

Голові спеціалізованої вченої ради Д26.002.14
у Національному технічному університеті
України “Київський політехнічний інститут
імені Ігоря Сікорського”

03056, м. Київ, пр. Берестейський 37

ВІДГУК

офіційного опонента на дисертацію **Астраханцева Андрія Анатолійовича** «МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТА ЯКОСТІ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ МОБІЛЬНОГО ЗВ’ЯЗКУ», представлену до захисту на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі».

Актуальність теми дисертаційної роботи. Розвиток і впровадження мобільних мереж 5G є важливою частиною вдосконалення мобільних мереж. Користувачі отримують нові сервіси з високою швидкістю та низькою затримкою, але при цьому виникають нові виклики стосовно захищеності та якості передачі даних в системах мобільного зв’язку, які зумовлюють актуальність представленої роботи.

Так, активне впровадження нових джерел трафіку призводить до неповного врахування специфіки інформації, що поступає на вхід мережі зв’язку та недостатнього рівня адаптації існуючих методів класифікації та визначення пріоритетів трафіка для забезпечення відповідного рівня якості обслуговування. Зростання обсягів трафіку і поява нових типів навантаження (massive IoT, V2V, eMBMS, URLLC) призводять до погіршення ефективності існуючих методів обробки та кластеризації даних, які не були на це розраховані. Високі швидкості в 5G досягаються в тому числі застосуванням більш високорівневих алгоритмів модуляції, які є дуже вимогливими до помилок в каналі, що вимагає нових підходів до вдосконалення завадостійкого кодування в мобільних мережах.

Недостатня адаптація системи захисту інформації до загроз, що виникають під час впровадження новітніх послуг, сервісів та додавання додаткових елементів в мережу. Це потребує вирішення завдання віддаленої автентифікації, в тому числі посилення біометричної автентифікації шляхом

поєднання різних біометричних ознак, впровадження методів захисту персональних даних в мобільному пристрої користувача, а також забезпечення шифрування під час розмови.

Через відсутність методологічної бази та єдиного підходу для організації класифікації трафіка, мережні ресурси використовуються не в повному обсязі, задачі оптимізації вирішені частково або локально, а методи захисту даних частково застарілі, що призводить до погіршення показників захищеності та якості послуг для кінцевих користувачів. Вирішення вищезначених проблем обумовлює актуальність дисертаційної роботи Астраханцева А.А. на тему “Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв’язку”.

Зв’язок роботи з науковими програмами, планами, темами. Тематика роботи і отримані результати безпосередньо пов’язані з виконанням положень Міністерства Цифрової трансформації України про «Створення тестових центрів розвитку 5G в Україні», «Концепції національної інформаційної політики», «Концепції Національної програми інформатизації», «Концепції розвитку цифрових компетентностей до 2025 року». Робота проводилась згідно з планами науково-дослідних робіт кафедри інформаційно-телекомунікаційних мереж КПІ ім. Ігоря Сікорського у рамках держбюджетних тем №2117-п «Технологія побудови динамічних реєстрів електронних інформаційних ресурсів та засобів їх ефективною обробки у датацентрах гетерогенної структури» (№ ДР 0118U003522), №2297/19-1 «Гетерогенна мережа збору, передачі та обробки інформації для системи розподіленої генерації» та роботи кафедри ТКС ХНУРЕ № 235-1 «Методи проектування телекомунікаційних мереж NGN та управління їх ресурсами» (№ ДР 0109U000662).

Загальна характеристика роботи. Дисертація складається з вступу, 5 розділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 377 сторінок.

У **вступі** обґрунтовується актуальність теми дисертаційної роботи. Визначено мету роботи, основні задачі та методи досліджень. Сформульовано наукову новизну і практичне значення отриманих результатів.

За мету обрано вирішення важливої науково-технічної проблеми підвищення захищеності та якості передачі й обробки даних в інформаційно-комунікаційних мережах мобільного зв’язку. У якості об’єкту дослідження обрано процеси обробки і забезпечення захисту інформації в інформаційно-

комунікаційних мережах мобільного зв'язку. Для досягнення поставленої мети сформульовано ряд наукових задач, які досить повно розглянуті в розділах дисертації.

У **першому розділі** проаналізовано особливості передачі трафіка в 5G мережі та наявні загрози, а також визначено основні показники якості та захищеності інформаційно-телекомунікаційної мережі. Проаналізовано особливості функціонування мобільної мережі на основі стандарту 5G-NR, визначено її складові, основні технологічні особливості, показники захищеності даних та якості обслуговування користувачів, фактори впливу на них.

