networks is insufficient. The possibility remains of further increasing the maximum flow by dynamically reconfiguring communication channels during rapid changes in the network structure.

It is concluded that existing solutions are insufficient to comprehensive support the modern requirements for encryption, protection and data management in mobile ad-hoc IoT networks. There is a need for post-cryptographic data protection regardless of existing hardware support, proactive methods of dynamic data encryption, protection and distribution, remediation of vulnerabilities in legacy operational technologies, as well as reducing the human factor impact in cybersecurity issues.

Considering this, the goal was set to develop a method of crypto-stable dynamic coding based on a multi-level formal grammar and the construction of a non-deterministic applied Turing machine, as well as computer algorithms for crypto-resistant dynamic coding and data distribution in an ad-hoc Internet of things network.

In the **second chapter,** the main theoretical propositions are substantiated regarding the synthesis of a model and method of crypto-resistant dynamic data encoding to increase the cyber-security of a mobile ad-hoc Internet of things network. The first three scientific results of the work are formulated. The evolution of the "Robotics Eco-System" is studied, as well as methods and models of automated design the robotic mobile complexes and platforms.

The features are analysed of data coding and structuring in Ethernet local area network technologies and its wireless analogue WiFi technology. A multi-level formal grammar is substantiated for flexible frame structuring in a mobile ad-hoc IoT network. A generalized functional scheme is considered of remote control the Internet of Things' mobile platform. A three-level interfaces structure is developed for a robotic mobile complex, as well as a formal grammar for constructing frames in a communication channel with ternary linear signals for non-standard formation of a digital stream from by separate independent functional elements in an arbitrary order and composition. Based on this, the model of dynamic data coding is improved for a mobile ad-hoc Internet of Things network, that allows increasing the channel efficiency by 1.5÷6.6 times and making it more difficult to hack due to the reduction of overhead information and unpredictable data format (**first scientific result**).

A command system and a generalized formal grammar have been defined for an applied Turing machine with the frame stream coding semantics rules. A nondeterministic Turing machine has been developed for data structuring in a communication channel, which differs in that at random intervals of time, the code tuples of commands are permutated and change their semantics in an order known only to particular addressee. Thus, the methodology of applying automata theory *was further developed*, which *allows* creating a variety of algorithms for cryptographic info protection regardless of existing hardware and software (**second scientific result**).

Firstly a method of dynamic synchronization of the crypto-resistant coding profile key between the on-board controller of a mobile object and the remote control base station with nondeterministic Turing machine is proposed, distinguished in that for each mission of a mobile object, a unique random sequence of profile keys is generated and stored in the memory of both parties, and the key number in this sequence plays the role of a public key for transmission over the communication channel, which allows increase proactive cyber protection of the network, simplify its hardware and software implementation and increase the efficiency of communication channels, as well as mitigate the human factor in privacy issues (**third scientific result**).

In the **third** chapter, a computer algorithm for crypto-stable dynamic coding in a mobile ad-hoc Internet of Things network is developed based on a nondeterministic Turing machine, the theoretical foundations of which formulated in section 2. A flowchart of the algorithm and a TMSend program Python module are constructed. Typical examples of simulation of a nondeterministic Turing machine NdTM in the Python/Mac OS environment given. The following three basic profiles of the algorithm's operation defined. a) "Flexible structure" (without crypto-protection): flexible formation of the frame structure in the absence of cyber threats to reduce overhead data and increase efficiency of the communication channel; provides a gain in information efficiency of 1.5÷6.6 times. b) "Crypto-protection": dynamic crypto-stable encoding of a frame with a variable key that is synchronized between the interacting parties; provides an equivalent level of protection to existing methods ("normal") by simple means independently (or in addition) to traditional encryption methods; provides sufficient resistance to hacking for an ad-hoc network and a gain in information efficiency of 2.5÷9.6 times (depending on the data size and type of encapsulation). c) "Post-encryption": additional crypto-encoding of useful/service data with a temporary key, the number of which is transmitted by a public parameter and determines the value of the key in a secret array, which is randomly generated in advance and loaded into the memory of the interacting parties; this mechanism implements an increased proactive level of data protection in addition to known encryption methods and allows to increase the level of protection of known methods; increases protection independently and in addition to existing methods.

