

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного технічного
університету України
"Київський політехнічний інститут
імені Ігоря Сікорського"
д.т.н., проф.
Сергій СТРИКО



ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів докторської дисертації Астраханцева Андрія Анатолійовича на тему "Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв'язку", поданої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 "Телекомунікаційні системи та мережі".

(Витяг з протоколу № 3 від 13 вересня 2024 р. розширеного засідання кафедри Інформаційних технологій в телекомунікаціях НН ІТС Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського")

Тему дисертаційної роботи "Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв'язку" затверджено на засіданні Вченої ради НТУУ КПІ ім. Ігоря Сікорського (протокол №8 від 04 жовтня 2021 року).

Науковим консультантом затверджений д.т.н., проф. Глоба Л.С.

Структурний підрозділ для проведення попередньої експертизи дисертації та рецензентів затверджено Вченою радою КПІ ім. Ігоря Сікорського (протокол №7 від "09" вересня 2024 року).

Заслухавши та обговоривши доповідь Астраханцева А.А., а також за результатами попередньої експертизи представленої дисертації ухвалили прийняти такий висновок:

1. Актуальність теми дослідження

Впровадження новітніх мобільних мереж 5G відкриває перед користувачами нові можливості за рахунок істотного підвищення швидкості та зниження затримки, але при цьому виникають нові виклики стосовно захищеності та якості передачі даних в системах мобільного зв'язку.

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 вибагливими 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 для недопущення витоку персональних даних.

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. Розроблені в роботі моделі та методи є складовими єдиної архітектури управління ресурсами і захистом даних на рівні провайдера мобільного зв'язку.

Таким чином, створення і наукове обґрунтування комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв'язку з метою підвищення рівня захищеності та якості передачі й обробки даних є актуальною науково-технічною проблемою.

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

Дисертація пов'язана 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 виконувалась 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 ефективної 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).

3. Наукова новизна отриманих результатів

У дисертації вперше одержані такі нові наукові результати:

1. Запропоновано комплексну методологію обробки даних у вузлі мережі, яка використовує інтелектуальну систему управління та відрізняється додатковими елементами попередньої обробки пакетів у вузлі мережі, оптимізацією параметрів класифікації трафіка та модифікованим алгоритмом кластеризації трафіка, що дозволило визначити оптимальний набір ознак класифікації та визначити налаштування нейронної мережі, забезпечуючи високу точність класифікації.

2. Запропоновано новий 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. Запропоновано новий 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. Запропоновано нові методи захисту приватних даних у пристрої користувача, які відрізняються наявністю оригінальних 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. Запропоновано нові методи 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.

4. Ступінь обґрунтованості наукових положень та висновків, сформульованих у дисертаційній роботі

Обґрунтованість та достовірність наукових положень і результатів, рекомендацій і висновків підтверджується коректною постановкою завдань досліджень, а також апробацією результатів дисертаційної роботи у виробничих умовах. Основні теоретичні і експериментальні результати досліджень опубліковано у двох розділах монографіях, 3 навчальних посібниках (1 з грифом МОНУ) у співавторстві, 28 публікаціях – у наукових фахових виданнях України, 3 статтях в закордонних періодичних фахових виданнях, 33 матеріалах тез конференцій і симпозіумів, 6 патентах на винахід.

Прикладне наукове значення розробленої методології полягає в розробці моделей та методів підвищення захищеності та якості передачі й обробки даних в 5G мережі мобільного оператора. Підвищення завадостійкості, якості передачі та обробки даних в системах мобільного зв'язку досягається за рахунок вдосконалення методів попередньої обробки інформації на боці користувача, методів класифікації, кластеризації та попередньої обробки трафіка у вузлі мережі (на базовій станції), а підвищення захищеності систем мобільного зв'язку – за рахунок вдосконалення методів захисту особистих даних на боці користувача та вдосконалення методів захисту інформації для граничних елементів мережі, які базуються на результатах класифікації трафіку для виявлення загроз.

Розроблені теоретичні та практичні методи і рекомендації, які викладені в науковому 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.

Для вибору параметрів та вдосконалення методів класифікації та кластеризації трафіка була використана багатокритеріальна оптимізація та методи математичної статистики, при цьому для візуалізації результатів були використані теорія множин і теорія графів. За допомогою 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 програмне середовище імітаційного моделювання створене за допомогою Python 3.0.

5. Теоретичне та практичне значення результатів роботи, впровадження

Теоретичне значення результатів роботи полягає у вирішенні важливої науково-технічної проблеми створення і наукового обґрунтування комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв'язку з метою підвищення рівня захищеності та якості передачі й обробки даних.

До основних теоретичних результатів роботи відноситься:

1. Проведений аналіз особливостей та наявної якості передачі трафіка в 5G мережі та можливих загроз дозволив виявити основні проблеми, такі як зростання обсягів та поява нових джерел трафіка, поява нових вразливостей під час реалізації новітніх сервісів та послуг, що призводить до суттєвого погіршення якості та захищеності процесів надання послуг через відсутність комплексної методології підвищення захищеності та якості передачі даних в мобільній мережі в цілому.