В **другому розділі** запропоновано комплексну методологію забезпечення якості передачі та захищеності даних у системі мобільного зв'язку, яка базується на удосконаленій структурі мережі мобільного зв'язку 5G. Запропонована структура забезпечує покращення наведених в розділі 1 показників якості (рівень помилок і втрат пакетів, швидкість передачі інформації, затримка передачі й обробки інформації) та показників захищеності (конфіденційність, цілісність, доступність та спостереженість).

В **третьому розділі** для зменшення сумарної затримки передачі трафіка наведено вдосконалення методів обробки пакетів у вузлі мережі за рахунок раціонального вибору параметрів та методів класифікації трафіка, оптимізації кількості ознак, які використовують під час класифікації, а також описано розроблений метод обробки даних у вузлі мережі, який підвищує ефективність застосування технології граничних обчислень з множинним доступом.

В **четвертому розділі** описано вдосконалення методів завадостійкого кодування пакетів під час їх передачі мобільною мережею для зменшення рівня помилок і втрат пакетів. Вдосконалення методів завадостійкого кодування полягають у новому методі формування коду Raptor і обґрунтуванні вибору його елементів.

В **п'ятому розділі** описано нові методи захисту приватних даних у пристрої користувача, які відрізняються наявністю нових методів формування біометричного шаблону, об'єднання різних типів біометричних даних, запропонованого завадостійкого методу приховання біометричних даних під час передачі, а також забезпечення двобічної автентифікації та

наскрізного шифрування під час дзвінка, що дозволяє уникнути підміни користувача на іншому боці і отримати доступ до сервісів лише авторизованому користувачу, що підвищує показники конфіденційності, цілісності та спостереженості.

Висновки дисертаційної роботи підкреслюють наукову та практичну цінність проведених досліджень. Основні результати мають як теоретичну так і практичну складову, створюючи в сукупності комплексну методологію управління процесом обслуговування у інформаційно-комунікаційній мережі і сукупність нових моделей та методів передачі, зберігання й обробки даних.

У **додатках** містяться документи, що підтверджують впровадження дисертаційної роботи.

Таким чином, усі положення, які винесені на захист висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів. Побудова дисертації відповідає прийнятим для наукового дослідження вимогам. Зміст та структура роботи у повній мірі відповідають завданню з викладення основних результатів вирішення поставленої наукової проблеми та сформульованим окремим задачам дослідження, які відповідають паспорту спеціальності 05.12.02 – телекомунікаційні системи та мережі.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих в дисертаційній роботі, їх достовірність. Обґрунтованість та достовірність наукових положень і результатів, рекомендацій і висновків Астраханцева А.А. підтверджується чітким формулюванням мети, коректною постановкою завдань досліджень, а також апробацією результатів дисертаційної роботи у виробничих умовах. Розроблені теоретичні та практичні методи і рекомендації, які викладені в дисертаційному дослідженні є достатніми та належним чином обґрунтованими. Теоретичні дослідження базуються на використанні методів теорії масового обслуговування, багатокритеріальної оптимізації, методів математичної статистики, теорії множин і теорії графів, теорії динамічного програмування, теорії ігор і прийняття рішень, методи математичного та імітаційного моделювання, теорії алгоритмів тощо.

Отримані результати апробовані на міжнародних вітчизняних та закордонних конференціях.

Наукова новизна отриманих автором результатів. У результаті виконання дисертаційної роботи набули подальшого розвитку методи обробки даних у вузлах мережі, пристроях користувача, а також методи захисту інформації у пристроях користувача. Основними науковими результатами дисертації можна вважати такі:

1. Вперше розроблено комплексну методологію обробки даних у вузлі мережі, яка базується на новій онтологічній моделі, використовує інтелектуальну систему управління та відрізняється моделлю попередньої обробки пакетів у вузлі мережі, оптимізацією параметрів класифікації трафіка та модифікованим алгоритмом кластеризації трафіка, що дозволило визначити оптимальний набір ознак класифікації та налаштувати модель нейронної мережі, забезпечуючи високу точність класифікації.

2. Вперше розроблено метод обробки даних у вузлі інфокомунікаційної мережі, який відрізняється наявністю процедур ідентифікації та автентифікації учасників розподілених периферійних обчислень МЕС, виділенням додаткових ресурсів з мобільної мережі, включаючи процедуру підготовки зв'язку точка-точка, а також призначенням обчислювальних вузлів і балансуванням навантаження між ними, за рахунок внесення змін в протокол обміну повідомленнями між базовою станцією та мобільними пристроями, що дозволило економити мережні ресурси, спростити процедуру організації розподілених периферійних обчислень та знизити вартість її розгортання.

3. Вперше розроблено модель коду Raptor та метод формування коду у пристрої користувача, що дозволило на відміну від існуючих моделей та методів одночасно забезпечити підвищення завадостійкості та зменшення ймовірності втрат пакетів.

