

ВІДГУК

офіційного опонента д.т.н., проф. **Голубничого Олексія Георгійовича**
на дисертаційну роботу **Астраханцева Андрія Анатолійовича**
“**Моделі та методи підвищення захищеності та якості передачі даних в
системах мобільного зв’язку**”,

подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.12.02 – Телекомунікаційні системи та мережі

1. Актуальність обраної теми дисертації.

В останні роки суттєво зросла кількість країн, в яких було впроваджено мобільні мережі п’ятого покоління (5G). Перехід до мобільних мереж нового покоління дозволяє підключати «розумні» фабрики, керувати дорожнім рухом та забезпечувати роботу автономних і напівавтономних транспортних засобів. Це суттєво ускладнює процеси оброблення даних в мережах передавання даних, формує низку теоретичних та прикладних проблем, які потребують фундаментальних та прикладних наукових досліджень.

Через відсутність методологічної бази та єдиного підходу щодо класифікації трафіка мережні ресурси використовуються не в повному обсязі, пов’язані з максимізацією рівня використання цих ресурсів задачі оптимізації вирішені частково або не враховують актуальних на даний час обмежень.

Це вимагає нового підходу і створення комплексної методології, яка б охоплювала різні компоненти системи мобільного зв’язку.

Вдосконалення методів класифікації трафіка потребує розроблення вдосконалених методів оброблення даних і впровадження новітніх адаптивних методів класифікації трафіка.

Підключення великої кількості сенсорів вносить додаткове навантаження на мережу і вимагає вдосконалення методів розподілення і

оброблення навантаження на граничних вузлах мережі, а головною вимогою новітніх сервісів, таких як Remote Surgery чи віддалене керування, є низький рівень втрат пакетів. Це в свою чергу зумовлює потребу у вдосконаленні використовуваних методів завадостійкого кодування.

Вагомою складовою якісної роботи мережі є забезпечення захищеності даних. На цей час в мобільних пристроях користувачів впроваджені різні методи біометричної автентифікації, але на сьогодні не існує якісного методу формування біометричного шаблону на основі декількох ознак одночасно і таких, які б враховували мережні фактори під час віддаленої автентифікації по мережі і забезпечили додатковий захист самої процедури автентифікації. Також сучасні мобільні мережі пропонують методи автентифікації пристрою користувача під час розмови, але проблема автентифікації самого користувача залишається не вирішеною. Крім того, навіть найсучасніші мережі забезпечують шифрування лише на ділянці абонент – базова станція, наскрізне шифрування в мережі не застосовується.

Ще одним викликом до систем захисту інформації є розширення функціоналу пристроїв, що надає змогу, наприклад, з мобільного телефону віддалено керувати системами «розумного будинку», розпізнавати об'єкти і застосовувати до них відповідні дії. Такі можливості мають бути доступні користувачам лише за умов попередньої автентифікації та авторизації.

Вищенаведене обумовлює актуальність науково-прикладної проблеми підвищення захищеності та якості передавання й оброблення даних в інформаційно-комунікаційних мережах мобільного зв'язку, яка може бути вирішена шляхом створення комплексної методології управління процесом обслуговування у мобільній мережі і сукупності нових моделей та методів передавання, зберігання й оброблення даних.

2. Зв'язок роботи з науковими програмами, планами, темами.

Тематика роботи пов'язана з виконанням планів Міністерства цифрової трансформації України щодо створення тестових центрів розвитку 5G в Україні, реалізацією Національної програми інформатизації, передбаченою Законом України «Про Національну програму інформатизації», Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 № 167-р, виконанням Указу Президента України від 17.05.2019 № 242/2019 «Про забезпечення умов для впровадження системи рухомого (мобільного) зв'язку п'ятого покоління», реалізацією спільного проєкту навчально-наукового Інституту телекомунікаційних систем НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» та Університету Анхальт (Hochschule Anhalt) «DigIn.Net 2: Deutsch-Ukrainisches Netzwerk Digitaler Innovationen-2» (№ 57602278).