2. Запропоновано комплексну методологію підвищення захищеності та якості передачі даних в мобільній 5G мережі, яка відрізняється багатокритеріальною оптимізацією за критеріями якості та захищеності, де підвищення захищеності досягається за рахунок застосування інтелектуальної системи управління, нового методу формування ключа з біометричних ознак користувача, вдосконаленого протоколу обміну повідомленнями, запропонованої системи управління приватними даними користувача, що в цілому дозволяє покращити показники конфіденційності, цілісності, доступності та спостереженості; підвищення якості досягається впровадженням методу розподілу навантаження для граничних обчислень з множинним доступом, новітніх методів класифікації трафіка та методів завадостійкого кодування, що в цілому дозволяє покращити показники ймовірності помилки, рівня втрат пакетів, швидкості обробки пакетів, а також пропускної здатності.

3. Вдосконалено модель аналізу та обробки даних у вузлі мережі шляхом застосування методів та технік нечіткої логіки та машинного навчання для попереднього очищення даних від випадкових помилок, множини правил нечіткої бази знань від дублікатів та конфліктів, а також візуалізації за

допомогою метаграфу, що дозволяє покращити показники якості класифікації даних у вузлах мережі, пришвидшити обробку трафіка, виявляти аномалії у трафіку під час забезпечення захисту мережі.

4. Вдосконалено набір ознак для класифікації трафіка за критеріями складності і швидкодії шляхом зменшення їх кількості без суттєвої втрати точності, а саме: зменшення набору ознак з 82 до 56 (на 31.7%), що підвищило швидкість процедури класифікації на 3.4%.

5. Визначено найкращі методи машинного навчання (Random Forest, Decision Tree) для класифікації трафіка у вузлі мережі та їх гіперпараметри, які обираються інтелектуальною системою динамічно. Найвища продуктивність при прийнятній точності досягається при розмірі виборки 128, кількості епох 10 та використанні малого (18) або середнього (54) набору ознак. Запропоновані гіперпараметри та методи є першим етапом багатокрокової обробки пакетів в мережі, що разом з кластеризацією, слайсінгом та розподіленою обробкою дозволять підвищити ефективність системи мобільного зв'язку в цілому.

6. Вдосконалено метод розподілу навантаження для граничних обчислень з множинним доступом (МЕС), новизна якого полягає в інтелектуальному розподілі даних МЕС, додаванні надмірності під час розподілу (паралелізації обчислень), додаванні функції контролю помилок і оцінюванні ефективності кожного вузла обчислень шляхом присвоєння рівня довіри, що дозволяє мінімізувати ймовірність помилки розрахунків та обсяг використаних ресурсів мережі під час розподілу завдань граничних обчислень.

7. Вдосконалено метод завадостійкого кодування пакетів під час їх передачі мобільною мережею шляхом реалізації: нового методу формування коду Raptor з міжблоковою схемою перемежіння. Запропоновані модифікації коду дозволяють зменшити рівень втрат пакетів до 11% в каналах із затираннями.

8. Вдосконалено метод формування вектору ознак біометричних характеристик користувача шляхом реалізації нового модуля агрегації; визначення пріоритетів біометричних ознак; зашумлення невикористовуваних ознак; проріджування; завадостійкого кодування та врахування стану каналу зв'язку, що дозволило підвищити рівень послуг конфіденційності та спостереженості.

9. Вдосконалено процес підготовки біометричних даних користувача до передачі мережею зв'язку шляхом підвищення порогу спрацьовування системи у зашумлених каналах зв'язку і приховування сеансу віддаленої автентифікації в заголовках мережних протоколів, що дозволяє на 10% зменшити рівень помилок FRR і підвищити рівень спостереженості.

10. Вперше запропоновано метод взаємної автентифікації користувачів під час дзвінка, шляхом модифікації полів повідомлень SETUP, CONNECT АСК та застосуванням різних видів біометричної автентифікації (в залежності від сценарію), що дозволяє уникнути підміни користувача на

іншому боці, отримати доступ до сервісів лише авторизованому користувачу і підвищити рівні послуг конфіденційності, цілісності та спостереженості.

11. Підвищено рівень послуг конфіденційності й цілісності під час розмови по мобільній мережі шляхом застосування: протоколу Діффі-Хелмана для безпечного обміну ключами; короткого автентифікаційного рядка для протидії атаці "зловмисник-посередині"; хешу попереднього дзвінка для протидії спуфінгу телефонних номерів; симетричного шифрування мови алгоритмом AES(256) для протидії прослуховуванню і підвищення рівня конфіденційності при обміні. Для реалізації протоколу обміну ключами Діффі-Хелмана запропоновано модифікацію повідомлень SETUP і CONNECT в традиційній послідовності під час встановлення дзвінка.