The structural and parametric characteristics of the normalized planar graph of an ad-hoc network (ST-graph) are investigated. The basic combinatorics formulas are systematized and expanded with six new functions for calculating the parameters of the ST-graph by the number of its vertices. The structure of the paths of the ST-graph is considered in the context of constructing a shortest path searching tree.

The methods of combinatorial tasks on graphs solving *have been improved due to* justification the recursive construction of a shortest path searching tree on a free-oriented network graph along with the combinatorial formula for the graph vertices

number to determine the required number of iterations, which allows acceleration the algorithms for data flows optimizing in networks, as well as involve artificial intelligence into implementation of such algorithms (**fourth scientific result**).

A combinatorial model for optimizing data distribution in an ad-hoc Internet of Things network using artificial intelligence has been developed, as well as a computer algorithm for dynamic data distribution in an IoT network. The implementation of this algorithm expands the possibilities of adapting an ad-hoc Internet of things network to dynamically changing factors forthe most efficient use of available resources(energy reserves of mobile objects, communication channels, network interfaces, etc.). This enhances the functional stability of the network, and in particular, the cyber protection level, which is important when organizing special missions for a group of autonomous mobile robotic platforms that are combined into an ad-hoc network of variable topology and metrics.

In the conclusions, the main results of the dissertation research are indicated. The set of scientific results of the dissertation research allows solving a relevant scientific and applied task of creation proactive methods of cryptographic dynamic coding and data distribution to increase information protection in Internet of things systems and networks.

The *main scientific result* of the dissertation is creation a method of crypto-resistant dynamic data encoding and distribution in a mobile ad-hoc Internet of things network to increase information protection. *Unlike existing*, this method uses a nondeterministic Turing machine with a time-varying command system for flexible data structure formation in the communication channel, as well as a combinatorial model of optimal data distribution for recursive construction a shortest path searching tree on a free-oriented planar graph using artificial intelligence, *which allows* increase the proactive cyber defense of the network, simplify its hardware and software implementation, increase the efficiency of communication channels, mitigate the human factor in privacy issues, increase the speed of adaptive reconfiguration of data distribution, and enhance functional stability under dynamically changing impacts.

The following was obtained within the main scientific result of the work.

1) *Improved* dynamic data encoding model for mobile ad-hoc Internet of things network *due to* development and application of a three-level interface structure of a robotic mobile complex and the corresponding formal grammar for constructing frames in a communication channel with ternary linear signals for non-standard formation of a digital stream from separate independent functional elements in an arbitrary order and composition, which allows increase the channel efficiency by 1.5÷6.6 times and make it more difficult to crack due to reduction the overhead and unpredictable data format.

2) *Further advanced* a methodology of automata theory applying *by developing* a nondeterministic Turing machine for structuring data in a communication channel, *different in that* at random intervals of time, the code tuples of commands are permitted and changing their semantics in an order known only to the particular addressee, which allows to create a variety of algorithms for cryptographic information protection regardless of existing hardware and software.

3) *Firstly proposed* a method of dynamic synchronization of a crypto-stable encoding profile key between an on-board controller of a mobile object based on a non-deterministic Turing machine and a remote control base station, *different in that* for each mission of a mobile object, a unique random sequence of profile keys is generated and stored in the memory of both parties, and the key number in this sequence plays the role of a public key for transmission over the communication channel, *which allows* increase proactive cyber defense of the network, simplify its hardware and software implementation and increase the efficiency of communication channels by 2.5÷9.6 times, as well as limit the human factor in matters of confidentiality.

4) *Improved* methods of combinatorial tasks on graphs solving *due to* justification the recursive construction of a shortest path searching tree on a free-oriented network graph along with the combinatorial formula for the graph vertices number to determine the required number of iterations, *which allows* acceleration the algorithms for data flows optimizing in networks, as well as involve artificial intelligence into implementation of such algorithms.

The results of the dissertation facilitatei increasing the cyber protection of Internet of things systems and networks in the face of growing cyber threats and attacks complexity. Implementation of dissertation results enables resilience and functional reliability strengthen of critical systems and networks, which is a necessary prerequisite for sustainable development of a digital society.

The following results of the work are practically significant.

