ВІДГУК

офіційного опонента д.т.н., проф. **Агеєва Дмитра Володимировича**
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

Актуальність обраної теми дисертації

Кожне покоління стільникових технологій є більш безпечним, ніж попередня версія, і 5G не є винятком. 3GPP стандартизував 5G як найбезпечнішу базову бездротову технологію і першу технологію стільникового зв'язку, призначену для розгортання в хмарі, що вимагає додаткових рішень щодо безпеки. Функції мережі 5G для базової мережі та мережі RAN розвиваються і стають хмарними, це впливає на стан безпеки мереж 5G, оскільки необхідно враховувати найкращі практики безпеки, багаторівневі засоби контролю безпеки і архітектуру нульової довіри. Врахування цих факторів 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 для недопущення витоку персональних даних.

Крім того, слід враховувати, що існує наукова проблема, через активне впровадження нових джерел трафіку призводить до недостатнього рівня адаптації існуючих методів класифікації та визначення пріоритетів трафіка

для забезпечення відповідного рівня якості обслуговування, а зростання обсягів трафіку і поява нових типів навантаження (таких як mIoT, V2V) призводять до погіршення ефективності існуючих методів обробки та кластеризації даних, які не були на це розраховані.

Вищеперелічені фактори є складовими науково-прикладної проблеми, що пов'язана з підвищенням захищеності та якості передачі й обробки даних в інформаційно-комунікаційних мережах мобільного зв'язку, завдяки створенню комплексної методології управління процесом обслуговування у мобільній мережі і сукупності нових моделей та методів передачі, зберігання й обробки даних, вирішення якої являється актуальною науково-прикладною задачею.

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

Дослідження за темою дисертаційної роботи 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», спільного проекту ІТС НТУУ «КПІ» та університету Анхальт (Hochschule Anhalt) «DigIn.Net 2: Deutsch-ukrainisches Netzwerk digitaler Innovationen-2» (№57602278), а також виконувались у рамках держбюджетних тем кафедри ТКС ХНУРЕ № 235-1 «Методи проектування телекомунікаційних мереж NGN та управління їх ресурсами» (№ ДР 0109U000662) та кафедри інформаційно-телекомунікаційних мереж КПІ ім. Ігоря Сікорського №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».

Ступінь обгрунтованості наукових положень, висновків та рекомендацій, сформульованих в дисертації та їх достовірність

Обґрунтованість наукових положень дисертаційної роботи базується на відповідності з положеннями, які вже були відкриті іншими авторами і представлені в наукових публікаціях по напрямках захисту інформації в мобільних мережах, мобільних периферійних обчислень та забезпечення якості обслуговування. В дисертації приведено такий аналіз, зіставлені результати і показана спадкоємність, відповідність з вже відомими.

Обгрунтованість наукових результатів також підтверджується використанням для вирішення наукових задач методів багатокритеріальної оптимізації та методів математичної статистики для вибору параметрів та вдосконалення методів класифікації та кластеризації трафіка; методів теорії динамічного програмування та засобів теорії дослідження операцій було розв'язано ряд оптимізаційних задач пошуку найкращих параметрів класифікації трафіка в мережі. При розробленні методів розподілу трафіка розподілених граничних обчислень МЕС застосовувалися методи теорії масового обслуговування. Для синтезу інтелектуальної системи управління застосовані елементи теорії ігор і теорії прийняття рішень. Під час вдосконалення методів завадостійкого кодування використовувалися методи математичного моделювання. За допомогою імітаційного моделювання проводилася оцінка якості кластеризації трафіка, ефективності роботи інтелектуальної системи та порівняльний аналіз ефективності методів біометричної автентифікації в інформаційно-телекомунікаційній мережі. Методи математичного та імітаційного моделювання використано для

розробки методів шифрування та автентифікації користувачів в процесі дзвінка, методів формування біометричного шаблону та об'єднання різних типів біометричних даних. Для оцінки адекватності отриманих теоретичних рішень використано програмні засоби імітаційного моделювання.

Отримані теоретичні та практичні результати дисертаційної роботи мають апробацію на провідних фахових наукових конференціях та опубліковані у рецензованих періодичних виданнях.

Структура та зміст дисертації

У *вступі* обґрунтовується 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.

1) 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 і онтологічній моделі. Запропонована структура забезпечує покращення наведених в першому розділі показників якості, таких як рівень помилок і втрат пакетів, швидкість передачі інформації, затримка передачі й обробки інформації, а також показників захищеності (конфіденційність, цілісність, доступність та спостереженість). Для підвищення значень показників якості передачі даних запропоновано поетапне впровадження у вузлі мережі

вдосконалення методів попередньої обробки даних у вузлах мережі для підвищення точності класифікації і обробки трафіка та зменшення затримки на обробку даних; впровадження новітніх адаптивних методів класифікації трафіка для підвищення ефективності використання мережних ресурсів під час застосування мережних зрізів (Network Slicing); впровадження нових методів розподілу трафіка на граничних елементах мережі для підвищення якості застосування технології граничних обчислень з множинним доступом (Mobile Edge Computing); вдосконалення методів завадостійкого кодування пакетів під час їх передачі мобільною мережею для зменшення рівня помилок і втрат пакетів.

При цьому, вдосконалення методів завадостійкого кодування пакетів пропонується до реалізації у модемній частині обладнання користувача.

Для вдосконалення показників захищеності, комплексна методологія пропонує 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 обгрунтуванні 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 прихування 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 на один рівень надання послуг показників конфіденційності, цілісності та спостереженості.