12. Розроблено нові методи управління приватними даними користувача для забезпечення захищеності даних під час реалізації нових сервісів, що дозволяють надавати користувачу додаткові можливості без зниження рівня захищеності. Перший метод пропонує використання біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об'єктами. Другий – зберігання приватних даних користувача в захищеному ієрархічному вигляді і доступ до них різного рівня у надзвичайних випадках для збереження життя користувача. Запропоновані рішення запатентовані і впроваджені в обладнанні Samsung.

13. Виконано оцінку ефективності запропонованих рішень. Результати апробації показали зменшення рівня втрат пакетів на 11%, зменшення затримки на обробку трафіка і вдосконалення рівня послуг із захищеності на 29%.

Практичне значення одержаних результатів 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 (є акт впровадження), що дозволило в комплексі з технологіями 5G підвищити швидкість передачі даних до 1.3Гбіт/сек.

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

4. Отримані результати впроваджено в навчальному процесі кафедри інформаційних технологій в телекомунікаціях: у лекційних курсах й на практичних заняттях з дисциплін «Завадостійке кодування в ТКС», «Системне проектування телекомунікаційних мереж» і «Основи захисту інформації в ТКС» (є акт 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).

6. Апробація результатів дисертації

Основні положення і результати дисертаційної роботи були представлені, повідомлені й одержали схвалення на 21 науково-технічній конференції: 1-а Міжнародна конференція «Безпека та захист інформації в інформаційних та телекомунікаційних системах» (м. Харків, ХНЕУ, 2008), 13-й, 14-й, 15-й, 19-й, 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті» (м. Харків, ХНУРЕ, 2009-2011, 2015, 2017), Інфокомунікації – сучасність та майбутнє: 1-й міжнар. наук.-пр. конф. молодих вчених (м. Одеса, ОНАЗ, 2011), International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science TCSET'2012 (м. Львів-Славсько, 2012), 9-я Міжнародна молодіжна науково-технічна конференція «Сучасні проблеми радіотехніки і телекомунікацій RT-2013» (м. Севастополь, СевНТУ, 2013), 23rd International Crimean Conference «Microwave&Telecommunication Technology» (м. Севастополь, СевНТУ, 2013), International Scientific-Practical Conference Problems of Infocommunications Science and Technology "PICS&T" (м. Харків, 2014, 2015, 2019), Міжнародна науково-практична конференція «Проблеми і перспективи розвитку IT-індустрії» (м. Харків, ХНЕУ, 2017), IEEE 9th International Conference on Dependable Systems, Services and Technologies "DESSERT" (м. Харків, 2018), 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів (м. Одеса, ОНАЗ, 2018), Workshop on Cybersecurity Providing in Information and Telecommunication Systems "CPITS" (м. Київ, 2021), International Conference on Information and Digital Technologies "IDT" (Zilina, Slovakia, 2021), 17-а Міжнародна науково-технічна конференція "Перспективи телекомунікацій" (м. Київ, НТУ КІП, 2023), IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (м. Київ, НТУ КІП, 2023), 2024 IEEE International Black Sea Conference on Communications and Networking (Tbilisi, Georgia).

7. Оцінка змісту дисертації

Дисертація складається з анотацій, вступу, 5 розділів основного змісту, висновків, списку використаних джерел. Загальний обсяг роботи становить 367 сторінок друкарського тексту, в тому числі список літератури із 291 найменування, робота містить ілюстрації та таблиці.

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, 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 розділі 2 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 розділі 3 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 розділі 4 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 розділі 5 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.

В якості зауважень по роботі слід відмітити наступне:

- модифікації полів повідомлень SETUP, CONNECT ACK приведуть до зміни протоколу, а це може привести до відсутності взаємодії;
- захист інформації підвищує затрати на розгортання системи на порядок;
- класифікація трафіка та оптимізація кількості ознак потребують додаткового часу.

8. Дотримання принципів академічної доброчесності

За результатами науково-технічної експертизи дисертація Астраханцева А.А. визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

9. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 76 наукових праць, у тому числі:

- 31 стаття у наукових фахових виданнях, серед яких: 3 статті у виданнях категорії «А», в тому числі одна у виданні, віднесеного до третього квартилю (Q3) відповідно до класифікації SCImago Journal, 3 статті у виданнях іноземних держав, 25 статей у науково-фахових виданнях України;
- 6 патентів на корисну модель, що пройшли міжнародну кваліфікаційну експертизу та 1 авторське свідоцтво України;
- 3 навчальних посібника (в т.ч. 1 з грифом МОНУ);
- 35 тезах доповідей на наукових конференціях (в т.ч. 10, що включені до міжнародних наукометричних баз SCOPUS).

Усі наукові результати, що виносяться на захист дисертації, отримано здобувачем самостійно. Автору належить постановка задач досліджень, теоретичне обґрунтування, їх алгоритмічне забезпечення, експериментальна перевірка нових моделей, методів та принципів.