Частина нових наукових та науково-технічних (прикладних) результатів отримані автором дисертації в рамках НДР кафедри інформаційно-телекомунікаційних мереж НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», держбюджетних тем № 2117-п «Технологія побудови динамічних реєстрів електронних інформаційних ресурсів та засобів їх ефективної обробки у датацентрах гетерогенної структури» (ДР № 0118U003522), №2297/19-1 «Гетерогенна мережа збору, передачі та обробки інформації для системи розподіленої генерації», НДР «Методи проектування телекомунікаційних мереж NGN та управління їх ресурсами» (ДР № ДР 0109U000662).

Результати дисертаційного дослідження також знайшли відображення в Міжнародному проєкті «PROJECT JEAN MONNET MODULE EU5G4UA».

3. Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих в дисертації та їх достовірність.

Обґрунтованість отриманих Астраханцевим А.А. наукових результатів забезпечується достатнім для досягнення поставленої мети обсягом проведених експериментальних досліджень точності роботи методів класифікації трафіка, а також методів розподілу трафіка в різних умовах їх практичного застосування.

Про достовірність результатів дисертаційного дослідження свідчать:

- достатня для досягнення поставленої мети дослідження повнота та достовірність використаних та запропонованих математичних моделей;
- узгодженість отриманих результатів з розрахунковими та експериментальними результатами інших дослідників, отриманих ними при розв’язанні суміжних задач і проблем;
- наукові положення та експериментальні результати, отримані в дисертації, опубліковані в рецензованих фахових виданнях та пройшли апробацію на авторитетних наукових конференціях і семінарах;
- достовірність практичних результатів по методам захисту даних користувача та підвищенню якості підтверджена міжнародними патентами, актом впровадження у промисловість (зокрема, в мережу мобільного оператора Lifecell) та освітній процес Інституту телекомунікаційних систем НТУУ «Київський політехнічний інститут імені Ігоря Сікорського».

4. Структура та зміст дисертації.

Зміст дисертації узгоджується з її темою, відповідає науковій спеціальності. У дисертації стисло, логічно та аргументовано представлено зміст і результати роботи з посиланнями на результати, отримані іншими авторами.

Дисертація та реферат оформлені відповідно до чинних вимог. Зміст та суть реферату відповідають змісту дисертації і дають повне уявлення про наукову цінність та практичну значущість роботи.

Загальний обсяг роботи становить 377 сторінок, з яких 31 сторінка відповідає переліку використаних джерел. Дисертаційна робота складається з анотації двома мовами, вступу, п'яти розділів, висновків, списку використаних джерел з 294 найменувань та двох додатків, що відповідає чинним вимогам до докторських дисертацій.

У вступі обґрунтовано актуальність теми дисертаційної роботи, визначено мету роботи, основні задачі та методи досліджень, сформульовано наукову новизну і практичне значення отриманих результатів.

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

В другому розділі запропоновано узагальнений опис комплексної методології забезпечення якості передавання та захищеності даних у системі мобільного зв'язку, яка базується на удосконаленій структурі мережі мобільного зв'язку 5G і онтологічній моделі. Запропонована структура забезпечує покращення наведених в першому розділі показників якості, таких як рівень помилок і втрат пакетів, швидкість передачі інформації, затримка передавання й оброблення інформації, а також показників захищеності (конфіденційність, цілісність, доступність та спостереженість). Запропоновано шляхи підвищення показників якості передавання даних, які більш детально розкриваються автором в наступних розділах.

