МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

Кваліфікаційна наукова праця
на правах рукопису

АСТРАХАНЦЕВ АНДРІЙ АНАТОЛІЙОВИЧ

УДК 621.391

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТА ЯКОСТІ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Спеціальність: 05.12.02 – телекомунікаційні системи та мережі

технічні науки

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____А.А. Астраханцев

Науковий консультант: Глоба Лариса Сергіївна, д.т.н., проф.

Київ – 2024

АНОТАЦІЯ

Астраханцев А. А. **Моделі та методи підвищення якості передачі даних сервісів в системах мобільного зв'язку**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського" Міністерства освіти і науки України, м. Київ, 2024.

Дисертаційна робота присвячена вирішенню актуальної наукової проблеми створення і наукового обґрунтування комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв'язку з метою підвищення рівня захищеності та якості процесу обслуговування користувачів.

В роботі продемонстровано передумови для виникнення протиріччя, оскільки досі немає єдиної концепції, моделей та методів управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв'язку з метою підвищення рівня захищеності та якості процесу обслуговування користувачів. Показано, що поява нових джерел трафіку та впровадження нових сервісів, зумовлює підвищення вимог щодо швидкості та якості надання послуг, що в свою чергу вимагає удосконалення програмної частини ядра мережі та обладнання користувача. Також визначено, що в 5G мережі підвищуються вимоги щодо показників

захищеності інформаційно-комунікаційних систем через появу нових загроз та реалізацію нових сервісів.

На сьогодні дане протиріччя можливо розв’язати шляхом розробки нових принципів, математичних моделей та методів управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв’язку.

У дисертаційній роботі вирішено важливу науково-технічну проблему створення і наукового обґрунтування комплексної методології управління процесом обслуговування у інформаційно-комунікаційній мережі мобільного зв’язку з метою підвищення рівня захищеності та якості процесу обслуговування користувачів.

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

Перший розділ роботи містить огляд літературних джерел за темою дисертації, проведення аналізу сучасного стану та тенденцій розвитку, особливостей функціонування інформаційно-телекомунікаційної системи на основі 5G, її ключові сервіси та технології. Визначені основні показники якості та захищеності передачі даних у інформаційно-телекомунікаційних системах. Для інформаційно-телекомунікаційних систем на основі мережі 5G визначені основні вразливості та загрози, що можуть впливати на ступінь повноти надання послуг із захисту інформації. Окремо розглянуто вразливості та атаки на існуючі методи віддаленої автентифікації

користувачів, визначені їх слабкі місця, які потребують вдосконалення. Проведено огляд методів завадостійкого кодування в мобільних мережах.

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), показників захищеності (конфіденційність, цілісність, доступність та спостереженість). Для підвищення значень показників якості передачі даних запропоновано поетапне впровадження у вузлі мережі таких кроків, як: 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; впровадження нових методів розподілу трафіка на граничних елементах мережі для підвищення якості застосування технології граничних обчислень з множинним доступом; 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, запропоновано впровадження таких кроків як: вдосконалення 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. Також в розділі запропоновано онтологічну модель системи мобільного зв'язку з урахуванням показнників якості та захищеності.

В третьому розділі для зменшення сумарної затримки передачі трафіка було 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 нових методів кластеризації трафіка. Розроблений новий метод обробки даних у вузлі мережі, який підвищує якість 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 новому методі формування коду Raptor, вдосконаленні

коду LDPC, як прекодеру коду Raptor, а також методі декодування коду Raptor. Вдосконалення моделі Raptor кодів відбувається шляхом внесення процедури перемежіння і змін у матриці формування коду, що дозволило знизити рівень помилок, що не виправляються, а також підвищити швидкість декодування.

В п’ятому розділі описано нові моделі 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 на один рівень надання послуг показників конфіденційності, цілісності та спостереженості.

Ключові слова: управління мобільними мережами, розподілені граничні обчислення, класифікація та кластеризація трафіка, набір ознак, нейронні мережі, завадостійке кодування, фонтанні коди, управління захищеністю даних, конфіденційність даних, захист від атак, взаємна автентифікація користувачів під час дзвінка, наскрізне шифрування під час дзвінка, мережна стеганографія.

ABSTRACT

Astrakhantsev A.A. Models and methods for improving the quality of data services transmission in mobile communication systems. – Proficiency scientific treatise on the rights of the manuscript.

A thesis submitted in fulfilment of the Doctor of Engineering Science degree in technical sciences on specialty 05.12.02 “Telecommunication Systems and Networks”. – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" of Ministry for Education and Science of Ukraine, Kyiv, 2024.

The dissertation is devoted to solving the urgent scientific problem of creating and scientific substantiation of a comprehensive methodology for managing the service process in the information and telecommunications network of mobile communications in order to increase the level of security and quality of the user service process.

The paper demonstrates the prerequisites for the emergence of a contradiction, since there is still no single concept, models and methods for managing the service process in the information and telecommunications network of mobile communications in order to increase the level of security and quality of the user service process. It is shown that the emergence of new sources of traffic and the introduction of new services leads to increased requirements for the speed and quality of service provision, which in turn requires improvement of the software part of the network core and user equipment. It is also determined that in a 5G network, the requirements for the security of information and telecommunication systems are increasing due to the emergence of new threats and the implementation of new services.

Today, this contradiction can be resolved by developing new principles, mathematical models and methods for managing the service process in the information and telecommunications network of mobile communications.

The thesis solves an important scientific and technical problem of creating and scientific substantiation of a comprehensive methodology for managing the service

process in a mobile information and telecommunications network in order to improve the level of security and quality of the user service process.

The introduction substantiates the relevance of the topic of the dissertation. The purpose of the work, main tasks and research methods are defined. The scientific novelty and practical significance of the results are formulated.

The first section of the paper contains a review of the literature on the topic of the dissertation, an analysis of the current state and trends of development, features of the functioning of the 5G-based information and telecommunications system, its key services and technologies. The main indicators of quality and security of data transmission in information and telecommunication systems are determined. For information and telecommunication systems based on the 5G network, the main vulnerabilities and threats that may affect the degree of completeness of information security services are identified. Vulnerabilities and attacks on existing methods of remote user authentication are considered separately, and their weaknesses that need to be improved are identified.

The second section proposes a comprehensive methodology for ensuring the quality of data transmission and security in the mobile communication system, based on the improved structure of the 5G mobile communication network. The proposed structure ensures improvement of the quality indicators (error and packet loss rate, information transmission rate, information transmission and processing delay) and security indicators (confidentiality, integrity, availability and observability). To increase the values of data transmission quality indicators, we propose a step-by-step implementation of the following steps in a network node: improvement of data pre-processing methods in network nodes to improve the accuracy of traffic classification and processing and reduce data processing delays; introduction of the latest adaptive traffic classification methods to improve the efficiency of network resources use when applying network slices; introduction of

new methods of traffic distribution on network edge elements to improve the quality of application of edge computing technology with multiple access; improvement of methods of noise-resistant packet coding during packet processing. At the same time, improvement of methods of noise-resistant packet coding is proposed for implementation in the modem part of the user's equipment. To improve security indicators, the following steps are proposed: improving the method of forming a user's biometric template, including a new method of combining various biometric features of the user; application of network steganography and noise-resistant coding methods to increase the secrecy and noise resistance of information during the remote authentication procedure; introduction of a new method of mutual authentication of users during a call, which covers a number of threats related to fraud. The section also proposes an ontological model of the mobile communication system, taking into account quality and security indicators.

In the third section, in order to reduce the total traffic transmission delay, the methods of packet processing in a network node were improved by rationally selecting parameters and methods of traffic classification, optimizing the number of features used in classification, and new methods of traffic clustering. A new method of data processing in a network node has been developed, which improves the quality of the application of edge computing technology with multiple access. The proposed methods, combined with the use of network slices, reduce traffic transmission latency and improve the efficiency of the 5G network as a whole, which is reflected in the copyright certificate.

The fourth section describes improvements to the methods of noise-resistant coding of packets during their transmission over a mobile network to reduce the level of errors and packet loss. Improvement a noise-resistant code includes a new model of forming the Raptor code, improving the LDPC code as a pre-coder of the

Raptor code, and a method of decoding the Raptor code. The Raptor code model is improved by introducing an interleaving procedure and changes to the code formation matrix, which allowed to reduce the level of uncorrectable errors and increase the decoding speed.

The fifth section describes new models and methods for protecting private data in a user's device, which are distinguished by the availability of new methods for generating a biometric template, combining different types of biometric data, the proposed noise-resistant method for hiding biometric data during transmission, as well as providing two-way authentication and end-to-end encryption during a call, which avoids user substitution on the other side and allows only an authorized user to access services, which increases the level of service provision by one level.

Keywords: mobile network management, distributed edge computing, traffic classification and clustering, feature set, neural networks, noise-resistant coding, fountain codes, data security management, data privacy, attack protection, mutual user authentication during a call, end-to-end encryption during a call, network steganography.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у фахових виданнях України, які включені до міжнародних наукометричних баз (Scopus)

1. Astrakhantsev A., Liashenko, G. “Data protection management process during remote biometric authentication”, System Research and Information Technologies, №3 2022, pp. 71–85.

2. Astrakhantsev A., Pedan S. “Improving user security during a call”, Radioelectronic and Computer Systems, 2024, no. 2(110), pp.173-185.

3. 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.

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.

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.

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

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.

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

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.

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.

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.

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.

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.

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

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.

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.

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

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.

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

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

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

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.

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.

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.

25. Astrakhantsev 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.

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

27. Astrakhantsev 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.

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

Статті у виданнях інших держав та додаткова література:

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.

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

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.

32. 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.

33. 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.

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

Патенти та авторські свідоцтва:

35. 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)

36. 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).

37. 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).

38. 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).

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

40. Progonov D., Popov O., Astrakhantsev A., Motchanyi A. “Device and method for acquiring biosignal”, WO2024096391A1.

41. 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., Євдокименко М.О., Даніель Я.Д.

Матеріали та тези наукових конференцій, які індексуються у Scopus:

42. 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. **(Scopus)**

43. 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)**

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

45. 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)**

46. 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)**

47. Astrakhantsev A., Globa L, Novogrudska 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)**

48. 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)**

49. 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)**

50. 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)**

51. 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)**

<u>Матеріали та тези міжнародних наукових конференцій:</u>

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.

58. Астраханцев А.А., Бєлікова 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.

59. Астраханцев А.А., Красянський 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.

60. 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.

61. Астраханцев А.А., Кузнєцова 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

62. 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.

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

71. 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.

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

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

74. 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 XXI столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 44-45.

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

76. 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 КПІ. – 2023. – pp. 232-235.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

3GPP – 3rd Generation Partnership Project

5QI – ідентифікатор якості обслуговування в 5G

АБГШ (AWGN) – адитивний білий гаусівський шум

ІСРР – інтелектуальної системи розподілу ресурсів

ІТС – інформаційно-телекомунікаційна система

КЗЗ – комплекс засобів захисту

ЛПС – логарифмо-подібні співвідношення

ЯТП – якість телекомунікаційної послуги

AKA (Authentication and Key Agreement) – процедура автентифікації та узгодження ключів

AMF (Access and Mobility Management Function) – функція управління доступом і мобільністю

ANN (Artificial Neural Networks) – алгоритм штучних нейронних мереж

AR (Augmented Reality) – доповнена реальність

BER (Bit Error Rate) – бітова ймовірність помилки

BEC (Binary Erasure Channel) – бінарний канал із стираннями

BPSK (Binary Phase-Shift Keying) – двійкова фазова маніпуляція

CBAM (Constitution block attention module) – блок уваги

CN (5GC, Core Network) – ядро мережі

DDoS-атаки (Distributed Denial of Service) – розподілена відмова у обслуговуванні

DF (Digital Fountain) – цифровий фонтанний код

DNS (Domain Name System) – сервер системи доменних імен

DPI (Deep Packet Inspection) – глибока перевірка пакетів

eMBMS (evolved Multimedia Broadcast Multicast Service) – розширені мультимедійні широкосмугові сервіси

FAR/FRR (False Acceptance Rate/False Rejection Rate) – помилки першого/другого роду

GFBR (Guaranteed Flow Bit Rate) – гарантована швидкість потоку

gNB (gNodeB) – базова станція

HICCUPS (Hidden Communication System for Corrupted Networks) – метод вбудовування, що використовує пошкоджені пакети

IMSI (International Mobile Subscriber Identity) – міжнародний ідентифікатор абонента

KNN (*k*-nearest neighbor) – алгоритм *k*-найближчих сусідів

LACK (Lost audio packets steganography) – метод вбудовування на основі втрачених аудіо пакетів

LDPC (Low-density parity-check codes) – коди з малою перевіркою на парність

LT (Luby Transform) – метод кодування Лабі

LTE (Long-Term Evolution) – “довготерміновий розвиток»”, робоча назва 4G

MCS (Modulation and Coding Scheme) – схема модуляції і кодування

MEC (Mobile Edge Computing) – граничні обчислення з множинним доступом (мобільні периферійні обчислення)

MIMO (Multiple Input Multiple Output) – системи зв'язку з рознесеними передавальними і приймальними антенами

MitM (Man-in-the-Middle) – атака людина-посередині

mIoT (massive Internet Of Things) – масивний Інтернет речей

mMTC (massive Machine-Type Communication – масова комунікація машинного типу

MOTA (Multiple object tracking accuracy)– метрика якості алгоритмів трекінгу

MSE (Mean Squared Error) – середньоквадратичне відхилення

NFV (Network Functions Virtualization) – віртуалізація мережних функцій

QAM (Quadrature Amplitude Modulation) – квадратурна амплітудна модуляція

QoS (Quality of Service) – якість обслуговування

QPSK (Quadrature Phase-Shift Keying) – квадратурна фазова модуляція

RAN (Radio Access Network) – мережа радіодоступа

RF (Random Forest) – алгоритм «випадкового лісу»

RRC (Radio Resource control) – рівень управління радіоресурсом

RS (Reed-Solomon error correction) – код Ріда-Соломона

RSTEG (Retransmission steganography) – метод вбудовування, що використовує повторну відправку пакетів

SAS (Short Authentication String) – короткий автентифікаційний рядок

SDN (Software Defined Networking) – програмно-керовані мережі

SNR (Signal-Noise-Ratio) – співвідношення сигнал-шум

SVM (Support Vector Machines) – метод опорних векторів

TMSI (Temporary Mobile Subscriber Identity) – тимчасовий ідентифікатор мобільної станції (абонента)

UE (User Equipment) – обладнання користувача

UMTS (Universal Mobile Telecommunications System) – мобільна мережа 3G

UPF (User Plane Function) – функція площини користувача

URLLC (Ultra-Reliable and Low-Latency Communication – наднадійний зв'язок з низькою затримкою

VR (Virtual reality) – віртуальна реальність

ВСТУП

Актуальність теми. Впровадження 5G відкриває перед користувачами нові можливості за рахунок появи нових джерел трафіка (таких як Massive IoT, V2V/V2I, eMBMS), істотного підвищення швидкості та зниження затримки. В той же час сама мережа перейшла на новий рівень якості обслуговування за рахунок впровадження таких технологій як розподілені граничні обчислення (MEC), віртуалізація мережних функцій (NFV), мережні зрізи (Network Slicing) та масивний Інтернет речей (mIoT). При цьому поява нових джерел трафіка ускладнює існуючи методи класифікації та обробки трафіка; підвищення швидкості вимагає меншого рівня помилок і, відповідно, більш якісного завадостійкого кодування. Такі технології як NFV та Network Slicing дозволяють ефективніше використовувати ресурси мережі, але трафік який потрапляє до цих сервісів має бути підготовленим. Для вже відомої протягом значного часу технології MEC мережа 5G привносить також нові можливості, пов’язані з розподіленим інтелектом мережі між вузлами, швидкою обробкою трафіка на границі мережі та прямим з’єднанням пристроїв користувача девайс-девайс (D2D), при цьому виникають нові виклики стосовно захищеності та якості передачі даних в системах мобільного зв’язку:

- 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 кластерізації 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-комунікаційній мережі мобільного зв’язку з метою підвищення рівня

захищеності та якості передачі й обробки даних є актуальною науково-технічною проблемою.

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).

Мета і задачі дослідження. Дисертаційна робота присвячена вирішенню важливої науково-технічної проблеми, пов’язаної з розробкою 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.

Метою дослідження є підвищення 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.

Для досягнення мети дослідження було поставлено та вирішено такі основні задачі:

1) аналіз особливостей передачі трафіка в 5G мережі та наявних загроз, а також визначення основних показників якості та захищеності інформаційно-телекомунікаційної мережі;

2) розробка комплексної методології підвищення захищеності та якості передачі даних в мобільній мережі;

3) визначення набору ознак класифікації трафіку, моделей та методів для адаптивної класифікації трафіка, що підвищує ефективність використання мережних ресурсів під час застосування мережних зрізів (Network Slicing);

4) розробка нового методу обробки даних у вузлі мережі, який підвищує ефективність застосування технології граничних обчислень з множинним доступом (MEC, Mobile Edge Computing);

5) вдосконалення моделей та методів завадостійкого кодування пакетів під час передачі мобільною мережею для зменшення рівня помилок і втрат пакетів;

6) вдосконалення методу формування біометричного шаблону користувача, в тому числі нового методу об’єднання різних біометричних ознак користувача для підвищення рівня конфіденційності та спостереженості;

7) вдосконалення процедури віддаленої автентифікації шляхом застосування методів мережної стеганографії та завадостійкого кодування для підвищення прихованості та завадозахищеності інформації;

8) розробка нового методу взаємної автентифікації користувачів під час дзвінка, що перекриває ряд загроз пов’язаних із шахрайськими схемами підміни користувача;

9) вдосконалення існуючих протоколів обміну повідомленнями під час дзвінка шляхом застосування процедур наскрізного шифрування та перевірки цілісності для підвищення рівня захищеності під час передачі даних в 5G мережі;

10) розробка нових моделей управління приватними даними користувача для забезпечення захищеності даних під час реалізації нових сервісів;

11) оцінка роботи запропонованих рішень.

Об’єктом дослідження є процеси обробки і забезпечення захисту інформації в інформаційно-комунікаційних мережах мобільного зв’язку.

Предметом дослідження є моделі, методи та засоби підвищення захищеності та стійкості до атак, а також якості зберігання, обробки та передачі даних в інформаційно-комунікаційних мережах мобільного зв’язку**.**

Методи дослідження. Основні методи дослідження загальної проблеми – методи теорії масового обслуговування, багатокритеріальної оптимізації, методи 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 використовувалася 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 додатки для імітаційного моделювання створені за допомогою Python 3.0.

Наукова новизна отриманих результатів. Наукова новизна одержаних результатів полягає у 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 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 одержаних результатів. 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.

1. 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.

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

3. Отримані результати використано в навчальному процесі кафедри інформаційних технологій в телекомунікаціях: в лекційних заняттях та компьютерних 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.

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 на твір.

Особистий внесок здобувача. Усі наукові результаті, 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.

В роботі [47] автором запропоновано інтелектуальну систему розподілу ресурсів в 5G мережі, при цьому показники ефективності та завадостійкості автором визначено в роботі [5].

В роботах [23,25,48,50] автором 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. Робота [21] висвітлює вдосконалений метод кластеризації трафіка.

В роботах [8-9] автором запропоновано вдосконалені методи формування коду Raptor, формування коду LDPC, як одного з елементів коду Raptor, а також вдосконалення методу декодування коду Raptor.

Новий метод обробки даних у вузлі мережі, який підвищує якість застосування технології граничних обчислень з множинним доступом представлено в роботі [3].

Новий метод зберігання приватних даних користувача в захищеному ієрархічному вигляді, який надає нові можливості під час взаємодії користувача з пристроями mIoT запропоновано в статті [49] та патентах [35,39]. Новий метод формування біометричного шаблону та спосіб

об’єднання різних типів біометричних даних описано в роботах [14,17] і патенті [40].

В роботах [20,22] автором розроблено методи підвищення завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами. В [1,24,44-46,51] автором запропоновано стеганографічні методи прихованої передачі біометричних даних із забезпеченням підвищеної стійкості до атак та завад в каналах зв’язку.

Запропоновані автором завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв’язку наведено в [6,7,11-16,18,29-31,43]. Методику оцінювання важливості характеристик стеганографічних алгоритмів наведено в [10].

Запропоновані вдосконалення протоколів обміну повідомленнями під час дзвінка для підвищення рівня захищеності 5G мережі наведено в [2,42].

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 об’єктами, наведено в патентах [36,37].

Запропоновані методи у поєднанні з застосуванням мережних зрізів, які дозволять зменшити затримку передачі і покращити ефективність 5G мережі в цілому, знайшли відображення у авторському свідоцтві [41].

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи були представлені, повідомлені й одержали схвалення на 27 науково-технічних конференціях: 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

міжнародна науково-практична конференція 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 РТ-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 ІТ-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 КПІ, 2023), IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (м. Київ, НТУ КПІ, 2023), International Scientific and Technical seminar Critical Computer Technologies and Systems (CriCTecS 2024), 2024 IEEE International Black Sea Conference on Communications and Networking (Tbilisi, Georgia).

Публікації. Основні положення дисертації, які в достатній мірі висвітлюють результати роботи, що виносяться на захист, опубліковано у 76 наукових працях, у тому числі у 3 навчальних посібниках (зокрема 1 з грифом МОНУ), 31 публікаціях у наукових фахових виданнях (3 статті у

виданнях категорії «А», 3 статті у виданнях іноземних держав, 23 статей у науково-фахових виданнях України), 6 патентів на корисну модель, 1 авторське свідоцтво на твір, 35 тезах доповідей в збірниках матеріалів конференцій (в тому числі 10, які включені до міжнародних наукометричних баз).

Структура і обсяг дисертації. Дисертація складається із анотацій, вступу, 5 розділів основного змісту, висновків, списку використаних джерел, додатків. Загальний обсяг роботи становить 377 сторінок друкарського тексту, в тому числі список літератури із 294 найменувань, робота містить ілюстрації та таблиці.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ТА ЗАХИЩЕНОСТІ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Впровадження технології 5G забезпечує більш високу швидкість передачі даних, більшу кількість пристроїв Інтернету речей на квадратний кілометр та меншу затримку, що дозволяє забезпечити впровадження та високу якість та швидкість нових сервісів. Однак впровадження нових технологій та сервісів ускладнює існуючи методи класифікації та обробки трафіка і призводить до появи нових проблем пов’язаних із захистом інформації в мережі. В даному розділі будуть проаналізовані ключові особливості мережі 5G, нові сервіси які розгортання 5G дозволяє впровадити. Також описуються затверджені в нормативній документації показники якості та захищеності, а також аналізуються методи забезпечення якості та захищеності, які вимагають вдосконалення.

1.1 Архітектура та основні сервіси мережі 5G

1.1.1 Основні сервіси мережі 5G

Для розуміння найбільш важливих характеристик мережі, розглянемо основні сервіси, які отримали поширення при розгортанні мереж 5G [1-5]:

- eMBMS (evolved Multimedia Broadcast Multicast Service – розширені мультимедійні широкосмугові сервіси) – це розширення послуг, що вперше включається мережами 4G LTE, яке забезпечує високу швидкість передачі даних у широкій зоні покриття. eMBMS забезпечує більшу ємність, необхідну для підтримки пікових швидкостей передавання даних як для великих скупчень людей, так і для кінцевих користувачів, які перебувають у русі. Технологія має забезпечити ще вищий рівень обслуговування для

абонентів і ще вищі швидкості передачі даних. В якості цільових значень для швидкості передачі даних в 5G розглядаються десятки Гб на секунду (а саме до 20 Гбіт/с у низхідному каналі). Для того, щоб забезпечити такі високі швидкості передачі даних, використовуються дуже широкий канал (до 1-2 ГГц) і багатоантенні технології передачі даних і необхідно якісне завадостійке кодування.

- URLLC (Ultra-Reliable and Low-Latency Communication – наднадійний зв'язок з низькою затримкою) – цей тип сервісу відрізняється низькими затримками передавання даних (<1 мс в один бік) і високою надійністю та доступністю з'єднання. Прикладами сценаріїв або сфер застосування, де висуваються такого роду вимоги, слугують: віддалене керування різними механізмами і роботами; автоматизація виробничих ліній; різні сценарії в галузі безпілотного транспорту (Vehical to Everything, V2X) тощо. Для того, щоб підтримати висунуті цими сценаріями вимоги, у специфікаціях 5G передбачено набір спеціальних механізмів. Наприклад, підтримка так званих mini-slot, яка дає змогу передавати дані на радіоінтерфейсі між базовою станцією (gNB) та обладнанням користувача (UE) протягом дуже короткого інтервалу часу (частки мс). Крім цього, у технології 5G помітно вищі вимоги до часу обробки даних як на боці базової станції, так і на боці мобільного терміналу (тобто часу на обробку даних відводиться істотно менше порівняно з тим, що було відведено в технології LTE).

- mMTC (massive Machine-Type Communication – масова комунікація машинного типу) – ця сфера застосування характеризується можливістю під'єднання дуже великої кількості дешевих пристроїв. Прикладами таких пристроїв слугують різні датчики (наприклад, датчики пожежної сигналізації, задимлення, температури), лічильники (води, газу, тепла тощо), сенсори тощо. Крім низької вартості, особливістю таких пристроїв є низьке

енергоспоживання. Це необхідно для того, щоб забезпечити тривалий час роботи від автономних джерел живлення. Обсяги даних, що передаються цими пристроями, також незначні. Тому високі швидкості передачі даних в mMTC області не є критичним аспектом.

Як видно з наведеного вище, важливим є забезпечення високої швидкості передачі інформації, низької затримки (в тому числі під час обробки) та високої надійності. Крім того, для кожної з наведених вище послуг необхідно забезпечити заданий рівень захищеності від негативних зовнішніх впливів на мережу (атак). Розглянемо загальну архітектуру мережі 5G і основні технології, щоб визначити ті елементи які мають забезпечити вказані характеристики.

1.1.2 Загальна архітектура мережі 5G

Побудова моделей та методів, що будуть забезпечувати якісну і захищену передачу даних неможлива без попереднього аналізу архітектури мережі. Відповідно до стандартів [1-6], структуру мережі варто розглядати у вигляді декомпозиції 3 елементів (рис. 1.1, [6])

Схематично система 5G використовує ті ж елементи, що і попередні покоління [1]: обладнання користувача, яке складається з мобільної станції і сім-карти (USIM), мережу радіодоступу (5G-RAN) і ядро мережі (5GC). Відповідно до рис. 1.1:

- Обладнання користувача, наприклад смартфони, підключаються через нову мережу радіодоступу 5G до ядра 5G і далі до мереж передачі даних, таких як Інтернет.
- 5G RAN – канал зв’язку, радіомережа, яка поєднує користувацьке обладнання з базовими станціями;
- Edge (межа) – представляє формальний перетин користувацького й

обчислювального рівнів.

- Core Network – ядро мережі, яке відповідає за всі функції та взаємодії в 5G, включаючи автентифікацію, безпеку, управління сеансами та агрегацію трафіку з кінцевих пристроїв.

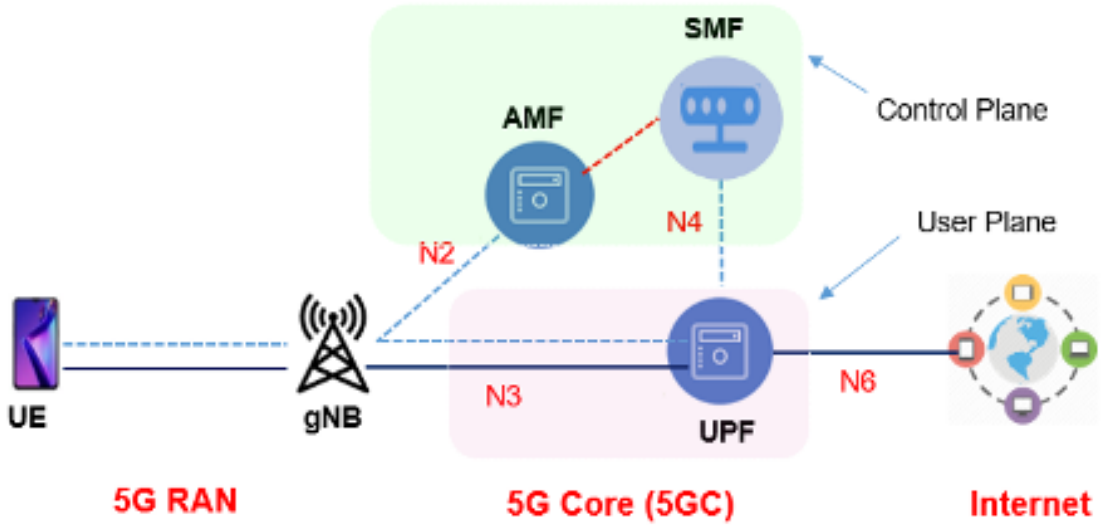


Рис. 1.1. Узагальнена архітектура мережі 5G [6]

Ядро мережі може бути схематично представлений об'єктом AMF/UPF (рис. 1.2): функція площини користувача (UPF), що обробляє дані користувача, і функція управління доступом і мобільністю (AMF), яка отримує доступ до обладнання користувача (UE) і 5G RAN.

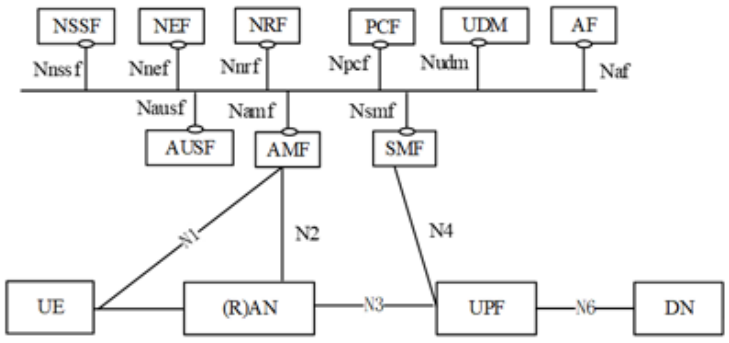


Рис. 1.2. Архітектура мережних функцій 5G [1]

До основних мережних функцій (рис. 1.2) відносяться [4]:

– *NRF (Network Repository Function – функція мережного сховища)*: усі функції мережі 5G у мережі оператора зберігаються централізовано за допомогою функції мережевого сховища. NRF надає заснований на стандартах API, який дозволяє різним функціям 5G реєструватися та знаходити одна одну.

– *PCF (Policy Control Function – функція контролю політики):* дозволяє розробляти та впроваджувати політики в мережі 5G.

– *BSF (Binding Support Function – функція підтримки зв'язування):* BSF використовується для прив'язки запиту прикладної функції до конкретного екземпляра функції управління політикою (PCF). Це можна порівняти з функцією зв'язування Policy and Charging Rules Function (PCRF), що надається агентом маршрутизації 4G Diameter Routing Agent (DRA) для VoLTE і VoWiFi.

– *SCP (Service Communication Proxy – проксі для зв'язку зі службами):* нова мережева функція на основі HTTP/2, що забезпечує динамічне масштабування і управління зв'язком і послугами в мережі 5G. Роль SCP певним чином можна порівняти з його попередниками, такими як Signaling Transfer Point (STP), центральним сигнальним маршрутизатором, що використовується в 2G і 3G для маршрутизації сигнальних повідомлень SS7, а також з Diameter Signaling Controller (DSC), що виконує те ж саме для повідомлень Diameter в 4G. Ключова відмінність від цих застарілих маршрутизаторів полягає в тому, що SCP може відповідати за вирішення запитів на виявлення мережевих функцій (NF) через зв'язок з функцією мережевого сховища (NRF) і може ініціювати пошук IP-адрес сервера доменних імен (DNS A-запис) в DNS, щоб знайти кожен живий екземпляр для кожної доступної мережевої функції [7].

– *NSSF (Network Slice Selection Function – функція вибору нарізки мережі):* система є рішенням для вибору оптимального зрізу мережі, доступного для надання запитуваного користувачем сервісу в 5G.

– *UDM (Unified Data Management – уніфіковане керування даними)* і *UDR (Unified Data Repository – сховище даних користувача):* UDM створений для 5G і схожий на домашній абонентській сервер (HSS) у LTE. Він відповідає за створення облікових даних, автентифікацію, надання доступу залежно від підписки користувача та надання цих облікових даних іншим функціям мережі. Він отримує облікові дані зі сховища даних користувача (UDR).

– *AUSF (Authentication Server Function – функція сервера автентифікації):* забезпечує автентифікацію у мережі 5G і метод узгодження ключа. Під час процесу реєстрації функція доступу та мобільності AMF відповідає за вибір відповідної функції сервера автентифікації (AUSF).

1.1.3 Основні технології мережі 5G

Високі швидкості передачі, надійність та мала затримка забезпечуються застосуванням таких технологій, як віртуалізація мережних функцій, граничні обчислення з множинним доступом, формування променів та масивне MIMO (multiple-in-multiple-out), нарізка мережі. Наведемо їх короткий опис, оскільки частина з них має бути вдосконалена у наступних розділах.

1. *Massive MIMO.* У сучасних системах зв'язку, наприклад, у стільникових системах зв'язку, високошвидкісних локальних обчислювальних мережах тощо, є необхідність підвищення пропускної здатності [8]. Пропускна здатність може бути збільшена шляхом розширення смуги частот. Проте застосовність цих методів обмежена через вимоги біологічного захисту, обмежену потужність джерела живлення (у мобільних

пристроях) та електромагнітну сумісність. Тому якщо в системах зв'язку ці підходи не забезпечують необхідну швидкість передавання даних, то ефективним може виявитися застосування адаптивних антенних решіток зі слабо корельованими антенними елементами. Системи зв'язку з такими антенами отримали назву систем MIMO.

Розглянемо MIMO-систему з N передавальними і M приймальними антенами (антенними елементами). Властивості MIMO-каналу, що з'єднує n-й передавальний елемент з m-м приймальним елементом, описуються комплексними канальними коефіцієнтами h_{nm}, що утворюють канальну матрицю H розміру $N \times M$. Їхні значення випадково змінюються з часом через наявність багатопроменевого поширення сигналу. Якщо

$\vec{s}$ – вектор переданих сигналів;

$\vec{z}$ – вектор власних шумів приймальних елементів антени;

$\vec{x}$ – вектор прийнятого повідомлення,

то сигнал на приймальній стороні записується таким чином:

$$\vec{x} = H * \vec{s} + \vec{z}\,. \tag{1.1}$$

Матриця H вважається нормованою.

Технологія MIMO використовується в базових станціях стільникового зв'язку стандарту 4G [8]. Стандартом передбачено до 8 портів введення та 8 виведення на одну станцію. Massive MIMO (рис. 1.3) – це система, в якій кількість терміналів користувачів набагато менше, чим кількість антен базової станції. Особливістю Massive MIMO є використання багатоелементних цифрових антенних решіток з кількістю антенних елементів 128, 256 і більше. Спрощення обробки сигналів може досягатися адаптивною зміною кількості каналів у системі Massive MIMO в залежності

від поточної завадової ситуації в ефірі, що забезпечується на основі кластеризації окремих груп антенних елементів цифрової антенної решітки у підрешітки. Модель каналу MIMO наведено на рис. 1.4.