У спільних публікаціях за темою дисертації автор зробив внесок, який полягає у формалізації ідей, виборі підходів до реалізації, аналізі та узагальненні одержаних результатів.

Перелік публікацій і особистий внесок здобувача наведені нижче.

1. Статті у наукових фахових виданнях України, віднесених до категорії «А»

1. Astrakhantsev A., Liashenko, G. "Data protection management process during remote biometric authentication", System Research and Information Technologies, №3 2022, pp. 71–85. (**Scopus**)

Особистий внесок: запропоновано стеганографічні методи прихованої передачі біометричних даних із забезпеченням підвищеної стійкості до атак та завад в каналах зв'язку.

2. Astrakhantsev A., Globa L., Fedorov O., Romanko Y. "An improved approach to organizing mobile edge computing in a 5G network", System Research & Information Technologies, 2024, No 2, pp. 82-92.

Особистий внесок: запропоновано новий метод обробки даних у вузлі мережі, який підвищує якість застосування технології граничних обчислень з множинним доступом представлено в роботі.

3. Astrakhansev A., Pedan S. "Improving user security during a call", *Radioelectronic and Computer Systems*, 2024, no. 2(110), pp.173-185. (Scopus), Q3 SCImago

Особистий внесок: запропоновані вдосконалення протоколів обміну повідомленнями під час дзвінка для підвищення рівня захищеності 5G мережі.

2. *Статті у наукових фахових виданнях України:*

4. Астраханцев А.А., Волотка В.С., Семашко Е.М. "Захист інформації в системах мобільного зв'язку за допомогою гамування" [рос], *Східно-Європейський журнал передових технологій*. – 2009. – №4/3 (40). – С. 20-23.

Особистий внесок: аналіз методів захисту мовної інформації в мобільних мережах.

5. Астраханцев А.А., Войтюк А.А. "Аналіз ефективності і завадостійкості системи OFDM", *Східно-Європейський журнал передових технологій*. – 2011. – №3/9 (51). – С. 21-23.

Особистий внесок: визначено показники ефективності та завадостійкості системи мобільного зв'язку. Виконаний аналіз ефективності та підготовлені рекомендації по підвищенню завадостійкості системи OFDM.

6. Астраханцев А.А., Дорожан А.В., Вовк О.О. "Дослідження характеристик методів приховування з використанням НЗБ на тлі адитивного шуму", *Вісник НТУ «ХП»*. – 2012. – №18. – С. 37-40.

Особистий внесок: аналіз поведінки стеганографічних методів у каналах з адитивним гаусовим шумом.

7. Астраханцев А.А., Дорожан А.В., Вовк О.О. "Дослідження стійкості методів приховування інформації в нерухомих зображеннях" [рос], *Системи обробки інформації*. – Х.: ХУПС – 2012. – №2. – С. 104-109.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

8. Астраханцев А.А., Новіков Р.С. "Аналіз характеристик завадостійких кодів" [рос], *Системи обробки інформації*. – Х.: ХУПС – 2013. – №9 (116) – С. 164-167.

Особистий внесок: запропоновано вдосконалені методи формування коду Raptor, формування коду LDPC, як одного з елементів коду Raptor, а також вдосконалення методу декодування коду Raptor.

9. Астраханцев А.А., Новіков Р.С. "Вибір параметрів LDPC кодів для каналів з АБГШ" [рос], *Системи обробки інформації*. – Х.: ХУПС – 2014. – №1 (117). – С. 195-199.

Особистий внесок: запропоновано вдосконалені методи формування коду Raptor, формування коду LDPC, як одного з елементів коду Raptor, а також вдосконалення методу декодування коду Raptor.

10. Астраханцев А.А., Вовк О.О. "Розробка методики та оцінювання важливості характеристик стеганографічних алгоритмів", *Вісник національного університету Львівська Політехніка «Інформаційні системи та мережі*. Львів, 2014. – № 805. – С. 52-60.

Особистий внесок: запропоновано методику оцінювання важливості характеристик стеганографічних алгоритмів.

11. Астраханцев А.А., Вовк О.О. "Аналіз ефективності застосування вейвлет-перетворення в стеганографічних системах передавання даних", *Вісник національного університету Львівська Політехніка «Інформаційні системи та мережі*. Львів, 2015. – № 832. – С. 9-17.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

12. Астраханцев А.А., Вовк О.О. “Синтез методу прихованої передачі інформації, ефективного за критеріями надійності та захищеності”, Проблеми телекомунікацій. – Х.: ХНУРЕ. – 2015. – №1. – С. 103-115.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

13. Астраханцев А.А., Шостак Н.В., Романько С.В. “Дослідження стійкості авторських прав на відеопродукцію”, Системи обробки інформації. – Х.: ХУПС – 2017. – №2 (148). – С. 138-143.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

14. Астраханцев А.А., Ляшенко Г.С. “Дослідження ефективності методів біометричної автентифікації”, Системи обробки інформації. – Х.: ХУПС – 2017. – №2 (148). – С. 111-114.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку. Вдосконалення методу формування біометричного шаблону.