4. Вперше розроблено методи захисту приватних даних у пристрої користувача, які відрізняються наявністю вдосконалених методів: формування біометричного шаблону, об'єднання різних типів біометричних даних, завадостійкого методу приховування біометричних даних під час передачі, а також забезпечення двобічної автентифікації та наскрізного

шифрування під час дзвінка, що дозволило уникнути підміни користувача на іншому боці і отримувати доступ до сервісів лише авторизованому користувачу, підвищити на один рівень надання послуг для забезпечення критеріїв конфіденційності, цілісності та спостереженості.

5. Вперше розроблено моделі для захисту приватних даних у пристрої користувача, які відрізняються: використанням біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об'єктами; вдосконаленим методом зберігання приватних даних користувача в захищеному ієрархічному вигляді, що дозволило надати нові можливості під час взаємодії користувача з пристроями mIoT і забезпечити підвищений рівень послуг для критерія конфіденційності при управлінні доступом до персональних даних користувача.

Практичне значення результатів, отриманих в дисертаційній роботі полягає в доведенні здобувачем отриманих наукових результатів до конкретних архітектурних рішень, протоколів взаємодії та методів управління сервісами у інформаційно-телекомунікаційних системах нового покоління, які можуть бути використані під час розгортання та обслуговування мереж оператора мобільного зв'язку.

1. Запропонована удосконалена система обробки даних і розподілу ресурсів показала свою ефективність в лабораторіях компанії Lifecell, що дозволило в комплексі з технологіями 5G підвищити швидкість передачі даних до 1.3Гбіт/с.

2. Розроблені методи керування та зберігання приватними даними користувача впроваджено в програмні засоби захисту приватних даних у мобільних пристроях Samsung.

3. Доведено, що сучасні методи захисту не вирішують проблеми наскрізного шифрування та взаємної автентифікації під час дзвінка. Запропоновані методи вирішують ці проблеми.

4. Отримані результати впроваджено в навчальному курсі «Основи побудови і захисту мереж 5G» в рамках Міжнародного проекту «PROJECT JEAN MONNET MODULE EU5G4UA», що підтверджується авторським свідоцтвом.

Практичне значення отриманих результатів підтверджено актами впровадження у тестову мережу 5G компанії Lifecell, патентах центру досліджень та розробок «Самсунг РнД Інститут Україна», а також в начальний процес Інституту телекомунікаційних систем НТУУ «Київський політехнічний інститут імені Ігоря Сікорського».

Цінність дисертаційної роботи для науки. Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної проблеми підвищення захищеності та якості передачі й обробки даних в мережі мобільного оператора, завдяки створенню комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі і сукупності нових моделей та методів передачі, зберігання й обробки даних. Запропоновані у роботі моделі та методи можуть бути використані для підвищення як захищеності й якості так і характеристик системи мобільного зв'язку в цілому.

Відповідність теми і змісту дисертації паспорту спеціальності, за якою вона подана на захист. Тема дисертації та її зміст відповідають формулі й галузі досліджень, відповідно до положень, що викладені в паспорті спеціальності 05.12.02 – телекомунікаційні системи та мережі.

Ідентичність змісту реферату й основних положень дисертації. Реферат дисертації за своїм змістом з необхідною повнотою відповідає викладеним в дисертаційній роботі результатам, в ньому ідентично відображено загальну характеристику, основний зміст та висновки роботи. Стиль викладення реферату забезпечує повноту і доступність сприйняття. Наукові задачі дослідження та шляхи їх вирішення викладені чітко і лаконічно. З тексту зрозуміла наукова і практична значущість роботи та особистий внесок здобувача.

Мова та стиль дисертації. Дисертація написана державною мовою. Виклад матеріалу в роботі має логічну послідовність, наукова термінологія є загальновизнаною, розділи взаємопов'язані та цілком розкривають поставлену мету. Стиль викладення результатів досліджень, нових наукових положень та висновків забезпечує доступність їх сприйняття. Результати проілюстровані високоякісними рисунками.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Астраханцева А.А. є результатом самостійних досліджень і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Повнота викладення та апробації основних результатів дисертаційної роботи у наукових публікаціях. За результатами досліджень опубліковано 76 наукових праць, у тому числі: 31 стаття у наукових фахових виданнях (з них 3 статей у виданнях, включених до категорії “А” Переліку наукових фахових видань України, проіндексованих у базах даних Scopus; 28 статей у науково-фахових виданнях України, 3 статті у закордонних наукових виданнях), 3 навчальних посібники (у співавторстві), 6 патентів на винахід (у співавторстві), 1 авторське свідоцтво на твір (у співавторстві), 35 тез доповідей в збірниках матеріалів конференцій. Зазначені публікації повною мірою висвітлюють наукові результати роботи, що виносяться на захист.