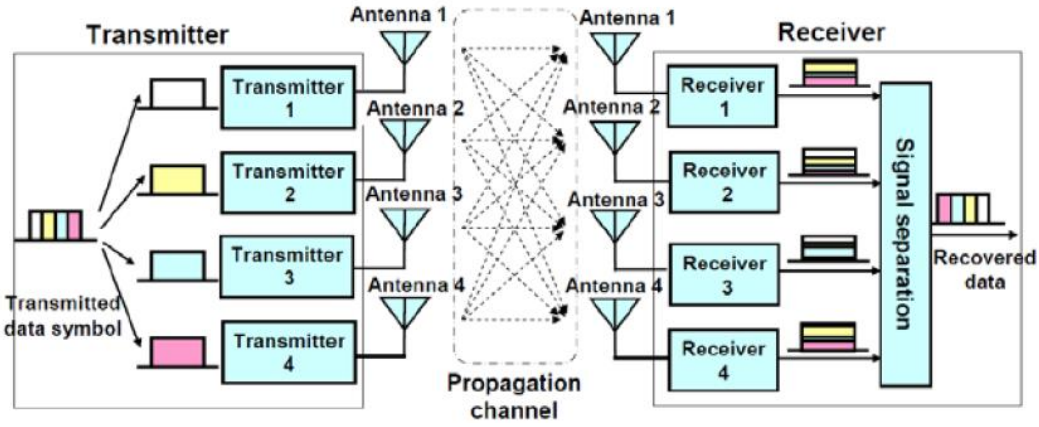


Рис. 1.3. Масивне MIMO

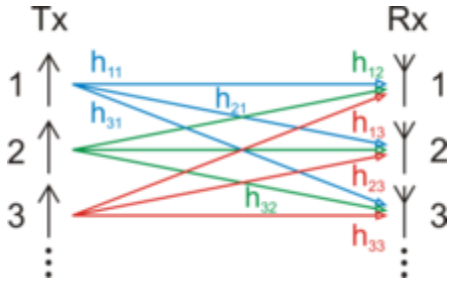


Рис. 1.4. Модель каналу MIMO [8]

2. *Формування променю*. Звичайні базові станції мають направлені секторні антени і передають сигнали незалежно від розташування користувачів. Завдяки використанню антенних масивів із декількома входами та декількома виходами (mMIMO), які містять велику кількість малих антен (до 64), об'єднаних в одну конструкцію, алгоритми обробки сигналу використовуються для визначення найбільш ефективного шляху передачі для кожного користувача (рис. 1.5).

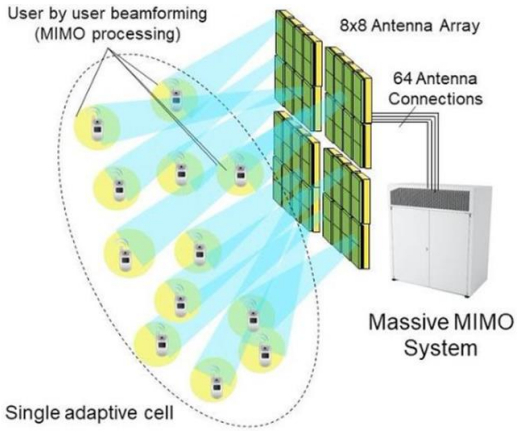


Рис. 1.5. Формування променю для покращення якості обслуговування

3. *Віртуалізація мережних функцій* (NFV) відокремлює програмне забезпечення від апаратного, замінюючи різні мережеві функції. Як показано на рис. 1.2, всі мережні функції взаємодіють через загальний інтерфейс і тому можуть бути розташовані де завгодно. Це забезпечує набагато більшу гнучкість у розгортанні мережі. Обслуговування також значно спрощується, оскільки можна легко створити тимчасову мережну функцію (рис. 1.6).

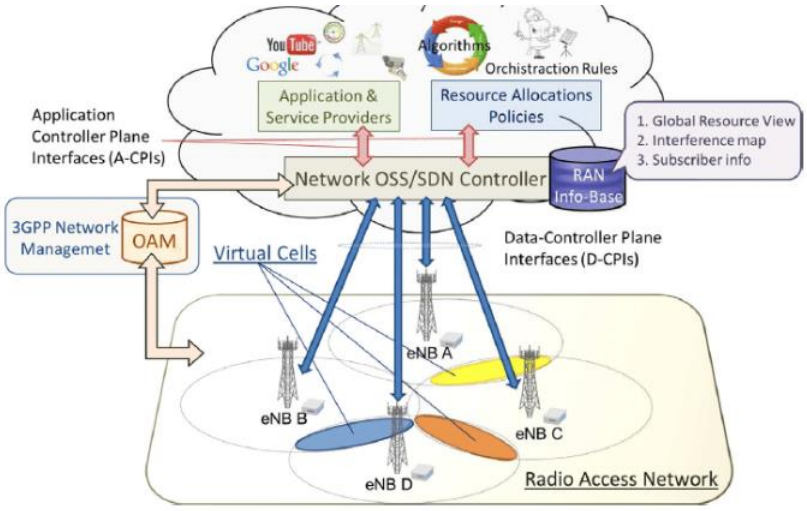


Рис. 1.6. Віртуалізація мережних функцій

4. *Граничні обчислення з множинним доступом* (MEC). Деякі обчислювальні потужності вводяться якомога "фізично ближче" до кінцевого

користувача [88]. Річ у тому, що деякі додатки, такі як віртуальна реальність, фабрики майбутнього або автономне водіння, дуже вимогливі до часу відгуку передачі даних/мережі. Щоб скоротити цей час, деякі "локальні реплікації" головного сервера впроваджуються ближче до кінцевого користувача. Функція *MEC* дозволяє частину розрахунків винести безпосередньо на границю (Edge) мережі і забезпечити низьку затримку, високу пропускну здатність і обробку інформації у режимі реального часу. Також це дозволяє суттєво розвантажити мережу, оскільки до ядра буде передаватися не вся інформація, а лише результат обробки.

Розподіл обчислювальної потужності є важливою до кінця не вирішеною задачею, оскільки необхідно забезпечити підключення і обробку даних від великого обсягу пристроїв, більшість яких є рухомими.

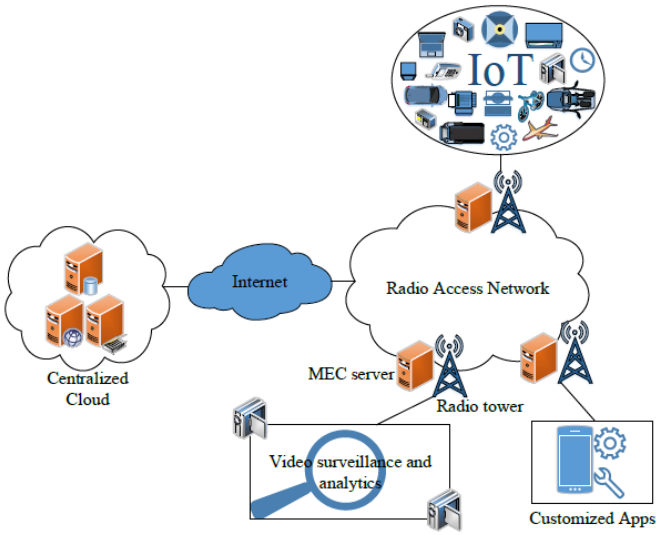


Рис. 1.7. Граничні обчислення з множинним доступом

5. Масивний Інтернет речей (mIoT). MIoT обслуговує мільярди недорогих, далекобійних, ультра-енергоефективних підключених пристроїв у віддалених місцях, а також хмарні додатки, які не потребують частого зв'язку

або зв'язку в реальному часі. Забезпечує збір даних від сенсорів та керування ними. Згідно [1], архітектура mIoT в 5G поділяється на три рівні (рис. 1.8):

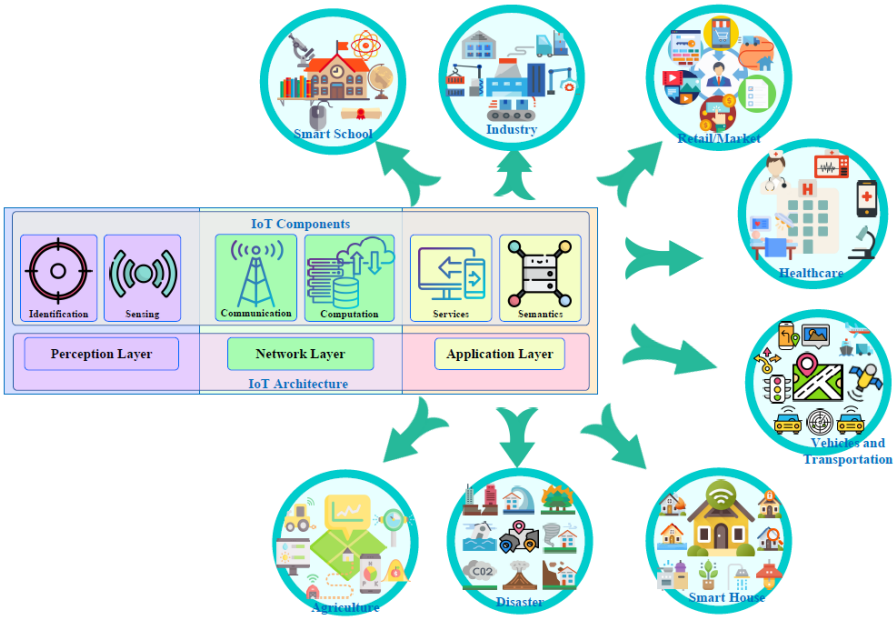


Рис. 1.8. Архітектура системи масивного Інтернету речей для 5G

На першому рівні сприйняття, об'єкти (пристрої) представляють собою фізичні сенсори для збору корисної інформації/даних від навколишнього середовища (місцезнаходження, температура, вага, рух, вібрація, прискорення, вологість), які потім перетворюються в цифрову форму.

Відповідальність мережевого рівня полягає в тому, щоб забезпечити і захистити передачу даних між рівнем сприйняття і прикладним рівнем.

Прикладний рівень надає персоналізовані послуги відповідно до потреб користувача і далі поділяється на три підрівні:

- рівень управління послугами – полегшує обробку інформації, прийняття рішень і контроль запитів на сполучення або обробку інформації для відповідних завдань;

- рівень запитів – надання клієнтам інтелектуальних високоякісних послуг відповідно до попередніх запитів клієнтів;
- бізнес-рівень – представляє бізнес-модель і дані, отримані з прикладного рівня.

6. Нарізка мережі (Network Slicing). Ключовим компонентом для реалізації повного потенціалу архітектури 5G є нарізка мережі (рис. 1.9).

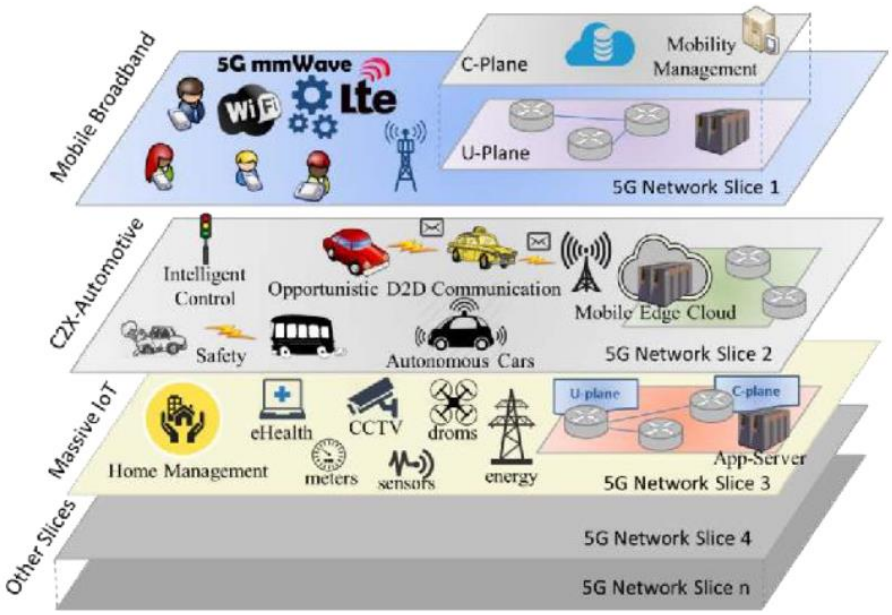


Рис. 1.9. Нарізка мережі

Ця технологія підкреслює можливості NFV, дозволяючи кільком логічним мережам працювати одночасно на основі спільної фізичної мережевої інфраструктури. Ця можливість реалізується в архітектурі 5G шляхом створення наскрізних віртуальних мереж. Нарізка мережі дозволяє операторам ефективно керувати різними сервісами застосування з різними вимогами до пропускної здатності, затримки та доступності, розподіляючи мережеві ресурси між кількома користувачами. Також вона необхідна для підтримки граничних обчислень та обслуговування Інтернету речей, де

кількість користувачів може бути надзвичайно великою, а рівні необхідних сервісів – різними.

1.2 Канали передачі і їх характеристики

Як було показано вище, канал передачі є елементом архітектури мережі 5G. В якості каналу передачі в мобільних мережах використовуються бездротові лінії передачі інформації (радіолінії), які можна класифікувати по довжині хвилі. Метрові, дециметрові і сантиметрові хвилі об'єднують в групу ультракоротких хвиль (УКХ) тому, що нерідко виникають випадки, коли кордони використовуваного діапазону не збігаються з межами стандартних діапазонів. Слід зазначити, що саме до УКХ діапазону відноситься більшість цивільних цифрових систем передачі даних, наприклад телебачення, радіолокації, бездротові комп'ютерні і сенсорні мережі (WiFi, WiMAX і DASH-7 відповідно), Bluetooth, мобільний зв'язок (UMTS, LTE, 5G), супутниковий зв'язок, GPS. Також радіолінії використовуються для забезпечення зв'язку з підводними човнами, в геофізичних дослідженнях і радіомовленні. Методи покращення характеристик передачі інформації, які досліджуються у даній дисертації, направлені на використання в вище зазначеному середовищі передачі повідомлень.

1.2.1 Різновиди завад у каналах передачі інформації

Інформація, яка була передана по каналах передачі даних, про які говорилося раніше, пошкоджуються і відтворюється з деякими помилками. Можливою причиною таких помилок є завади, що впливають на сигнал.

Пошкодження часто обумовлені відомими характеристиками радіоліній і можуть бути усунені шляхом належної корекції.

Завади ж заздалегідь невідомі і тому не можуть бути повністю усунені. Вони дуже різноманітні як за своїм походженням, так і за фізичними властивостями. Залежно від місця виникнення, завади поділяють [9]:

на атмосферні завади;

- промислові (індустріальні);
- космічні;
- електризаційні;
- перешкоди сторонніх каналів;
- внутрішні шуми.

Атмосферні завади обумовлені електричними процесами в атмосфері. Енергія цих завад зосереджена, головним чином, в області довгих і середніх хвиль.

Промислові завади виникають через різкі зміни струму в електричних ланцюгах. До них відносяться завади від електротранспорту, електричних моторів, медичних установок, систем запалювання двигунів і т.д.

Космічні завади створюються радіовипромінюванням позаземних джерел. Вони створюють загальний шумовий фон і найбільшою мірою проявляються на ультракоротких хвилях.

Електрізаційні завади, часто виникають під час заметілі або піщаної бурі, створюються наелектризованими сніговими частками або піщинками.

Завади сторонніх каналів передачі інформації обумовлені роботою сторонніх радіостанцій. З урахуванням джерела походження їх називають також стаціонарними. Цей вид завад найбільш характерний для КВ діапазонів.

За способом впливу на сигнал розрізняють: адитивну (шум) і мультиплікативну (завмирання) завади. Тому в процесі передачі на приймаючій стороні сигнал можна представити у вигляді

$$U(\mathrm{t}) = \mathrm{S}(\mathrm{t}) + \mathrm{n}(\mathrm{t}), \tag{1.2}$$

де *S(t)* – переданий сигнал в одиницю часу *t*; *n(t)* – адитивна завада. У разі ж завмирань сигнал виглядає як

$$U(\mathrm{t}) = \mathrm{S}(\mathrm{t}) \times \mu(\mathrm{t}), \tag{1.3}$$

У реальних бездротових системах передачі інформації часто діють обидві завади, прийнятий сигнал в таких системах виражається як

$$U(\mathrm{t}) = \mathrm{S}(\mathrm{t}) \times \mu(\mathrm{t}) + \mathrm{n}(\mathrm{t}), \tag{1.4}$$

Іншим типом поділу завад на групи є класифікація за характером змін в часі:

- імпульсні завади (зосереджені в часі);
- вузькосмугові (зосереджені по спектру завади);
- флуктуаційні.

Імпульсні завади являють собою випадкову послідовність коротких сигналів, зазвичай виникаючих настільки рідко, що реакція приймача на поточний імпульс встигає зменшитися до нуля до моменту появи чергового імпульсу. Типовими прикладами таких завад є сигнали, які створюються розрядами блискавок.

Зосереджені по спектру завади займають порівняно вузьку смугу частот, відносно імпульсної смуги частот сигналу. Найчастіше вони обумовлені сигналами сторонніх радіостанцій або випромінюванням промислових або медичних генераторів високої частоти різного призначення.

Флуктуаційна завада являє собою безперервне коливання, яка змінюється випадковим чином. У тому випадку, якщо флуктуаційні завади швидко змінюються в часі або, коли в межах смуги пропускання системи спектральну щільність завади можна наближено вважати постійною, то такі завади називають білим шумом. Часто такий шум описується нормальним законом розподілу (розподілом Гауса).

Широко розповсюдженим для використання в розрахунках і моделювання реальних систем передачі даних, у тому числі в даній дисертації, є адитивний білий гаусівський шум (АБГШ). За своєю природою це білий шум з нормальним розподілом значення амплітуди при адитивному способі впливу.

Оскільки існує безліч різних каналів передачі даних, значить передану інформацію необхідно представити у вигляді, відповідно даному каналу. Таке перетворення зазвичай пов'язане з модуляцією сигналів, а зворотне перетворення з демодуляцією, різновидності яких будуть розглянуті далі.

1.2.2 Застосовані види модуляції

Модулятор в системі передачі інформації відображає послідовність інформаційних символів у відповідну послідовність сигналів. Ці сигнали можуть відрізнятися за амплітудою, по фазі або по частоті або можуть залежати від двох або більше сигнальних параметрів. Застосування різних видів модуляції необхідно для визначення необхідних властивостей каналів, скорочення надмірності сигналів і модульованого, внаслідок цього, раціонального використання потужності передавальних пристроїв, а також вирішення проблем електромагнітної сумісності різних систем передачі інформації.

Існує аналогова і цифрова модуляція. Оскільки в роботі розглядаються цифрові сигнали, тому розглянемо докладно цифрову модуляцію [78], класифікація якої представлена на рис. 1.10.

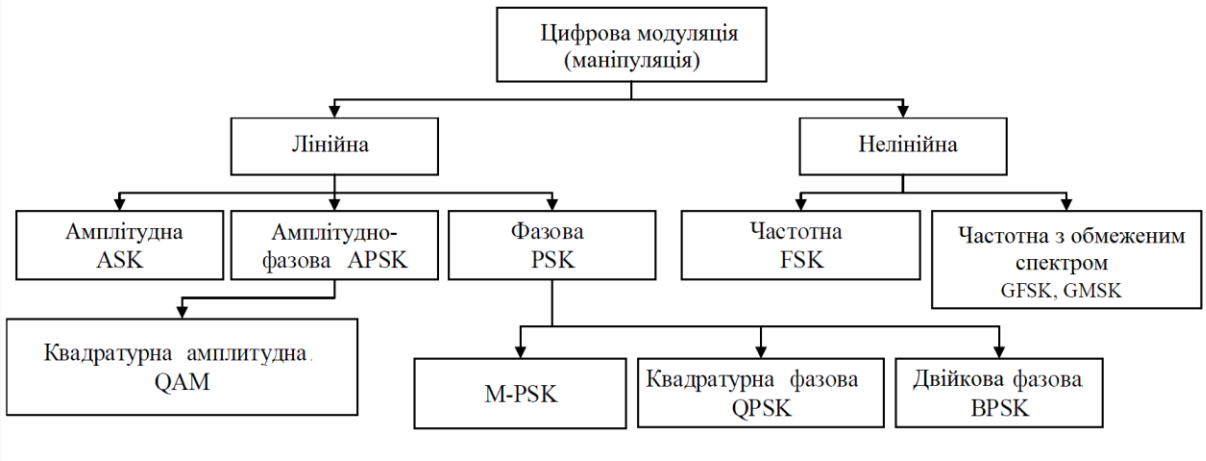


Рис. 1.10. Класифікація типів цифрової модуляції

У сучасних модемах найчастіше використовуються наступні види модуляції:

- частотна (FSK);
- фазова (PSK);
- амплітудна (ASK):
- амплітудно-фазова (APSK).

Кожна зі схем модуляції має позитивні і негативні особливості.

Наприклад, при застосуванні ASK модуляції ефективно використовуються смуги частот, але мають місце слабка завадостійкість і висока споживана потужність. У випадку з FSK модуляцією спостерігається висока енергетична ефективність, але нераціональне використання смуги частот. На відміну від попередніх, фазова модуляція (PSK) ефективна в обох випадках, найпростіша схема її має назву двійковій фазової маніпуляції

(BPSK). У ній використовується єдиний зсув фази між «0» і «1» – 180 градусів, половина періоду. Існують також н інші види фазової модуляції:

- QPSK використовує 4 різних зсуву фази (по чверті періоду) і може кодувати 2 біта в символі (01, 11, 00, 10);

- 8-PSK використовує 8 різних зсувів фаз і може кодувати 3 біта в символі.

Однією з частих реалізацій амплітудно-фазової модуляції є Quadrature Amplitude Modulation (квадратурна амплітудна модуляція), яка поєднує два амплітудно-модульованих сигналу в одному каналі. Це дозволяє збільшити вдвічі ефективну пропускну здатність. У QAM використовуються дві несучі з однаковою частотою, але з різницею у фазі на чверть періоду.

Найбільш поширені алгоритми модуляції, що застосовуються в 4G/5G та наведені в табл. 1.1.

Таблиця 1.1 – Параметри модуляції і кодування в мережа 4G

	Before Rel.12			*Rel.12 and beyond*		
CQI	Modulation	Code rate	Bits per RE	Modulation	Code rate	Bits per RE
0	Out of range					
1	QPSK	0.0762	0.1524	QPSK	0.0762	0.1524
2	QPSK	0.1172	0.2344	QPSK	0.1885	0.377
3	QPSK	0.1885	0.377	QPSK	0.4385	0.877
4	QPSK	0.3008	0.6016	16QAM	0.3691	1.4764
5	QPSK	0.4385	0.877	16QAM	0.4785	1.914
6	QPSK	0.5879	1.1758	16QAM	0.6016	2.4064
7	16QAM	0.3691	1.4764	64QAM	0.4551	2.7306
8	16QAM	0.4785	1.914	64QAM	0.5537	3.3222
9	16QAM	0.6016	2.4064	64QAM	0.6504	3.9024
10	64QAM	0.4551	2.7306	64QAM	0.7539	4.5234
11	64QAM	0.5537	3.3222	64QAM	0.8525	5.115
12	64QAM	0.6504	3.9024	256QAM	0.6943	5.5544
13	64QAM	0.7539	4.5234	256QAM	0.7783	6.2264
14	64QAM	0.8525	5.115	256QAM	0.8634	6.9072
15	64QAM	0.9258	5.5548	256QAM	0.9258	7.4064

Після модулятора сигнал передається по каналу, а потім надходить на вхід демодулятора, принцип роботи якого часто залежить від виду каналу передачі інформації. Тому далі розглянемо різновиди моделей каналів.

1.2.3 Різновиди моделей каналів передачі інформації

1.2.3.1 Канали зі стираннями

Канали зі стираннями важливі, оскільки багато телекомунікаційних каналів можуть бути змодельовані або спрощені, щоб апроксимувати канали зі стираннями. Еліас ввів поняття каналів зі стираннями в 1955 році [10]. Проста модель *M*-тих каналів зі стиранням без пам'яті показана на рис. 1.11 де p ймовірність стирання і s_i і r_i вхідний і вихідний канал, відповідно. Стирання це особливий екземпляр виходу, якщо символи втрачені або викинуті. У цьому випадку, кожен вхід $\mathbf{s_i}$ може бути стертим з імовірністю p. Еліас також довів, що швидкість коду $R < 1 - p$ може бути побудована для передачі даних по каналах з ймовірністю $1 - p$.

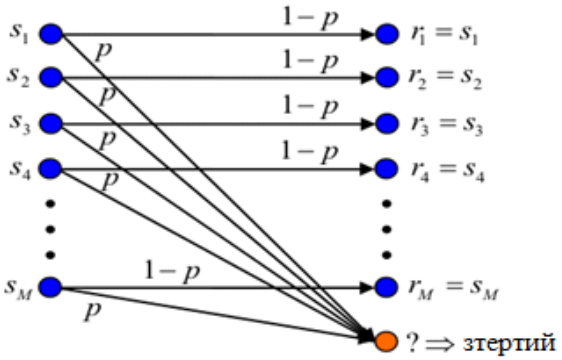


Рис. 1.11. Модель каналу зі стиранням

Вхідні і вихідні s_i та r_i це всі символи даних у каналі і s_i=r_i, тобто канал в деякому сенс без помилок. Якщо M= 2, канал називається двійковим каналом зі стиранням (binary erasure channel, BEC) [11,13]. Для служби доставки пакетів даних, кожен пакет може розглядатися як символ корисного навантаження. Символи, прийняті приймачем або декодера вважаються правильними, хоча, в реальності, є невелика вірогідність того, що виявляться помилки при у прийняті пакета. В цій роботі така можливість знехтувана.

Канал зі стираннями може бути бітовим каналом зі стираннями або пакетним каналом зі стираннями, так вибраний код стирання повинен бути на рівні біт або пакетному рівні, відповідно. Але багато умов у канали зі стиранням, розподіляють одні й ті ж, або подібні теорії і проблеми в Інтернет, вони можуть бути зведені до BEC.

1.2.3.2 Канали з адитивним білим гаусовським шумом

Джерела шуму в каналі зв'язку можуть бути техногенні та природні. [11-13]. Термін адитивний білий гаусовський шум (AWGN) часто використовують в наукових дослідженнях. В даній роботі досліджується канал з гаусовським шумом без пам'яті і спектральною щільністю потужності (power spectral density, PSD) шуму, однаковою для всіх частот. PSD білого шуму визначається формулою:

$$S_n(f0) = \frac{N_0}{2}, \tag{1.5}$$

де N_0 є однобічною спектральною щільністю потужності. Таким чином, автокореляційна функція білого гаусовського шуму буде:

$$R_{nn}(\tau) = \frac{N_0}{2}\delta(\tau), \tag{1.6}$$

де $\delta(\tau)$ – дельта-функція Дірака. Враховуючи переданий біт x в антипод формі, прийнятий біт може бути виражений по формулі:

$$y = x + n, \tag{1.7}$$

де n – змінна AWGN. В цій роботі передбачається, що адитивний гаусів шум, нульовий середній, так що функція щільності ймовірності (probability density function, PDF) прийнятого біта може бути сформульована як умовне PDF:

$$f_Y(y \mid x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\left[-\frac{1}{2}\left(\frac{(y-x)^2}{\sigma}\right)\right]}, \tag{1.8}$$

де $\sigma = N_0 / 2$ – дисперсія шуму. Рівняння (1.4) достатньо описує адитивний білий гаусів канал (AWGN). Нехай $x = \pm 1$ і $\sigma = 0{,}5$ і умовна щільність імовірності прийнятого біта показана на рис. 1.12. E_b – середня енергія отриманого біту. У приймачі, $y = 0$ – поріг розрізнення.

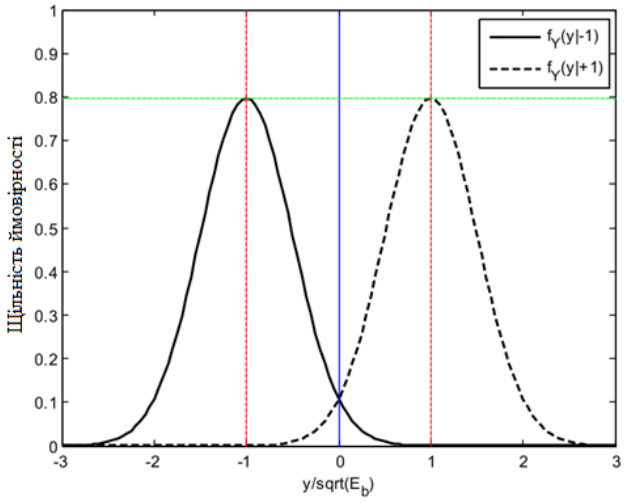


Рис. 1.12. Функція щільності ймовірності прийнятих біт в каналі з АБГШ

1.2.3.3 Канали з завмираннями Релея

Релеївське завмирання є одним з видів частотно-неселективного (плоского) багатопроміневого завмирання [11]. Плоскі завмирання одна з найбільш поширених моделей в наземних системах стільникового радіозв'язку. Це означає що багатопроменевий розкид затримки набагато менше, ніж тривалість переданого символу. В бездротовому середовищі, багатопроменеве завмирання викликано додаванням кількох прийнять корисного сигналу. Прийняті сигнали відрізняються по амплітуді / або фазі, тому додавання може бути корисне або шкідливе. Багатопроменеве завмирання, яке іноді називають маломасштабним зниканням, майже не залежить від відстані розповсюдження між антенами. Це може якимось чином залежати від несучої частоти. Таким чином, у цій роботі, багатопроменеве завмирання сприймає всі частотні компоненти сигналу однаково (отримує одну і ту ж величину) і вибір частоти в заданому діапазоні не впливає на характер загасання.

У стані Релея, фазові і квадратурні компоненти, отриманого смугового сигналу, добре моделюються як незалежні і однаково розподілені (independent and identically distribute) нульові гаусовські випадкові величини. Амплітуда прийнятої комплексної обвідної є випадковий процес Релея, який підпорядковується розподілу

$$f_A(a) = \frac{a}{b} e^{\left[-\frac{a^2}{2b}\right]}, \tag{1.9}$$

де a ≥ 0 і b – дисперсія синфазних і квадратурних компонентів.

1.3 Основні типи та характеристики завадостійких кодів

1.3.1 Основні типи завадостійких кодів

У теорії й техніці завадостійкого кодування відома множина коректувальних кодів, які можуть бути класифіковані за різними ознаками. Класифікація кодів наведена на рис. 1.12. За способом формування завадостійкі коди поділяються на блокові й неперервні. Формування блокових кодів передбачає розбивку переданих цифрових послідовностей на окремі блоки, які подаються на вхід кодеру. Кожному такому блоку на виході кодеру відповідає блок кодових символів, робота кодеру визначається алгоритмом кодування. Формування неперервних кодів здійснюється неперервно в часі, без поділу на блоки, що й визначає найменування цього класу кодів. Блокові коди історично були запропоновані й вивчені раніше, на зорі розвитку теорії кодування. У класі неперервних кодів слід зазначити згорткові коди, які за характеристиками перевершують блокові коди, і, з цієї причини, знаходять широке застосування в телекомунікаційних системах.

Для опису процедур кодування/декодування як блокових, так і згорткових кодів використовують адекватний математичний апарат. Для опису лінійних кодів використовується добре розроблений апарат лінійної алгебри. Формування нелінійних кодів виконується із застосуванням нелінійних процедур. Такий підхід дозволяє в деяких випадках одержати нелінійні коди з рядом спеціальних властивостей. У теорії й техніці кодування важливої є проблема складності реалізації процедур кодування/декодування й, особливо, процедур декодування. Тому деякі класи кодів (коди Хемінга, циклічні коди Боуза-Чоудхурі-Хоквінгема, Ріда-Соломона, Файра й ін.) були розроблені разом з алгоритмами декодування, зв'язаними зі структурними властивостями цих кодів. І, навпаки, розробка

нових алгоритмів декодування згорткових кодів (алгоритм А. Вітербі, послідовне декодування, порогове декодування) ініціювала пошуки відповідних згорткових кодів. Суттєві переваги корегувальних кодів (як блокових, так і згорткових) спонукували пошуки нових підходів до реалізації шляхів підвищення завадостійкості й ефективності телекомунікаційних систем.

Важливим етапом у розвитку теорії кодування є поява каскадних кодів, представником яких є код Raptor. В основі побудови каскадних кодів лежить ідея спільного використання декількох складових кодів. Даний підхід дозволяє ефективно декодувати всю кодову конструкцію за допомогою декодерів досить простих складових кодів. Широке застосування в системах передачі даних (CCSDS, DVB-H/T/S, IEEE 802.16, TIA-1008) знайшла каскадна схема, в якій дані спочатку кодуються зовнішнім кодом, а потім внутрішнім кодом, причому комбінації кодів можуть бути різними. Часто в даній схемі між зовнішнім і внутрішнім кодером/декодером або після них включаються блоки перемежіння і відновлення (деперемежіння), які здійснюють псевдовипадкову перестановку символів зовнішнього коду і відновлення вихідного порядку символів відповідно.

Ці блоки призначені для розбиття пакетів помилок, з'являються при декодуванні прийнятого з каналу повідомлення за допомогою декодера внутрішнього коду, що дозволяє істотно поліпшити ефективність каскадної конструкції в цілому. На рис. 1.13 показані існуючі і нові методи кодування: сигнально-кодові конструкції, турбокоди, фонтанні коди і т.п.

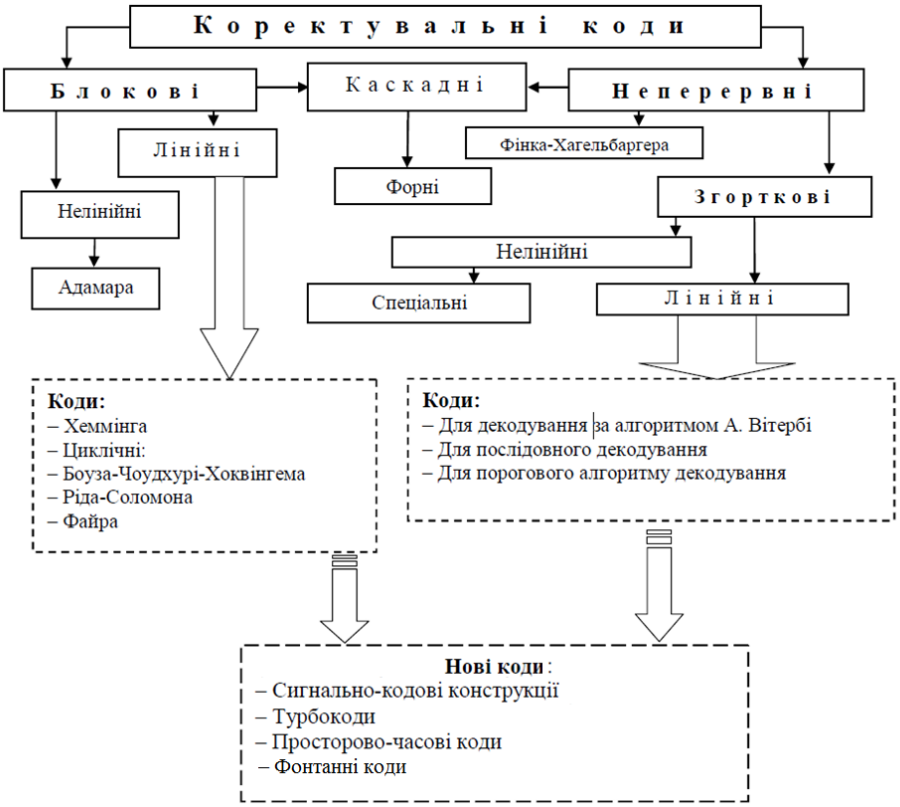


Рис. 1.13. Класифікація корегувальних кодів

1.3.2 Основні характеристики завадостійких кодів

Будь-який коригувальний код характеризується рядом показників: довжиною n, базою m, кількістю інформаційних символів k та надлишкових символів $p = n - k$, повним числом усіх можливих кодових комбінацій $N_0 = m^n$ (для двійкових кодів $N_0 = 2^n$), числом дозволених кодових комбінацій (потужність коду) N, вагою кодової комбінації, вагою вектору помилки, кодовою відстанню та ін. Проте основним показником якості коригуючого коду є його здатність забезпечити правильний прийом кодових комбінацій при наявності спотворень під впливом завад.

Кількісна оцінка завадостійкості коду може бути здійснена по-різному.

Завадостійкість коду характеризує його здатність забезпечить правильну передачу повідомлень в умовах впливу завад. Тому для кількісної оцінки завадостійкості коду доцільно використовувати ймовірність правильного прийому кодових комбінацій

$$P_{пр} = 1 - P_{пом}, \tag{1.10}$$

де $P_{пом}$ – ймовірність помилкового прийому кодових комбінацій.

Якщо код не володіє коригуючими властивостями, то ймовірність помилкового прийому $P_{пом}$ буде дорівнює ймовірності спотворення кодових комбінацій P_k. Для коригуючого коду $P_{пом} < P_к$. У реальних умовах $P_{пом} < 1$, тому більш зручним критерієм оцінки завадостійкості коду є логарифмічна величина

$$S_k = \lg \frac{1}{P_{пом}} = \lg \frac{1}{1 - P_{пр}}, \tag{1.11}$$

Іноді для оцінки якості коригувальних кодів користуються поняттям коефіцієнта виявлення помилок

$$K_{вияв} = \frac{P_{пп}}{P_к}, \tag{1.12}$$

де $P_{пп}$ – ймовірність появи помилок.