15. Астраханцев А.А., Щербак А.О., Щербак О.В. “Аналіз скритності та стійкості до шуму в каналах зв'язку методів мережної стеганографії”, Проблеми телекомунікацій. – Х.: ХНУРЕ. – 2018. – №2. – С. 89-98.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

16. Астраханцев А.А., Шостак Н.В., Безрук В.М. “Вибір переважного алгоритму вбудовування цифрових водяних знаків в відеофайли”, Радіоелектроніка, інформатика, управління. – Запоріжжя, ЗНТУ. – 2018. – №3(46). – С. 167-173.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

17. Астраханцев А.А., Чернікова В.Г., Ляшенко Г.С. “Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока”, Системи озброєння і військова техніка. – 2018. – №1. – С. 195-202.

Особистий внесок: запропонований метод формування біометричного шаблону та спосіб об'єднання різних типів біометричних даних.

18. Астраханцев А.А., Шостак Н.В. “Аналіз стійкості стеганографічних методів вбудовування даних в відеофайли до атак”, Системи обробки інформації. – Х.: ХУПС – 2019. – №3. – С. 110-116.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

19. Astrakhansev A., Ostapenko M., Shtogrina O., Globa L. “Developing a computer vision re-identification system”, Information and Telecommunication Sciences. – 2020. – №1. – P. 35-40.

Особистий внесок: запропонована інтелектуальна система прийняття рішень.

20. Astrakhtantsev A., Liashenko G., Shcherbak A. "Noise resistance of remote authentication via LTE network", Information and Telecommunication Sciences. – 2020. – №2. – P. 38-43.

Особистий внесок: розроблено методи підвищення завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами.

21. Astrakhtantsev A., Davydiuk A. "Improved cluster management method for industrial "Internet of Things" network", Information and Telecommunication Sciences. – 2020. – №2. – P. 81-85.

Особистий внесок: запропонований вдосконалений метод кластеризації трафіка.

22. Астраханцев А.А., А.О. Щербак, О.В. Щербак, Г.Є. Ляшенко. "Дослідження завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами", Проблеми телекомунікацій. – 2020. – №1 (26). – С. 63-72.

Особистий внесок: розроблено методи підвищення завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами.

23. Астраханцев А.А., Л.С. Глоба, А.М. Давідюк, О.В. Сушко. "Дослідження ефективності алгоритмів машинного навчання для класифікації трафіка в мобільних мережах", Проблеми телекомунікацій. – 2022. – №1 (30). – С. 3-17.

Особистий внесок: визначено оптимальний набір ознак для класифікації трафіка, оцінено ефективність застосування методів машинного навчання для вирішення задач класифікації трафіка та запропоновано рекомендації щодо їх використання і значень гіперпараметрів.

24. Астраханцев А.А. Г.Є. Ляшенко. "Процес керування захищеністю даних під час віддаленої біометричної автентифікації", System research and information technologies. – 2022. – №3. – С. 71-85.

Особистий внесок: запропоновано стеганографічні методи прихованої передачі біометричних даних із забезпеченням підвищеної стійкості до атак та завад в каналах зв'язку.

25. Astrakhtantsev A., Globa L., Sushko O., Davydiuk A. "Adjusting the parameters of machine learning algorithms to improve the accuracy of traffic classification", Information and Telecommunication Sciences. – 2023. – P. 26-32.

Особистий внесок: визначено оптимальний набір ознак для класифікації трафіка, оцінено ефективність застосування методів машинного навчання для вирішення задач класифікації трафіка та запропоновано рекомендації щодо їх використання і значень гіперпараметрів.

26. Астраханцев А. Глоба Л., Цуканов С. "Класифікація мережевого трафіку методами машинного навчання", Проблеми телекомунікацій. – 2023. – №2. – С. 3-13.

Особистий внесок: визначено оптимальний набір ознак для класифікації трафіка, оцінено ефективність застосування методів машинного навчання для вирішення задач класифікації трафіка та запропоновано рекомендації щодо їх використання і значень гіперпараметрів.

27. Astrakhtantsev A., Leliak A. "Improve mobile driving license data transfer security via BLE/Wi-Fi aware with UWB ranging", Problemi Telekomunikacij. – 2023. – №2 (33) – С. 62-74.

Особистий внесок: проаналізовані методи захисту мобільного пристрою користувача під час користування мобільними документами та BLE.

28. Astrakhantsev A., Hryshuk I., Pedan S., Globa L. "Analysis of routing protocols characteristics in ad-hoc network", Information and Telecommunication Sciences. – 2024. – №1 – P. 12-17.

Особистий внесок: сформовано рекомендації по застосуванню протоколів маршрутизації інтелектуальною системою прийняття рішень в ad-hoc мережі.