– For critical infrastructure entities and industrial enterprises, the method of crypto-resistant dynamic data encoding and distribution can be used for reliable and resilient protection against DoS attacks, malicious code injections, and unauthorized access. This will prevent the failure of Smart Grid energy systems, industrial IoT networks, and transportation systems.

– For IoT device developers and manufacturers, the algorithms and protocols that use artificial intelligence for adaptive coding control can be integrated into the software of new devices. This will provide proactive protection, allowing systems to autonomously confront unknown threats without the need for operator intervention.

– For developers and users of mobile robotic objects and ad-hoc networks. The proposed methodology enables increased communication stability and traffic masking in conditions of active electronic warfare. Dynamic data distribution and adaptive coding allow to counteract intentional interference, prevent the loss of control and information in swarms of drones and other autonomous systems operating in a hostile environment. This is critically important for the safety and effective performance of combat, reconnaissance and rescue missions.

– For scientific institutions and higher education institutions, the developed methodological base serves as a theoretical basis for further scientific research in the field of cybersecurity of decentralized systems. The results of the work can be used to modernize training courses and specialized disciplines in information security and artificial intelligence.

Some results of the work were implemented at Raduga-N Ltd for the Smart Home services (a method of dynamic synchronization of the current profile key between the MO controller and the BS, Appendix B), in the academic disciplines of

the SUITT: “Information technologies of coding and ensuring system protection” (methods of the theory of automata and nondeterministic Turing machine for crypto-resistant coding), “Internet of Things” (a context-defined interaction model of open systems for studying IoT cybersecurity problems), “Artificial intelligence methods and systems” (algorithm for combinatorial optimization of data distribution using artificial intelligence (Appendix B), as well as in the educational process and scientific activities of the Odesa Polytechnic National University (Appendixes G, D).

The main results of the dissertation work were presented and discussed at 7 international scientific and practical conferences (SPC) and reflected in 11 scientific publications, including 4 articles in scientific professional publications indexed in Scopus (in co-authorship), 7 published abstracts of reports at international SPCs (5 of them solo).

The dissertation work was prepared in accordance with the laws of Ukraine “On the Basic Principles of Ensuring Cybersecurity of Ukraine”, 03.27.2025, “On Information Protection in Information and Communication Systems” dated 04/20/2025, “On the Cybersecurity Strategy of Ukraine” (decision of the National Security and Defence Council of Ukraine, 05/14/2021). The topic of the work correlates with paragraph 1.2.9.5 (“Research and development of methods for information security of computer systems and networks”) of the provisions of the National Academy of Sciences of Ukraine “Main scientific directions and important problems of fundamental research in the field of natural, technical and humanities of the National Academy of Sciences of Ukraine for 2024-2028” No. 8, 01.10.2024.

The dissertation topic corresponds to the scientific plans and research topics, as well as the training programs of students of the National University "Odesa Polytechnic" in the field of cybersecurity, intelligent systems and robotics. The dissertation is a component of the Research and Development Project No. 199-64 "Models, development methods and hardware solutions of high-frequency components of programmable mobile systems" of the Institute of AI and Robotics of the National University "Odesa Polytechnic" (state registration № 0121U110245).

Keywords: computer systems and networks, Internet of things, mobile ad-hoc network, coding, information security, communication interface, remote control, robotics, formal grammar, Turing machine, dynamic data distribution, normalized graph, combinatorics, artificial intelligence.