Це недостатньо повна характеристика якості завадостійкого коду. Нею доцільно користуватися в основному для оцінки кодів, призначених тільки для виявлення помилок.

Коригувальна спроможність коду забезпечується за рахунок надмірності,

тобто розширення кодових комбінацій. При розширенні кодових комбінацій ускладнюється апаратура, збільшується час передачі та обробки інформації. Тому надмірність також є важливою характеристикою коду.

Для оцінки надмірності коду користуються поняттям коефіцієнта надмірності

$$K_{над} = \frac{p}{n} = \frac{n-k}{n}, \tag{1.13}$$

де p – кількість надлишкових символів в кодової комбінації

У загальному випадку завадостійкий код характеризується наступними параметрами [13]:

– швидкість кодування r_k:

$$r_k = \frac{k}{k+r} = \frac{k}{n}, \tag{1.14}$$

де n – довжина кодового слова, k – число інформаційних біт в кодовому слові, r – число перевірочних біт в кодовому слові;

здатність до виправлення t, біт [13]:

$$t = \frac{d_{\min} - 1}{2}, \tag{1.15}$$

де $d_{\min}$ – кодова відстань, яке визначає мінімальне число позицій біт кодового слова, в яких розрізняються будь-які два кодові слова.

Таким чином, при використанні завадостійкого кодування з метою підвищення достовірності прийому сигналів з деякого початкового значення $p_б$ до деякого необхідного значення $p_{б\_тр}$, прагнуть вибрати такий код, щоб

забезпечити $p_{б\_тр}$, але при цьому кращим код вважається тоді, коли швидкість кодування і виправляюча здатність коду максимальні.

1.3.3 Гранична межа пропускної здатності каналу

Шеннон [14] довів, що пропускна здатність адитивного білого гаусовського каналу може бути виражена як (1.16). Рівняння (1.16) називається також теоремою Шеннона-Хартлі.

$$C = W \log_2(1 + \frac{S}{N}), \tag{1.16}$$

де W являє собою смугу пропускання каналу, S є середня потужність сигналу, яка приймається, і N середня потужність гаусовського шуму, S / N – середня потужність сигналу до середнього коефіцієнта потужності шуму, часто визначається як співвідношення сигнал-шум (SNR). Для цифрових комунікацій, E_b/N_0, як правило, продуктивність. E_b – середня енергія біту і N_0 – спектральна щільність гаусовського шуму. Фактично E_b/N_0 є нормалізованою версією SNR:

$$\frac{E_b}{N_0} = \frac{S / R_b}{N / W} = \frac{W}{R_b}(\frac{S}{N}), \tag{1.17}$$

де R_b – швидкість передачі біт.

Для зручності E_b/N_0 також називатимемо SNR. Статистика помилкових бітів в каналі за своєю природою залежить від сигналів і каналу. З конкретної схеми сигналізації, бітова ймовірність помилки (BER) є функцією E_b/N_0. У площині ймовірність помилки зображується у вигляді кривої з меншою ймовірністю помилки при більш високому значенні E_b/N_0.

Для передачі двійкових даних, у найпростішому випадку може бути застосована двійкова фазова маніпуляція (BPSK) яка забезпечує низьку BER без введення кодування. В роботі [15] міститься висновок про ймовірність помилки на біт для BPSK з когерентним прийомом. Ця ймовірність визначається за наступною формулою

$$P_B = \int^{\infty} \sqrt{2E_b / N_0}\, \frac{1}{\sqrt{2\pi}} e^{(-\frac{z^2}{2})} dz\,, \tag{1.18}$$

Рівняння (1.18) також часто записується у вигляді (1.19):

$$P_B = Q(\sqrt{\frac{2E_b}{N_0}})\,, \tag{1.19}$$

Функція Q – це додаткова функція помилок. Залежність ймовірності бітової помилки від співвідношення сигнал/шум (1.19), показано на рис. 1.14.

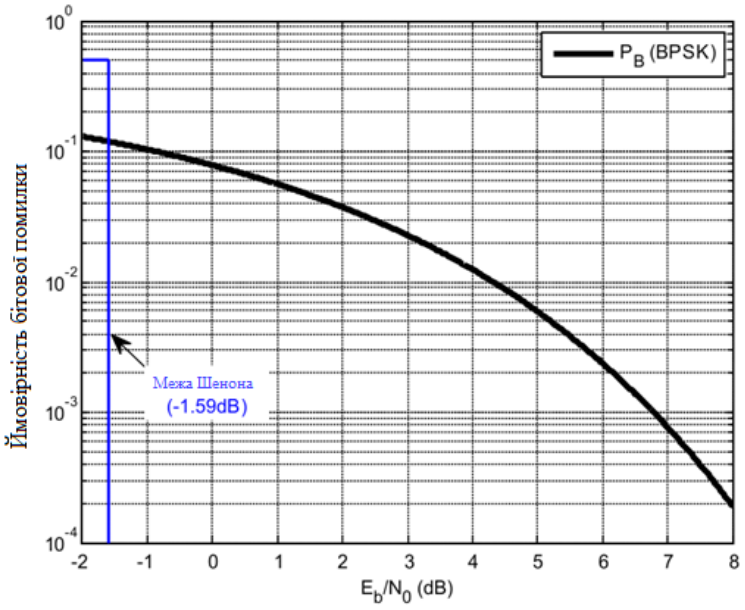


Рис. 1.14. Ймовірність бітової помилки для BPSK

Значення E_b/N_0= –1,59 дБ зветься межею Шеннона. Шеннон доказав, що для будь-яких заданих завад в каналі, можна досягти передачу цифрової інформації без помилок, або майже без помилок, з максимальною швидкістю в каналі. Досягти цього пропонував за допомогою методу кодування, але Шеннон не описав, як зробити такий код з корекцією помилок.

Межа Шеннона це теоретична межа для кодів нескінченної довжини і нескінченним часом обробки, яку абсолютно неможливо створити на практиці. Хоча виявлено, що ортогональна модуляція з великим значенням M може досягти кращих показників ймовірності помилок ніж BPSK, вона як і раніше вимагає M=+∞, щоб досягти межі Шеннона. Таким чином, будемо орієнтуватися на кінцеву довжину коду при проектуванні для забезпечення працездатності коду.

1.4 Показники якості інформаційно-телекомунікаційних систем і телекомунікаційних послуг мереж 5G

Розглянемо основні визначення, що запозичені з [16] і регламентують поняття телекомунікаційних мереж, систем та якості надаваних послуг.

Телекомунікаційна мережа загального користування – телекомунікаційна мережа, що використовується повністю або частково для надання загальнодоступних телекомунікаційних послуг.

Телекомунікації – технічний процес відправлення, передачі та отримання будь-якого виду повідомлень у вигляді знаків, голосу, зображень або звуків за допомогою телекомунікаційних систем.

Телекомунікаційні послуги – надання телекомунікацій та надання інших додаткових послуг, які тісно пов'язані з наданням телекомунікацій тісно

пов'язані з наданням телекомунікаційних послуг, таких як, наприклад, виставлення рахунків, довідкові послуги.

Телекомунікаційні системи – технічне обладнання або системи, здатні відправляти, передавати, комутувати, приймати, керувати або контролювати як повідомлення ідентифіковані електромагнітні сигнали.

Користувач – фізичні особи, включаючи споживачів, або організації, які використовують або запитують загальнодоступні телекомунікації послуги.

Згідно [17], якість телекомунікаційної послуги – сукупність показників, які характеризують споживчі властивості телекомунікаційної послуги та визначають її здатність задовольнити заявлені, встановлені і замовлені потреби споживача послуги.

При цьому, показник якості телекомунікаційної послуги (ЯТП) – кількісна характеристика послуги, яка отримана шляхом розрахунку з параметрів якості та визначає результат діяльності оператора, провайдера телекомунікацій з надання послуг та обслуговування споживачів.

Метою вимірювань є оцінка відповідності ЯТП систем рухомого мобільного зв’язку (РМЗ) вимогам, що встановлені відповідним нормативно-правовим актом [18-22].

Відповідно до мети вимірювань, об’єктом вимірювання є телекомунікаційні мережі РМЗ в частині показників якості послуг, що надаються в мережах рухомого мобільного зв’язку. Розглянемо основні показники якості відповідно до [17,23].

- Коефіцієнт непридатності мережі ($К_{\text{нпрм}}$);
- Коефіцієнт недоступності мережі ($К_{\text{ндм}}$);
- Відсоток спроб підключення та реєстрації у мережі, які відповідають нормам за часом підключення та реєстрації у мережі ($Q_{\text{прм}}$);

- Відсоток неуспішних спроб приєднання до мережі з комутацією пакетів ($Q_{\text{нсп}}$);
- Відсоток спроб приєднання до мережі з комутацією пакетів, які відповідають нормам за часом приєднання ($Q_{\text{пкп}}$);
- Відсоток неуспішних викликів для національних викликів ($Q_{\text{нув}}$);
- Відсоток викликів, які відповідають нормам за часом завершення викликів для національних викликів ($Q_{\text{ввчз}}$);
- Відсоток з'єднань, що відповідають нормам за якістю передачі мовної інформації ($Q_{\text{звям}}$);
- Відсоток встановлених з'єднань, які закінчилися передчасним роз'єднанням не за ініціативою абонента для національних з'єднань ($Q_{\text{рвз}}$);
- Відсоток неуспішних спроб встановлення TCP/IP-з'єднань для отримання послуги HTTP ($Q_{\text{н HTTP}}$);
- Відсоток TCP/IP-з'єднань для доступу до послуги HTTP, під час встановлення яких відбулось перевищення нормованого часу ($Q_{\text{невч\_IP}}$);
- Середня швидкість передавання даних ($V_{\text{шв}}$);
- Час затримки між пакетами відправлення та приймання (T_{ping});
- Варіація затримки пакетів (тремтіння, J);
- Втрата пакетів (відсоток втрати пакетів, $\text{Ping}_{\text{drop\_ratio}}$);
- Відсоток текстових повідомлень SMS, що відповідають нормам за часом доставки від кінця до кінця ($Q_{\text{н\_дост\_пов\_КК}}$);
- Відсоток недоставлених текстових повідомлень SMS ($Q_{\text{н\_дост\_SMS}}$).

Розглянемо більш детально показники якості, що мають бути вдосконалені в даній роботі.

1. *Середня швидкість передавання даних* ($V_{\text{шв}}$) [16]. Для вимірювання $V_{\text{шв}}$ застосовують тестовий сеанс «Data». $V_{\text{шв}}$ визначається як відношення

розміру отриманих даних до часового інтервалу від початку передачі даних до кінця. Середню швидкість передавання даних у кбіт/с обчислюють за формулою:

$$V_{\text{шв } HTTP} = \frac{W_{\text{роз дан}}}{T_{\text{ПД зав}} - T_{\text{ПД поч}}}, \quad (1.20)$$

де $W_{\text{роз дан}}$ – розмір даних користувача (файлу або веб-сторінки), кбіт;

$T_{\text{ПД зав}}$ – час завершення передачі даних, с;

$T_{\text{ПД поч}}$ – час початку передачі даних, с.

Значення показника обчислюється лише для сеансів успішно переданих даних.

2. *Час затримки між пакетами відправлення та приймання* (T_{ping}). Для вимірювання T_{ping} застосовують тестовий сеанс «Data». T_{ping} визначається як половина часу в мілісекундах, між відправкою запиту до отримання відгуку (PING) за протоколом ICMP на дійсну IP-адресу. Середній час затримки між пакетами T_{ping} розраховується за формулою:

$$T_{ping} = \frac{\sum_{i=0..n} Ti}{n} \quad (1.21)$$

де T_i – половина часу затримки пакета з номером *i*;

n – кількість пакетів у вимірювальному циклі.

3. *Варіація затримки пакетів* (тремтіння, J). Для вимірювання J застосовують тестовий сеанс «Data». Тремтіння – значення максимального відхилення часу затримки передачі (прийому) пакетів відносно середнього значення часу затримки передачі (прийому) пакетів впродовж вимірювання. Розраховується за формулою:

$$J = \max_n(D_{сер} - d_i) \quad (1.22)$$

де $D_{сер}$ – середня затримка передачі пакетів;

d_i – затримка окремого пакета.

4. *Втрата пакетів* (відсоток втрати пакетів, $Ping_{drop\_ratio}$). Для вимірювання $Ping_{drop\_ratio}$ застосовують тестовий сеанс «Data». Втрата пакетів визначається як кількість неотриманих відгуків (PING) після відправлення запитів.

Відсоток втрати пакетів розраховується за формулою:

$$Ping_{drop\_ratio} = Ping_{lost} / Ping_{total} \times 100\% \quad (1.23)$$

де $Ping_{lost}$ – загальна кількість відправлених Запитів.

$Ping_{total}$ – кількість неотриманих Відкликів

Згідно [16], параметри якості обслуговування (QoS) пов'язані в першу чергу з послугами та функціями послуг, а не з технологією, що використовується для надання послуг. Тому параметри повинні бути придатними для використання, коли послуги надаються за новими технологіями.

Параметри QoS, перелічені в [16], не призначені для оцінки повного QoS телекомунікаційної послуги. Документи [24,25] надають набір параметрів QoS, який охоплює специфічні аспекти QoS, пов'язані з користувачем, а не повний перелік параметрів QoS. Цей набір було обрано для розгляду областей, де моніторинг QoS, ймовірно, буде найбільш корисним, тобто областей, на які, швидше за все, можуть вплинути будь-які проблеми з QoS.

Набір параметрів QoS призначений для розуміння користувачами різних телекомунікаційних послуг. Підгрупи цих параметрів можуть бути обрані для

використання в різних обставинах. Параметри, визначені в [16], застосовні до будь-якого виду доступу до Інтернету незалежно від технології, що лежить в його основі.

Опишемо основні визначення, що будуть використані в роботі і взяті з [16]:

– автентифікація: процес перевірки заявленої ідентичності, щоб переконатися, що заявлена ідентичність користувача є правильною

– авторизація: процес визначення того, чи має особа, яка надає певні облікові дані, право на доступ до ресурсу або використання послуги користуватися послугою

– виклик: загальний термін для опису встановлення, використання та розриву з'єднання (шляху до носія) або потоку даних

– хост: комп'ютер, який надає клієнтським станціям доступ до файлів і принтерів як спільних ресурсів комп'ютерної мережі

– Інтернет: комп'ютерна мережа, що складається зі всесвітньої мережі комп'ютерних мереж, які використовують протоколи TCP/IP протоколи TCP/IP для полегшення передачі та обміну даними

– Доступ до Інтернету: надання в користування засобів та/або послуг з метою забезпечення доступу до загальнодоступної мережі Інтернет з метою надання користувачеві доступу до послуг або ресурсів мережі Інтернет

– процес входу в систему (логін): багатоетапний процес, який включає в себе як автентифікацію та авторизацію, так і інші завдання для запуску системи завдання, щоб надати користувачеві доступ до послуг або ресурсів

– користувач: фізичні особи, включаючи споживачів, або організації, які використовують або запитують загальнодоступні телекомунікації послуги

Згідно [16] наведені показники якості мають різний ступінь впливу на різні додатки, що передаються 5G мережею (табл. 1.2, 1.3).

Поєднуючи результати наведені в табл. 1.2 з вищенаведеними характеристиками, можна побачити, що для голосових додатків, ключовими факторами якості є час затримки, тремтіння і в меншому ступені показник втрат пакетів. Згідно табл. 1.3, для якісної передачі даних необхідно забезпечення швидкості передачі даних і низький рівень помилок та втрат пакетів.

Таблиця 1.2 – Аудіо та відео додатки і оцінка ефективності їх роботи

Додаток		Оцінка ефективності роботи
Аудіо	Діалоговий голос (Conversational voice)	На розмовний голос сильно впливає одностороння затримка. Існує два різних ефекти затримки. Перший – це створення відлуння в поєднанні з перетворенням двопровідного зв'язку в 4-провідний або навіть з акустичним з'єднанням в терміналі. Це починає викликати зростаючу деградацію якості голосу через затримки ~ десятків мілісекунд, і в цей момент необхідно вжити заходів з ехоконтролю. Другий ефект виникає, коли затримка збільшується до такої міри, що починає впливати на динаміку розмови, тобто затримка відповіді співрозмовника стає помітною. Це відбувається при затримках ~ декількох сотень мілісекунд. Однак людське вухо дуже нетерпиме до короткочасних коливань затримки (тремтіння). На практиці, для всіх голосових сервісів затримка може змінюватися через мінливості часу надходження вхідних пакетів, які необхідно усунути за допомогою буфера, що усуває тремтіння. Вплив втрати пакетів зумовлений тим, що людське вухо людське вухо толерантне до певної кількості спотворень мовного сигналу. В IP-системах передачі системах передачі основним джерелом погіршення якості голосу є використання кодеків стиснення мови з низьким бітрейтом та їх продуктивність в умовах втрати пакетів.
	Голосові повідомлення (Voice messaging)	Вимоги до втрати інформації по суті ті ж самі, що і для розмовного голосу (тобто залежать від кодера мови), але ключова відмінність полягає в тому, що існує більша толерантність до затримки, оскільки немає безпосередньої розмови. Тому основним питанням стає яку затримку можна допустити між користувачем, який віддає команду на відтворення голосового повідомлення, і фактичним початком відтворення звуку. Точних даних щодо цього не існує, але затримка порядка декількох секунд є прийнятною.
	Аудіо стрімінг (Streaming	Очікується, що потокове аудіо забезпечить кращу якість, ніж звичайна телефонія, а вимоги до втрати інформації з точки

	audio)	зору втрати пакетів будуть відповідно жорсткішими. Однак, як і у випадку з голосовими повідомленнями, тут немає розмовного елементу, і вимоги до затримки самого аудіопотоку можна послабити, навіть більше, ніж для голосових повідомлень, хоча команди управління повинні оброблятися належним чином.
Відео	Відеофон (Videophone)	Під відеофоном мається на увазі повнодуплексна система, що передає як відео так і аудіо, і призначена для використання в розмовному середовищі. Таким чином, в принципі, ті ж самі вимоги до затримки, що і для розмовного голосу, тобто відсутність відлуння і мінімальний вплив на динаміку розмови, з додатковою вимогою, що аудіо і відео повинні бути синхронізовані в певних межах, щоб забезпечити "синхронізацію губ". Людське око толерантне до деякої втрати інформації, такщо деякий ступінь втрати пакетів є прийнятним, залежно від конкретного відеокодера та рівня захисту від помилок, що використовується.
	Одностороннє відео (One-way video)	Головною відмінною рисою одностороннього відео є відсутність розмовного елемента, а це означає, що вимоги до затримки не будуть такими жорсткими і можуть відповідати вимогам до потокового аудіо.

Таблиця 1.3 – Пакетні додатки і оцінка ефективності їх роботи

Додаток		Оцінка ефективності роботи
Дані (Data)	Перегляд web-сторінок (Web-browsing)	З точки зору користувача, основним фактором продуктивності є те, як швидко з'являється сторінка після запиту. Затримки в кілька секунд є прийнятними, але не більше близько 10 секунд.
	Великі дані (Bulk data)	Ця категорія включає передачу файлів, і на неї явно впливає розмір файлу. Якщо є ознаки того, що передача файлу відбувається тривалий час, можна припустити дещо більшу толерантність до затримки ніж для однієї веб-сторінки.
	Пріоритетні транзакційні послуги (Highpriority transaction services)	Основна вимога до продуктивності полягає в тому, щоб надати користувачеві відчуття, що транзакція проходить безперебійно, і бажано, щоб затримка не перевищувала декількох секунд.
	Управління (Command/control)	Управління передбачає дуже жорсткі обмеження на допустиму затримку, значно менше секунди, а також нульову толерантність до втрати інформації.
	Нерухомі зображення (Still image)	Ця категорія повинна мати майже нульову втрату пакетів. Втім, вимоги до затримки для передачі нерухомих зображень не є жорсткими.
	Інтерактивні ігри (Interactive	Вимоги до інтерактивних ігор дуже залежать від конкретної гри, але вимагають дуже короткі затримки, порядку долі

	games)	секунди.
	Telnet	Telnet вимагає коротку затримку у долі секунди, щоб забезпечити по суті миттєвий характер відповіді.
	Електронна пошта E-mail (server access)	Під час взаємодії користувача з локальним поштовим сервером, очікується, що пошта буде передана протягом декількох секунд.
	Миттєві повідомлення (Instant messaging)	Обмін миттєвими повідомленнями в першу чергу стосується тексту, але може також включати аудіо, відео та зображення. У будь-якому випадку це не спілкування в реальному часі в сенсі розмовного голосу, і затримки в декілька секунд є прийнятними.
	Фонові додатки (Background applications)	Єдиною вимогою до додатків цієї категорії є те, що інформація має бути доставленою користувачеві практично без втрат. Однак, також існує обмеження щодо максимальної затримки.

Зменшення рівня помилок і втрат пакетів під час їх доставки можна досягти вдосконаленням методів завадостійкого кодування, в тому числі застосуванням фонтанних кодів.

Зменшення затримки під час обробки та передачі можна досягти вдосконаленням процедур класифікації трафіка, кластеризації та інтелектуальної обробки на основі заздалегідь заготовлених правил.

1.5 Методи підвищення показників якості

Як було зазначено вище (п.1.4) для підвищення якості надання послуг в цілому, необхідно запропонувати моделі та методи для зменшення часу затримки, рівня помилок і втрат пакетів під час їх доставки. Розглянемо для цього існуючі методи завадостійкого кодування та методи класифікації трафіка, що використовуються або можуть бути застосовані в мережах 4G/5G.

1.5.1 Огляд досліджуваних методів завадостійкого кодування в інформаційно-телекомунікаційних системах

На сьогоднішній день можна говорити про створення нового класу завадостійких кодів для каналів зі стираннями та завмираннями. Кодами з цього класу можна закодувати повідомлення кінцевого розміру (або файл) потенційно-необмеженим потоком незалежних пакетів. Ця властивість нового класу кодів принципово відрізняє його від класичних блокових або згорткових, завадостійких кодів із заданою швидкістю. При кодуванні файлу цими кодами отримуємо також файл кодованих даних, а не потік. Новий клас кодів також називають класом фонтанних кодів (Digital Fountain Codes).

Кодер такого коду за запитом завжди може додати "на льоту" невелике число кодових пакетів. При цьому час формування кожного кодового пакету постійний. Цю властивість кодеру в зарубіжній літературі [26] іноді іменують терміном "local encodability". Незалежність генерування кодових символів забезпечується застосуванням статистичного кодування. Додати "на льоту" декілька перевірочних символів для класичних кодів не завжди вдається. Кодові символи виявляються залежними один від одного. Розглянемо основні корегувальні коди, що застосовуються в інформаційно-телекомунікаційних мережах: код Ріда-Соломона, LDPC код, LT-код.

1.5.1.1 Код Ріда-Соломона

Код Ріда-Соломона являє собою блоковий код, в якому символи складаються з k біт. Якщо ці символи розглядати як пакети повідомлення, то код може бути використаний для доставки повідомлень в каналі зі стиранням. Основною властивістю коду є наступне: для доставки K інформаційних символів достатньо прийняти будь K символів з N. Або

інакше: для правильного прийому повідомлення з K символів у блоці з N пакетів будь-які з $M = NK$ символів можуть бути стертими.

Оптимальність коду в зазначеному вище сенсі досягається його жорсткою алгебраїчною структурою. В результаті існує проблема додавання «на льоту» невеликого числа перевірочних символів. При переході від $M = N - K$ перевірочних символів до більшого числа $M = N' - K'$ всі перевірочні символи потрібно заново розрахувати. Код існує лише при $N < q = 2 \times k$. Жорстка структура коду призводить і до значних обчислювальних витрат при кодуванні і декодуванні. У кожен перевірочний символ коду входять всі K вихідних символів (пакетів) повідомлення. Тому при кодуванні потрібно $K \times (\mathrm{N} - \mathrm{K})$ операцій над символами (додавання і множення) [27-29, 31].

Імовірність появи помилки в декодованому символі, P_e, можна записати через ймовірність появи помилки в канальному символі, p, визначається за формулою:

$$Pe = \frac{1}{n} \times \sum_{j=t+1}^{n} j \times \left(\frac{n!}{j!(n-j)!}\right) \times p^{j} \times (1-p)^{n-j}, \qquad (1.24)$$

де: m – позитивне ціле число, більше одиниці; p – імовірність появи помилки в канальному символі; n – число кодових символів у кодованому символі; t – кількість помилкових бітів в символі, які може виправити код; n – число контрольних символів.

Коди Ріда-Соломона (RS) [27-29, 31] це циклічні лінійні коди над GF(2^k) з поліноміальними генераторами. Ці коди можуть бути використані для апроксимації ідеального коду, так як, при передачі повідомлення з K

символів, коди RS можуть відновити всі вихідні символи з N отриманих кодованих символів, з n більше, ніж k. Тим не менш, коди Ріда-Соломона втрачають ефективність при великих k і n, вимагаючи квадратичний час кодування/декодування.

1.5.1.2 Код з малою перевіркою на парність (LDPC код)

Low-density parity-check codes (коди з малою перевіркою на парність), також відомі як коди Галлагера, були винайдені Галлагером і опубліковані в 1963 році [30,32]. Ці коди, можуть забезпечити передачу даних близьку до границі Шеннону. Продуктивність коду LDPC визначається його матрицею контролю парності і алгоритму декодування [38-40]. Загальні схеми декодування включають алгоритми поширення віри і максимальної ймовірності (правдоподібності). Перша схема виконує декодування інформації багаторазово між v-вузлами і c-вузлами уздовж країв в графі Таннера в матриці контролю парності. В цілому, чим більше ітерацій декодування, тим більш високу продуктивність реалізує код. Схема максимальної ймовірності декодування схожа на алгоритм Гауса. Проте, LDPC-код не може гарантувати ефективну і надійну передачу по багатоадресній та / або широковіщальній мережі, де існують або асинхронні різні або невідомі зразки втрати даних, доступ до яких потрібен.

Матриця має розмірність $M \times N$ в кожному стовпці матриці – j = кількості одиниць, в кожному рядку – k = кількості одиниць. Для практики важливі коди з дуже низькою щільністю перевірок на парність, для яких $j << M$ і $k << N$. Дуже низька щільність значно знижує обчислювальні витрати на реалізацію алгоритму декодування при великих розмірах матриць. Галлагером була запропонована ітеративна обмінна ймовірнісна процедура декодування. Інтерпретація обмінного алгоритму декодування особливо

наочна на перевірочному графі коду (рис. 1.15). Цей граф також називають графом Таннера [30]. Він має дві групи перевірочних вузлів (Bipartite Graph). Перший набір відповідає правдоподібностям прийнятих *N* кодових символів, другий – правдоподібностям *M* перевірок на парність. Відзначимо, що для розглянутих кодів породжуюча матриця *G* в корені відрізняється від перевірочної матриці і має високу щільність одиниць (High Density).

Імовірність появи помилки в декодованому символі визначається за формулою:

$$P = \int_{\sqrt{\frac{2Ec}{No}}}^{\infty} \frac{1}{\sqrt{2\pi}} \times e^{\frac{-x^2}{2}} dx, \tag{1.25}$$

де: *Ec/No* – співвідношення сигнал/шум в каналі передачі даних.

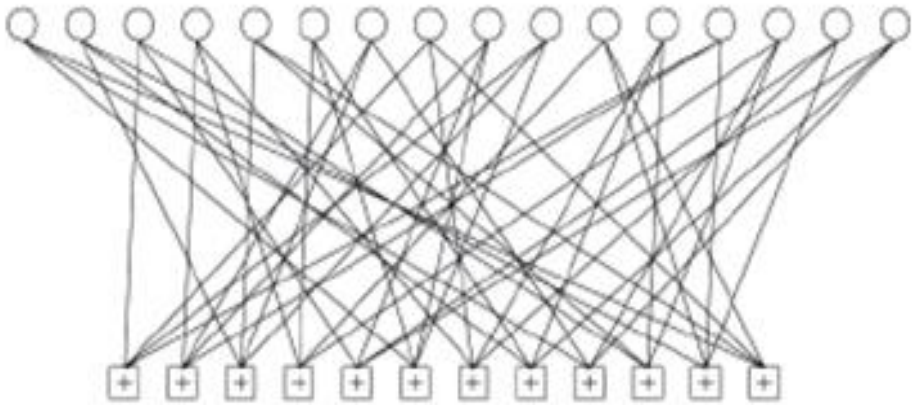


Рис. 1.15. Перевірочний граф LDPC коду

1.5.1.3 Метод кодування Лабі (Luby Transform)

Код був створений М. Лабі (Michael Luby) в 1998р. Свою назву він отримав від «Laby transform» (перетворення Лаби) [33, 35].

В основі знаходження розподілу ймовірності і алгоритму декодування лежить нескладна ймовірнісна задача. Є повідомлення з *K* вихідних символів. З цієї множини з ймовірністю *1/K* формується *K'* випадкових вибірок

символів. В результаті формується множина з K' кодових символів. $K'\sim = K \ln (K / \delta)$ при досить великому K, це робиться для того, щоб з ймовірністю $1–\delta$ кожен з усіх K вихідних символів виявився хоча б один раз серед K' кодових символів. Маючи таке число кодових символів, можна реконструювати вихідне повідомлення з ймовірністю $1–\delta$. Алгоритм реконструкції гранично швидкий і використовує лише інформацію про нумерацію символів.

Вартість декодування, для коду, виявляється порядку $\ln(K/\delta)$ операцій XOR. Ця величина при досить великих K і прийнятних δ виявляється набагато менше K, і тому код можна віднести до класу кодів з низькою щільністю матриці, що породжує.

Як лінійний код, код LT може генерувати змінну кількість кодових символів. Використовуючи породжуючу матрицю, декодер LT може відновити вихідне повідомлення на льоту з довільно зібраних закодованих символів з невеликими витратами на декодування. Звичайні коди LT швидкі і ефективні з ітеративним алгоритмом декодування передачі повідомлень при жорсткому декодуванні інформації. Вони можуть адаптуватися до багатоадресного і широкомовного середовища Інтернету тільки через розподіл ступеня для вихідних кодованих символів. У приймачі сусідня інформація кожного кодованого символу використовується для побудови графа Таннера матриці генератора. Існує досить мало способів правильно поширити інформацію про індекси вихідних символів на декодер.

Ключовим аспектом розробки LT-кодів є розробка щільності розподілу ймовірності $f(d)$. Ідеальним розподілом називається розподіл, щільність розподілу ймовірності якого задається згідно такої формули:

$$\rho(d) = \begin{cases} \frac{1}{K}, d = 1, \\ \frac{1}{d(d-1)}, d = 2,3...,K \end{cases}, \quad (1.26)$$

Цей розподіл ідеальний з точки зору вартості кодування, яка мінімальна і дорівнює *lnK* [34]. Щільність робасного солітонівського (robust Soliton) розподілу *μ(d)* задається формулою:

$$\mu(d) = \frac{\rho(d) + \tau(d)}{\sum_d \rho(d) + \tau(d)}, \quad (1.27)$$

де *ρ(d)* визначається згідно (1.26), а *τ(d)* згідно (1.28):

$$\tau(d) = \begin{cases} \frac{S}{Kd}, d = 1,2,..., \frac{K}{S} - 1, \\ \frac{S}{K}\ln(\frac{S}{\delta}), d = \frac{K}{S}, \\ 0, d > \frac{K}{S}. \end{cases}, \quad (1.28)$$

У формулі (1.28) *S* визначається виразом:

$$S(K,\delta) = c\ln(\frac{K}{\delta})\sqrt{K}, \quad (1.29)$$

де *c* – параметр розподілу; задається як позитивне число, величина якого менше одиниці. Саме в цьому випадку вартість декодування виявляється порядку *ln (K / δ)* операцій XOR.

1.5.1.4 Код Raptor

Raptor код [36,37] – це наступний етап розвитку коду LT. Raptor коди були розглянуті на 3rd Generation Partnership Project (3GPP) ще в грудні 1998

року. В рамках 3GPP, коди Раптор використовуються для надійної доставки даних в мобільних / бездротових мережах, в першу чергу для широкосмугового доступу і багатоадресної доставки.

Код являє собою кодову конструкцію з внутрішнім (по відношенню до каналу) LT кодом. В якості зовнішнього коду можна використовуватися «майже» будь-який блоковий код (з фіксованою швидкістю). Розробкою та дослідженням коду займався A. Shokrollahi [36,37].

Аналіз конструкції показує, що вихідне повідомлення може бути реконструйовано з імовірністю $1–\delta$ по $K'= K (1 + \varepsilon)$ символам, де ε – невелике позитивне число. Вартість декодування виявляється порядку $ln(1/\varepsilon)$ операцій XOR. Для декодування повідомлення потрібно близько $Kln(1/\varepsilon)$ операцій XOR. На сьогоднішній день код є, можливо, кращою апроксимацією ідеального фонтанного коду [41,42].

1.5.1.5 Вибір напрямку дослідження

З кожним роком вимоги, пропоновані до реальних систем передачі інформації, стають все жорсткіші і жорсткіші, також все активніше розвиваються бездротові системи передачі інформації, де в якості середовища поширення сигналу використовуються багатопроменеві канали. Це пов'язано з простотою технічного розгортання таких мереж. Але поряд з зручністю використання, такі системи мають дуже низьку завадозахищеність. В даному випадку проблема забезпечення заданої швидкості та достовірності переданих даних постає особливо гостро. Одним із способів вирішення поставленої проблеми є підвищення ефективності використовуваних методів завадостійкого кодування.

Алгоритми, пов'язані з розглянутими кодами, використовуються в таких програмно-апаратних виробах для комп'ютерних мереж як Digital Fountain

Multicast Client, DF Raptor for Streaming, DF Broadcast і т.п. та починають проникати і в інші пакетні мережі. Коди Raptor включені в стандарти мобільного зв'язку третього, четвертого та п’ятого поколінь.

В Україні проблемою завадостійких кодів займалися такі дослідники: Різник О. [79], Пятін І.С., Бойко Ю.М. [80,81], Василенко В.М. [82,83] Основним напрямком досліджень були коди Хемінга, Ріда-Соломона та циклічні коди, а також LDPC коди [80]. На сьогодні, більшість з цих кодів не здатна забезпечити показниками якості передачі даних, що висувають сучасні інформаційно-телекомунікаційні системи.

Представлений огляд відомих кодів і методів їх декодування дозволяє зробити висновок про те, що найкращу корегувальну здатність мають фонтанні коди (LT і Raptor), а також LDPC коди. Слід зазначити, що складність декодування Raptor коду дещо менше, ніж у LDPC кодів, але перевершує складність LT кодів. Якщо взяти до уваги складність методу декодування, і його ефективність, то для високошвидкісних систем передачі даних найкращим виявляється Raptor код, що пояснює його вибір в якості одного з об'єктів дослідження в даній дисертаційній роботі. Для підвищення ефективності інформаційно-телекомунікаційної системи в цілому, необхідно забезпечити низький рівень втрат пакетів і відповідно високу коригувальну здатність для групових помилок. Цього можна досягти за допомогою введення додаткового блоку перемежіння, вибору оптимального каскадного методу декодування, та вдосконалення методу кодування.

1.5.2 Огляд методів класифікації трафіка

Існує три загальних підходи до ранньої класифікації мобільного трафіку [86]:

- підходи на основі портів;

- підходи на основі глибокої перевірки пакетів;
- підходи на основі розміру пакетів.

Для високої точності класифікації аналізують тип джерела та основні поля пакетів, на основі цього формують патерни трафіка [85]. Додаткове посилення класифікації в цьому випадку можливе за рахунок застосування глибокої перевірки пакетів (DPI).

В роботі [85] застосовують методи навчання на основі аналізу даних для класифікації типів джерел за номерами серій або ідентифікаторами. Після того, як тип ідентифіковано, параметри для вилучення ознак можуть бути виміряні за допомогою випробувального та вимірювального обладнання. В [85] типи джерел оцінюють за наступними полями:

- Тип пристрою,
- Інформація про можливості користувача (FGI),
- DNS (TTL),
- HTTP (User Agent).