3. *Статті у періодичних наукових виданнях інших держав:*

29. Astrakhantsev A., Dorozhan A. "Research methods for improving noise immunity of secure data transmission", Science Publishing Group. – №1(4), New York, USA, 2013. – pp. 28-36.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

30. Astrakhantsev A., Vovk O. "Synthesis of optimal steganographic method meeting given criteria", Informatyka Automatyka Pomiaru w Gospodarce i Ochronie Środowiska (technical and scientific journal), Lublin, Poland, 2015. – pp. 27-34.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

31. Astrakhantsev A., Shostak N., Romanko S. "Comparative analysis of effectiveness video watermarking techniques", Global Science Center LP. – Sciences of Europe (Praha, Czech Republic) # 15-1 (15), 2017. – pp. 92-95.

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

4. *Патенти на винахід і авторські свідоцтва*

32. Sun-Kyung Kim, Astrakhantsev A., Yakishyn Y., Korobov M. "System and method for providing information using near field communication", US Patent App. US15/781,636, 2020 (US10986462B2)

Особистий внесок: оригінальний метод зберігання приватних даних користувача в захищеному ієрархічному вигляді, який надає нові можливості під час взаємодії користувача з пристроями mIoT і забезпечує підвищений рівень послуг критерія конфіденційності.

33. Astrakhantsev A., Shchur O., Korobov M., Oliynyk A., Jae-Hong Kim "Electronic device and method for providing user information", US Patent App. US15/778,818, 2018 (EP3367277A1).

Особистий внесок: оригінальний метод зберігання приватних медичних даних користувача в захищеному ієрархічному вигляді.

34. Popov A., Popov O., Astrakhantsev A., Pedan S., Shapoval I., Konoval O. "Electronic device and method of operating the same", US Patent App. US18/163,589 (US20230259652A1).

Особистий внесок: запропоновані нові методи захисту приватних даних на боці пристрою користувача, які відрізняються використанням біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління пристроями.

35. Popov A., Popov O., Kulakov A., Astrakhantsev A., Shchur O., Tatarinova Y. "Method for securing image and electronic device performing same", US Patent App. US17/378,032, 2021 (US20210342967A1).

Особистий внесок: запропоновані нові методи захисту приватних даних на боці пристрою користувача, які відрізняються використанням біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління пристроями.

36. Pedan S., Kopysov O., Popov O., Chalyi O., Astrakhantsev A. "Folderable devices and methods of operation thereof", Korean patent KR20220007352.

Особистий внесок: оригінальний метод зберігання приватних даних користувача в захищеному ієрархічному вигляді, який надає нові можливості під час взаємодії користувача з пристроями IoT і забезпечує підвищений рівень послуг критерія конфіденційності.

37. Progonov D., Popov O., Astrakhantsev A., Motchanyi A. "Device and method for acquiring biosignal", WO2024096391A1.

Особистий внесок: запропонований новий метод формування біометричного шаблону та спосіб об'єднання різних типів біометричних даних.

38. Авторське право на твір №116973 від 10.03.2023: Науковий твір «Силабус навчальної дисципліни «EU5G4UA: Застосування інструментарію та фреймворків ЄС для мереж 5G для України (EU5G4UA: Application of EU toolbox and frameworks of 5G networks for Ukraine)» // Турута О.П., Турута О.В., Астраханцев А.А., Свдокименко М.О., Даніель Я.Д.

Особистий внесок: запропоновані методи викладання параметрів якості та захищеності мереж 5G.

5. Навчальні посібники

39. Інформаційні мережі зв'язку. Т. 2. Телекомунікаційні технології стаціонарних мереж зв'язку [Текст]: навч. посібник // упорядники: Безрук В.М., Бідний Ю.М., Астраханцев А.А., Колтун Ю.М. – Х.: ХНУРЕ. – 2011. – 502с.

40. Інформаційні мережі зв'язку. Т. 4. Технології надання інформаційних послуг [Текст]: навч. посібник // упорядники: Безрук В.М., Корольов В.М., Золотарьов В.А., Астраханцев А.А. – Х.: ХНУРЕ. – 2011. – 424с.

41. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв'язку [Текст]: навч. посібник з грифом МОНУ – Х.: ТОВ «Компанія СМІТ». – 2011. – 368с.

6. Тези доповіді на наукових конференціях

42. Астраханцев А.А., Вакуленко В.С. "Підвищення ефективності алгоритмів приховування інформації в нерухомих зображеннях" [рос], 1-а Міжнародна конференція «Безпека та захист інформації в інформаційних та телекомунікаційних системах». – Х.: ХНЕУ, 2008. – С. 27-28.

43. Астраханцев А.А., Бондар І.В. "Конфіденційність і захист в мережах стандарту GSM. Пакетна передача даних в з розробкою механізмів захисту трафіка" [рос], 1-а Міжнародна конференція «Безпека та захист інформації в інформаційних та телекомунікаційних системах». – Х.: ХНЕУ, 2008. – С. 20-21.