Дискусійні положення та зауваження щодо дисертаційної роботи.

1. Перший розділ дисертації загалом перевантажений довідковою інформацією. Наприклад рис. 1.1-1.9, 1.16-1.20, табл.1.1-1.3, мають ілюстративний характер, рис.1.1 продубльовано у другому розділі (рис.2.1), наведена теоретична та аналітична інформація є надлишковою та не використовується в подальшому дослідженні. Відповідно його було б доцільно скоротити на 25-30% за рахунок зменшення деталізації відомих прикладів та більшої структуризації матеріалу.

2. У першому розділі, автор аналізуючи стан наукових досліджень описав велику кількість метрик якості, серед яких середня швидкість передачі даних, час затримки між пакетами відправлення і приймання, варіація затримки та рівень втрат пакетів. Але показники не всіх вказаних метрик були вдосконалені. Тому, автору було б доцільно залишити лише метрики, що підлягали вдосконаленню.

3. Автор використовує поняття «єдиного критерію якості обслуговування» гібридних телекомунікаційних послуг в мережах 5G, проте, у роботі відсутнє його змістовне наповнення.

4. В третьому розділі, під час оцінювання ефективності класифікації даних у вузлі мережі слід було б навести більш детальне обґрунтування використання методів на основі нейронних мереж. А також навести результати порівняльного аналізу з іншими підходами, такими як глибока перевірка пакетів (deep packet inspection) чи аналіз шаблонів трафіку.

5. В пп. 3.4.4 автор зазначає, що найкращих показників точності при використанні алгоритмів машинного навчання для класифікації трафіку можна досягти при використанні ANN та RF алгоритмів, проте в роботі наведено аналіз впливу гіперпараметрів на точність та швидкість класифікації лише для алгоритму ANN (табл. 3.9, 3.10).

6. У наведеному на рис. 4.15. алгоритмі модифікації Raptor коду було б доцільно відзначити, які саме блоки запропоновані автором.

7. Опис підходів до формування біометричного шаблону та проходження віддаленої автентифікації наведений в пп. 5.2. та опис роботи протоколу обміну ключами Діффі-Хелмана наведений в пп. 5.6.3 є загально відомим, не відноситься до наукових здобутків автора і відповідно могли б бути опущеними або перенесеними в п.1.6. де розглядаються теоретичні питання захищеності інформації.

8. У п'ятому розділі зазначено, що для навчання штучної мережі була підготовлена вибірка мережних станів, проте не зазначена методика її формування, що, в свою чергу, породжує сумніви в достовірності отриманих результатів.

9. В дисертаційній роботі було б доцільно навести приклади застосування інтелектуальної системи управління, призначеної для підвищення захищеності та якості передачі даних, з врахуванням характеристик продуктивності та обчислювальних ресурсів реального обладнання, а також навести практичні рекомендації по її використанню.

Слід зазначити, що наведені зауваження не носять визначального характеру та жодним чином не знижують позитивне враження про роботу, її наукову новизну та практичну значимість результатів.

Загальний висновок щодо відповідності дисертації встановленим вимогам. Дисертаційна робота Астраханцева Андрія Анатолійовича “Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв’язку”, є завершеним науковим дослідженням, виконаним

здобувачем самостійно, характеризується єдністю змісту, містить нові наукові положення та обгрунтовані теоретичні результати, які підтверджено результатами проведених експериментів і відповідними актами впровадження. В цілому робота забезпечує суттєвий внесок в теорію та практику побудови мобільних мереж.

Усі результати, що виносяться на захист є достовірними та отримані автором особисто. Робота відповідає принципам академічної доброчесності. Наявність академічного плагіату, фальсифікації, фабрикації не виявлено. Використання результатів, які виносилися на захист в кандидатській дисертації, у даній роботі не виявлено.

Вважаю, що за актуальністю обраної теми, обсягом та рівнем теоретичних і експериментальних досліджень, достовірністю та обгрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики, дисертаційна робота задовольняє вимогам пп.7, 8 та 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого Постановою Кабінету Міністрів України від 17.11.2021 №1197 (із змінами, внесеними згідно з Постановами Кабінету Міністрів України № 502 від 19.05.2023 № 507 від 03.05.2024), а її автор, Астраханцев Андрій Анатолійович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі».

Офіційний опонент,

доктор технічних наук, професор,
професор кафедри телекомунікацій
Національного університету
«Львівська політехніка»

Мар'ян КИРИК

«Підпис д.т.н., професора Кирика М.І. засвідчую»:

Вчений секретар
Національного університету
«Львівська політехніка»



Роман БРИЛИНСЬКИЙ