На основі цього формується шаблон потоку трафіку (TFT) призначений для фільтрації пакетів на відповідні джерела та типи якості обслуговування (QoS). TFT фільтрує пакети відповідно до *IP-адреси, номера порту, протоколу та напрямку пакетів*. Однак цієї інформації недостатньо для того, щоб відрізнити завантаження веб-файлів, перегляд новин у фейсбук та чат-повідомлень і надати різний рівень QoS для цих додатків.

Для вирішення цієї проблеми необхідна інша архітектура, яка інтегрує глибоку перевірку пакетів (DPI) з TFT, щоб забезпечити більш високу деталізацію рівнів QoS для додатків. Коли певний потік трафіку буде ідентифіковано як певний тип програми, TFT буде поінформовано про це для

оновлення правил пакетних фільтрів. Завдяки цьому вдосконаленому методу потік трафіку може бути доставлений через носія відповідного рівня QoS.

В дослідженні [86] запропоновано модель для характеристики та класифікації потоків TCP та UDP з точки зору прикладного рівня, і результати показали, що цей метод значно покращує точність класифікації, ніж класифікація з точки зору транспортного рівня, з мінімальним покращенням загальної точності на 15-30%. Крім того, дослідження [86] показало, що найефективніша кількість пакетів, що використовується для моделі класифікації, становить від 5 до 7 пакетів після того, як вони застосували свої моделі класифікації трафіку з декількома алгоритмами ML, такими як Naïve Bayes, SVM, Random Forest. Це означає, що занадто багато пакетів і занадто мало пакетів знижують точність моделі. Зокрема, в дослідженні [85] було запропоновано прихований ланцюг Маркова (Hidden Markov Model, HMM) для класифікації потоку інтернет-трафіку мобільних широкосмугових додатків, використовуючи розмір пакетів і напрямок передачі пакетів з точністю 99,17% для 6 типів мобільних додатків.

Також варто відзначити рекомендований 3GPP набір ознак для класифікації трафіка [87]. Цей набір має містити наступні загальні параметри: ідентифікатор 5G QoS (5QI), пріоритет розподілу та утримання (ARP).

Для потоків з негарантованою швидкістю (non-GBR) до них має додаватися атрибут відображення QoS (Reflective QoS Attribute, RQA). А для потоків з гарантованою швидкістю (GBR) до ознак мають бути додані:

- Гарантована швидкість потоку (GFBR) - UL та DL;
- Максимальна швидкість потоку (MFBR) - UL та DL;
- Максимальна швидкість втрати пакетів - UL та DL.

1.5.3 Застосування нейронних мереж для класифікації трафіка

Класифікатори трафіку дозволяють ідентифікувати шаблони трафіку, які відповідають одному з апріорно відомих класів. Для класифікації широке застосування отримали алгоритми на основі штучних нейронних мереж (artificial neural networks, ANN), *k*-найближчих сусідів (*k*-nearest neighbor, KNN), «випадкового лісу» (Random Forest, RF) [43-52]. Розглянемо їх принципи роботи, переваги та недоліки більш детально.

Алгоритм штучних нейронних мереж (ANN). Штучна нейронна мережа – це система з'єднаних і взаємодіючих між собою штучних нейронів [53, 54]. Кожен штучний нейрон має справу з сигналами, які він періодично отримує, і сигналами, які він періодично посилає іншим нейронам.

Принцип роботи штучної нейронної мережі [55] полягає в підсумовуванні сигналів, що надходять на входи нейронів. При цьому враховується синаптична вага, тобто значимість кожного з входів. Вага кожного такого зв'язку може бути позитивною (збуджуючі зв'язки) або негативною (гальмівні зв'язки). Вони визначають обчислення нейронної мережі, а відповідно її пам'ять та поведінку. Штучна нейронна мережа (ШНМ) складається з трьох компонентів (рис. 1.16):

- вхідний шар;
- приховані (обчислювальні) шари;
- вихідний шар.

Для отримання результату – виконання класифікації трафіка необхідно попередньо виконати навчання нейронної мережі.

Під навчанням будемо розуміти пошук набору вагових коефіцієнтів, які при проходженні через суматор дозволять отримати потрібний сигнал. Навчання таких нейромереж відбувається у два етапи: пряме поширення помилки і зворотне поширення помилки. Під час прямого поширення

помилки робиться прогноз відповіді. При зворотному поширенні помилка між фактичною відповіддю та передбаченим мінімізується.

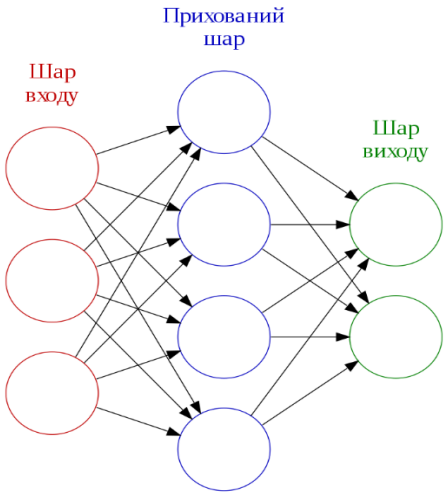


Рис. 1.16. Загальний вигляд штучної нейронної мережі [55]

Перевагами штучних нейронних мереж (ANN) є:

1. Висока надійність роботи. Інформація в ШНМ кодується і запам'ятовується не в окремих елементах пам'яті, а в розподілі зв'язків між нейронами і в їх силі, тому стан кожного окремого нейрона визначається станом багатьох інших нейронів, пов'язаних з ним. Тому, втрата одного або декількох зв'язків не має істотного впливу на результат роботи системи в цілому, що забезпечує її високу надійність

2. Висока «природна» завадостійкість і функціональна надійність стосуються як спотворених (зашумлених) потоків інформації, так і відмов окремих нейронів. Цим забезпечуються висока оперативність і достовірність обробки інформації, а просте донавчання і перенавчання мереж дозволяють при зміні зовнішніх чинників своєчасно здійснювати перехід на новий рівень вирішуваних завдань.

Алгоритм k-найближчих сусідів (KNN) [56]. Це простий, непараметричний класифікаційний алгоритм де для класифікації об'єктів у рамках простору властивостей використовуються відстані розраховані до усіх інших об'єктів [55,56]. З метою згладжування шумового впливу викидів, алгоритм класифікує об’єкти шляхом голосування за k найближчими сусідами. Кожен із сусідів $y^{(j)}, (j = \overline{1,k})$ голосує за віднесення реалізації образу до свого класу. Алгоритм відносить реалізацію, що розпізнається, до того класу, який набере найбільше число голосів. У разі використання зваженого способу до уваги береться не тільки кількість об’єктів, що потрапили в область певних класів, а й їхня віддаленість від нового значення [56]. Для кожного класу j визначається оцінка близькості:

$$Q_j = \sum_{i=1}^{N} \frac{1}{d(x,a_i)^2}. \quad (1.30)$$

де $d(x, a_i)$ – відстань від нового значення x до об’єкту a_i. У якого класу вище значення близькості той і присвоюється об’єкту. Для кожного об’єкта перевіряється, чи правильно він класифікується за своїми k найближчими сусідами (рис. 1.17). Тестовий зразок (зелене коло, рис. 1.16) повинен бути класифікований як синій квадрат (клас 1) або як червоний трикутник (клас 2). Якщо k = 3, то тестовий зразок класифікується як 2-й клас, якщо k = 5, то він буде класифікований як клас 1.

Для віднесення «сусідами» тестового зразку до свого класу можуть використовуватися різноманітні оцінки відстані при оцінюванні міри близькості. Найбільш поширеними є манхеттенська відстань та ступенева відстань, окремим випадком якої є евклідова відстань.

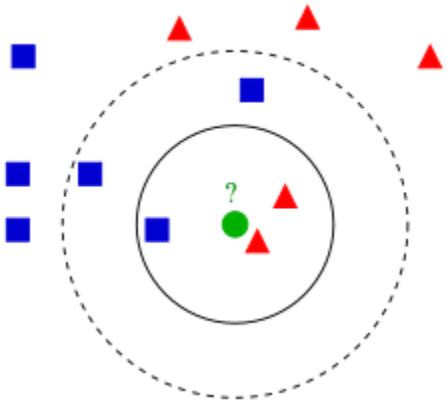


Рис. 1.17. Приклад класифікації *k* найближчих сусідів [56]

Манхеттенська відстань (1.31) є середньою різницею за координатами. В більшості випадків ця міра відстані призводить до таких результатів, як і евклідова відстань. Однак для цієї міри вплив окремих великих різниць (викидів) зменшується.

$$d(x, y) = \sum_{i=1}^{N} |x_i - y_i|. \tag{1.31}$$

Також може бути для порівняння використана ступенева відстань, яка застосовується у випадках, коли необхідно збільшити чи зменшити вагу, яка відноситься до розмірності і розраховується за формулою (1.32).

$$d(x, y) = r\sqrt{\sum_{i=1}^{N} (x_i - y_i)^p}\,, \tag{1.32}$$

де r і p – параметри, визначені користувачем.

Параметр r відповідальний за поступове зважування різниць по окремим координатам, а параметр p відповідальний за прогресивне зважування великих відстаней між об’єктами. Якщо r і p дорівнюють двом, то ця відстань

співпадає з відстанню Евкліда. Міра близькості підбирається індивідуально для конкретних типів даних.

Алгоритм KNN має як переваги так і недоліки. До переваг слід віднести:

−алгоритм стійкий до аномальних викидів, тому що імовірність влучення такого запису в число *k*-найближчих сусідів мала. Якщо ж це відбулося, то вплив на голосування (особливо зважене) (при k>2) також, швидше за все, буде незначним, і, отже, малим буде і вплив на підсумок класифікації;

−програмна реалізація алгоритму відносно проста;

−результат роботи алгоритму легко піддається інтерпретації;

−можливість модифікації алгоритму, шляхом використання найбільш придатних функцій сполучення і метрик дозволяє підбудувати алгоритм під конкретну задачу.

До недоліків алгоритму відносять те, що набір даних, використовуваний для алгоритму, повинний бути репрезентативним, а також те, що модель не можна "відокремити" від даних: для класифікації нового прикладу потрібно використовувати всі приклади. Ця особливість сильно обмежує використання алгоритму.

Алгоритм «випадкового лісу» (Random Forest, RF). RF базується на деревах рішень і може бути використаний як для класифікації, так і для регресійних завдань [57,58]. У машинному навчанні дерева рішень є алгоритмом створення моделей прогнозування. Їх називають деревами прийняття рішень, оскільки передбачення слідує за кількома гілками рішення “якщо… тоді…”, поділеним на гілки дерева. Цей поділ можна розглядати як функцію в машинному навчанні. Рішення будуть прийматися, поки не відбудеться перехід до наступної гілки і не повториться той самий процес прийняття рішень, поки не буде більше гілок. Ця кінцева точка називається

листом, а в деревах рішень – кінцевий результат: прогнозований клас або значення. У кожній гілці є порогові значення, які найкраще розділяють дані (що залишилися). RF робить прогнози шляхом комбінування результатів з багатьох окремих дерев рішень.

Для налаштування навчання алгоритму використовують гіперпараметри. Гіперпараметри – це аргументи, які можна встановити перед тренуванням і які визначають, як проводиться навчання. Основними гіперпараметрами в Random Forest є:

- кількість дерев рішень, які необхідно об'єднати;
- максимальна глибина дерев;
- максимальна кількість ознак, що розглядаються при кожному розбитті;
- виконується паралельне чи послідовне навчання класифікаторів (bagging/boosting).

Переваги Random Forests полягають у тому, що він є відносно швидким і потужним алгоритмом навчання, класифікації та регресії. Розрахунки можуть бути паралелізовані і добре виконуються при багатьох задачах, навіть при малих наборах даних, а вихідні дані повертають ймовірності прогнозування.

Недоліки Random Forests полягають у тому що не має можливості інтерпретувати рішення, прийняті моделлю, тому що вони занадто складні. RF також дещо схильні до перенавчання, і вони, як правило, погано прогнозують недостатньо представлені класи в незбалансованих наборах даних.

Аналіз ефективності застосування вказаних методів класифікації буде розглянутий в розділі 3 даної роботи.

1.6 Показники захищеності інформаційно-телекомунікаційних систем і телекомунікаційних послуг

Для забезпечення захищеності інформаційних ресурсів в інформаційно-телекомунікаційній системі має бути виконана оцінка стану і оцінка захищеності. При цьому, згідно [59] виділяють два типи оцінок:

- *оцінка (оцінювання) стану захищеності* державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах – це сукупність заходів, спрямованих на виявлення загроз державним інформаційним ресурсам від здійснення несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (ІТС);
- *оцінка (оцінювання) захищеності інформації* в інформаційній, телекомунікаційній та інформаційно-телекомунікаційній системі – заходи щодо виявлення в інформаційній, телекомунікаційній, інформаційно-телекомунікаційній системі технічних рішень, що створюють можливість здійснення дій з порушення цілісності, конфіденційності та доступності інформації, яка в ній циркулює.

Відповідно до [60] захищеність в інформаційно-телекомунікаційній системі може розглядатися як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого і зростають до значення n, де n – унікальне для кожного виду послуг. Також показники захищеності регламентуються джерелами [61,62,84].

Розглянемо основні критерії та послуги якими вони забезпечуються.

Функціональні критерії розбиті на чотири групи [60], кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

1) Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям конфіденційності, комплекс засобів захисту (КЗЗ) оцінюваної ІТС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації).

Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні. Опишемо їх більш детально.

Довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів і наведені в табл. 1.4.

Адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

Таблиця 1.4 – Рівні надання послуги «Аналіз прихованих каналів» [60]

<table>
<tr><th>КК-1. Виявлення прихованих каналів</th><th>КК-2. Контроль прихованих каналів</th><th>КК-3. Перекриття прихованих каналів</th></tr>
<tr><td colspan="3">Повинен бути виконаний аналіз прихованих каналів</td></tr>
<tr><td colspan="2">Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані
Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів
Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність</td><td rowspan="2">Всі (затверджена підмножина) знайдені під час аналізу приховані канали повинні бути усунені</td></tr>
<tr><td>—</td><td>КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів</td></tr>
</table>

Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

КЗЗ розглядає ресурси ІТС в якості об'єктів і управляє взаємодією цих об'єктів відповідно до реалізованої політики безпеки інформації. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне подання (форма, синтаксис). Об'єкт характеризується своїм станом (змістом), що в свою чергу характеризується атрибутами, і поводженням, яке визначає засоби зміни стану.

Таблиця 1.5 – Рівні надання послуги «Конфіденційність при обміні» [60]

<table>
<tr><th>КВ-1. Мінімальна конфіденційність при обміні</th><th>КВ-2. Базова конфіденційність при обміні</th><th>КВ-3. Повна конфіденційність при обміні</th><th>КВ-4. Абсолютна конфіденційність при обміні</th></tr>
<tr><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати</td><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих</td></tr>
</table>

множину об'єктів і інтерфейсних процесів, до яких вона відноситься	інтерфейсних процесів
Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності	
КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається	
—	Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження
—	Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
—	і приймальника об'єкта
—	Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
—	і джерела об'єкта
—	Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника
Політика конфіденційності при обміні повинна включати опис інформації , яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів Повинен бути виконаний аналіз прихованих каналів обміну. Всі знайдені приховані канали обміну і максимальна пропускна здатність кожного із них мають бути документовані. Повинна бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення	

Локалізований КЗЗ (наприклад, операційна система з функціями захисту) розглядає тільки логічне подання об'єктів. Фізичне подання об'єктів захищене тільки від внутрішніх об'єктів, а не від впливу з боку зовнішніх сутностей (агентів). Захист від зовнішніх щодо ІТС загроз реалізується організаційними заходами і заходами фізичного захисту. До зовнішніх впливів схильні об'єкти, що зберігаються в енергонезалежній пам'яті (зовнішніх носіях).

У розподіленому оточенні не можна гарантувати, що зовнішній агент не може отримати доступ до фізичного подання об'єктів. Особливо це відноситься до ліній зв'язку (каналів взаємодії). Таким чином, необхідно, щоб об’єкти були захищені під час їх експорту із фізично безпечного оточення.

Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування (табл. 1.5). Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Так, реалізація даної послуги на рівні КВ-1 ([60], табл. 1.5) забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Реалізація даної послуги на рівні КВ-2 дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити криптографічне розділення каналів обміну і є необхідною для забезпечення взаємодії КЗЗ, що підтримують обробку інформації рівня секретної або реалізують різні політики безпеки.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити захист від компрометації за рахунок аналізу трафіку і від витоку інформації прихованими каналах обміну, що існують. Для реалізації даного рівня від розробника вимагається виконання аналізу прихованих каналів.

2) Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності.

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної ІТС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Адміністративна цілісність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів.

Відкат – можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану.

Цілісність при обміні дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування (таб. 1.6).

Таблиця 1.6 – Рівні надання послуги «Цілісність при обміні» [60]

ЦВ-1: Мінімальна цілісність при обміні	**ЦВ-2: Базова цілісність при обміні**	**ЦВ-3: Повна цілісність при обміні**
Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності		
КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається		
—	а також фактів його видалення або дублювання	
Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу		

—	і приймальника об'єкта
Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу	
—	і джерела об'єкта
Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження	
—	Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника

3) Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

Для того, щоб ІТС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної ІТС повинен надавати послуги щодо забезпечення можливості використання ІТС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність ІТС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в ІТС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Стійкість до відмов гарантує доступність ІТС після відмови її компонента.

Гаряча заміна дозволяє гарантувати доступність ІТС в процесі заміни окремих компонентів.

Відновлення після збоїв забезпечує повернення системи у відомий захищений стан після відмови або переривання обслуговування.

Використання ресурсів дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг для користувача (табл. 1.7).

Таблиця 1.7 – Рівні надання послуги «Використання ресурсів» [60]

<table>
<tr><td>Квоти</td><td colspan="2">ДР-2. Недопущення захоплення ресурсів</td><td>ДР-3. Пріоритетність використання ресурсів</td></tr>
<tr><td>Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="3">Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів КС</td></tr>
<tr><td colspan="4">Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються</td></tr>
<tr><td colspan="3">окремому користувачу</td><td>окремому користувачу і довільним групам користувачів</td></tr>
<tr><td colspan="4">Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td>—</td><td colspan="3">Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку</td></tr>
<tr><td colspan="3">окремого користувача</td><td>окремого користувача і довільних груп користувачів</td></tr>
</table>

4) Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості.

Для того, щоб ІТС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної ІТС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в ІТС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Реєстрація дозволяє контролювати небезпечні для ІТС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю,

складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до ІТС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації і наведені в табл. 1.8. Відомі три основних типу автентифікації: щось, відоме користувачеві; щось, чим володіє користувач; щось, властиве користувачеві.

Таблиця 1.8 – Рівні надання послуги «Ідентифікація і автентифікація» [60]

НИ-1. Зовнішня ідентифікація і автентифікація	**НИ-2. Одиночна ідентифікація і автентифікація**	**НИ-3. Множинна ідентифікація і автентифікація**
Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ		
Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен		
з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача	автентифікувати цього користувача з використанням захищеного механізму	автентифікувати цього користувача з використанням захищених механізмів двох або більше типів
—	КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування	

Згідно [60] пароль, персональний номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

Такі фізичні об'єкти як смарт-карта, магнітна картка, генератор запитів-відповідей, електронний ключ або фізично прошитий криптографічний ключ є прикладами того, що називається "дещо, чим володіє користувач".

Основною перевагою даного типу автентифікації є складність або висока вартість дублювання інформації автентифікації. З іншого боку, втрата пристрою автентифікації може стати причиною потенційної компрометації. Проте, в більшості випадків достатньо просто установити факт втрати такого пристрою і попередити адміністратора безпеки про необхідність зміни інформації автентифікації.

Результати таких біометричних вимірювань, як відбитки пальців, параметри райдужної оболонки ока або геометрія руки служать прикладами того, що називають "дещо, що властиве користувачеві". Реалізація даного типу автентифікації повинна забезпечувати значно сильнішу автентифікацію, ніж два попередніх типи. Основною перешкодою для використання даного механізму є висока вартість пристроїв автентифікації. Крім того, використання цих достатньо дорогих засобів автентифікації не гарантує безпомилкової роботи. Рівень (ймовірність) помилок першого і другого роду для таких пристроїв може стати непридатним для деяких застосувань.

Для підвищення ефективності захисту від специфічних загроз несанкціонованого доступу для найбільш високого (3-го) рівня даної послуги вимагається використання комбінації мінімум двох різних типів автентифікації, наприклад, введеного з клавіатури пароля і носимого ідентифікатора.

Достовірний канал дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Розподіл обов'язків дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні

даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Ідентифікація і автентифікація при обміні. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації і наведені в табл. 1.9.

Таблиця 1.9 – Рівні надання послуги «Ідентифікація і автентифікація при обміні» [60]

НВ-1: Автентифікація вузла	**НВ-2: Автентифікація джерела даних**	**НВ-3: Автентифікація з підтвердженням**
Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації		
—	КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується	
—		Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною

Реалізація рівня НВ-1 [60] даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні. Реалізація рівня НВ-2 даної послуги дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення. Реалізація рівня НВ-3 даної послуги дозволяє виключити можливість деяких видів внутрішнього шахрайства.

Автентифікація відправника. Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною і наведені в табл. 1.10.

Таблиця 1.10 – Рівні надання послуги «Автентифікація відправника» [60]

НА-1: Базова автентифікація відправника	**НА-2: Автентифікація відправника з підтвердженням**
Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною
Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною

Найширше для реалізації даної послуги, як і послуги автентифікації одержувача, використовується цифровий підпис, оскільки використання несиметричних криптоалгоритмів (на відміну від симетричних) дозволяє забезпечити захист від внутрішнього шахрайства і автентифікацію за взаємної недовіри сторін. Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація.

Автентифікація отримувача. Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною (табл. 1.11).

Таблиця 1.11 – Рівні надання послуги «Автентифікація отримувача» [60]

НП-1: Базова автентифікація отримувача	**НП-2: Автентифікація отримувача з підтвердженням**
Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для однозначного підтвердження факту одержання об'єкта
Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій системи.

Наведені вище критерії будуть використовуватися нижче (розділ 6) для оцінки ступеня захищеності інформаційно-телекомунікаційної системи, побудованої на основі мережі 5G. Другим критерієм оцінювання захищеності був обраний рівень перекриття атак і вразливостей в мережі 5G. Розглянемо більш детально архітектуру безпеки і типові вразливості в мережі 5G.

1.7 Архітектура безпеки в мережі 5G

Сучасну архітектуру безпеки мобільної мережі 5G можна представити у наступному вигляді (рис. 1.18).

Архітектура безпеки поділена на 3 логічні рівні в залежності від їх мережевих особливостей, що дозволяє змогу досягти комплексної захищеності існуючих сервісів та надає змогу планувати нові заходи безпеки в існуючих моделях. Згідно з 3GPP архітектура безпеки 5G поділена на 5 основних доменів [63-65]:

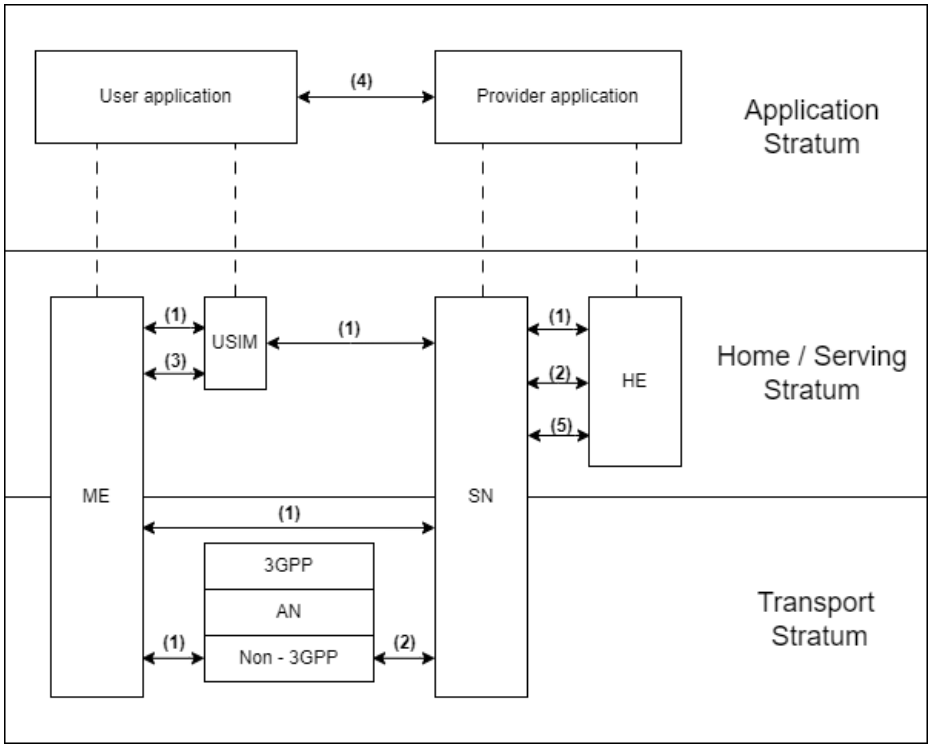


Рис. 1.18. Архітектура безпеки мережі 5G [63-65]

- Захист доступу до мережі – заходи безпеки, що надають користувацькому обладнанню можливість безпечно автентифікуватись й отримувати доступ до мережі, по різним (3GPP і Non-3GPP) технологіям доступу та передачі контексту безпеки від мережі до користувача.
- Захист мережевих доменів – заходи безпеки, орієнтовані на мережеві вузли, що являють собою функції обміну сигналами та користувацькими даними.
- Захист користувацького домену – функції, що забезпечують безпечне використання користувацького обладнання.
- Захист домену застосунків – заходи безпеки, що дозволяють застосункам (домени користувачів і провайдерів) безпечно обмінюватись повідомленнями.

• Захист доменів – функції, що забезпечують безпеку реєстрації, авторизацію елементів мережі, а також сервісно-орієнтованих інтерфейсів.

• Спостережність та контрольованість безпеки – функції, що інформують користувача про поточний стан засобів безпеки.

Основні класи управління безпекою – це управління ідентифікацією та доступом, забезпечення автентифікації, відмовостійкісті, конфіденційності, цілісності, доступності та приватності інформації, також необхідний аудит та відповідність вимогам (будуть наведені нижче). Механізми захисту, засновані на класах управління безпекою – це, наприклад, надання довгострокових (IMSI у 3GPP) та короткострокових (TMSI або GUTI у 3GPP) ідентифікаторів для управління ідентифікацією та доступом; AKA в 3GPP та HTTP Digest для автентифікації користувачів або використання асиметричної криптографії та цифрових підписів для забезпечення відмовостійкості.

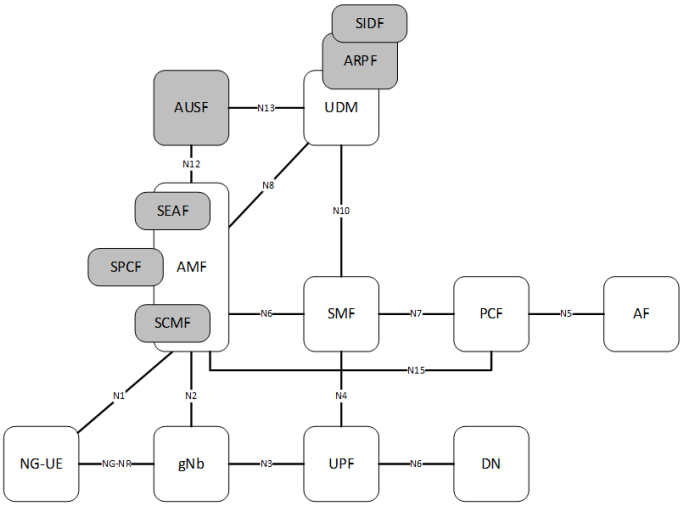


Рис. 1.19. Архітектура побудови опорної мережі 5G та компоненти безпеки

Концепція безпеки мобільних мереж 5G ґрунтується на перевикористанні технологій, прийнятих у стандарті 4G. На рис. 1.19 [66] наведено загальну архітектуру побудови ядра мережі 5G з виділеними

темним кольором функціональними об'єктами, що реалізують механізми безпеки.

Охарактеризуємо коротко об'єкти, що реалізують механізми безпеки:

1. *Security Anchor Function (SEAF)* – якірна функція безпеки – забезпечує автентифікацію обладнання користувача (разом з AUSF) при його реєстрації в мережі для будь-якої технології доступу.

2. *Authentication Server Function (AUSF)* – функція сервера аутентифікації – відіграє роль сервера аутентифікації, термінуючи запити SEAF і транслюючи їх в репозиторій облікових даних аутентифікації (ARPF).

3. *Authentication Credential Repository and Processing Function (ARPF)* – репозиторій облікових даних аутентифікації забезпечує зберігання персональних секретних ключів та параметрів криптографічних алгоритмів, а також генерацію векторів аутентифікації відповідно до алгоритмів 5G-AKA або EAP-AKA. Розміщується у захищеному від зовнішніх фізичних впливів центрі обробки даних оператора зв'язку, може бути інтегровано в уніфіковану базу даних (UDM).

4. *Security Context Management Function (SCMF)* – функція керування контекстом безпеки.

5. *Security Policy Control Function (SPCF)* – функція управління політикою безпеки – забезпечує узгодження та застосування політик безпеки щодо обладнання користувача. При цьому в розрахунок приймаються можливості мережі, можливості обладнання користувача та вимоги конкретної послуги. Застосування політик безпеки включає: вибір AUSF, вибір алгоритму аутентифікації, вибір алгоритмів шифрування даних і контролю цілісності, визначення довжини і життєвого циклу ключів.

6. *Subscription Identifier De-concealing Function (SIDF)* – функція вилучення ідентифікатора користувача.

Процедура автентифікації та узгодження ключів (Authentication and Key Agreement – AKA) застосовується для виконання взаємної автентифікації між обладнанням користувача та мережею, а також генерація ключа функції безпеки KSEAF. Одного разу згенерований ключ KSEAF може використовуватися для формування кількох сеансів безпеки.

Ініціація та вибір методу автентифікації. Відповідно до політики безпеки оператора зв'язку функціональний модуль SEAF може ініціювати автентифікацію обладнання користувача в рамках будь-якої процедури, що передбачає встановлення сигнального з'єднання, наприклад, при реєстрації в мережі (attach request), або оновленні локації (tracking area update).

Для автентифікації обладнання користувача SEAF використовує раніше створений і ще незадіяний вектор автентифікації, або надсилає запит "Authentication Initiation Request" (5G-AIR) в AUSF. Далі AUSF перевіряє правомочність використання імені обслуговуючої мережі (SN-name) та при успішній перевірці – транслює отриманий запит до уніфікованої бази даних UDM, де (за потреби) виконується розшифровування прихованого ідентифікатора користувача, після чого здійснюється вибір відповідного алгоритму автентифікації.

Загалом концепція безпеки 5G має включати:

1) взаємну автентифікацію користувача та мережі.

2) процедуру узгодження криптографічних ключів між мережею та обладнанням користувача.

3) Шифрування та контроль цілісності сигнального трафіку на рівнях RRC (між UE та gNb) та NAS (між UE та AMF).

4) Шифрування та контроль цілісності трафіку користувача (між UE та gNb).

5) Захист ідентифікатора користувача та захист інтерфейсів між різними елементами мережі відповідно до концепції домену безпеки, описаного в рекомендації 3GPP TS 33.310 [67].

6) Ізоляцію різних шарів архітектури (Network slicing) та визначення для кожного шару власного рівня безпеки.

1.8 Аналіз вразливостей мережі 5G, існуючих загроз і методів їм протидії

Під час аналізу актуальних атак на 5G в першу чергу потрібно звернути увагу на вже існуючі атаки в минулих стандартах. Певні проблеми пов'язані з самою особливістю мобільних мереж й не мають остаточно методу вирішення, починаючи з самого початку. Проте боротьба з іншими активно просувається, винаходяться нові стандарти безпеки й технології протидії.

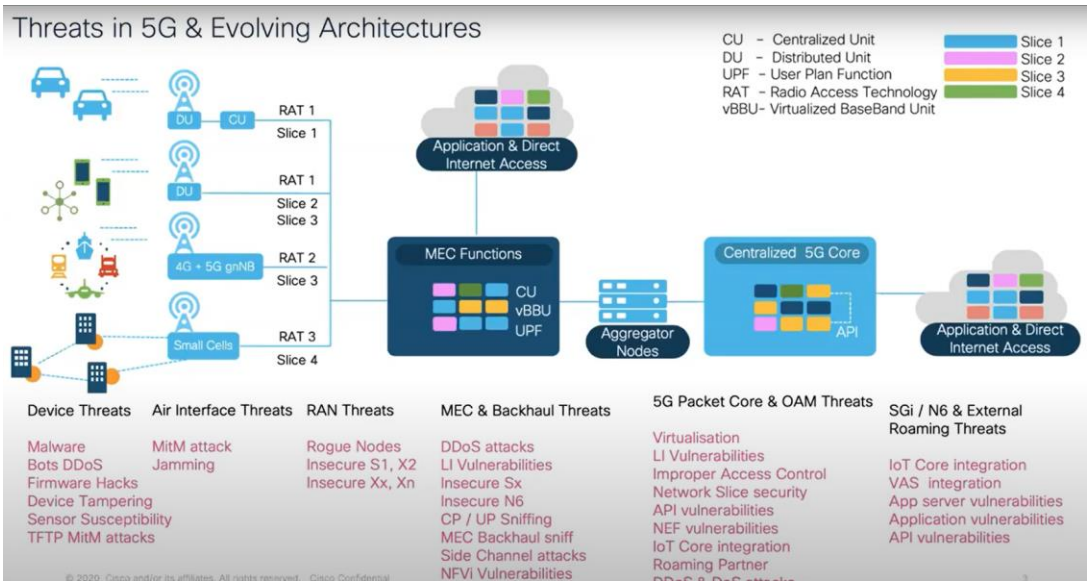


Рис. 1.20. Класифікація загроз в мережі 5G [65]

Згідно [63-65,72,77] атаки на 5G мережу можуть бути класифіковані на декілька груп (рис. 1.20):

- 5G загрози пов’язані зі звичайним та масовим інтернетом речей (*IoT/mIoT threats*);
- загрози обладнанню користувача (*UE threats*);
- загрози ядру мережі (*Core network threats*);
- загрози радіочастині і базовим станціям (*RAN threats*), в тому числі фейкові базові станції (*Rogue Base Station Threat)*;
- загрози конфіденційності абонентів;
- загрози новітнім мережним функціям (*Slicing, NFV, SDN threats*);
- загрози міжмережній взаємодії та роумінгу (*Interworking and roaming threats*).

Розглянемо кожну з наведених груп більш детально.

1.8.1 Загрози пов’язані зі звичайним та масовим інтернетом речей

MIoT охоплює широкий спектр нових і захоплюючих можливостей, таких як автономний зв'язок транспортних засобів, інтелектуальні мережі, датчики дорожнього руху, зв'язок безпілотників, медичні датчики та доповнена і віртуальна реальність (AR/VR) [68, 69]. Можливості ринку MIoT, його унікальні вимоги і міркування щодо кібербезпеки безпосередньо впливають на архітектуру 5G. Хакери можуть використовувати вразливості "нульового дня" в пристроях MIoT для запуску DDoS-атаки (Distributed Denial of Service) на мережу 5G RAN. Це призведе перенавантаження вузла надмірною кількістю трафіку або виснаженням ресурсів. Ця атака є особливо актуально для мобільних мереж п’ятого покоління через очікуване підключення до мережі великої кількості пристроїв при реалізації MIoT.

1.8.2 Загрози обладнанню користувача

Різні атаки на користувацькі пристрої в мережах 5G можна розділити на чотири основні категорії [63-65]:

1. Атаки з мобільних пристроїв на інфраструктуру: Мобільний ботнет з великої кількості інфікованих пристроїв, керованих серверами управління і контролю (C&C) зловмисника, запускає DDoS-атаки на інфраструктуру 5G з метою зробити недоступними функції і сервіси мережі 5G.

2. Мобільний інтернет: Мобільний ботнет з великої кількості інфікованих пристроїв, керованих C&C-серверами, здійснює DDoS-атаки на загальнодоступні веб-сайти через мережу 5G.

3. З мобільного на мобільний: Низка заражених пристроїв здійснює атаки на інших мобільних клієнтів з метою спричинити відмову в обслуговуванні або поширення шкідливого програмного забезпечення (наприклад, вірусів, черв'яків).