44. Астраханцев А.А., Катюшина О.Р. "Підвищення стійкості алгоритмів захисту мови в мережах мобільного зв'язку" [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.2 – С. 62.

45. Астраханцев А.А., Варич В.В. "Керування трафіком і забезпечення якості обслуговування в IP-мережах" [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.1 – С. 197.

46. Астраханцев А.А., Вакуленко В.С. “Дослідження методів підвищення надійності стеганосистем” [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.2 – С. 60.
47. Астраханцев А.А., Гулякова Т.Б. “Аналіз якості мови в корпоративних мережах супутникового зв'язку” [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.1 – С. 194.
48. Астраханцев А.А., Белікова І.В. “Дослідження захищеності електронних платежів в корпоративних мережах” [рос], 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 225.
49. Астраханцев А.А., Краснянський В.В. “Аналіз характеристик корпоративних супутникових мереж зв'язку” [рос], 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 228.
50. Астраханцев А.А., Копитова М.О. “Аналіз якості та захищеності мови в мережі IP-телефонії”, 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 244.
51. Астраханцев А.А., Кузнецова Є.О. “Дослідження характеристик стеганографічних систем передачі інформації”, 14-й Міжнародний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 192
52. Астраханцев А.А., Лесковець Л.І. “Застосування ймовірнісного підходу для побудови систем захисту інформації в мережах зв'язку”, 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 200.
53. Астраханцев А.А., Шостак О.В. “Дослідження методів забезпечення якості у IP-мережах”, 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 209.
54. Астраханцев А.А., Афанасьєвський Ю.В. “Аналіз характеристик систем електронної ідентифікації на основі систем RFID” [рос], 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 140.
55. Астраханцев А.А., Войтюк А.А. “Дослідження завадозахищеності та ефективності в бездротових мережах з OFDM модуляцією”, 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 158.
56. Астраханцев А.А., Вовк О.О. “Дослідження стійкості цифрових водяних знаків у відеофайлах і зображеннях”, 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 156.
57. Астраханцев А.А., Шостак О.В. “Аналіз методів керування трафіком у мультисервісній мережі”, 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 208.
58. Астраханцев А.А., Дорожан А.В. “Дослідження стійкості стеганосистем” [рос], Інфокомунікації – сучасність та майбутнє: матеріали першої міжнар. наук.-пр. конф. молодих вчених. – Одеса: ОНАЗ. – 2011. – Ч.1, С.118-120.
59. Астраханцев А.А., Войтюк А.А. “Дослідження завадостійкості алгоритмів модуляції OFDM та DMT”, Інфокомунікації – сучасність та майбутнє: матеріали першої міжнар. наук.-пр. конф. молодих вчених. – Одеса: ОНАЗ. – 2011. – Ч.1, С.109-111.
60. Астраханцев А.А., Вовк О.О. “Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у

мережах зв'язку", Інфокомунікації – сучасність та майбутнє: матеріали першої міжнар. наук.-пр. конф. молодих вчених. – Одеса: ОНАЗ. – 2011. – Ч.1, С.105-108.

61. Астраханцев А.А., Романько С.В., Шостак Н.В. "Дослідження стійкості до атак алгоритмів захисту авторських прав на відеопродукцію", Міжнародна науково-практична конференція «Проблеми і перспективи розвитку ІТ-індустрії». – Х. – 2017. – С. 64.

62. Астраханцев А.А., Щирова Ю.А. "Багатокритеріальний аналіз ефективності систем автентифікації користувача", 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в ХХІ столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 136-137.

63. Астраханцев А.А., Жмакіна В.В. "Порівняльний аналіз протоколів мультикаст доставки контенту в мережі IPTV", 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в ХХІ столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 155-156.

64. Астраханцев А.А., Чернікова В.Г., Стрілець А.М. "Дослідження характеристик системи біометричної ідентифікації по радужній оболонці ока", 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в ХХІ столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 44-45.

65. Астраханцев А.А., Форостянко К.Ю. "Efficiency of user authentication methods in mobile networks", 17-а міжнародна науково-технічна конференція "Перспективи телекомунікацій". – К.: НТУ КПП. – 2023. – pp. 229-232.

66. Астраханцев А.А., Сушко О.В. "Study of the efficiency of machine learning algorithms for traffic classification in mobile networks", 17-а міжнародна науково-технічна конференція "Перспективи телекомунікацій". – К.: НТУ КПП. – 2023. – pp. 232-235.

7. Тези доповіді на наукових конференціях, включених до бази Scopus

67. Astrakhantsev A., Doroghan, O., Poponin, O., Shostak, N. "Studying of stability of the information hiding methods in still images", Modern Problems of Radio Engineering, Telecommunications and Computer Science – Proceedings of the 11th International Conference, TCSET'2012. – P. 409. **(Scopus)**

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку.