Крім того, запропоновано кроки по вдосконаленню показників захищеності, зокрема: впровадження у обладнанні користувача

вдосконаленого методу формування біометричного шаблону користувача, в тому числі нового методу об'єднання різних біометричних ознак користувача; застосування методів мережної стеганографії та завадостійкого кодування для підвищення прихованості та завадозахищеності інформації під час проходження процедури віддаленої автентифікації; впровадження нового методу взаємної автентифікації користувачів під час дзвінка, що перекриває ряд загроз пов'язаних із шахрайськими схемами підміни користувача; впровадження нового методу наскрізного шифрування під час дзвінка для підвищення рівня показника конфіденційності; впровадження нових методів управління приватними даними користувача для забезпечення захищеності під час реалізації нових сервісів.

В третьому розділі для зменшення сумарної затримки передачі трафіка вдосконалено методи обробки пакетів у вузлі мережі за рахунок раціонального вибору параметрів та методів класифікації трафіка, оптимізації кількості ознак, які використовують під час класифікації, а також розроблено новий метод обробки даних у вузлі мережі, який підвищує ефективність застосування технології граничних обчислень з множинним доступом. Запропоновані методи у поєднанні з застосуванням мережних зрізів дозволяють зменшити затримку передачі трафіка і покращити ефективність 5G мережі в цілому, що знайшло відображення у авторському свідоцтві.

В четвертому розділі описано вдосконалення моделей та методів завадостійкого кодування пакетів під час їх передачі мобільною мережею для зменшення рівня помилок і втрат пакетів. Вдосконалення завадостійкого кодування полягає у новій моделі формування коду Raptor і обґрунтуванні вибору його елементів.

В п'ятому розділі описано нові моделі та методи захисту приватних даних у пристрої користувача, які відрізняються наявністю нових методів

формування біометричного шаблону, об'єднання різних типів біометричних даних, запропонованого завадостійкого методу приховування біометричних даних під час передавання, 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 якість надання послуг за показниками конфіденційності, цілісності та спостереженості.

У висновках сформульовані основні результати дисертаційного дослідження, які дозволили оцінити внесок здобувача в подальший розвиток моделей та методів забезпечення захищеності та якості в системах мобільного зв'язку.

У додатках наведено копії документів, які підтверджують впровадження результатів дослідження.

5. Наукова новизна отриманих в роботі результатів, сформульованих положень та висновків.

Аналіз представлено до захисту наукового дослідження та публікацій дозволяють дійти висновку про наукову обґрунтованість і достовірність викладених здобувачем результатів. Основні результати, викладені в дисертаційній роботі, відповідають критерію новизни в галузі телекомунікаційних систем та мереж. Серед найважливіших результатів слід зазначити забезпечення двобічної автентифікації та наскрізного шифрування під час дзвінка та визначення оптимальних методів класифікації трафіка.

В цілому в дисертації отримано такі нові наукові результати:

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.

Отримані в дисертації наукові положення мають загальнонаціональне значення в контексті впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління.

6. Практичне значення дисертації.

Практичне значення дисертаційного дослідження полягає в успішних результатах перевірки запропонованих методів на тестовій мережі компанії Lifecell та у користувальницькому обладнанні компанії Samsung. Всі представлені в роботі результати спрямовані на вирішення конкретних практичних задач та доведені до архітектурних рішень та протоколів взаємодії. Обсяг та рівень опрацювання матеріалу, представленого у дисертації, свідчить про ґрунтовну експериментальну роботу, проведеному здобувачем для апробації та підтвердження отриманих результатів.

7. Повнота викладення результатів роботи у наукових працях.

Основні положення і висновки дисертаційного дослідження повністю викладені в 76 наукових та науково-методичних працях, серед яких: 3 навчальних посібника (зокрема, 1 з грифом Міністерства освіти і науки України), 31 стаття у наукових періодичних виданнях, включених до Переліку наукових фахових видань України (в тому числі 3, включені до категорії «А», з них 1 стаття у виданнях, віднесених до квартилю Q3 відповідно до класифікації SCImago Journal and Country Rank); 3 статті у наукових періодичних виданнях інших держав з напрямку, з якого

підготовлено дисертацію; 6 міжнародних патентів на винахід, 1 авторське свідоцтво України; 35 тез та доповідей на наукових конференціях.