4. Атака "Інтернет на мобільний": У цій атаці зловмисний сервер в Інтернеті атакує кожен користувацький пристрій за допомогою шкідливого програмного забезпечення, вбудованого в додатки або ігри з ненадійних магазинів додатків. Після завантаження та встановлення шкідливе програмне забезпечення дозволяє зловмиснику викрадати персональні дані, що зберігаються на пристрої, поширювати його на інші пристрої або керувати пристроєм для запуску атак на інші пристрої та мережі.

1.8.3 Загрози ядру мережі

Через свою архітектуру послуг на основі IP-технологій мережі 5G можуть бути вразливими до IP-атак, поширених в Інтернеті, включаючи DDoS-атаки. Крім того, велика кількість заражених мобільних пристроїв, керованих зловмисними серверами управління і контролю (C&C), можуть

здійснювати атаки як на рівні користувача, так і на рівні сигналізації на основні функції мережі 5G, щоб погіршити якість або зробити критичні послуги недоступними для легальних користувачів.

Функція управління доступом і мобільністю (AMF), функція сервера автентифікації (AUSF) і уніфіковане управління даними (UDM) є основними мережевими функціями в 5G. AMF надає послуги автентифікації, авторизації та управління мобільністю UE. AUSF зберігає дані для автентифікації UE, а UDM зберігає дані про підписку UE. Оскільки ці функції є критично важливими в 5G, DDoS-атака на ці функції з Інтернету або мобільного ботнету потенційно може значно знизити доступність послуг 5G або навіть спричинити відключення мережі.

1.8.4 Загрози радіочастині і базовим станціям

Ця група поєднує достатньо велику кількість загроз, які в свою чергу поділяються на [70,71]:

- викрадення конфігурації базової станції (sniffing base station configuration);
- перехоплення IMSI та іншого трафіку;
- глушіння сигналу;
- фейкові базові станції;

Викрадення конфігурації базової станції використовується злонамірником для конфігурації власної 5G станції і реалізації атаки фейкової базової станції. Вона виконується через перехоплення Master Information Block (MIB) та System Information Block (SIB), з яких девайс отримує всю інформацію про станцію: ідентифікацію станції та оператора, пріоритетні частоти, потужність та інші. Атака з викрадення налаштувань базової станції є однією з загроз, від якої дуже важко захиститись.

Перехоплення ідентифікатора абонента IMSI (International Mobile Subscriber Identity) можлива лише після проведення деградації мережі з 5G до 4G, оскільки в 5G цю проблему вирішили впровадженням Subscriber Permanent Identifier (SUPI). Перехоплення трафіку в 5G не використовується широко, оскільки потребує багато ресурсів і має маленьку потенційну область проведення атаки за рахунок меншого розміру стільників.

Глушіння сигналу базової станції є одним з методів блокування її роботи шляхом випромінювання сигналу або хвиль певної частоти, які заважають або порушують нормальне функціонування [63,72]. В 5G найчастіше застосовують глушіння саме Physical Broadcast Channel (PBCH). При його реалізації користувацькі пристрої не зможуть отримати доступ до критично важливої інформації, необхідної для підключення до станцій.

Атака фейкової базової станції (рис. 1.21) виконується через встановлення зловмисником станції мобільного зв’язку з налаштуваннями існуючих. Вона працює через відсутність будь-якої перевірки валідності станції перед підключенням.

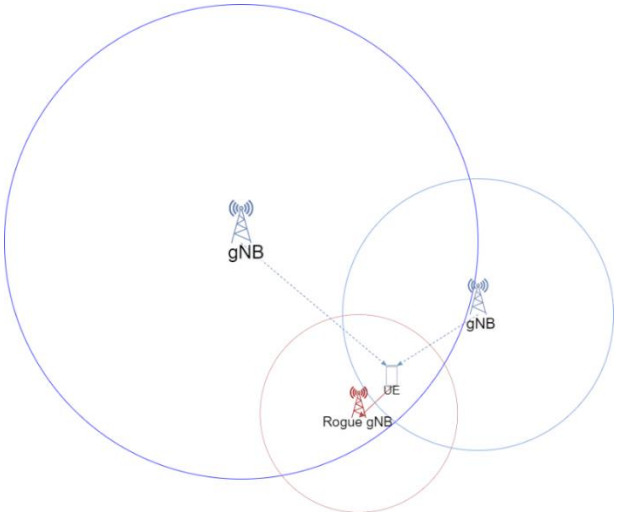


Рис. 1.21. Атака фейкової базової станції

Ця атака надає зловмиснику можливості виконувати атаку людина-посередині (MITM) через налаштування нешифрованого з'єднання з обмеженою швидкістю передачі й подальшим перехопленням трафіку. Також стає можливим DOS девайсів, а також мережевих ресурсів за допомогою ботнетів без загрози блокування від станції.

1.8.5 Загрози новітнім мережним функціям

Вразливості віртуалізації мережевих функцій полягають в розширенні поверхні атаки на 5G вразливостями віртуального середовища: атаки на оркестрацію, DoS та інші.

Вразливості площини керування полягають в присутності вразливості Web/API, витік облікових даних, несанкціонований доступ та передача даних, крадіжка даних.

До основної функції software-defined networking (SDN), впровадженого в 5G, полягає в розділенні керуючих площин (control planes) та площин передачі даних (data planes). На відміну від звичайних мереж, де кожний маршрутизатор та комутатор працюють незалежно, у SDN їх функції управління передаються на SDN-контролер, залишаючи тільки переадресацію. Тобто налаштування маршрутизації та переадресації мережі може бути виконано на рівні застосунку. Така архітектура надає гнучкості мережі, проте приносить і нові вразливості:

- Control plane – зловмисник може отримати політику переадресації мережевих пристроїв через аналіз показників продуктивності пристрою з площини управління.
- Data Plane – зловмисник може провести атаки на протоколи й девайси з площини передачі даних. Атаки на протоколи використовують вразливості мережевих протоколів.

1.8.6 Загрози міжмережній взаємодії та роумінгу

Атаки на сервіси роумінгу базується на можливість використання в мережах 5G старих сімкарт без “особливої безпеки”. Через вразливість вбудованих застосунків зловмисник може надіслати службове SMS й змусити пристрій переключитись на режим роумінгу, що в свою чергу надає можливість підключити його до фейкової базової станції в обхід прийнятих процедур безпеки.

1.8.7 Загрози конфіденційності абонентів. Вразливості систем віддаленої автентифікації користувачів через мережу 5G

Згідно з наведеним вище [60], реалізація біометричної автентифікації забезпечить кращий рівень захисту у порівнянні з іншими видами автентифікації. Розглянемо принцип роботи системи біометричної автентифікації та основні загрози та вразливості що виникають під час її виконання.

В загальному вигляді схема біометричної автентифікації [73] складається з етапів реєстрації (рис. 1.22) і перевірки (рис. 1.23). Система автентифікації в базі даних зберігає біометричні шаблони зареєстрованих користувачів, дані про них та інструкції щодо режиму доступу певних об’єктів. Біометричний датчик на вході зчитує унікальні біометричні характеристики користувача, система порівнює їх з тими, що внесені до бази даних, авторизує користувача та при співпадінні характеристик користувача з шаблоном, що внесений до бази даних, надає рішення щодо допуску до певної інформації/об'єктів/тощо.

Під час віддаленої автентифікації дані, що мають автентифікувати користувача, передаються мережею, під час чого можуть бути спотворені

завадами в каналах зв’язку та скомпрометовані в результаті різних типів атак. Біометричні характеристики людини є унікальними і невід'ємними.

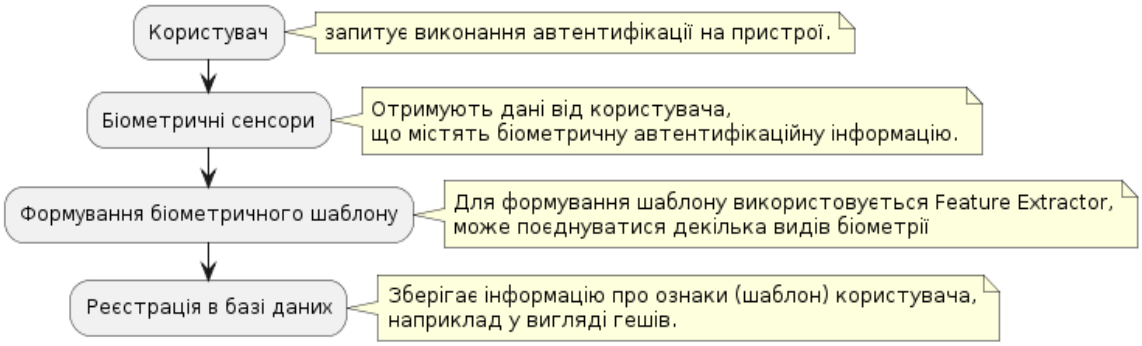


Рис. 1.22. Узагальнена схема біометричної автентифікації: фаза реєстрації

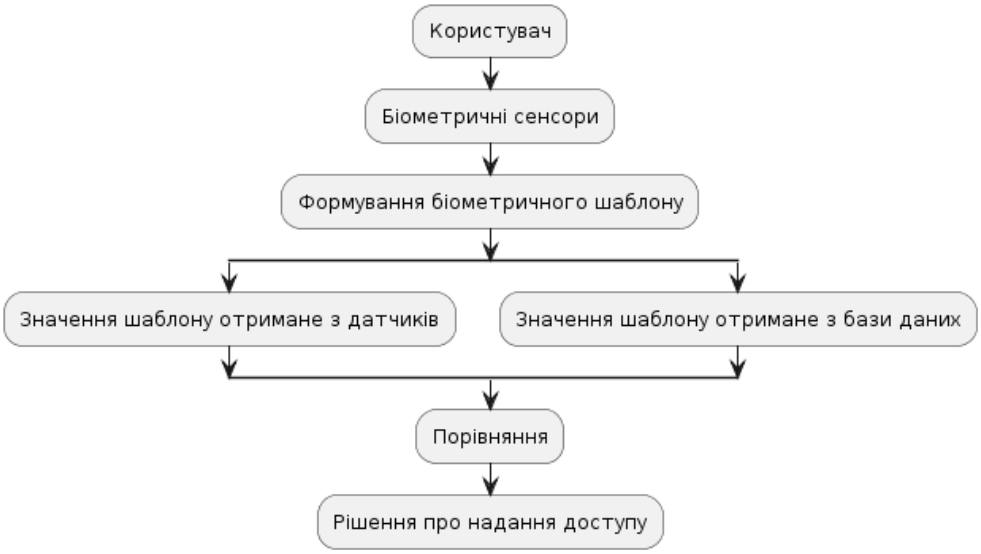


Рис. 1.23. Узагальнена схема біометричної автентифікації: фаза перевірки

Це дає великі переваги для вірного надання доступу при використанні цих характеристик, але вони не можуть бути замінені, тому передача їх у відкритому вигляді або навіть зашифрованому не є можливою.

На систему віддаленої автентифікації є можливими різні типи атак (рис. 1.24). В самому початку системи передачі даних можлива фальсифікація

даних (spoofing attack) – використання фальсифікованих біометричних характеристик користувача, поновлення та використання старих даних, які були використані раніше під час автентифікації. Також є ймовірність атаки у вигляді несанкціонованого доступу до сформованого біометричного шаблону під час автентифікації, його підміна або підміна шаблону (substitution attack) [74-76], який зберігається в базі даних.

Рис. 1.24. Можливі вразливості в системі віддаленої біометричної автентифікації

Небезпечною є атака маскарад (masquerade attack), коли цифровий образ може бути створений з шаблону біометричного образу. Також є ймовірність впливу з метою підміни рішення під час порівняння біометричних шаблонів.

Окрім вище зазначених атак, слід відмітити, що під час передачі даних каналом зв'язку є загроза того, що дані будуть перехоплені.

Під час спуфінгових атак зловмисник для отримання доступу в систему використовує штучно створені біометричні ознаки. Наприклад, маску

обличчя, надруковане зображення райдужної оболонки ока, тощо, або імітує поведінкові характеристики, що використовуються під час динамічної автентифікації, наприклад, динамічний підпис. Такі загрози виникають на етапі роботи з датчиками, що розпізнають особу, тому для захисту від таких загроз необхідним є використання мір, що будуть попереджати від розпізнавання підроблених зразків. Прикладом біометричних властивостей, які мають високий рівень захищеності від підробки є такі властивості, як температура, електрична провідність, пульсоксиметрія та опір шкіри.

Для боротьби зі спуфінгом на рівні пристроїв використовують апаратні методи. Вони полягають в інтеграції у сканер спеціальних апаратних пристроїв, які дозволять розпізнавати конкретні характеристики живих біометричних зразків (рухи ока, тепло пальців та ін.), також вони можуть перевіряти реакцію на зовнішні сигнали, що потребують наявність певного користувача. Наприклад, для того, щоб попередити використання підробних відбитків пальців, що створені зі штучного матеріалу сканери відбитків пальців використовують механізми виявлення підробних відбитків.

Для вирішення проблеми використання підроблених зображень використовують ідентифікацію користувачів за рухами зіниць, які виникають під час змін їх розмірів. На рівні функцій використовують програмні методи. Ці методи інтегруються в системі після сканерів. Робота таких методів полягає в екстракторі ознак і вони працюють вже з послідовностями ознак, які получено за певний проміжок часу.

Також під час перших етапів роботи системи автентифікації важливо уникнути можливості відновлення старих, введених іншим користувачем даних для отримання несанкціонованого доступу.

Для здійснення біометричної автентифікації після сканування певних біометричних ознак формується біометричний шаблон. Біометричний

шаблон – це цифрове представлення даних, що були вилучені з біометричного зразка. Вони зберігаються в базі даних та використовуються під час порівняння для автентифікації. Існує ризик поновлення створеного шаблону та використання старих даних. Є ймовірність підміни шаблону на інший та перехват шаблону в каналі зв'язку під час передачі, тому важливим завданням є захист шаблонів.

1.9 Висновки

1) Базуючись на аналізі складових інформаційно-телекомунікаційної системи на основі 5G, визначено її основні складові, такі як ядро мережі, радіомережу (включаючи канал зв’язку) і обладнання користувача. Показано, що поява нових джерел трафіку та впровадження нових сервісів, зумовлює підвищення вимог щодо швидкості та якості надання послуг, що в свою чергу вимагає удосконалення програмної частини ядра мережі та обладнання користувача.

2) Описано ключові сервіси та технології мережі 5G, до яких віднесені технологія мережних зрізів (network slicing), технологія граничних обчислень з множинним доступом (MEC), масовий Інтернет речей (mIoT), масивне MIMO і формування променів, а також віртуалізація мережних функцій (NFV). Обґрунтовано, що вдосконалення технології розподілу даних між елементами, що виконують їх обробку, може підвищити ефективність технології MEC, а вдосконалення методів класифікації трафіка дозволить покращити ефективність технологій мережних зрізів та віртуалізації мережних функцій. При цьому застосування завадостійких кодів дозволить зменшити рівень помилок і покращити якість надання послуг в рамках кожної з наведених технологій.

3) Проаналізовано узагальнену структурну схему інформаційно-телекомунікаційної мережі 5G, та показано місце в ній завадостійких коригуючих кодів. Наведена їх класифікація і описані завадостійкі коди, що застосовуються або можуть бути застосовані в мобільних мережах. Для вказаних завадостійких кодів оцінені їх властивості та характеристики, які потребують вдосконалення. Обґрунтовано перелік завадостійких кодів для дослідження та вдосконалення.

4) Визначені основні показники якості передачі даних у інформаційно-телекомунікаційних системах, які включають швидкість передачі пакетів, затримку передачі, тремтіння та рівень втрат пакетів. На основі аналізу джерел, показано, що більшість телекомунікаційних послуг, пов’язаних з пакетними даними потребують безперебійного сервісу з мінімальними втратами пакетів, при цьому бажано, щоб затримка не перевищувала декількох секунд. Таким чином для підвищення якості надання послуг в цілому, необхідно запропонувати моделі та методи для зменшення часу затримки, рівня помилок і втрат пакетів під час їх доставки.

5) Зменшення рівня помилок і втрат пакетів під час їх доставки можна досягти вдосконаленням методів завадостійкого кодування та застосуванням фонтанних кодів. Зменшення затримки під час обробки та передачі можна досягти вдосконаленням процедур класифікації трафіка, кластеризації та інтелектуальної обробки на основі заздалегідь заготовлених правил. Підвищення швидкості передачі пакетів може бути досягнуто застосуванням інтелектуальної системи управління зі зворотним зв’язком для контролю параметрів каналу зв’язку і вибору оптимальних за певних умов параметрів завадостійкого коду.

6) Визначено, що в 5G мережі підвищуються вимоги щодо показників захищеності інформаційно-телекомунікаційних систем через появу нових

загроз та реалізацію нових сервісів, а саме до конфіденційності, цілісності, доступності та спостереженості. Кожний з зазначених показників забезпечується набором власних послуг. Кожна з послуг має власні якісні критерії для оцінювання ступеню повноти її надання.

7) Реалізація біометричної автентифікації дозволяє забезпечувати значно сильнішу автентифікацію, ніж парольна автентифікація та автентифікація за допомогою фізичних об’єктів.

8) Реалізація вищого рівня послуги «ідентифікація та автентифікація при обміні» дозволяє виключити можливість деяких видів внутрішнього шахрайства.

9) Для інформаційно-телекомунікаційних систем на основі мережі 5G визначені основні вразливості та загрози, що можуть впливати на ступінь повноти надання послуг із захисту інформації. Окремо розглянуто вразливості та атаки на існуючі методи віддаленої автентифікації користувачів, визначені їх слабкі місця, які потребують вдосконалення.

2 КОМПЛЕКСНА МЕТОДОЛОГІЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТА ЯКОСТІ ПЕРЕДАЧІ Й ОБРОБКИ ДАНИХ

Інтелектуальна система управління обслуговуванням гібридних телекомунікаційних послуг в мережах 5G вирішує завдання організації процесів управління на принципово новому рівні відповідно до можливостей, опублікованих в архітектурі 5G RPP [89], що дозволить підготуватися до впровадження Smart Connectivity як платформи для Інтернету наступного покоління з використанням гнучкої інфраструктури з'єднання, полегшуючи при цьому управління обробкою і зберіганням даних користувачів, забезпечуючи якісне обслуговування і знижуючи енерговитрати.

Це вимагає комплексного підходу до забезпечення процесу надання якісних послуг та інтелектуальних інструментів управління, що враховують оцінку вимог і потреб в ефективній, безперебійній і безпечній інтероперабельності з обчислювальними ресурсами (наприклад, розподіленими центрами обробки даних, периферійними обчисленнями) і набором інноваційних пристроїв.

Також актуальним є завдання розробки методології, яка б враховувала взаємозв'язок між якістю обслуговування кінцевих користувачів та процесами розподілу обчислювальних ресурсів між віртуальними сутностями з урахуванням енергоефективності та продуктивності обчислювальних процесів [90]. Наразі віртуалізація мережевих функцій все ще потребує вирішення питань, пов'язаних з реалізацією віртуалізованих мережевих елементів [7], та питань, пов'язаних з масштабуванням мережі до великої кількості IoT-пристроїв з обмеженими ресурсами [91].

На ефективність та якість управління процесом обслуговування гібридних телекомунікаційних послуг у мережах 5G суттєво впливає розподіл завдань у комп'ютерних вузлах інформаційно-комунікаційної мережі 5G (рис. 2.1), який характеризується значним енергоспоживанням [92]. Мінливість навантаження, яка фіксується в сучасних інформаційно-комунікаційних системах, впливає на розміщення віртуальних машин, що відбувається постійно і в режимі реального часу, тому виникає потреба в оптимізації їх розміщення [94].

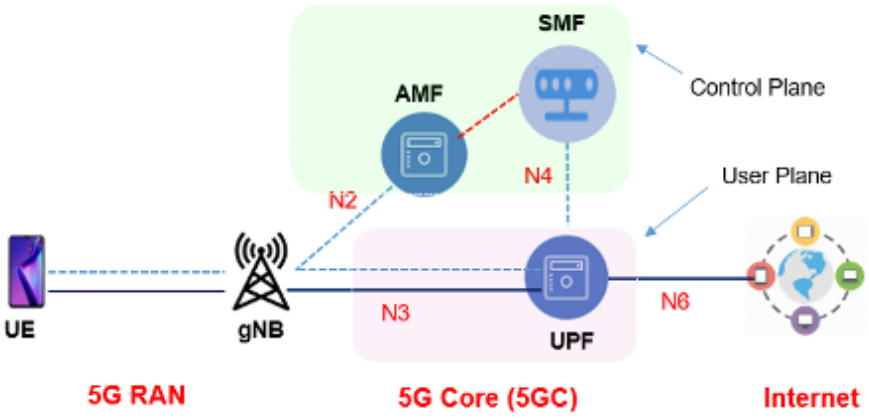


Рис. 2.1. Спрощена архітектура мобільної мережі

Інтелектуальні інструменти дозволяють інтегрувати елементи інформаційно-комунікаційного середовища, включаючи фізичні мережі, мережі SDN, вузли хмарних і туманних обчислень, сховища інформаційних ресурсів і сервісів, дотримуючись єдиного критерію якості обслуговування гібридних телекомунікаційних послуг в мережах 5G.

Наразі не існує комплексних технологічних рішень, які б одночасно враховували ефективність як комунікаційної, так і інформаційної складової, як єдиного фактору надання якісних послуг як на рівні користувача, так і в масштабах сучасних цифрових підприємств.

2.1 Цілі і методи управління якістю і захищеністю в системах мобільного зв’язку

Останнім часом багато робіт [111-118] присвячуються вдосконаленню якості послуг що надаються і захищеності даних користувачів. При цьому, зазвичай вдосконалюються окремі елементи [наприклад, 105,110,114-116] і не приділяється увага системі в цілому.

В даній роботі пропонується комплексна методологія та підхід до вдосконалення як окремих елементів так і системи мобільного зв’язку в цілому. Запропонована методологія забезпечує покращення наведених в розділі 1 показників якості (рівень помилок і втрат пакетів, швидкість передачі інформації, затримка передачі і обробки інформації) і показників захищеності (конфіденційність, цілісність, доступність та спостереженість).

Для підвищення значень показників якості запропоновано поетапне впровадження у вузлі мережі (рис. 2.1), наступних модифікацій (рис. 2.2):

- вдосконалення методів попередньої обробки даних у вузлах мережі, що дозволить підвищити точність класифікації і обробки трафіка та зменшити затримки на обробку;
- впровадження новітніх адаптивних методів класифікації трафіка, що дозволить підвищити ефективність використання мережних ресурсів під час застосування мережних зрізів (Network Slicing);
- впровадження нових методів розподілу трафіка на граничних елементах мережі, що дозволить підвищити якість застосування технології граничних обчислень з множинним доступом (Mobile Edge Computing);
- вдосконалення методів завадостійкого кодування пакетів під час їх передачі мобільною мережею, що дозволить зменшити рівень помилок і втрат пакетів.

Більш наочно взаємозв'язок запропонованих елементів та існуючих рішень показує рис. 2.2.

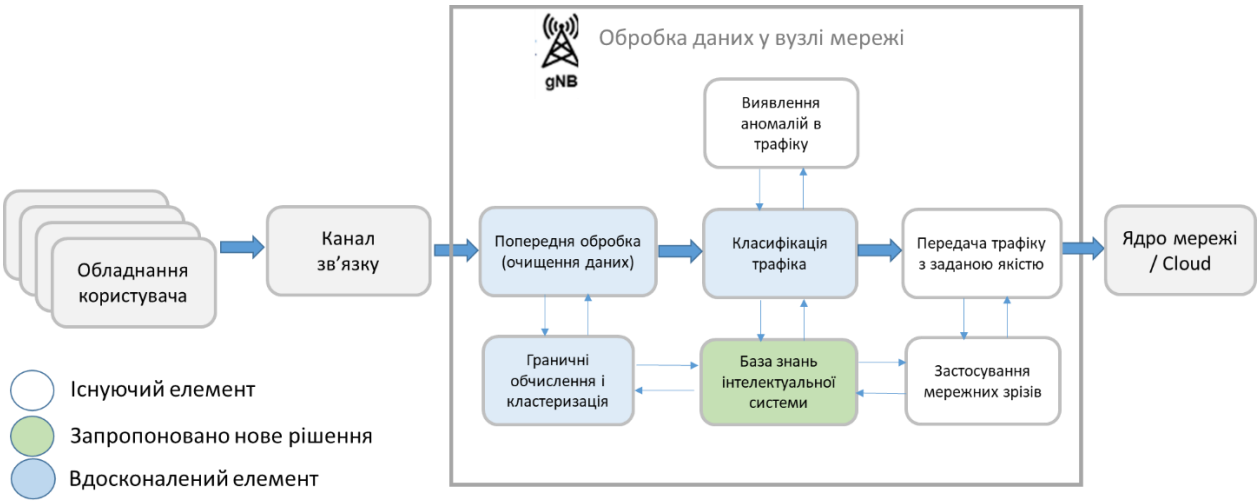


Рис. 2.2. Вдосконалення обробки даних у вузлі мобільної мережі

При цьому, в даній роботі вдосконалення методів завадостійкого кодування пакетів пропонується до реалізації у модемній частині обладнання користувача (рис. 2.3).

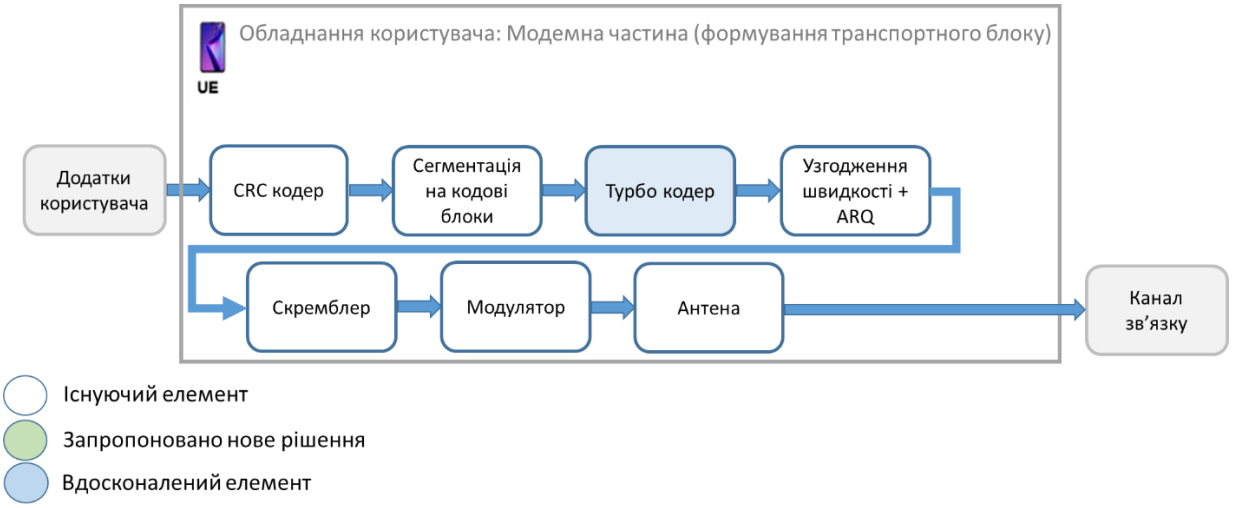


Рис. 2.3. Вдосконалення обробці даних в модемній частини обладнання користувача

Для вдосконалення показників захищеності, комплексна методологія пропонує поетапне впровадження у обладнанні користувача (рис. 2.1), наступних модифікацій (рис. 2.5):

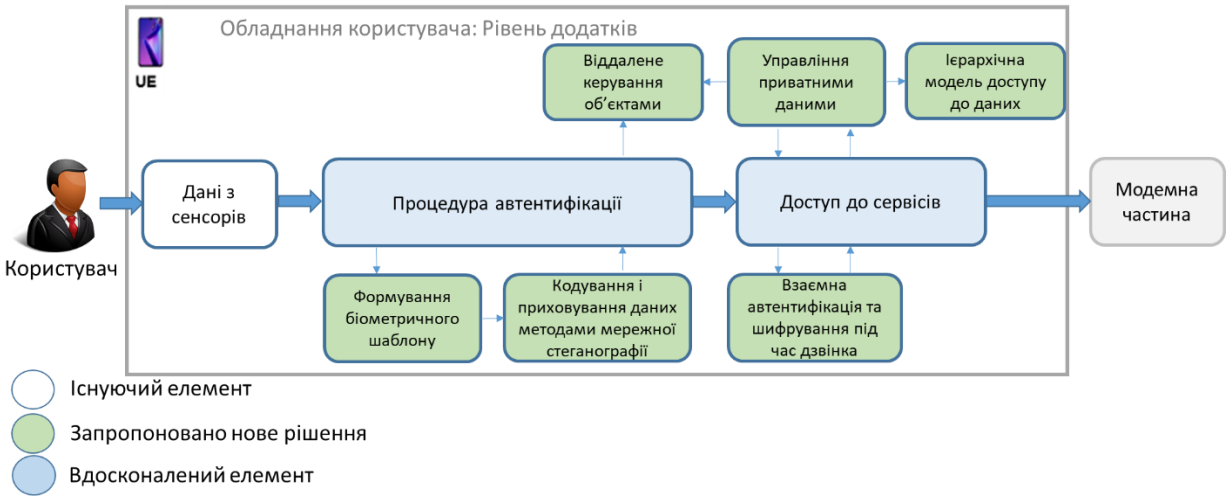


Рис. 2.4. Вдосконалення показників захищеності через зміни в програмній частині обладнання користувача

– вдосконалення методу формування біометричного шаблону користувача, в тому числі нового методу об'єднання різних біометричних ознак користувача;

– застосування додаткових методів завадостійкого кодування для підвищення завадозахищеності даних під час проходження процедури віддаленої автентифікації;

– застосування методів мережної стеганографії для підвищення прихованості 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, що дозволить підвищити рівень показника конфіденційності;

−впровадження нових методів управління приватними даними користувача для забезпечення захищеності під час реалізації нових сервісів.

Відповідно до запропонованої комплексної методології, підвищення захищеності та якості передачі даних в мобільній мережі (рис. 2.2-2.4), в наступних розділах будуть описані вдосконалення наведених елементів системи, описаної вище. Так, розділ 3 дисертаційної роботи присвячений вдосконаленню обробки даних на рівні вузла мобільної мережі (рис. 2.2). Розділ 4 висвітлює питання вдосконалення методів завадостійкого кодування (рис. 2.3), а розділ 5 присвячений підвищенню показників захищеності системи та даних користувача (рис. 2.4).

Оскільки базовим елементом для вдосконалення є саме інтелектуальна система управління, яка дозволяє виконувати попередню обробку даних (рис. 2.3), розглянемо її більш вдосконалення в першу чергу.

2.2 Узагальнена модель інтелектуальної системи для управління якістю в мережі мобільного зв’язку

Враховуючи всі особливості наступного покоління мереж зв'язку, а також гнучкі можливості, які надає віртуалізація мережевих функцій та рівень розвитку технології хмарних обчислень, в даному дослідженні запропоновано архітектуру мережі 5G, яка узагальнює основні тенденції розвитку мереж наступного покоління. Узагальнена архітектура мобільної мережі наступного покоління показана на рис. 2.5, особливістю якої є можливість застосування інтелектуального управління для всіх вузлів і підсистем мережі.

На рис. 2.5 показано сценарій, коли мобільний абонент зв'язується з ретранслятором R1, який перетворює радіосигнал в оптичний, далі сигнал надходить до ретранслятора R2, керованого SDN-контролером, який також знаходиться в дата-центрі. Потрапивши в дата-центр, сигнал обробляється віртуальною базовою станцією. Далі, згідно з технологією LTE, потік направляється в ядро оператора для подальшої обробки.

Підсистема BBU (блок генерації модуляційного сигналу) базується на технології програмно-конфігурованих мереж і віртуалізованих мережевих функціях. Це система, яка не тільки підтримує віртуальні базові станції, але також може бути використана для гібридних рішень 2G / 3G / 4G / 5G.

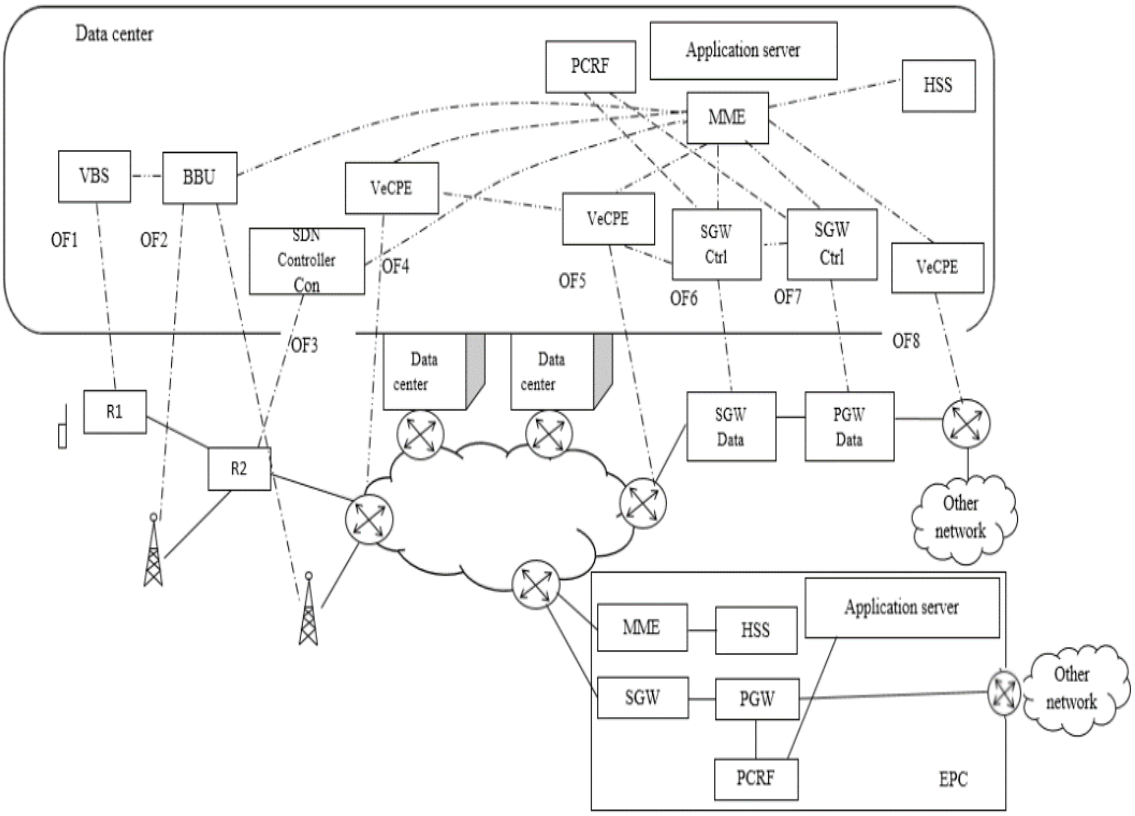


Рис. 2.5. Узагальнена архітектура мобільної мережі

Обслуговування в ядрі визначає подальший напрямок потоку даних. Якщо потік спрямований у внутрішню мережу оператора, то відразу в дата-центрі він направляється для обслуговування на відповідну віртуальну базову станцію, а потім через ретранслятори R2 і R1 відправляється до абонента. Якщо ж його призначення лежить за межами локальної мережі оператора, то потік спрямовується на віртуальний маршрутизатор локального кордону, який знаходиться безпосередньо в дата-центрі, після обслуговування в якому потік виходить в зовнішні мережі.

Таким чином, в даному підрозділі ставиться задача створення інтелектуальної системи розподілу ресурсів, яка буде:

- координувати якість зв'язку (через підготовку модифікованої системи розподілу ресурсів);
- використовувати онтологічну модель та систему нечіткої логіки для покращення обробки даних в модифікованій системі розподілу ресурсів;
- забезпечувати високий рівень безпеки (за допомогою врахування та впровадження підходів безпеки 5G).