68. Astrakhantsev A., Liashenko G., Chernikova V. "Network steganography application for remote biometric user authentication", Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018. – pp. 326-330. **(Scopus)**

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку

69. Astrakhantsev A., Liashenko G. "Investigation of the influence of image quality on the work of biometric authentication methods", 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings. – pp. 543-546. **(Scopus)**

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку

70. Astrakhantsev A., Shcherbak A., Shcherbak O., Liashenko G. "Biometric templates noise immunity during transmission by mobile networks", CEUR Workshop Proceedings, 2021, 2923, pp. 175–181. **(Scopus)**

Особистий внесок: запропоновані стеганографічні завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку

71. Astrakhantsev A., Globa L., Novogradskaya R., Skulysh M., Stryzhak O. "Improving resource allocation system for 5G networks", 2021 International Conference on Information and Digital Technologies (IDT) – 2021. – pp. 182-188. **(Scopus)**

Особистий внесок: запропоновано інтелектуальну систему розподілу ресурсів в 5G мережі.

72. A. Astrakhantsev, L. Globa, A. Davydiuk and O. Sushko, "Feature Set Optimization for Machine Learning Traffic Classification in Mobile Networks," 2023 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Istanbul, Turkiye, 2023, pp. 369-370, doi: 10.1109/BlackSeaCom58138.2023.10299767. **(Scopus)**

Особистий внесок: визначено оптимальний набір ознак для класифікації трафіка, оцінено ефективність застосування методів машинного навчання для вирішення задач класифікації трафіка та запропоновано рекомендації щодо їх використання і значень гіперпараметрів.

73. Astrakhantsev A., Globa L., Pedan S., Mysko N. "Secured method of providing hierarchical private data via a smartphone", IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics – 2023. – pp.50-53. **(Scopus)**

Особистий внесок: запропоновано новий метод зберігання приватних даних користувача в захищеному вигляді, який надає нові можливості під час взаємодії користувача з пристроями mIoT.

74. Astrakhantsev A., Liashenko G. "Implementation biometric data security in remote authentication systems via network steganography", Advances in Information and Communication Technology and Systems: Lecture Notes in Networks and Systems, Springer International Publishing 2021, 152, pp. 257–273. **(Scopus)**

Особистий внесок: запропоновано стеганографічні методи прихованої передачі біометричних даних із забезпеченням підвищеної стійкості до атак та завад в каналах зв'язку.

75. Astrakhantsev A., Globa L., Astrakhantsev O. "Computational Intelligence for Voice Call Security: Encryption and Mutual User Authentication", Digital Ecosystems: Interconnecting Advanced Networks with AI Applications. TCSET 2024. Lecture Notes in Electrical Engineering, vol 1198. Springer, Cham. pp. 714-733.

Особистий внесок: запропоновані вдосконалення протоколів обміну повідомленнями під час дзвінка для підвищення рівня захищеності 5G мережі.

76. Astrakhantsev A., Globa L., Tsukanov S. "Approach to Traffic Classification in 5G Networks", 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 332-336. **(Scopus)**

Особистий внесок: визначено оптимальний набір ознак для класифікації трафіка, оцінено ефективність застосування методів машинного

навчання для вирішення задач класифікації трафіка та запропоновано рекомендації щодо їх використання і значень гіперпараметрів.

Якість та кількість публікацій відповідають “Порядку присудження та позбавлення наукового ступеня доктора наук”.

ВВАЖАТИ, що дисертаційна робота Астраханцева Андрія Анатолійовича “Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв’язку”, що подана на здобуття наукового ступеня доктора технічних наук, є кваліфікаційною науковою працею, виконаною здобувачем самостійно, за своїм науковим рівнем та практичною та теоретичною цінністю, змістом та оформленням повністю відповідає вимогам п.7 та 9 “Порядку присудження та позбавлення наукового ступеня доктора наук”, що їх пред’являють до докторських дисертацій, та паспорту спеціальності 05.12.02 “Телекомунікаційні системи та мережі”.

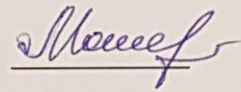
РЕКОМЕНДУВАТИ дисертаційну роботу “Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв’язку”, подану Астраханцевим Андрієм Анатолійовичем на здобуття наукового ступеня доктора технічних наук, до захисту у спеціалізованій раді Д26.002.14 за спеціальністю 05.12.02 “Телекомунікаційні системи та мережі”.

Головуючий на засіданні
д.т.н., проф.,
завідувач кафедри ІТТ



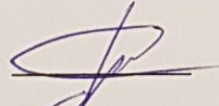
Скулиш М.А.

Рецензент
д.т.н., проф.,



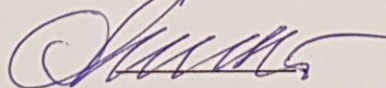
Мошинська А.В.

Рецензент
д.т.н., проф.,



Романов О.І.

Рецензент
д.т.н., проф.,



Лисенко О.І.