List of publications of the applicant on the topic of the dissertation

1. Tikhonov S.V. Secure coding of network interfaces in distributed Internet of Things systems based on multi-level formal grammars. *Proc. of the VII International Scientific and Practical Conference «Science and Technology: Problems, Prospects and Innovations»* (Osaka, 13-15 April, 2023). P. 174-180. URL: https://sci-conf.com.ua/wp-content/uploads/2023/04/SCIENCE-AND-TECHNOLOGY-PROBLEMS-PROSPECTS-AND-INNOVATIONS-13-15.04.23.pdf.
2. Tikhonov Serhii. Hierarchical data coding approach based on adaptive formal grammar. *Proc. of the XIV International Scientific and Practical Conference "Science and Practice: Implementation to Modern Society"* (Manchester, 26-28 April, 2023), № 152. P. 559-563. URL: https://archive.interconf.center/plugins/generic/pdfJsViewer/pdf.js/web/viewer.html.2C1040%2C899%5D.
3. Sitnikov V.S., Tikhonov S.V. Principles of information protection in Internet of Things computer systems based on hierarchical coding in formal grammars *Zbirnyk tez 24-th Msznarodnoi NPK «Suchasni informaciyni ta electronni technologii» CIET/MIET-2023* (Odesa, 29-31 May 2023). P. 31-32. URL: https://old.tkea.com.ua/siet/archive/2023/31.pdf.
4. Tikhonov S.V. Formal Turing machine grammar for resistant coding of Ethernet frames based on ternary linear signals. *Proc. of XII Internetional Scientific and Practical Conference «Innovations and Prospects in Modern Science»* (Stockholm, 20-22 November, 2023). C. 315-325. URL: https://sci-conf.com.ua/wp-content/uploads/2023/11/INNOVATIONS-AND-PROSPECTS-IN-MODERN-SCIENCE-20-22.11.23.pdf.

5. Tikhonov S. The cybersecurity issues in basic Internet of things technologies. *Proc. of XII International Scientific and Practical Conference "Current Challenges of Science and Education"* (Berlin, 29-31 July, 2024). P. 165-171. URL: https://sci-conf.com.ua/wp-content/uploads/2024/07/CURRENT-CHALLENGES-OF-SCIENCE-AND-EDUCATION-29-31.07.24.pdf.
6. Tikhonov V., Tikhonov S., Yavorska O. Research of combinatorial flow problems on a planar graph of a computer network. *Proc. of XI International Scientific and Practical Conf. "Science in the Modern World: Innovations and Challenges"* (Toronto, 10-12 July 2025). C. 45-52. URL: https://sci-conf.com.ua/wp-content/uploads/2025/07/SCIENCE-IN-THE-MODERN-WORLD-INNOVATIONS-AND-CHALLENGES-12-14.06.2025.pdf.
7. Tikhonov S.V. Increasing the resilience of an ad-hoc IoT network based on a fast data distribution AI driven algorithm. *Proc. of V International Scientific and Practical Conference "International Experience in Scientific Rresearch"* (Chicago, 18-20 December 2025). P. 300-308. URL: https://sci-conf.com.ua/wp-content/uploads/2025/12/INTERNATIONAL-EXPERIENCE-IN-SCIENTIFIC-RESEARCH-18-20.12.25.pdf.
8. Tikhonov V., Taher A., Tikhonov S., Shulakova K., Hluschenko V., Chaika A. Turing Machine Development for High-secure Data Link Encoding in the Internet of Things Channel. *Hochschule Anhalt Edition "Applied Innovations in Information and Communication Technology" (ICAIIT)*. 2024. V. 12, № 1. P. 1-10. ISSN 2199-8876. DOI: http://dx.doi.org/10.25673/115635.
9. Tikhonov V., Siemens E., Vasiliu Y., Sitnikov V., Taher A., Tykhonova O., Shulakova K., Tikhonov S. Context-Defined Model of Open Systems Interaction for IoT Cybersecurity Issues Study. *Hochschule Anhalt Edition "Proceedings of the International Conference on Applied Innovations in IT" (ICAIIT).* 2024. V. 12, № 2, P. 35–44. ISSN 2199-8876. DOI: http://dx.doi.org/10.25673/118112.
10. Tikhonov V., Taher A., Shulakova K., Tikhonov S., Demchenko O. Turing Machine Development for High Protected Remote Control of the IoT Mobile Platform. *Springer Nature Link, Lecture Notes in Networks and Systems, ICAIIT-*

2024. 2025. V. 1338. P. 61–80. ISSN 2367-3370, 2367-3389 (electronic). DOI: https://doi.org/10.1007/978-3-031-89296-7_5.

11. Tikhonov V., Sitnikov V., Tikhonov S. An Improved AI-Driven Algorithm of Data Flow Optimization on the Normalized Bipolar Planar Free-Oriented Network Graph. *Hochschule Anhalt Edition "Proceedings of the International Conference on Applied Innovations in IT" (ICAIIT).* 2025. V. 13, № 5. P. 7–14. ISSN 2199-8876. DOI: http://dx.doi.org/10.25673/122800.