2.3 Створення онтологічної моделі комплексної методології підвищення захищеності і якості

Підвищення захищеності і якості передачі й обробки інформації в інформаційно-комунікаційній мережі є складним процесом, на який впливають перелічені в розділі 1 фактори захищеності і фактори якості. При цьому, для оцінки цього процесу існує ряд показників та вимог щодо їх значень. Тому, виникає необхідність встановлення взаємозв’язків між впливаючими факторами та показниками ефективності досліджуваного процесу. Для цього необхідно побудувати модель процесу, що дозволила б

якісно аналізувати впливаючі фактори у сукупності. Серед існуючих методів формалізації складних систем було обрано онтологічну модель, яка дозволяє відображати складні взаємозв’язки у рамках досліджуваного процесу [292].

2.3.1 Аналіз існуючих підходів щодо формалізації складних систем та процесів

Існує багато підходів до формалізації складних систем. Зокрема, система може бути представлена за допомогою реляційної моделі, об'єктно-орієнтованої моделі [293], мережевої моделі або онтологічної моделі [292, 294].

Реляційна модель заснована на упорядкуванні даних у двовимірні таблиці. До її переваг слід віднести простоту та зручність реалізації. Основними недоліками реляційної моделі є відсутність стандартних засобів ідентифікації окремих записів та складність опису ієрархічних та мережевих взаємозв’язків між сутностями системи.

Об'єктно-орієнтована модель описується через такі поняття як клас і об'єкт. Класи визначають структуру даних і набір атрибутів (текстовий рядок, ціле число, зображення тощо). Екземпляри класу (об'єкти) зберігають внутрішню будову описану на рівні класу і можуть утворювати довільні ієрархічні структури. Як правило, системи, засновані на об'єктно-орієнтованій моделі даних, є функціональними, гнучкими, але в той же час більш складними, за рахунок того, що дочірній клас не може піідтримувати функції відсутні у батьківського класу.

Частково вирішити цю проблему дозволяє мережева модель, яка використовує графи для опису класів та відносин, що робить її більш гнучкою.

Онтологічна модель – це спроба всебічної та детальної формалізації певної галузі знань за допомогою концептуальної схеми [292]. За допомогою онтологічної моделі дані можуть бути представлені у вигляді сукупності різних типів інформаційних об’єктів та зв’язків між ними. Головною перевагою онтологічної моделі є те, що на відміну від об'єктно-орієнтованої та мережевої моделі, вона дозволяє детально описувати не лише класи та об'єкти, а й складні семантичні зв'язки між ними. Ці переваги дозволили обрати онтологічну модель для формалізації комплексної методології забезпечення захищеності та якості передачі й обробки даних.

2.3.2 Онтологічна модель системи мобільного зв’язку з урахуванням показників якості і захищеності

Онтологічна модель дозволяє структурувати та систематизувати дані необхідні для забезпечення захищеності та якості в мережі мобільного зв’язку та прозоро відобразити взаємозв’язки між параметрами системи для спрощення її аналізу та масштабування. Будучи структурованим поданням інформації в якійсь предметній області, онтологічна модель базується на необроблених вхідних даних, що зберігаються в певній інформаційній базі даних (рис. 2.6).

Прикладами таких вхідних даних є інформація про обмеження на втрати пакетів і затримку для певних додатків, інформація про стан каналу і типові налаштування завадостійких кодерів, тощо. Онтологічна модель перетворює ці необроблені дані у знання. Моделюючи систему обробки даних як онтологію, ми можемо виділити 3 окремі структурні частини системи. Ці частини відповідають трьом підкомпонентам онтологічної моделі відповідно: 1. Онтологія вхідних параметрів; 2. Онтологія показників оцінки якості системи; 3. Онтологія показників захищеності системи.

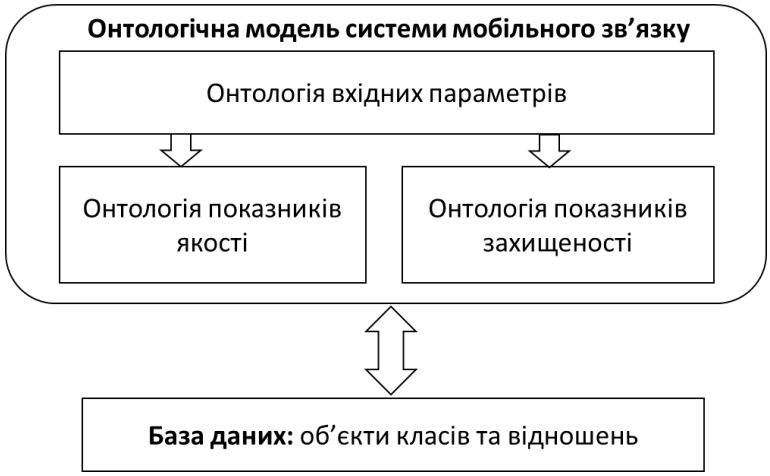


Рис. 2.6. Загальна структура запропонованої онтологічної моделі системи мобільного зв’язку з урахуванням показників якості і захищеності

Розглянемо запропоновані підсистеми окремо. Класи якості які мають певні обмеження і відповідають певним видам трафіку входять до підсистеми вхідних даних. Також до неї включені параметри зовнішнього середовища, які впливають на якість надання послуг. Крім вищенаведеного, онтологія вхідних параметрів охоплює частково джерела трафіку, оскільки вони генерують різні обсяги трафіку і впливають на параметр інтенсивності навантаження.

Онтологія показників оцінки якості системи охоплює опис тих параметрів, які оцінюються для системи та показують ефективність її функціонування. Для ефективної обробки системи мобільного зв’язку потрібно забезпечити низький рівень втрат пакетів, низький рівень мережної затримки і джитера, високий рівень середньої швидкості передачі.

Онтологія показників захищеності системи охоплює набір параметрів, що впливають на рівень захищеності системи в цілому і базується на

чотирьох основних показниках – конфіденційність, цілісність, доступність, спостереженість. Відповідні моделі якості та захищеності зображені на рис. 2.7 та рис. 2.8.

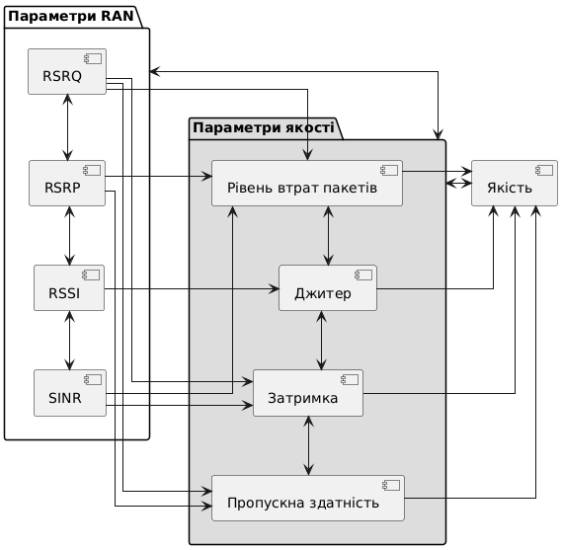


Рис. 2.7. Складові та взаємні впливи показників якості

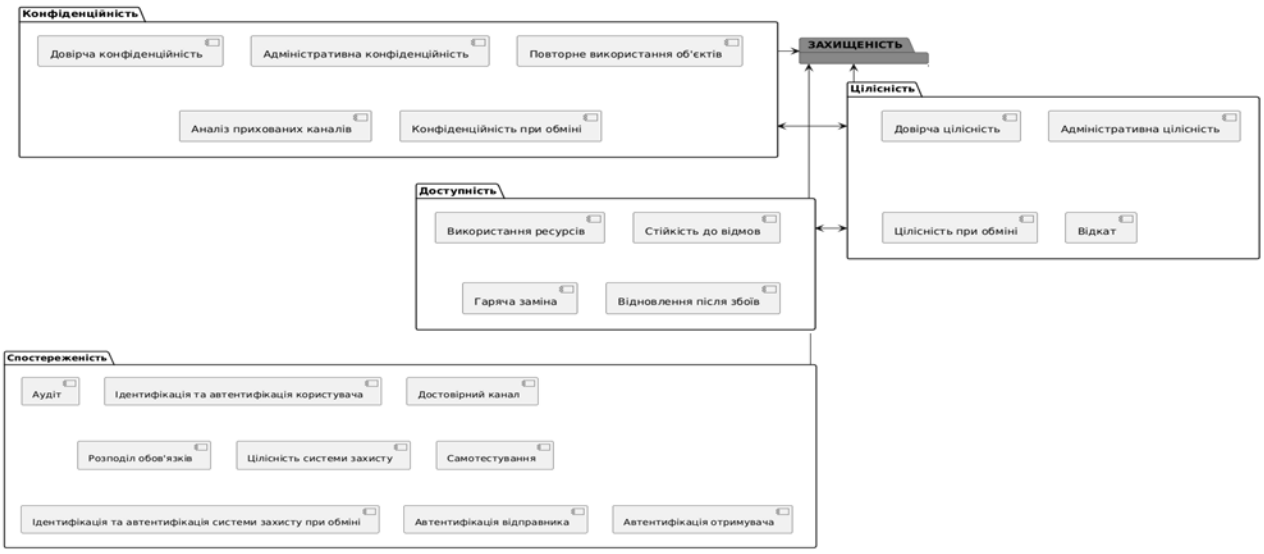


Рис. 2.8. Складові та взаємні впливи показників захищеності

На рис. 2.9 зображено запропоновану онтологічну модель системи, що формально описується за допомогою виразу:

$$O = \{C,A,R,T,F,D\}, \quad (2.1)$$

де C – множина класів; A – множина атрибутів; R– множина відношень; T – множина типів значень; F– множина обмежень на значення відношень; D – множина екземплярів класів.

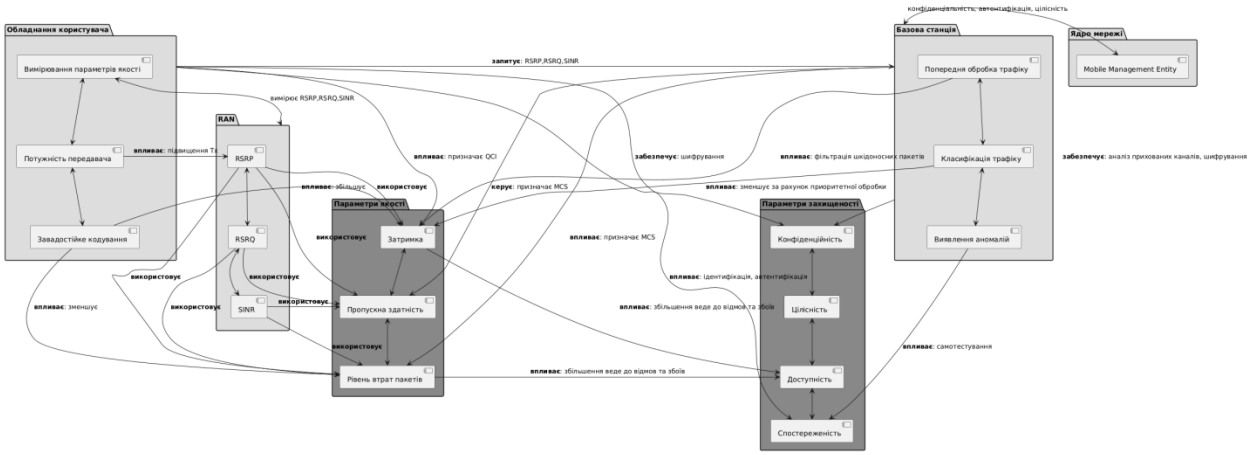


Рис. 2.9. Запропонована онтологічна модель системи розподіленого обслуговування навантаження інформаційно-комунікаційної мережі

При цьому, множина класів онтології: $C = \{C1, C2, \ldots, C_n\}$, де:

С1 – Клас обладнання користувача. Цей клас описує поняття обладнання користувача як фізичну сутність. До цього класу віддносяться суб’єкти, що можуть виступати в якості джерел трафіка

С2 – Клас обчислювальних вузлів для граничних розподілених обчислень. Є підкласом класу С1. До цього класу відносяться таке

обладнання користувача яке може виступати в якості обчислювальних вузлів граничних розподілених обчислень (наприклад смартфони або ноутбуки).

С3 – Клас мережа радіодоступу. До цього класу відносяться поняття, пов’язані з суб’єктами, що прямо або опосередковано визначають параметри якості системи мобільного зв’язку в цілому (сила сигналу, рівень шуму та інтерференції, тощо).

С4 – Клас базова станція. Включає мережу базових станцій на яких можуть бути розгорнуті різноманітні засоби впливу на якість і захищеність.

С5 – Клас ядро мережі. Цей клас відповідає за процеси керування в мережі. До нього відносяться мережні елементи які відповідають за вибір локації для обладнання користувача, його автентифікацію, хендовери.

С6 – Клас параметрів якості. Цей клас охоплює множину параметрів якості системи.

С7 – Клас параметрів захищеності. Цей клас охоплює множину параметрів захищеності системи.

Для вказаних класів доступні наступні асоціативні відношення:

“використовує” – відображає зв’язок між класами Мережа радіодоступу та Параметри якості та показує пряме або опосередковане використання мережею радіодоступу параметрів якості для забезпечення найкращих налаштувань ефективності;

“впливає” – зв’язок показує відношення між різноманітними класами;

“керує” – відображає опосередкований зв’язок між класами Базова станція та елементом затримка класу Параметри якості;

“визначає” – цей зв’язок описує відношення між класом Ядро мережі та Обладнання користувача. Суть цього зв’язка полягає у відображенні впливу параметрів якості мережі на налаштування мобільного пристрою.

Відношення “частина-ціле”. Відношення „частина-ціле” визначаються між класами «Обчислювальні вузли МЕС» та «Обладнання користувача».

Запропонована онтологічна модель дозволяє систематизувати та якісно описати складні взаємозв’язки між показниками ефективності досліджуваного процесу обслуговування навантаження в інформаційно-комунікаційній мережі та параметрами, що впливають на них. Однак, постає необхідність кількісного опису цих взаємозв’язків та кожного з впливаючих параметрів. Тому необхідно визначити моделі та методи, які дозволяють вплинути на наведені вище параметри якості і захищеності.

2.4 Вдосконалена інтелектуальна система для попередньої обробки даних та кластеризації

2.4.1 Загальний опис запропонованої інтелектуальної системи

Наразі актуальним є завдання розробки методології, яка б враховувала взаємозв'язок між якістю обслуговування кінцевих користувачів та процесами розподілу обчислювальних ресурсів між віртуальними сутностями з урахуванням енергоефективності та продуктивності обчислювальних процесів. Вказане завдання вирішується шляхом створення інтелектуальної системи розподілу ресурсів. Розробка інтелектуальної системи розподілу ресурсів (ICPP) передбачає інтеграцію інтелектуальних інструментів управління для обслуговування гібридних телекомунікаційних послуг різної природи в інформаційно-комунікаційному середовищі 5-го покоління.

Такі інструменти враховують оцінку вимог і потреб в ефективній, безперебійній і безпечній взаємодії з обчислювальними ресурсами (наприклад, розподіленими центрами обробки даних, периферійними обчисленнями) і різноманітними пристроями. Інструменти інтелектуального

управління дозволять інтегрувати елементи інформаційно-комунікаційного середовища, включаючи фізичні мережі, мережі SDN, хмарні і туманні обчислювальні вузли, сховища інформаційних ресурсів і сервісів, дотримуючись єдиного критерію якості обслуговування гібридних телекомунікаційних послуг в мережах 5G. Використання інструментів інтелектуального управління в процесі проектування ICPP дозволить інтегрувати сучасні технології та архітектури, забезпечити мінімальну затримку та заданий рівень якості обслуговування при наданні послуг кінцевим користувачам.

Впровадження засобів інтелектуального управління в структурі ICPP реалізує поставлені завдання:

- семантичне зв'язування мережевих інформаційних ресурсів,

- аналітична підтримка пошуку та аналізу великих обсягів розподіленої інформації,

- інтеграція моделей обслуговування клієнтів,

- енергоефективний розподіл ресурсів,

- контроль вхідного навантаження на використання ресурсів сервісних підсистем,

- планування та прогнозування потреб користувачів у майбутніх періодах.

Інструментами інтелектуального управління в дослідженні є програмні та апаратні засоби, розроблені з використанням сучасних моделей і методів штучного інтелекту. Сьогодні спеціалізовані технології на основі штучного інтелекту використовуються для розробки інформаційних систем різного роду і призначення. Технології штучного інтелекту також пропонують широкий спектр спеціалізованих моделей, методів і технологічних засобів для зберігання, оперування, аналізу та оптимізації великих обсягів інформації

[99]. Моделі та методи штучного інтелекту, покладені в основу ІСРР, представлені на рис. 2.10 [119].

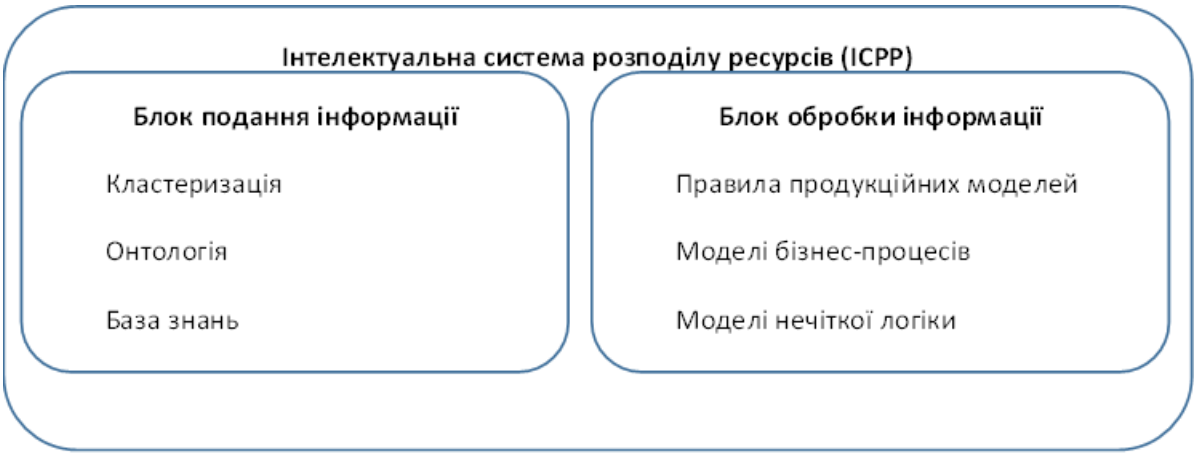


Рис. 2.10. Запропонована модель інтелектуальної системи розподілу ресурсів

Кожен елемент набору інтелектуальних моделей та методів, показаний на рис. 2.6, виконує певну функцію в ІСРР, а саме:

1. Кластеризація використовується в методі енергоефективного розподілу ресурсів, що підвищує енергоефективність обробки вхідного навантаження розподіленими обчислювальними системами при забезпеченні високого рівня обчислювальної продуктивності та дотримання вимог до якості обслуговування [100].

2. Онтологія інтегрує всі наявні компоненти інформаційно-комунікаційної системи та інтелектуальні компоненти управління процесами надання гібридних телекомунікаційних послуг і дозволяє динамічно формувати сценарії обслуговування в мережах 5G [101].

3. База знань виступає центральним репозиторієм і зберігає інформацію, якою оперує ІСРР, експертні правила, метаописи послуг та бізнес-процесів.

4. Дерева рішень реалізують механізми інтелектуального планування та прогнозування потреб користувачів у наступні періоди часу.

5. Правила дозволяють реалізувати механізми підтримки прийняття рішень (на основі експертних правил) щодо визначення обсягів вхідного навантаження для використання ресурсів підсистем обслуговування, які дозволять забезпечити обслуговування із заданими показниками якості.

6. Моделі бізнес-процесів реалізують формування послідовності надання послуг при динамічному формуванні сценаріїв обслуговування абонентів в мережах 5G, а також підвищують якість послуг за рахунок автоматизованого розрахунку оцінки якості їх надання.

7. Методи нечіткої логіки покладено в основу алгоритму оцінки поточного стану надання послуг оператором зв'язку. В основу такого алгоритму покладено інтегральний показник якості надання послуг. Мета досягається методами нечіткої логіки для спільного врахування впливу чітких та нечітких параметрів [102].

8. Механізми логічних висновків дозволяють зробити висновки про інформаційний простір онтологічної моделі, що забезпечує реалізацію зв'язності всіх елементів ІСРР, інформації та послуг.

9. Семантичний пошук забезпечує пошук великих обсягів розподіленої інформації на основі онтології, бази знань та дерев рішень.

Застосування онтологічного підходу при проектуванні ІСРР дозволяє підвищити ефективність інтеграції всіх елементів інформаційно-комунікаційної системи в процесі управління сервісом гібридних телекомунікаційних послуг в мережах 5G. Використання онтологічної моделі дозволить структурувати та систематизувати дані та сервіси ІСРР з метою контролю та аналізу роботи телекомунікаційної мережі, процесів обслуговування послуг та використання ресурсів. Онтологічна модель як базова інтелектуальна складова ІСРР дозволяє динамічно формувати сценарії обслуговування послуг в мережах 5G. Завдяки застосуванню онтологічного

підходу до формування робочих процесів, оцінка якості надання послуг оператором телекомунікацій дозволить заощадити трудові, часові та фінансові витрати на реалізацію таких процесів.

2.3.2 Принцип роботи запропонованої інтелектуальної системи

Як показано на рис. 2.10 [119], запропонована модель інтелектуальної системи розподілу ресурсів складається з двох основних блоків – блоку подання інформації і блоку аналізу та обробки даних.

Блок подання інформації відповідає за візуалізацію отриманих результатів і їх відображення в зручній для користувача формі. Прикладом способу візуалізації є метаграф.

Блок аналізу та обробки даних готує отриману з мережі інформацію (наприклад, пакети, що підлягають класифікації чи трафік, що має бути розподілений по вузлах граничних обчислень) до ефективного застосування методів класифікації трафіка чи кластеризації.

Сутність такої підготовки полягає в попередній обробці, побудові правил нечіткої логіки, видаленні дублікатів і застосуванні інших процедур, що можуть підвищити ефективність класифікації чи розподілу трафіку (рис. 2.11).

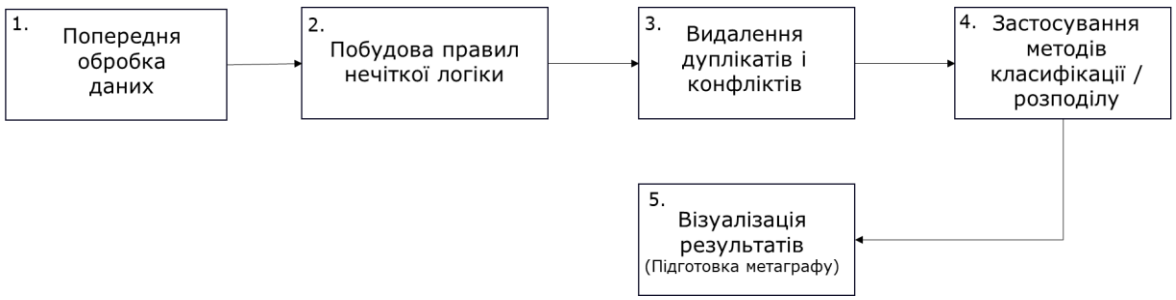


Рис. 2.11. Вдосконалена модель аналізу та обробки даних

Відповідно до рис. 2.11, попередня обробка наборів даних застосовує попереднє очищення даних від помилок, що випадково виникають. Підготовка нечітких логічних правил (відбувається за принципом вузлів і зв'язків) з використання алгоритмів класифікації / кластеризації дозволяє до початку роботи отримати рекомендації з використання тих чи інших алгоритмів і найкращі їх параметри, в залежності від зовнішніх умов, що дозволить під час роботи не витрачати час на пошук найкращого рішення, а згідно заздалегідь визначеним правилам підключити той чи інший алгоритм. Очищення масиву правил нечіткої бази знань від дублікатів і конфліктів необхідно для підвищення ефективності класифікації / кластеризації, оскільки неповні записи та викривлені пакети не зможуть бути правильно оброблені і призведуть до погіршення показників якості роботи системи (рис. 2.12). Після такої попередньої обробки, інформація потрапляє безпосередньо до методів класифікації / кластеризації і вже після отримання результату, він може бути для наочності додатково візуалізований за допомогою застосування онтологічної моделі для підготовки метаграфа (рис. 2.12).

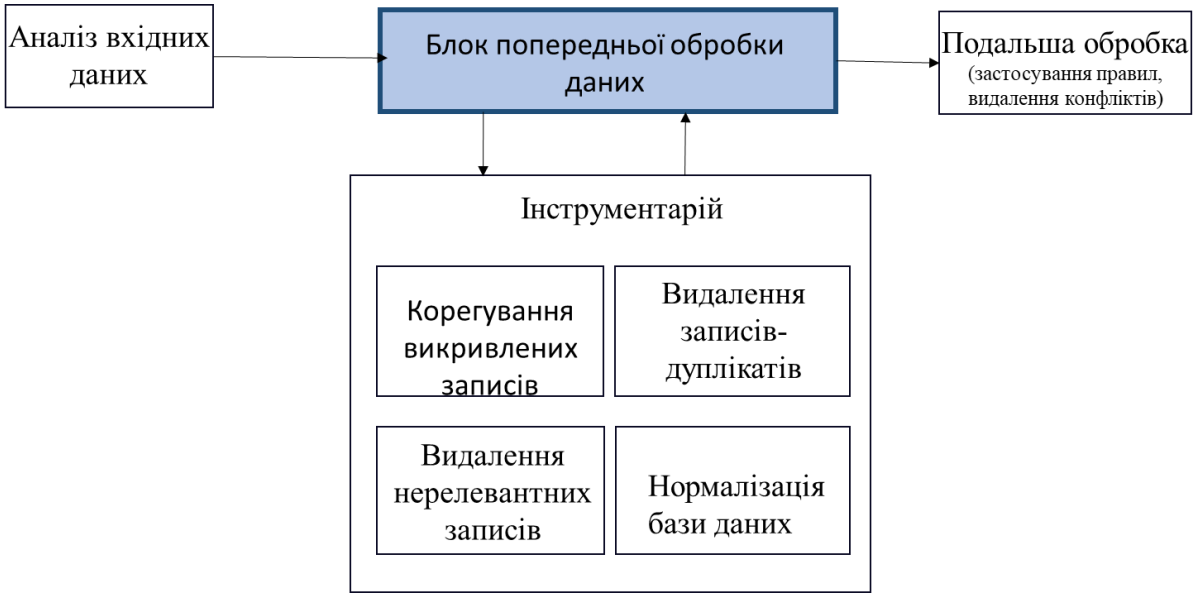


Рис. 2.12. Блок попередньої обробки даних

Онтологія інтегрує всі наявні компоненти інформаційно-комунікаційної системи та інтелектуальні компоненти управління процесами надання гібридних телекомунікаційних послуг і дозволяє динамічно формувати сценарії обслуговування в мережах 5G.

Для формування онтологічної моделі використовується наступна термінологія: характеристика об'єкта – набір правил на основі лінгвістичних змінних, при цьому під лінгвістичною змінною розуміють набір терм-вузлів (терм – опис значення параметра (наприклад, якість сигналу: низька, середня, висока)). Нехай

$V = \{v_r | r = \overline{1N_v}\}$ – набір терм-вузлів,

$M = \{m_q | q = \overline{1N_m}\}$ – набір мета-вузлів,

$E = \{e_h | h = \overline{1N_E}\}$ – набір ребер графа.

Використовуючи вищевказане можна отримати простий метаграф:

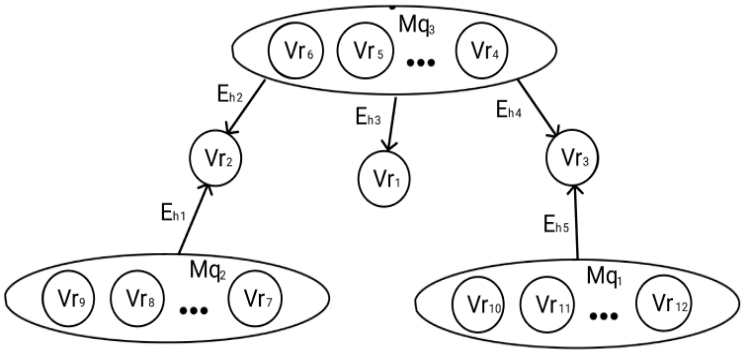


Рис. 2.13. Застосування онтології для побудови простого метаграфу

Використовуючи наведену вище онтологічну термінологію, та підхід наведений на рис. 2.13, отримаємо метаграф для інтелектуальної системи розподілу ресурсів (рис. 2.14).

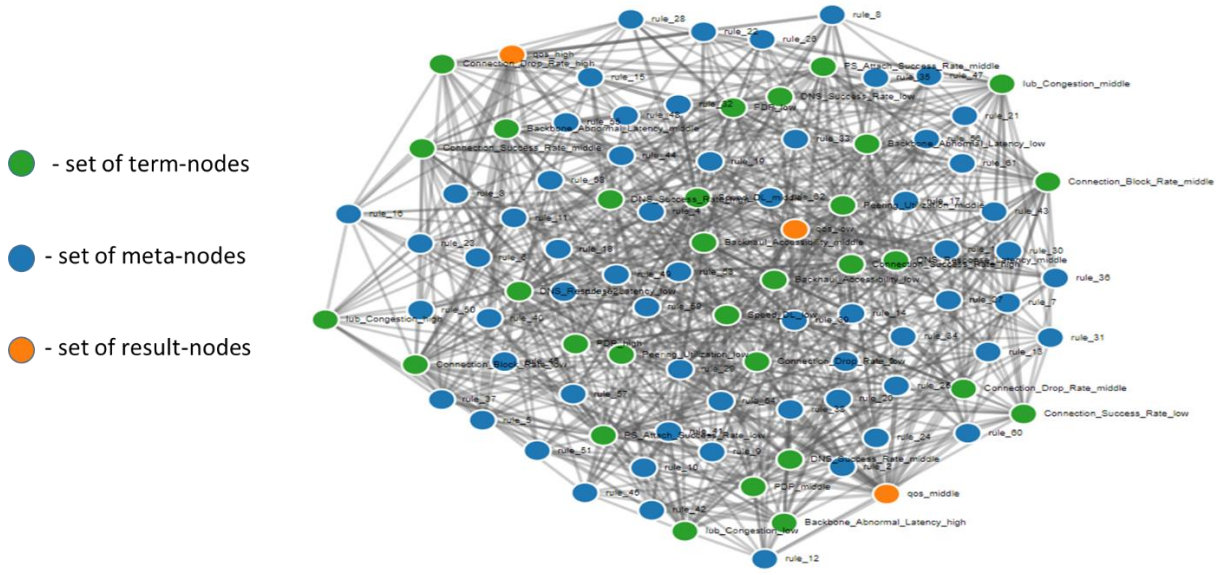


Рис. 2.14. Візуалізація результатів. Приклад метаграфа аналізованої системи

В подальшому з такого метаграфа можна отримувати зрізи, що відповідають актуальним задачам. В якості прикладу наведемо отриманий з метаграфа аналізованої системи (рис. 2.14) метаграф параметрів, які впливають на якість послуг в мережі 5G (рис. 2.15).

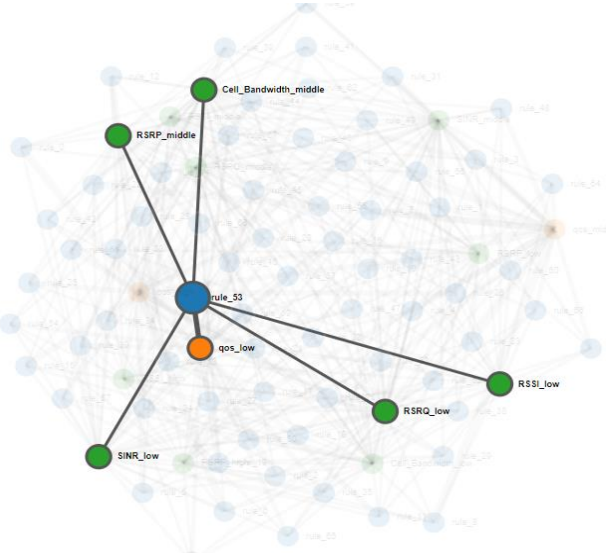


Рис. 2.15. Візуалізація результатів. Приклад метаграфа параметрів, що впливають на якість послуг в мережі 5G

2.5 Висновки

1. В даному розділі запропонована модель та підхід до вдосконалення як окремих елементів так і системи мобільного зв’язку в цілому. Вдосконалення полягає в покращенні наведених в розділі 1 показників якості (рівень помилок і втрат пакетів, швидкість передачі інформації, затримка передачі і обробки інформації) і показників захищеності (конфіденційність, цілісність, доступність та спостереженість).

2. Запропоновано інтелектуальну систему для попередньої обробки даних та управління в мережі мобільного зв’язку, яка дозволяє вдосконалили групу показників якості впровадженням у вузлі мережі методів завадостійкого кодування пакетів, методів попередньої обробки даних на вузлах мережі, новітніх адаптивних методів класифікації трафіка, а також нових методів розподілу трафіка на граничних елементах мережі.

3. Запропонована інтелектуальна система попередньої обробки даних, яка включає попереднє очищення даних від помилок, підготовку нечітких логічних правил, корегування даних та застосування онтологічної моделі.

4. В якості елементу інтелектуальної системи управління запропонована сукупність рішень для вдосконалення показників захищеності, які включають: вдосконалені методи формування біометричного шаблону та поєднання різних біометричних ознак користувача; застосуванням додаткових методів завадостійкого кодування та методів мережної стеганографії для підвищення захищеності та прихованості інформації; впровадженням нових методів управління приватними даними користувача для забезпечення захищеності під час реалізації нових сервісів; впровадження взаємної автентифікації користувачів та наскрізного

шифрування під час дзвінка, що перекриває ряд загроз пов’язаних із шахрайськими схемами підміни користувача.

5. Вдосконалено модель аналізу та обробки даних, шляхом застосування методів та технік нечіткої логіки та машинного навчання для попередньої обробки даних.

Новизна моделі полягає у попередньому очищенні даних від випадкових помилок, підготовці нечітких логічних правил за допомогою алгоритмів кластеризації, очищенні множини правил нечіткої бази знань від дублікатів та конфліктів і візуалізації за допомогою метаграфу, що дозволяє покращити показники якість класифікації даних на вузлах мережі, та пришвидшити їх обробку. Цей результат може бути використаний при виявленні аномалій у трафіку під час забезпечення захисту мережі.

3 ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ: ВДОСКОНАЛЕННЯ МЕТОДІВ ОБРОБКИ ДАНИХ

3.1 Постановка задачі вдосконалення обробки даних

Як було показано в розділі 1, до основних показників якості обслуговування та ефективності роботи мережі відносять швидкість передачі пакетів, затримку передачі, тремтіння та рівень втрат пакетів.

Процеси передачі пакетів по каналах зв'язку обмежені пропускною здатністю каналів і не вносять істотного впливу на сумарні значенні затримки передачі. Основний вклад в затримку передачі вносить час обробки пакетів у проміжних вузлах. Крім того, недостатньо ефективна обробка пакетів у проміжних вузлах також призводить до збільшення рівня втрат пакетів. Тому питання вдосконалення обробки пакетів у проміжних вузлах є надзвичайно важливими та актуальними. При цьому під процесом обробки будемо розуміти попередню обробку пакетів, класифікацію трафіку в залежності від затребуваної якості обслуговування, джерела трафіка і інших параметрів, описаних в розділі 1, а також кластеризацію і розподілені обчислення кожного типу трафіку для покращення швидкодії.

Нехай обробка пакетів в базовій станції мобільної мережі визначається наступними параметрами:

$\boldsymbol{n}$ – множина алгоритмів класифікації трафіка, точність ($\boldsymbol{Acc}$) яких визначається через гіперпараметри ($\boldsymbol{hyp}$)

$\boldsymbol{T_{зат}}$ – затримка на обробку трафіка у вузлі мережі складається з часу на класифікацію трафіка ($\boldsymbol{T_{клас}}$), часу очікування в черзі ($\boldsymbol{T_{очік}}$), згідно приоритету та інтенсивності навантаження ($\boldsymbol{\lambda}$).