8. Мова та стиль дисертації.

Дисертація написана державною мовою. Текст дисертації викладено аргументовано. Представлений в роботі матеріал має логічну послідовність, наукова термінологія є загальноновизнаною. Розділи дисертації взаємопов'язані та цілком розкривають поставлену мету. Стиль викладення результатів дослідження, наукових положень та висновків легко сприймається. Результати проілюстровані рисунками, графіками та таблицями.

9. Відповідність академічній доброчесності.

Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело, що, зокрема, підтверджується звітом подібності за результатами перевірки дисертації на текстові співпадіння.

В ході вивчення дисертаційної роботи фактів чи інших свідчень порушення академічної доброчесності (у тому числі академічного плагіату, фабрикації, фальсифікації, обману) не виявлено.

10. Дискусійні положення та зауваження щодо дисертаційної роботи.

1. Розробка методів підвищення показників якості систем мобільного зв'язку є сучасною проблемою, яка розглядається вже не одне десятиріччя, тому в першому розділі було б доцільно навести основні шляхи підвищення цих показників, які застосовувалися протягом розвитку таких систем.

2. Огляд методів класифікації трафіка не в повній мірі враховує здобутки вітчизняних фахівців в цій галузі.

3. Доцільно було б навести оцінки швидкодії, затримок та інших параметрів при роботі запропонованого методу завадостійкого кодування та

методу організації мобільних периферійних обчислень у реальних системах мобільного зв'язку 5G.

4. Оскільки запропоновані рішення доведені до конкретних протоколів взаємодії, то з тексту дисертаційної роботи не зовсім зрозуміло, яким чином вказані протоколи будуть взаємодіяти з існуючими рішеннями.

5. В дисертації використовуються запропоновані методи наскрізного шифрування та автентифікації під час дзвінка, для яких наведено кроки по впровадженню, виконано якісну оцінку підвищення захищеності, але доцільно було б також навести кількісні оцінки підвищення рівня захищеності при використанні запропонованих методів.

6. Підвищення захищеності, як правило, призводить до зниження швидкодії та інших показників якості послуг, що надаються. Тому доцільно було б оцінювати кількісні показники якості під час застосування запропонованих методів захисту інформації.

7. Науковий та прикладний інтерес становить застосування методів класифікації трафіка для виявлення шкідливих пакетів на базовій станції (eNb/gNb), згаданий у другому розділі, але не досліджений в інших розділах.

11. Відповідність реферату змісту дисертаційної роботи.

Реферат за структурою та оформленням відповідає встановленим чинним вимогам. В рефераті відображено головні результати дисертаційного дослідження та наукові здобутки автора. За змістом реферат є ідентичним до тексту дисертаційної роботи.

12. Висновок.

Вважаю, що дисертаційна робота Астраханцева Андрія Анатолійовича на тему “Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв'язку”, є завершеною науковою працею, що виконана на високому науковому і методичному рівнях, в якій представлені

нові наукові результати, спрямовані на вирішення важливої науково-прикладної проблеми підвищення захищеності та якості передавання й оброблення даних в мережах мобільних операторів завдяки створенню комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі і сукупності нових моделей та методів передавання, зберігання та оброблення даних.

За актуальністю, практичною цінністю та науковою новизною, змістом та оформленням, дисертаційна робота повністю відповідає вимогам пп. 7, 8, 9 “Порядку присудження та позбавлення наукового ступеня доктора наук”, затвердженого постановою Кабінету Міністрів України від 17.11.2021 № 1197 (із змінами), а її автор Астраханцев Андрій Анатолійович заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – Телекомунікаційні системи та мережі.

Офіційний опонент
професор кафедри
телекомунікаційних та
радіоелектронних систем
Національного авіаційного університету,
доктор технічних наук, професор
06.11.2024 р.



Олександр ГОЛУБИЧИЙ
Вчений секретар
Національного авіаційного університету