Наукова новизна результатів дисертаційного дослідження

Наукова новизна дисертаційної роботи полягає в наступному:

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 MEC, 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. *Набув подальшого розвитку* метод обробки даних у пристрої користувача, який забезпечує підвищення завадостійкості під час передачі даних мобільною мережею 5G шляхом вдосконалення методу формування коду Raptor, що зменшує ймовірність 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. *Набули подальшого розвитку* методи захисту приватних даних у пристрої користувача, відмінними рисами яких є: використання біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об'єктами; вдосконалений метод 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 роботи

Практичне значення роботи полягає в наступному:

1. Усі теоретичні розробки дисертаційної роботи доведено до конкретних архітектурних рішень, протоколів взаємодії та методів управління сервісами у інформаційно-телекомунікаційних системах нового покоління, які апробовано під час розгортання та обслуговування мереж оператора мобільного зв'язку.

2. Запропонована удосконалена система обробки даних і розподілу ресурсів протестована в лабораторіях компанії Lifecell Ukraine, що дозволило в комплексі з технологіями 5G підвищити швидкість передачі даних до 1.3Гбіт/сек, що підтверджується актом впровадження.

3. Розроблено та впроваджено програмні засоби, які реалізують нові методи захисту приватних даних у мобільних пристроях Samsung, що підтверджується патентами на винахід.

4. Отримані результати використано в навчальному процесі кафедри інформаційних технологій в телекомунікаціях: в лекційних заняттях та комп'ютерних практикумах з дисциплін «Завадостійке кодування в інформаційно-комунікаційних мережах», «Основи криптографічного захисту інформації» і «Основи побудови захищених банківських інформаційно-телекомунікаційних систем» що підтверджується актом впровадження.

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

Повнота викладення результатів роботи у наукових працях

Повнота викладення результатів підтверджується апробацією результатів дисертаційного дослідження в публікаціях у фахових рецензованих виданнях, оприлюдненням на міжнародних і всеукраїнських науково-практичних конференціях. Результати дисертації опубліковано у 76 наукових роботах, у тому числі 31 стаття у наукових періодичних виданнях, включених до Переліку наукових фахових видань України (в тому числі, 3 статті у виданнях, включених до категорії "А", з них 1 стаття у виданні віднесеному до квартилю Q3 відповідно до класифікації SCImago Journal and Country Rank), 6 міжнародних патентів на винахід, 1 авторське свідоцтво на твір, 35 тез доповідей на наукових конференціях, 3 навчальних посібника, що додатково відображають результати дисертації.

Мова та стиль дисертації

Дисертація написана державною мовою. Текст дисертації викладено аргументовано та логічно. Виклад матеріалу послідовний, наукова

термінологія є загальновизнаною, розділи взаємопов'язані та цілком розкривають поставлену мету. Формат викладення результатів досліджень та нових наукових положень забезпечує доступність їх сприйняття. Результати проілюстровані рисунками та таблицями.

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.

Дискусійні положення та зауваження щодо дисертаційної роботи

1. По представленому матеріалу є відчуття, що дисертаційна робота перевантажена дослідженнями. Це відноситься попередньо до третього розділу, де запропонований алгоритм контейнеризації та управління не увійшов до підсумкової наукової новизни і п'ятого розділу, де до підсумкової новизни не було включено вдосконалення системи ідентифікації людей на основі машинного навчання.

2. В роботі запропоновано метод організації розподілених обчислень, але окрім моделювання протоколу не наведено його числових оцінок.

3. Якщо стверджується, що «визначені оптимальні за критерієм точності параметри алгоритмів машинного навчання для розв'язання задачі класифікації трафіка в мережах мобільного зв'язку 5-го та 6-го поколінь», то виникає питання наскільки критичним є час пошуку оптимальних параметрів, а також коли це відбувається – безпосередньо під час роботи базової станції чи періодично під час модернізації системи.

4. По деяким результатам було порушено послідовний порядок викладання наукових та практичних результатів – так в п'ятому розділі спочатку було приведено метод віддаленого управління об'єктами, а потім система ідентифікації людей і об'єктів яка може бути використана в цьому методі.

5. Є ряд зауважень загального характеру – стилістичні та орфографічні неточності та помилки по тексту дисертації.

Висловлені зауваження не є критичними які унеможливлюють загальну позитивну оцінку дисертаційної роботи Астраханцева А.А.

Відповідність реферату змісту дисертаційної роботи

У тексті реферату відображено основні положення, зміст, результати та висновки виконаного дослідження. Зміст реферату та основні положення дисертаційної роботи є ідентичними.

Загальний висновок щодо відповідності дисертації встановленим вимогам

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 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.

Реферат повністю відображає основні положення дисертації. За актуальністю, практичною цінністю та науковою новизною, змістом та

оформленням, дисертаційна робота повністю відповідає вимогам п. 7, 8, 9 “Порядку присудження та позбавлення наукового ступеня доктора наук”, затвердженого Постановою Кабінету Міністрів України від 17.11.2021 №1197, а її автор Астраханцев Андрій Анатолійович, заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – Телекомунікаційні системи та мережі.

Офіційний опонент
професор кафедри
інфокомунікаційної інженерії ім. В.В. Поповського,
Харківського національного
університету радіоелектроніки
доктор технічних наук, професор, Дмитро АГЕЄВ

«11» 11 2024 р.

Підпис професора кафедри інфокомунікаційної інженерії
ім. В.В. Поповського Агеєва Д.В. засвідчую

Учений секретар ХНУРЕ, к.т.н. Ірина ЖАРІКОВА