$\boldsymbol{T_{обр}}$ – початкове значення часу на попередню обробку трафіка у вузлі мережі;

$\boldsymbol{T_{клас}}$ – час на класифікацію трафіка у вузлі мережі в свою чергу залежить від розміру набору ознак за якими виконується класифікація $\boldsymbol{N_{oznak.}}$

Відповідно до вищенаведених вхідних даних, результуюча функція, яка ставить на меті мінімізацію затримки на обробку пакетів, набуває вигляду:

$$Result\_Func\_1 \rightarrow \min(T_{зат}) = \{[\max(\text{Acc}|\text{T}_{\text{клас}} \rightarrow \min)] \,\&\, [\text{T}_{\text{обр}} \rightarrow \min] \,\&\, [f(\text{T}_{\text{клас}} |\text{N}_{\text{oznak}}) \rightarrow \min] \,\&\, [f(\text{T}_{\text{клас}} |\text{n, hyp})] \rightarrow \min\} \quad (3.1)$$

Виходячи з цього, в даній роботі для зменшення сумарної затримки передачі пропонуються методи вдосконалення обробки пакетів у вузлах мережі за рахунок оптимізації вибору параметрів та методів класифікації трафіка (розділ 3.3, [122,123,285,290]), оптимізації кількості полів, що використовуються під час класифікації (розділ 3.4, [124]), а також нових методів кластеризації трафіка (розділ 3.4, [121]). Запропоновані методи у поєднанні з застосуванням мережних зрізів дозволять зменшити затримку передачі і покращити ефективність 5G мережі в цілому, що знайшло відображення у авторському свідоцтві [120].

Також в роботі запропоновані нові методи розподілу трафіка на граничних елементах мережі, які дозволяють підвищити швидкодію та надати нові можливості під час застосування технології граничних обчислень з множинним доступом (розділ 3.5).

3.2 Вибір датасету та характеристик для оцінювання ефективності класифікації даних у вузлі мережі

Для дослідження ефективності застосування описаних в розділі 1.5 алгоритмів машинного навчання для вирішення задач класифікації трафіка, використаний розмічений датасет з [125]. Враховуючи, що більшість наборів даних класифікації мережевого трафіку спрямовані лише на ідентифікацію типу додатку, який використовує потік IP (www, dns, ftp, p2p, telnet тощо), цей набір даних йде на крок далі, дозволяючи виявити конкретні додатки, такі як Facebook, YouTube, Instagram тощо, зі статистики потоку IP.

Таблиця 3.1. Фрагмент датасету

Flow ID	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**	**Flow Duration**
172.19.1.46-10.200.7.7-52422-3128-6	172.19.1.46	52422	10.200.7.7	3128	45523
172.19.1.46-10.200.7.7-52422-3128-6	10.200.7.7	3128	172.19.1.46	52422	1
10.200.7.217-50.31.185.39-38848-80-6	50.31.185.39	80	10.200.7.217	38848	1
10.200.7.217-50.31.185.39-38848-80-6	50.31.185.39	80	10.200.7.217	38848	217
192.168.72.43-10.200.7.7-55961-3128-6	192.168.72.43	55961	10.200.7.7	3128	78068
172.19.1.56-10.200.7.6-50004-3128-6	10.200.7.6	3128	172.19.1.56	50004	105069

Відповідно до опису датасета він був зібраний в університеті Universidad Del Cauca (Колумбія), містить більш ніж 3,5 млн пакетів отриманих за 6 діб

від 75 додатків, наведених нижче. Зібрані дані структуровані у вигляді CSV файлу. Важливою особливістю даного датасету окрім великої кількості мережних додатків є значна кількість полів пакетів (82), які використовуються як ознаки для навчання моделі та класифікації пакетів. Далі цей набір має бути оцінений на можливість оптимізації кількості полів. Фрагмент таблиці (перші 5 ознак) з даними наведено в табл. 3.1.

Для оцінки якості роботи алгоритмів машинного навчання можуть бути використані різні метрики [52]. В даній роботі використані наступні характеристики: точність (*accuracy*), чіткість (*precision*), відкликання *(recall*) та метрика F1.

Наведемо формули, за якими вказані метрики можуть бути визначені. *Accuracy* (точність) відображає відношення правильно класифікованих зразків трафіку до загальної кількості зразків (3.2):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \tag{3.2}$$

де *TP* (True Positive) – кількість пакетів які були коректно класифіковані до певного додатку; TN (True Negative) – кількість пакетів які були вірно класифіковані як ті що не відповідають додатку; FP (False Positive) – кількість пакетів, що була невірно віднесена до додатку; FN (False Negative) – кількість пакетів невірно розпізнаних, як ті що не відносяться до додатку.

Для випадків, коли додаток представляє більшість значень вибірки, значення метрики точність буде не точно відображати якість класифікатора, тому додатково будуть використані інші метрики, такі як чіткість та F1.

Precision (чіткість) – вказує співвідношення позитивних правильно прогнозованих пакетів до загальної кількості позитивних прогнозів класифікації (3.3):

$$Precision = \frac{TP}{TP+FP}, \quad (3.3)$$

Recall (відкликання) вказує на співвідношення позитивних, правильно прогнозованих пакетів до суми правильно прогнозованих і неправильно прогнозованих (3.4):

$$Recall = \frac{TP}{TP+FN}, \quad (3.4)$$

Метрика F1 відображає середнє значення чіткості та відкликань (3.5):

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision+Recall}. \quad (3.5)$$

3.3 Вибір типу та параметрів нейронної мережі для вдосконалення точності класифікації трафіка

Для наведених в розділі 1.5 алгоритмів класифікації трафіка на основі методів машинного навчання, таких як RF, ANN, KNN, AdaBoost, SVM була досліджена ефективність класифікації. Для цього був підготовлений набір програм на мові Python 3.0, які дозволили провести оцінювання точності класифікації [285,290] відповідно до метрик наведених в розділі 3.1 та описаного вище датасету [122,123].

Враховуючи наведений в ряді джерел (наприклад, [47,52]) недолік пов’язаний з низькою точністю для малого об’єму вибірки, на першому етапі дослідження було відфільтровано список додатків, які не мали достатнього рівня репрезентації в датасеті [125]. За критерій фільтрації було взято кількість доступних пакетів. 25 додатків з найменшою кількістю пакетів

(менше 500 пакетів у наборі даних) були відкинуті. Прикладами таких додатків та веб-сервісів є 'H323', 'ORACLE', 'TEAMSPEAK', 'BGP', 'BITTORRENT', 'OPENSIGNAL', 'MAIL_IMAPS', 'IP_OSPF', 'RADIUS', 'OPENVPN', 'SNMP', 'STARCRAFT', 'QQ', '99TAXI' (рис. 3.1). Це дозволило підготувати збалансований набір даних.

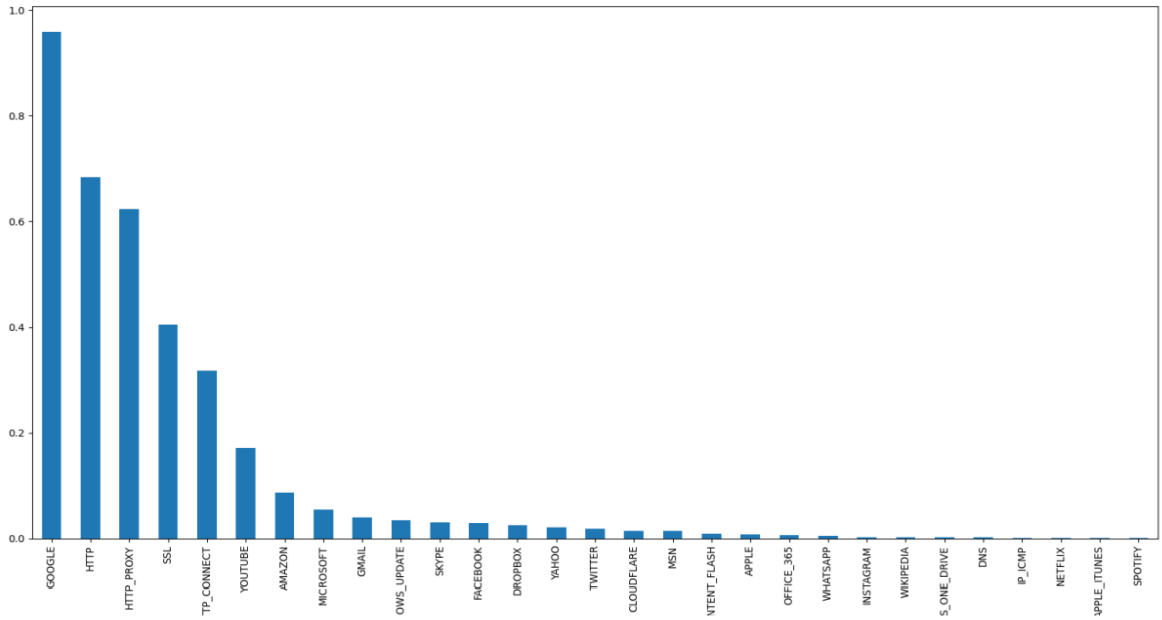


Рис. 3.1. Число пакетів від різних джерел в збалансованому наборі даних (по осі ординат – частота появи пакетів в датасеті $\times 10^6$)

Як видно з рис. 3.1, найбільш представленими в наборі даних є браузери (Google, http), які налічують понад 600 000 пакетів, а також широко представлені додатки класу медіа (Youtube) та пошта (Gmail).

Для збалансованого набору даних було визначено найкращі параметри моделі та точність класифікації.

Використовуючи збалансований набір даних для алгоритму штучної нейронної мережі (ANN), було проведено оцінку максимально досяжної точності та залежності від неї швидкодії (рис. 3.2, рис. 3.3).

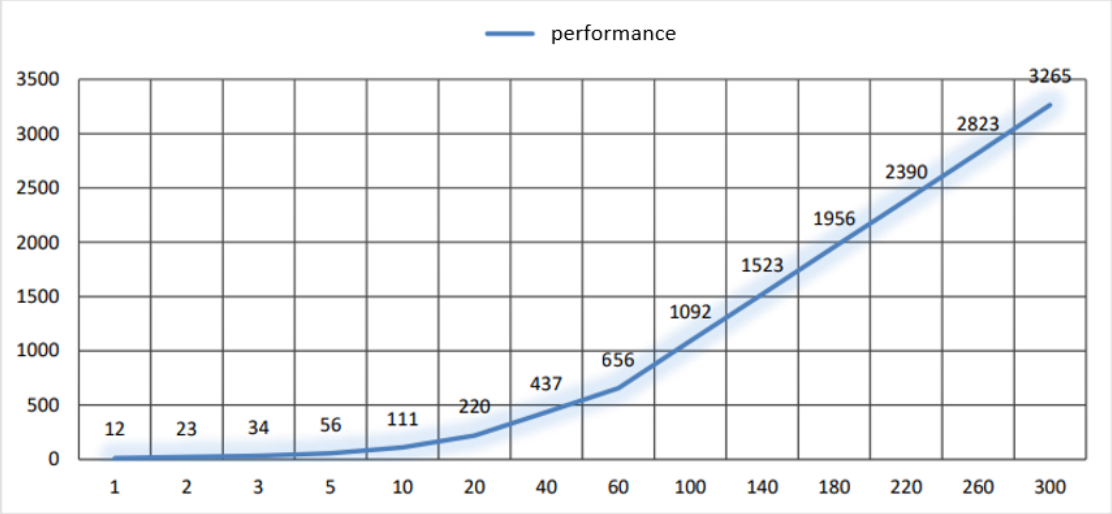


Рис. 3.2. Залежність швидкості класифікації (вісь ординат, мс) для алгоритму ANN від кількості шарів в мережі (вісь абсцис)

Як видно з наведених графіків (рис. 3.2, рис. 3.3), зі збільшенням кількості шарів точність зростає, але швидкість також зростає нелінійно. Тому для прискорення обробки або забезпечення розрахунків у реальному часі без затримок варто обмежити кількість шарів до 180-220 шарів (точність на навчальному датасеті 0.987-0.99 відповідно). Найкращим з точки зору точності є значення 512 шарів.

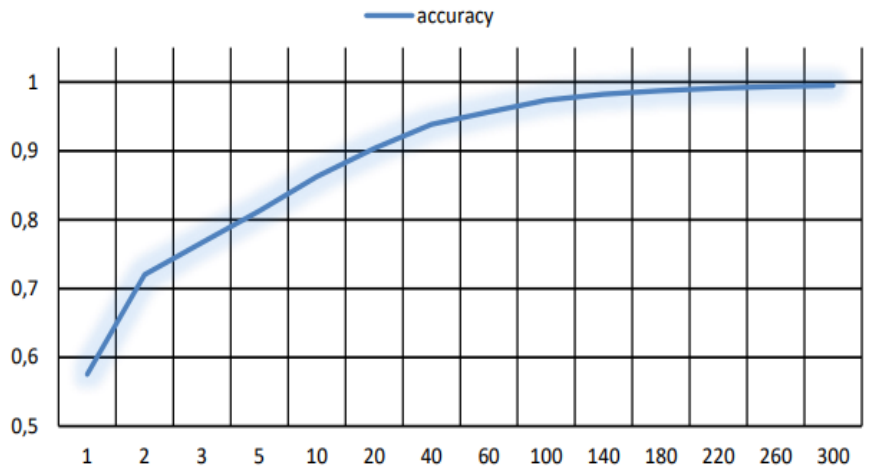


Рис. 3.3. Залежність точності класифікації (вісь ординат) для алгоритму ANN від кількості шарів в мережі (вісь абсцис)

Для алгоритму *k*-найближчих сусідів (KNN) в роботі [123] було проведено аналіз впливу кількості сусідів на точність (рис. 3.4) та визначено, що найвища точність класифікації забезпечується при використанні Манхеттенської відстані та при $k = 3$.

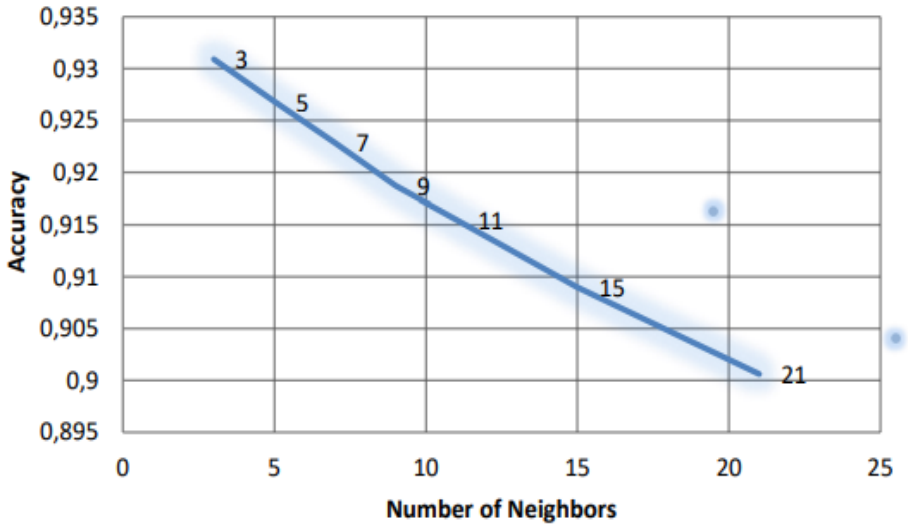


Рис. 3.4. Залежність точності класифікації (вісь ординат) для алгоритму KNN від кількості сусідів *k*

У цьому випадку вдається досягти точності класифікації на рівні 0.93 на навчальному наборі даних. Як видно з рис. 3.4, точність незначно змінюється зі збільшенням кількості сусідів, і для цього набору даних збільшення кількості сусідів не призводить до покращення результатів класифікації.

Також для збалансованого набору даних було проведено оцінку найкращих параметрів моделі та точності класифікації у випадку використання алгоритму "випадкового лісу" (RF). Для алгоритму RF за критерієм точності розпізнавання оптимальними виявилися такі параметри:

- кількість дерев рішень, які необхідно об'єднати (*n_оцінок*) – 50;
- максимальна глибина дерев – 40;
- максимальна кількість ознак, що враховуються на кожному розбитті – log2.

За таких умов можна досягти точності класифікації 0.993 на навчальному наборі даних. Порівняльні характеристики результатів оцінки точності класифікації за алгоритмом RF для різних значень кількості дерев наведено на рис. 3.5.

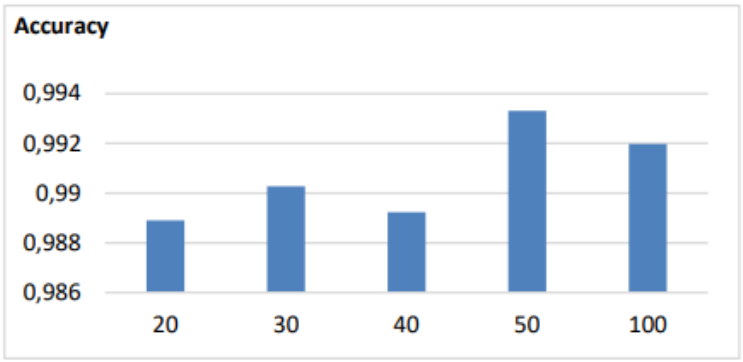


Рис. 3.5. Залежність точності класифікації (вісь ординат) для алгоритму RF від кількості дерев рішень

В табл. 3.2 наведено результати порівняння точності класифікації при використанні різних алгоритмів (RF, ANN, KNN на навчальному наборі даних та алгоритмів AdaBoost, SVM на тестовому наборі даних).

Таблиця 3.2. Порівняльний аналіз точності досліджуваних алгоритмів класифікації

Алгоритм	Accuracy	Precision	F1-score
ANN	0.991	0.992	0.991
KNN	0.933	0.933	0.933
RF	0.993	0.993	0.993
AdaBoost	0.828	0.806	0.764
SVM	0.651	0.812	0.822

Як видно з табл. 3.2, загальні результати класифікації є досить високими, але ці значення є усередненими, і різні додатки класифікуються з різним ступенем точності. У роботі також оцінювалася точність класифікації залежно від типу додатку (табл. 3.3).

Таблиця 3.3. Результати точності класифікації додатків для алгоритму KNN

Додатки з найкращою точністю класифікації	value	Додатки з найгіршою точністю класифікації	value
IP_ICMP	1	CITRIX_ONLINE	0.83
NTP	1	UPNP	0.82
TEAMVIEWER	1	GMAIL	0.79
DNS	1	WAZE	0.77
SSH	1	TWITTER	0.77
FTP_CONTROL	1	SKYPE	0.77

У табл. 3.3 показано результати для додатків з найкращим і найгіршим показниками розпізнавання, інші додатки мають проміжні значення точності класифікації.

Результати для більшості алгоритмів в табл. 3.2 отримані, коли для навчання використовувався весь набір даних, а для тестування – той самий набір даних. На практиці це припущення і потрібно використовувати різні частини набору даних для навчання і тестування. Це дозволить наблизити ситуацію до реальності. В роботі [123] був виконаний аналіз точності для різних способів поділу датасету на навчальну та тестову частини (табл. 3.4).

Таблиця 3.4. Результати точності класифікації при різних способах розподілу датасету

Співвідношення навчальної та тестової частини датасету	Точність
0.9/0.1	0.699
0.8/0.2	0.707
0.7/0.3	0.688
0.6/0.4	0.676
0.5/0.5	0.685
0.4/0.6	0.658
0.3/0.7	0.649
0.2/0.8	0.609
0.1/0.9	0.565

Згідно з табл. 3.4, розподіл 90%-10% між навчальною та тестовою частинами дозволяє отримати точність 0.699. При розподілі 50%-50% точність становить 0.685. Якщо розмір тренувальної частини буде меншим за 50%, точність значно погіршується до 0.56-0.65. Для подальших досліджень буде використовуватися розподіл 80%-20%.

3.4 Оптимізація вектору-ознак для вдосконалення продуктивності мережі під час класифікації трафіка

Під час обробки трафіку швидкість роботи класифікатора визначає швидкість і ефективність роботи мережі в цілому (виражену в швидкості обробки пакетів) і можливий рівень втрат пакетів. Тому завдання забезпечення максимальної продуктивності цього пристрою є актуальним. Продуктивність класифікатора напряму залежить від кількості полів, що обробляються. Тому в даній роботі [124] проведено аналіз можливості оптимізації кількості полів, що використовуються для класифікації. Як базовий метод класифікації було використано штучну нейронну мережу (ANN) з різними значеннями гіперпараметрів. Було використано набір даних з [125], що містить 82 ознаки і дає точність 0.707 (з розподілом 80%-20%).

Для оптимізації вектору-ознак класифікації можна застосовувати різні підходи. Найбільше розповсюдження отримали підходи на основі точності (accuracy) і взаємної інформації, що міститься в різних ознаках.

В роботі [282] пропонується застосування зваженої взаємної інформації. Для цього використовується класичний підхід запропонований Шеноном, на основі теорії інформації. Взаємна інформація дозволяє виміряти взаємну залежність між двома випадковими ознаками X і Y, а також визначити кількість інформації, яку містить випадкова ознака з набору. Згідно теорії

Шенона, інформація між двома випадковими величинами (ознаками) описується як:

$$\mathrm{I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)}, \tag{3.6}$$

де *H(X)* та *H(Y)* – ентропії величин (ознак) X та Y, а $H(X \mid Y)$ та $H(Y \mid X)$ – умовні ентропії. Базуючись на термінології та визначеннях Шенона [14], ентропію ознак також можна представити у вигляді:

$$\mathrm{H(X) = -\sum_{x \in X} p(x) \cdot \log p(x)} \tag{3.7}$$

$$\mathrm{H(Y) = -\sum_{y \in Y} p(y) \cdot \log p(y)} \tag{3.8}$$

і визначити спільну ентропію ознак X та Y – $H(X, Y)$:

$$\mathrm{H(X,Y) = -\sum_{x \in X} \sum_{y \in Y} p(x,y) \cdot \log p(x,y)} \tag{3.9}$$

В цих виразах *p(x)* та *p(y)* відповідають ймовірності появи випадкової ознаки в наборі. Далі виконується попарне порівняння різних ознак і залишаються ті ознаки, що є найбільш інформативними. Однак цей підхід є достатньо складним і незручним за умови великої кількості ознак. Вдосконаленням цього підходу є метод на основі зваженої взаємної інформації [282], але широкого розповсюдження він також не набув.

Другий підхід використовує аналіз впливу окремих ознак чи груп ознак на точність класифікації і саме його модифікація була використана в даній роботі. Для оцінювання впливу ознак був виконаний кілька-етапний аналіз, який використовував як попарні порівняння цілих груп ознак (об’єднаних за логічним принципом) так і аналіз впливу окремих ознак.

3.4.1 Аналіз впливу групи ознак на точність класифікації

Для виконання цієї частини об'єднаємо класифікаційні ознаки в групи. Для цього розділимо початкову множину з 82 ознак на 21 групу відповідно до їх характеристик та призначення (табл. 3.5).

Наприклад, група 1 (табл. 3.5) об'єднує порти та адреси відправника/одержувача, група 3 включає характеристики кількості відправлених та отриманих пакетів загалом, а група 7 – типові інтервали часу між сусідніми однотипними пакетами (час відхилення між двома пакетами).

Таблиця 3.5. Розподіл класифікаційних ознак на групи

Група	**Ознаки, що відносяться до групи**
1	Source.IP, Source.Port, Destination.IP, Destination.Port
2	Protocol, Flow.Duration
3	Total.Fwd.Packets,Total.Backward.Packets, Total.Length.of.Fwd.Packets, Total.Length.of.Bwd.Packets
4	Fwd.Packet.Length.Max, Fwd.Packet.Length.Min, Fwd.Packet.Length.Mean, Fwd.Packet.Length.Std
5	Bwd.Packet.Length.Max, Bwd.Packet.Length.Min, Bwd.Packet.Length.Mean, Bwd.Packet.Length.Std
6	Flow.Bytes.s, Flow.Packets.s
7	Flow.IAT.Mean, Flow.IAT.Std, Flow.IAT.Max, Flow.IAT.Min
8	Fwd.IAT.Total, Fwd.IAT.Mean, Fwd.IAT.Std, Fwd.IAT.Max, Fwd.IAT.Min
9	Bwd.IAT.Total, Bwd.IAT.Mean, Bwd.IAT.Std, Bwd.IAT.Max, Bwd.IAT.Min
10	Fwd.PSH.Flags, Bwd.PSH.Flags, Fwd.URG.Flags, Bwd.URG.Flags
11	Fwd.Header.Length, Bwd.Header.Length, Fwd.Packets.s, Bwd.Packets.s
12	Min.Packet.Length, Max.Packet.Length, Packet.Length.Mean, Packet.Length.Std, Packet.Length.Variance
13	FIN.Flag.Count, SYN.Flag.Count, RST.Flag.Count, PSH.Flag.Count, ACK.Flag.Count, URG.Flag.Count, CWE.Flag.Count, ECE.Flag.Count
14	Down.Up.Ratio,
15	Average.Packet.Size, Avg.Fwd.Segment.Size, Avg.Bwd.Segment.Size
16	Fwd.Header.Length, Fwd.Avg.Bytes.Bulk, Fwd.Avg.Packets.Bulk, Fwd.Avg.Bulk.Rate
17	Bwd.Avg.Bytes.Bulk, Bwd.Avg.Packets.Bulk, Bwd.Avg.Bulk.Rate
18	Subflow.Fwd.Packets, Subflow.Fwd.Bytes, Subflow.Bwd.Packets, Subflow.Bwd.Bytes
19	Init_Win_bytes_forward,Init_Win_bytes_backward, act_data_pkt_fwd, min_seg_size_forward,
20	Active.Mean, Active.Std, Active.Max, Active.Min
21	Idle.Mean, Idle.Std, Idle.Max, Idle.Min

Після такої комбінації вплив кожної групи було оцінено шляхом виключення її з процесу оцінювання точності класифікації. Результати обчислень впливу групи ознак наведено в табл. 3.6.

Як видно з табл. 3.6, всі групи, крім групи 1, мають незначний вплив і виключення (втрата) однієї групи не знижує загальну точність класифікації, але оскільки групи впливають одна на одну, то втрата відразу декількох груп може призвести до значного погіршення точності.

Таблиця 3.6. Вплив груп ознак на точність класифікації

Група ознак	**Accuracy**	**Precision**
1	0.624	0.865
2	0.716	0.882
3	0.715	0.886
4	0.695	0.879
5	0.710	0.893
6	0.704	0.883
7	0.700	0.875
8	0.708	0.883
9	0.706	0.887
10	0.706	0.866
11	0.705	0.880
12	0.714	0.878
13	0.697	0.882
14	0.707	0.867
15	0.707	0.886
16	0.705	0.871
17	0.701	0.873
18	0.709	0.879
19	0.686	0.881
20	0.703	0.873
21	0.705	0.878

Також важливо підкреслити важливість групи 1, яка містить порти та IP-адреси, для класифікації, і її неврахування одразу погіршує точність на 0.08.

3.4.2 Аналіз впливу окремих ознак на точність класифікації

Фільтрація класифікаційних ознак, які присутні лише в невеликій кількості пакетів (рідко зустрічаються в пакетах), може потенційно прискорити процес класифікації та спростити налаштування системи за рахунок незначного погіршення точності. В роботі [124] були запропоновані варіанти зменшення кількості ознак класифікації, які базувалися на попередніх результатах аналізу груп характеристик. В результаті кількість ознак було зменшено з 82 (табл. 3.5) до 56 (табл. 3.7) з незначним погіршенням точності з 0.708 (табл. 3.4) до 0.693 (табл. 3.10). Цей набір ознак позначено як "середній".

Таблиця 3.7. Набір ознак "середній"

Features in set
'Destination.IP', 'Destination.Port', 'Source.IP', 'Init_Win_bytes_forward', 'min_seg_size_forward', 'Fwd.Packet.Length.Max', 'Init_Win_bytes_backward', 'Flow.IAT.Max', 'Source.Port', 'Flow.Duration', 'Fwd.Packet.Length.Std', 'Bwd.IAT.Total', 'Avg.Fwd.Segment.Size', 'Fwd.Packets.s', 'Fwd.IAT.Total', 'Fwd.IAT.Max', 'Fwd.Packet.Length.Mean', 'Subflow.Fwd.Bytes', 'Flow.Bytes.s', 'Min.Packet.Length', 'Total.Length.of.Fwd.Packets', 'Bwd.IAT.Max', 'Packet.Length.Variance', 'Bwd.Packets.s', 'Flow.IAT.Mean', 'Fwd.Header.Length', 'act_data_pkt_fwd', 'Max.Packet.Length', 'Flow.Packets.s', 'Flow.IAT.Std', 'Packet.Length.Std', 'Idle.Max', 'Fwd.Header.Length.1', 'Bwd.Packet.Length.Mean', 'Bwd.IAT.Std', 'Fwd.Packet.Length.Min', 'Bwd.Packet.Length.Std', 'Avg.Bwd.Segment.Size', 'Average.Packet.Size', 'Total.Length.of.Bwd.Packets', 'Packet.Length.Mean', 'Fwd.IAT.Mean', 'Fwd.IAT.Std', 'Flow.IAT.Min', 'Bwd.IAT.Mean', 'Bwd.Packet.Length.Max', 'Subflow.Fwd.Packets', 'Total.Fwd.Packets', 'Total.Backward.Packets', 'Bwd.Header.Length', 'Subflow.Bwd.Bytes', 'Subflow.Bwd.Packets', 'Idle.Mean', 'Fwd.IAT.Min', 'Down.Up.Ratio', 'Idle.Min'

Наступним кроком була багатокритеріальна оптимізація ознак класифікації шляхом перевірки рівня впливу кожної ознаки на точність та подальше зменшення кількості ознак з прийнятною втратою точності. В результаті було отримано список з 18 найбільш важливих ознак (табл. 3.8),

який забезпечує точність 0,638 (табл. 3.10). Цей набір ознак позначено як "малий".

Таблиця 3.8. Набір ознак "малий"

Features in set
'Destination.IP', 'Destination.Port', 'Source.IP','Fwd.Packet.Length.Max', 'Source.Port', 'Flow.Duration', 'Fwd.Packet.Length.Std', 'Bwd.IAT.Total', 'Fwd.Packet.Length.Mean', 'Subflow.Fwd.Bytes', 'Flow.Bytes.s', 'Bwd.IAT.Max', 'Bwd.Packets.s','Flow.Packets.s','Bwd.IAT.Std', 'Fwd.Packet.Length.Min','Bwd.IAT.Mean', 'Subflow.Fwd.Packets'

3.4.3 Аналіз впливу гіперпараметрів на точність та швидкість класифікації

Крім кількості ознак в наборі, на точність і швидкість класифікації впливають налаштування двох гіперпараметрів. Оцінимо їх вплив на прикладі наведеного вище набору даних [125] та алгоритму класифікації ANN. Перший з них – розмір вибірки (*batch size*). Це гіперпараметр, який визначає кількість вибірок для опрацювання перед оновленням внутрішніх параметрів моделі. Другий – кількість епох (*number of epochs*). Це гіперпараметр, який визначає, скільки разів алгоритм навчання буде опрацьовувати весь навчальний набір даних. Ці два гіперпараметри взаємопов'язані, і результати показали, що зменшення параметра *batch* призводить до збільшення часу прорахунку на 1 епоху (табл. 3.9):

Таблиця 3.9. Вплив гіперпараметрів для алгоритму ANN

Batch size	**Epoch calculation time**
128	~ 6 sec
64	~ 10 sec
32	~ 17 sec

Підсумкові результати досліджень наведені в табл. 3.10.

Таблиця 3.10. Точність та швидкодія класифікації в залежності від гіперпараметрів для алгоритму ANN

Batch size / epoch number	**Швидкодія класифікації / Точність (accuracy)**		
	Базовий набір ознак (82)	**Середній набір ознак (56)**	**Малий набір ознак (18)**
128 / 10	70.1s / 0.707	**67.7s / 0.683**	**66.09s / 0.638**
64 / 10	108.28s / 0.711	105.1s / 0.699	98.21s / 0.646
32 / 10	189.1s / 0.723	184.7s / 0.714	174.3s / 0.655
128 / 50	**322.3s /0.773**	304.7s /0.765	281.7s /0.700
64 / 50	718.2s / 0.775	578.6s / 0.770	513.9s / 0.705
32 / 50	1166s / 0.784	897.3s / 0.772	805.6s / 0.71
128 / 100	**612.1s / 0.792**	**601.1s / 0.779**	547.6s / 0.719
64 / 100	1117.8s / 0.794	1043.7s/ 0.788	984.8s/ 0.725

Зі збільшенням розміру вибірки (табл. 3.10) з 64 до 128 швидкодія зростає з 105.1 сек до 67.7 сек, але точність погіршується з 0.699 до 0.683 (середній набір ознак). Збільшення кількості епох (10→100) покращує точність з 0.707 до 0.792, але час витрачений на класифікацію суттєво збільшується з 70.1 сек до 612.1 сек (базовий набір характеристик).

3.4.4 Висновки та рекомендації із застосування алгоритмів машинного навчання для класифікації трафіку

Результати порівняльного аналізу показали, що найкращих показників точності можна досягти при використанні ANN та RF алгоритмів.

Під час оптимізації набору ознак необхідну кількість ознак було зменшено з 82 до 18 (зменшення на 78%). Зменшення кількості ознак дозволило підвищити швидкість класифікації на 8% для великої кількості епох (50) і на 12% для кількості епох = 10, для параметра пакету 64.

Найвищу швидкість можна отримати для гіперпараметрів batch/epoch = 128/10, зменшивши кількість ознак до 54 (67.7 сек) та 18 (66.1 сек), однак це призводить до значного падіння точності до 0.668 та 0.611 відповідно.

Таким чином, якщо потрібна найвища продуктивність, рекомендовані налаштування: batch/epoch = 128/10 і використання малого (18) або середнього (54) набору функцій.

Найкраща точність досягається при збільшенні кількості епох і зменшенні параметра batch, що негативно впливає на продуктивність. Так, значення точності на тестовому наборі даних 0.794 досягається за ~1117 сек (при batch/epoch = 64/100), що може бути неприйнятним, коли необхідно забезпечити низькі затримки в мережі 5G.

Загалом результати (табл. 3.10) показують, що зменшення кількості ознак до 18 не є ефективним, оскільки виграш у швидкодії не перекриває втрати в точності, і майже всі результати мінімального набору ознак (18) перекриваються результатами середнього (зменшеного) набору (54) при інших значеннях гіперпараметрів (batch/epoch). Наприклад, час класифікації 98.21 с і точність 0.646 для мінімального набору ознак (batch/epoch = 64/10) перекриваються з 67-70.1 с / 0.67-0.7 для batch/epoch = 128 / 10 для середнього і базового наборів ознак відповідно.

Наукова новизна роботи полягає у визначенні параметрів алгоритмів машинного навчання, які є оптимальними з точки зору точності та швидкодії для вирішення задачі класифікації трафіку в мобільних мережах 5-го та 6-го поколінь. Крім того, до наукової новизни слід віднести оцінку важливості параметрів (полів) набору даних для класифікації. Запропоновані алгоритми та параметри є першим етапом багатокрокової обробки пакетів в мережі, що разом з кластеризацією, нарізкою та розподіленою обробкою дозволить підвищити ефективність системи мобільного зв'язку в цілому.

Практичне значення роботи полягає в можливості використання зазначених алгоритмів із запропонованими параметрами для підвищення

ефективності класифікації пакетів в мережі мобільного зв'язку 5-го та 6-го поколінь.

3.5 Кластеризація трафіку у вузлі мережі

3.5.1 Особливості кластеризації трафіка в сучасних мережах

Сучасні системи зв'язку вимагають організації обробки великих масивів інформації в розподіленому гетерогенному середовищі. Більшість робіт по обробці навантаження в дата-центрах не враховують, що обсяг навантаження, яке надходить, є пульсуючим і часто суттєво змінюється протягом дня.

Через мінливість навантаження, яке відчувають сучасні системи, розміщення віртуальних машин в гетерогенному інформаційно-комунікаційному середовищі необхідно постійно оптимізувати в режимі реального часу. З огляду на складність прогнозування пікових навантажень, система повинна використовувати комбінацію динамічного розподілу ресурсів і управління запитами для своєчасного реагування на зміни навантаження. Динамічний розподіл ресурсів дозволяє виділяти додаткові ресурси для служб прикладного програмного забезпечення, наприклад, серверів, щоб впоратися зі збільшенням навантаження, а управління процесом їх надання дозволяє вузлу управління навантаженням тимчасово відхиляти надлишкові запити, поки виділяються додаткові ресурси. У сучасних системах зв'язку проблема якості обслуговування модифікується.

Якщо раніше мова йшла про обмеженість мережевого ресурсу, обмеженість можливостей мережі доступу, а також ресурсів вузлів комутації, то зараз система має умовно необмежені технічні ресурси. Нові технології програмного управління програмно-керованим радіо, програмно-керованою мережею (SDN), а також технології віртуалізації мережевих функцій зводять

задачу організації інформаційно-комунікаційного середовища до трьох основних завдань:

- завдання розміщення приймально-передавальних пристроїв;
- завдання організації розподіленого програмного комплексу, який відтворює структуру та логіку роботи інформаційно-комунікаційної мережі;
- завдання інтелектуального управління складною системою.

3.5.2 Аналіз існуючих рішень із кластеризації трафіку у вузлі мережі

Загалом, кластеризація в серверній архітектурі може бути універсальним варіантом розподілу, а також потужним інструментом збереження даних від втрат. Крім того, ці рішення досить добре підходять для інтеграції на серверному рівні систем 5G mIoT.

Однією з основних частин цієї системи є база даних, що містить дані, зібрані з усіх пристроїв в мережі, тому їй потрібно приділяти достатньо уваги при розробці та підтримці системи. Взагалі, дані можуть зберігатися по-різному, але сьогодні є два найбільш популярних типи баз даних – реляційні та нереляційні (далі SQL та NoSQL відповідно). Який з них використовувати та комбінувати – все залежить від типу даних, які будуть зберігатися.

Наприклад, для зберігання масивів великих даних з однорідною структурою без виконання певних операцій над ними краще використовувати NoSQL, але для побудови логічної структури, а також для використання маніпуляцій з даними або навіть перенесення частини логіки рішення на рівень бази даних найкращим рішенням буде класичний SQL [126].

Наше рішення фокусується на зберіганні даних з кінцевих пристроїв і, виходячи з описаного вище, основною метою цієї роботи є поєднання кластеризації з контейнеризацією. Це допомагає досягти покращення масштабованості, доступності та безпеки, а також створити алгоритм, який

можна налаштувати для забезпечення оптимального управління вузлами кластера для конкретної промислової мережі mIoT.

Залежно від типу обраної бази даних, або їх комбінації, наприклад, зберігання необроблених даних з пристроїв на нереляційних базах даних, а обробленої та структурованої інформації на реляційних, потрібно обирати власну модель кластеризації та відмовостійкості баз даних [127].

Наприклад, для реляційних баз даних Microsoft SQL існує два найбільш поширених підходи [128]. Перший – це масштабування звичайного кластерного SQL Server (рис. 3.6).

Другий – Always On SQL Server [130], який, залежно від обраних налаштувань конфігурації, може підвищити ефективність та швидкість обробки даних. Перевагами цього рішення є хороший рівень масштабованості та висока доступність.

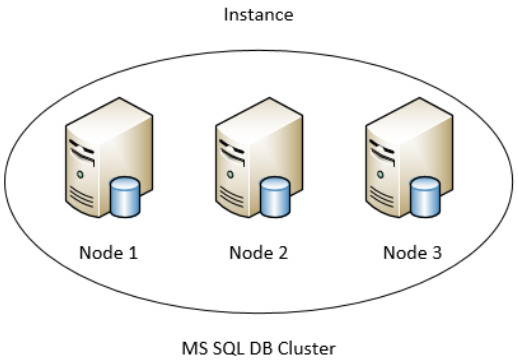


Рис. 3.6. Узагальнена кластерна структура реляційної бази даних

Найпопулярнішою робочою моделлю для балансування навантаження NoSQL баз даних є шардинг (або фрагментація) [129]. При фрагментації база даних розбивається на фрагменти (рис. 3.7), в які записуються і зчитуються дані, що дозволяє значно підвищити швидкість роботи з базою даних.

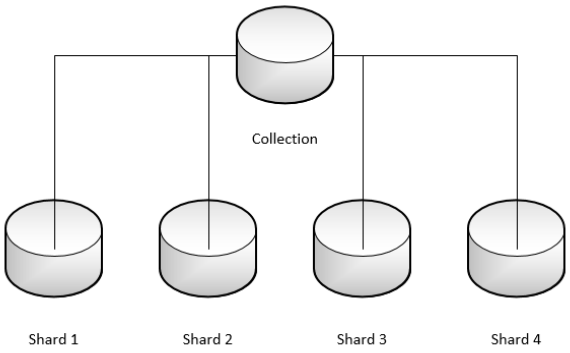


Рис. 3.7. Узагальнена кластерна структура нереляційної бази даних на основі дробового типу реплікації

У звичайних операційних системах для персональних комп'ютерів комп'ютерна програма може бачити (навіть якщо не має доступу) всі системні ресурси. Вони включають:

- апаратні засоби, які використовуються, наприклад, процесор і мережеве з'єднання;

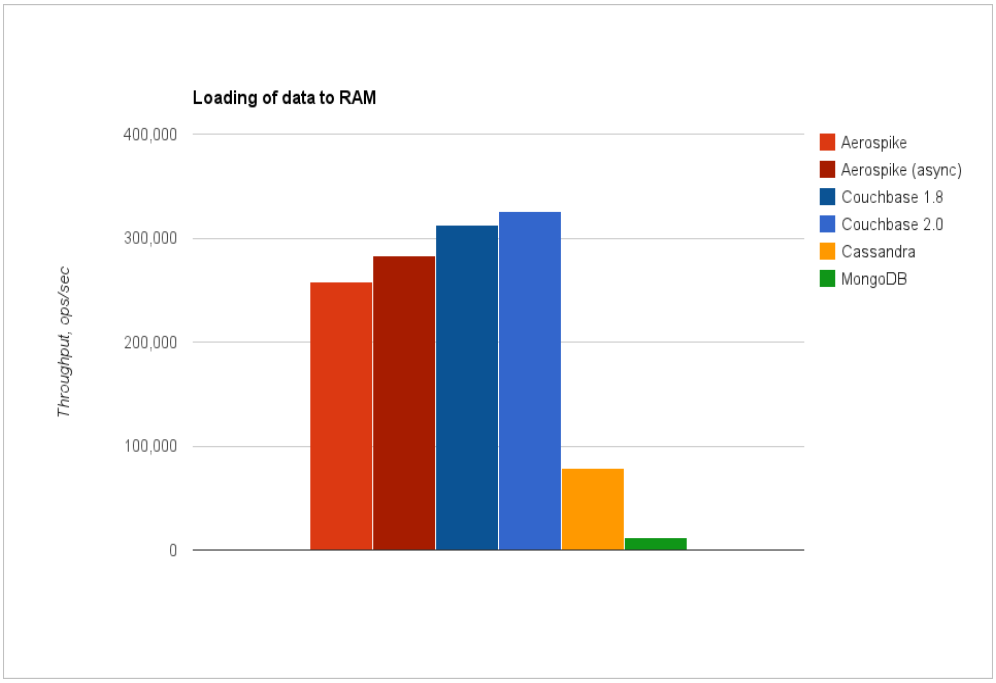
- дані, які можна читати або записувати, наприклад, файли, папки та мережеві папки;

- підключені периферійні пристрої, з якими вона може взаємодіяти, наприклад, веб-камера, принтер, сканер.

Завдяки віртуалізації або контейнеризації операційної системи хтось може запускати програми всередині контейнерів, які виділяють лише частину цих ресурсів. Програма, яка очікує побачити весь пристрій, коли запускається всередині контейнера, може побачити лише вибрані ресурси і знайти їх доступними. У кожній операційній системі можна створити кілька контейнерів, кожен з яких містить підмножину ресурсів. Кожен контейнер може містити будь-яку кількість програм. Ці програми можуть запускатися одночасно або окремо, навіть взаємодіяти між собою.

Виходячи з результатів, показаних на рис. 3.8, найбільш перспективною базою даних для високонавантажених систем може бути Couchbase. Крім того, ми можемо побачити динаміку того, наскільки продуктивнішою може бути нереляційна база даних, чим менше функцій SQL вона підтримує, порівнюючи Mongo та Aerospike.

Бази даних NoSQL мають оптимальні характеристики пропускної здатності і підходять для використання в промисловому IoT з великою кількістю кінцевих пристроїв. Крім того, багато постачальників мають вбудовані функції для контейнеризації та кластеризації.



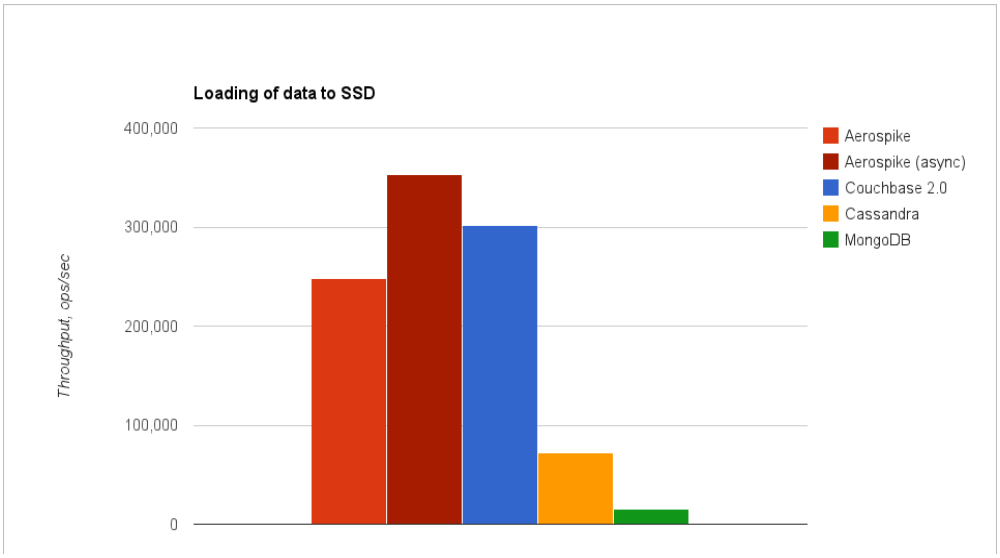


Рис. 3.8. Діаграми завантаження даних для деяких NoSQL БД [131].

Наведемо короткий огляд найбільш поширених рішень:

1. Шардинг від Mongo. Mongo використовує репліки як гарант відмовостійкості. Набір реплік – це група щонайменше з трьох екземплярів MongoDB, які зберігають однакові дані. Один вузол набору вважається первинним і відповідає за всі операції запису. Він записує всі зміни в журнал, щоб інші вузли (вторинні) могли точно відображати дані первинного вузла. Якщо первинний вузол стає недоступним, новий буде автоматично обраний з активних вторинних вузлів після невеликої затримки.

2. Кластеризація Couchbase. Розмір кластера Couchbase автоматично регулюється залежно від вхідного навантаження шляхом зміни кількості серверів БД (до 10 екземплярів на рівень) відповідно до наступних умов:

+1 вузол, якщо використання CPU/RAM становить >70% протягом щонайменше 5 хвилин;

-1 вузол, якщо використання CPU/RAM становить <40% протягом щонайменше 5 хвилин.

Коли вузол додається до кластера або видаляється з нього, автоматично виконується процес ребалансування даних. Він спрямований на рівномірний перерозподіл всієї інформації, що зберігається в кластері, між доступними вузлами. При цьому кластер залишається працездатним і продовжує обслуговувати та обробляти запити клієнтів.

3. Master-Slave. Кластер, що використовує модель master-slave, має один головний вузол і набір підлеглих вузлів, які зазвичай використовуються для збереження копії даних, а в разі падіння головного вузла один з підлеглих вузлів візьме на себе всі завдання головного вузла.

3.5.3 Запропонований алгоритм контейнеризації та управління

Для автоматизації роботи кластера було реалізовано спеціальний алгоритм аналізу вхідного потоку даних, який дозволить управляти вузлами кластера автоматично без втручання адміністраторів, в даному рішенні пропонується використовувати формулу, яка буде контролювати кількість вузлів бази даних в кластері.

$$k = \left\lceil \frac{E}{e} \right\rceil + \lambda\,, \tag{3.10}$$

де E – вхідний потік даних за один раз; e – обсяг даних, який може обробити вузол, λ – коефіцієнт динамічної зміни кількості вузлів кластера. Отже, виходячи з (3.10), максимальна пропускна здатність системи буде дорівнювати

$$E_{max} = e \cdot k. \tag{3.11}$$

Для визначення остаточної залежності λ необхідно спочатку визначити середню зміну кількості вхідних повідомлень за певний період:

$$\triangle E_{mid} = \sum_i^n (E_{max} - E_{mom\,i}) / n \ , \qquad (3.12)$$

де $E_{mid\,i}$ потік даних в певний момент часу, n – кількість часових відрізків, для яких проводилося вимірювання.

Також необхідно для кожної системи визначити приблизний час, витрачений на повне розгортання системи, це буде сума часу, витраченого на створення/видалення контейнера (t_c), часу, витраченого на приєднання вузла до кластера (t_d) та часу, витраченого на балансування кластера після створення/видалення вузлів (t_{cr}):

$$t_f = t_c + t_d + t_{cr} \, . \qquad (3.13)$$

На основі (3.10) - (3.12) коефіцієнт λ, в даний момент можна виразити через E_{mom}:

$$\lambda = \begin{cases} \frac{(E_{max} - E_{mom})}{\frac{|\triangle E_{mid}|}{t_f}} \leq \ \delta \text{ та } \triangle E_{mid} > 0 = 1, \\ \frac{(E_{max} - E_{mom})}{\frac{|\triangle E_{mid}|}{t_f}} \geq \ \delta \text{ та } \triangle E_{mid} < 0 = -1, \\ 0. \end{cases} \qquad (3.14)$$

Граничним рівнем є натуральне число δ >1, яке пропонується вибирати як оптимальне відношення прогнозованого часу сканування до реального часу сканування.

Наприклад, якщо сервер потрібно розгорнути якомога швидше до досягнення максимальної пропускної здатності, або, навпаки, мінімізувати час розгортання при падінні пропускної здатності до $E_{max} - e$, то δ = 1.

Таким чином, було запропоновано алгоритм управління кластерними промисловими IoT мережами, який дозволить клієнтам оптимізувати використання ресурсів при збереженні доступності та вхідної пропускної

здатності кластера. На першому етапі розроблене рішення потребує більших витрат на підготовку та адміністрування, але має перевагу під час експлуатації, оскільки система буде повністю підтримувати кластер без втручання людини.

3.6 Вдосконалений підхід до організації мобільних периферійних обчислень в мережі 5G з перевіркою даних

Технологія мобільних периферійних обчислень (Mobile Edge Computing, MEC) дозволяє використовувати обладнання користувача (UE) як обчислювальний ресурс. Іншою назвою технології є технологія граничних обчислень з розподіленим доступом. Це може, наприклад, дозволити виконувати обчислювальні завдання, пов'язані з таким обладнанням, зі зменшеною затримкою або вивантажувати обчислювальні завдання з мережі на обладнання користувача.

Для вибору обчислювальних вузлів та розподілу навантаження в існуючих рішеннях використовуються додаткові хардварні (фізичні) елементи (що вимагає додаткових витрат) або динамічно оновлювані карти чи бази даних (що вимагає додаткових мережевих ресурсів та навантаження на мережу).

Крім того, якщо в одній зоні знаходиться декілька пристроїв MEC, необхідна довірена сторона для автентифікації учасників.

3.6.1 Існуючі проблеми розподілених обчислень в мережі 5G.

На цей час для розподілених граничних обчислень, або як їх ще називають “мобільних периферійних обчислень”, існує декілька не вирішених проблем:

- потрібен метод балансування навантаження та вибору обчислювальних вузлів для MEC;
- потрібен додатковий метод розподілу ресурсів від мережі для зв'язку MEC без додаткових фізичних елементів;
- потрібен метод перевірки даних / результатів обчислень: Обчислювальний вузол може повідомляти неправильні результати обчислень, тому потрібен метод перевірки даних та потрібен рейтинг обчислювального вузла на основі рівня довіри.
- взаємна автентифікація для різних типів обладнання необхідна в мережі 5G для процесу мобільних периферійних обчислень або потрібен додатковий довірений арбітр.

При цьому немає існуючих рішень, які б одночасно виконували перевірку справжності серверів розподілу та обчислювальних вузлів, керували процесом розподілу обчислювальних блоків, мали процедуру перевірки коректності розрахунків та враховували параметри обчислювальних вузлів під час розподілу.

3.6.2 Аналіз існуючих рішень

Визначимо основних учасників процесу розподілених граничних обчислень (табл. 3.11) та їх функції згідно запропонованого в дисертації рішення. Аналогічний перелік учасників процесу, але з іншим набором функцій, наведено в [142,143, 288].

Серед рішень, які вирішують завдання розподілу навантаження між обчислювальними вузлами MEC та представлені в публікаціях, варто відмітити наступні (табл. 3.12):

Таблиця 3.11. Основні учасники процесу розподілених граничних обчислень

Позначення учасника	Функції
 Сервер MEC	збирає потік даних з одного або більше датчиків/сенсорів; має радіомодуль з підтримкою 5G; може запустити додаток з підтримкою MEC; має мережний ідентифікатор та підтримує функції білінгу;
 Обчислювальний вузол	обробка виклику API користувача MEC; має радіомодуль з підтримкою 5G; має процесор, який підтримує роботу фреймворку MEC; має мережний ідентифікатор та підтримує функції білінгу;
 Базова станція	виділення радіоресурсу, перевірка особи, підписання транзакції, безпечне з'єднання; підтримка вибору обчислювального вузла; підтримка зв'язку точка-точка; забезпечення верифікованого звязку MEC Сервер -> Обчислювальний вузол;

Таблиця 3.12. Аналіз існуючих рішень з граничних обчислень та їх недоліки

Патент / публікація	**Недоліки та варіанти їх вирішення**
CN108243245A Wireless access network based on hybrid fog calculation and resource allocation method thereof [132]	**Пропонується в патенті:** хмарна платформа: пул ресурсів BBU, який підключається до основної мережі через мережу передачі. **Недолік патенту:** Потрібна хмарна платформа; потрібен спеціальний вузол RRH. **Запропонований в дисертації варіант усунення недоліку:** Використовувати плоску структуру, розділену на зони; використовувати базову станцію в якості арбітра (не потрібно додаткового обладнання, оновлення програмного забезпечення може вирішити цю проблему)
WO2018089417A1 Systems and methods to create slices at a cell edge to provide computing services [133]	**Пропонується в патенті:** карта зберігає інформацію про місцезнаходження, обчислювальні потужності та доступне сховище кожного з вузлів; **Недолік патенту:** Потрібна динамічно оновлювана карта зі списком вузлів (потрібні додаткові ресурси) **Запропонований в дисертації варіант усунення недоліку:** широковіщальна трансляція запиту від серверу MEC і відповідь базової станції обчислювальним вузлам дозволяє не використовувати карту або таблицю маршрутів або базу

	даних -> економія мережевих ресурсів
CN109041130A Resource allocation method based on mobile edge computing [134]	**Пропонується в патенті:** визначення для точки доступу оптимальної кількості необхідних фізичних ресурсних блоків CRB, а також оптимальну кількість CRB, що надсилаються на приграничний сервер; **Недолік патенту:** вибір обчислювальних вузлів не описується; тільки розподіл ресурсних блоків
CN108174421A MEC-assisted data shunting method in 5G network [135]	**Недоліки патенту:** - процедура розподілу мережевих ресурсів не описана; - відсутня перевірка даних та контроль помилок; - засновано на зменшенні частоти відмов при хендовері;
CN107333267A Edge computing method for 5G ultra-dense networking scene [136]	**Недоліки патенту:** - централізований MEC (має бути центральний комп'ютер або хмарна макро-базова станція); - в якості критерія розподілу використовує лише затримку;
CN107404733A 5G mobile communication method and system based on MEC (Mobile Edge Computing) and hierarchical SDN (software defined network) [137]	**Недоліки патенту:** - вимагає наявності ієрархічної SDN; - ідентифікація та автентифікація обчислювальних вузлів відсутня; - перевірка даних та контроль помилок відсутні.
US 2019/0045409 A1 Method and apparatus for implementing mobile edge application session connectivity and mobility [138]	**Недоліки патенту:** - описана лише передача для MEC - перевірка даних та контроль помилок відсутні; - безпечний канал зв'язку, балансування навантаження та вибір UE не описано.
US20120316939A1 System and method for discount deal referral and reward sharing [139]	**Недоліки патенту:** - безпека (ідентифікація, автентифікація) не передбачена; - потрібен рекламний сервер.
US20170255981A1 Method and system for online redistribution of data and rewards [140]	**Недоліки патенту:** - безпека (ідентифікація, автентифікація) не передбачена; - потребує наявність центральної бази даних.
US20120290308A1 Rewarding Users for Sharing Digital Content [141]	**Недоліки патенту:** - процедура перевірки даних (контенту) не описана; - підтримка мережі 5G відсутня; - безпечний зв'язок для передачі винагород відсутній.

3.6.3 Сутність запропонованого підходу

Для вирішення описаних проблем в роботі було використано наведену в табл. 3.11 архітектуру та враховані недоліки існуючих рішень, наведені в табл. 3.12. При цьому, для підготовки власного рішення [288], визначимо множину вхідних даних, набір обмежень, залежності між ними, а також множину вихідних значень.

Нехай на вхід системи розподілу навантаження для розподілених граничних обчислень поступають наступні дані:

n – множина доступних для МЕС обчислювальних вузлів з обчислювальними потужностями r_i та початкових рівнем довіри d_i;

di – початковий рівень довіри до обчислювального вузла;

$p(x_i)$ – ймовірність помилки під час розрахунків *i*-тим вузлом;

T_p – час на розподіл обчислювальних завдань;

Res – мережні ресурси задіяні під час розподілу завдань МЕС;

V – обсяг обчислень, які мають бути виконані.

Під час розподілу виконання обчислень, необхідно забезпечити мінімальну імовірність помилки розрахунків *p(n)* (3.16) та мінімізувати використані ресурси мережі під часу розподілу і виконання обчислювальних завдань: *(Res→min*), за умови обмежень на очікуваний час обчислень ($T_o \leq T_{зад}$) (3.15):

$$Result\_Func\_2 \rightarrow \min \{[\mathrm{Res}|(\max(\mathrm{V}) \;\&\; T_o \leq T_{зад})], \mathrm{p_i}, \mathrm{T_o}\}. \qquad (3.15)$$

Для визначення імовірності помилки розрахунків використовувалося середньозважене значення (3.16):

$$p(n) = \frac{1}{n}\sum_i^n p(x_i), \qquad (3.16)$$

В якості вихідних даних запропонований метод [288] має надати:

$y \in n\{0,n\}$ – множину пристроїв, які виконують розрахунок розподілених обчислень з розподілом навантаження на основі потужностей r_i

$w \in n\{0,n–y\}$ – множину додаткових пристроїв, що забезпечують надмірність і надійність розподілених обчислень.

Δd_i – змінення рівня довіри до i-го вузла за результатами виконаної ним роботи.

Очікуваний час обчислень буде складатися безпосередньо з часу виконання розрахунків і часу на розподіл обчислювальних завдань і може бути визначений як:

$$T_o = \frac{V}{n \cdot r} + T_\text{p}, \tag{3.17}$$

Або враховуючи множину пристроїв, які виконують розрахунок та множину додаткових пристроїв:

$$T_o = \frac{V}{\sum_i^y (y_i \cdot r_i) + \sum_i^w (w_i \cdot r_i)} + T_\text{p}. \tag{3.18}$$

В результаті був запропонований метод організації розподілених обчислень, що включає в себе:

- широкомовний запит від сервера МЕС на розподілені обчислення;
- відповідь на пейджинг від принаймні одного обчислювального вузла до базової станції, яка містить набір параметрів (ідентифікатор запиту, часову мітку тощо);
- базова станція перевіряє доступні ресурси та надає мережеві параметри для сесії МЕС принаймні одного обчислювального вузла, що дасть змогу організувати в подальшому підключення точка-точка;

• сервер MEC може перевірити результати обчислень за допомогою валідації даних, дзеркального відображення та контрольного коду.

Сутність описаного вище метода може бути проілюстрована за допомогою рис. 3.9.

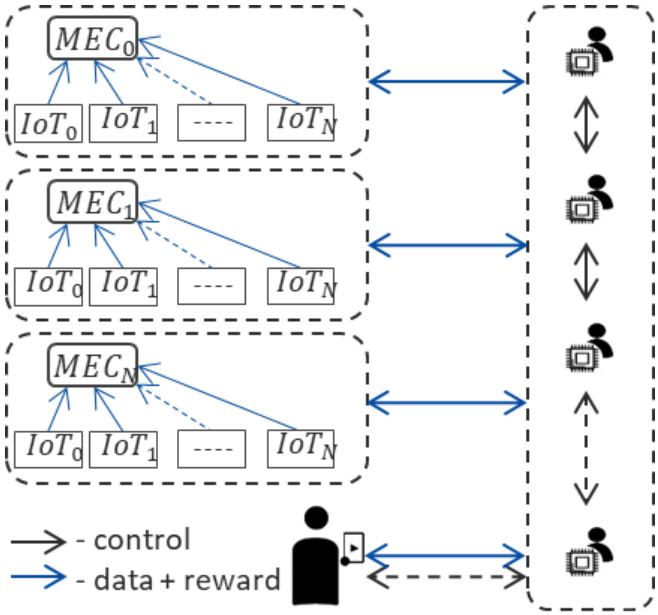


Рис. 3.9. Візуалізація принципу роботи запропонованого методу

В основу запропонованого способу зв’язку було покладено 2 нові методи:

- метод розподіленого зв'язку периферійних обчислень через 5G, який дозволяє визначити наявні вузли та здійснити розподіл обчислювальних блоків між ними;

- метод перевірки даних, віддзеркалення та пошуку помилок для системи MEC, який дозволяє контролювати появу помилок під час обчислень, захищати сервер від некоректних даних, а також пріоритезувати та нагороджувати вузли за результатами виконаних обчислень.

Розглянемо принцип роботи вказаних методів більш детально.

3.6.4 Запропонований метод захищеного вибору обчислювальних вузлів через мережу 5G

Принцип дії вказаного методу включає етап автентифікації і створення каналу точка-точка і етап обчислень та верифікації. На першому етапі (наведений на рис. 3.10) відбуваються наступні кроки:

1. Сервер MEC транслює запит на обчислення з наступною інформацією:
   - ідентифікатор MEC (тимчасовий або постійний ідентифікатор);
   - тип обчислення;

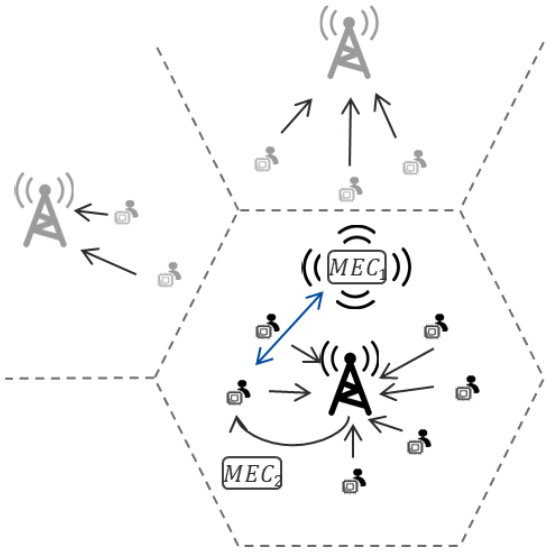


Рис. 3.10. Послідовність дій на першому етапі розподілених обчислень – автентифікації і створення каналу

2. Кожен обчислювальний вузол, отримавши пейджинг, відповідає на нього базовій станції:

$$E = F(\, C_{id}, T_{last}\,,\, E_{id}), \tag{3.19}$$

де (C_{id}) – ідентифікатор обслуговуючої соти (базової станції);

$(T_{last}\,)$ – мітка часу останнього отриманого слоту для обчислень;

(E_{id}) – ідентифікатор межі (тимчасовий або постійний).

3. Базова станція обирає обчислювальні вузли і призначає радіоканал:

- обирає обчислювальний вузол на основі отриманих значень E;
- призначає радіоканал, виходячи з наявних ресурсів;
- повідомляє про створений канал обміну інформацією сервер MEC та обчислювальний вузол.

На другому етапі, обчислень та верифікації виконуються наступні кроки (рис. 3.11):

1. Сервер MEC та обчислювальний вузол встановлюють радіоканал. Радіоканал формується на основі параметрів конфігурації каналу, які кожен з учасників отримує від базової станції.

2. Після цього сервер MEC та обчислювальний вузол виконують процедуру синхронізації.

3. На основі ETSI, обчислювальний вузол виконує API-дзвінок (рис. 3.12) і після завершення обчислень надсилає звіт до базової станції;

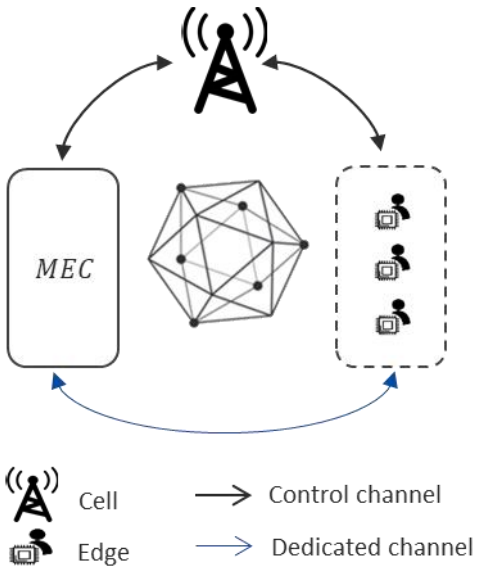


Рис. 3.11. Послідовність дій на другому етапі розподілених обчислень – обчислень та верифікації

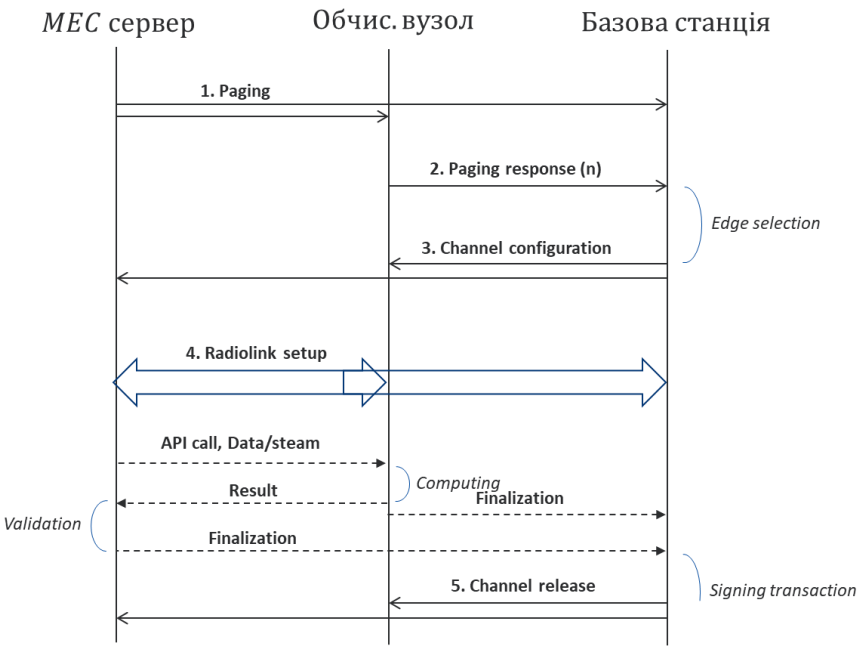


Рис. 3.12. Послідовність дій під час API-дзвінка на другому етапі

4. Після перевірки результату, сервер MEC звітує базовій станції.

5. Винагорода за виконання обчислень розраховується на основі складності виконаної операції, часу виконання та обсягу споживання дискового простору. Для захисту винагороди відбувається підписання блокчейн-транзакції між сервером MEC та обчислювальним вузлом.

Як було наведено вище, під час другого етапу сервер MEC має виконати перевірку обчислень на коректність та наявність помилок, крім того призначити кожному обчислювальному вузлу певний рівень довіри. Ці процедури передбачені у наступному запропонованому методі.

3.6.5 Запропонований метод перевірки результатів обчислень, виявлення помилок та встановлення рівня довіри для системи MEC

Кожне завдання, яке буде оброблятися на сервері MEC, містить частини, які можуть бути виконані незалежно. Ці частини додаються до завдання

розробниками програмного забезпечення (API). Результати таких зовнішніх обчислень несуть ризики обчислювальних помилок та різного роду атак. В даній роботі пропонуються комбіновані системи перевірки результатів роботи які включають аналіз рівнів довіри та надмірність.

Запропонований метод перевірки результатів обчислень та пошуку помилок, включає етапи:

1) обчислювальний пристрій сервера МЕС генерує код контролю помилок, як набір функцій низького обчислювального рівня.

Контрольний код (рис. 3.13) – це автоматично створене завдання з такою ж складністю, форматом і довжиною вхідних даних, як і реальне завдання, з тією лише різницею, що сервер МЕС знає точний результат, тому його можна перевірити.

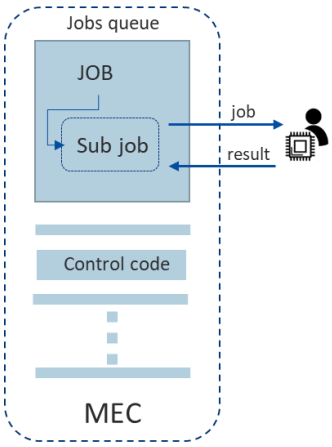


Рис. 3.13. Застосування контрольного коду для перевірки коректності обчислень

2) обчислювальний пристрій сервера МЕС розподіляє завдання між обчислювальними вузлами МЕС з додатковою надмірністю.

Додаткова надмірність (рис. 3.14) допомагає уникнути випадкових помилок в обчисленнях, які можуть виникнути навіть на автентифікованих

вузлах. Сервер MEC застосує результати роботи і надає винагороду тільки після того, як принаймні 51% вузлів, що отримали однакове завдання відправлять такі ж результати.

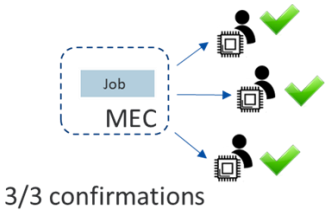


Рис. 3.14. Застосування додаткової надмірності для захисту обчислень від помилок

3) сервер MEC оновлює свій рівень довіри після успішного виконання завдання.

Кожен сервер MEC має власний "рівень довіри", який залежить від виконання контрольного коду та результатів раніше виконаних завдань. Якщо результати виконання контрольного коду правильні, рівень довіри (рис. 3.15) для цього обчислювального вузла підвищується. В іншому випадку, якщо пристрій обчислює контрольний код з помилками, рівень довіри знижується аж до повного блокування вузла.

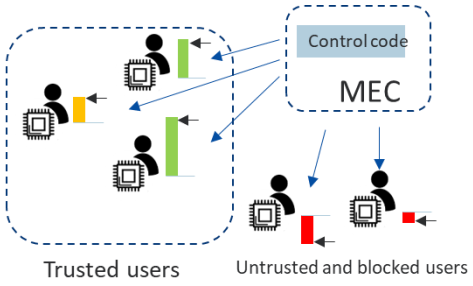


Рис. 3.15. Застосування рівня довіри для вибору обчислювальних вузлів

3.6.6 Переваги та наукова новизна запропонованого підходу

Переваги запропонованого методу можна розділити на переваги, які отримує користувач та переваги, які отримує мобільний оператор. До переваг користувача відносяться:

- *Простота налаштування*: як ідентифікатор обладнання користувача можна використовувати звичайні мережеві ідентифікатори (наприклад, IMSI) або номер блокчейн-гаманця.
- *Мобільність*: Розрахунок МЕС може бути зроблений без торгів за мобільні телефони/місцезнаходження.
- *Високий рівень безпеки*: Транзакція підписується за допомогою технології блокчейн.
- *Висока надійність*: Перевірка даних, дзеркальне відображення та контрольний код використовуються для захисту від шахрайства та виявлення помилок.

До переваг мобільного оператора відноситься:

- *Економія мережевих ресурсів* (порівняно з наведеними існуючими рішеннями [133-141]): Динамічна карта зі списком вузлів (або інша база даних / маршрутна таблиця) не потрібна.
- *Низька вартість* (порівняно з наведеними існуючими рішеннями [133-141]): не потрібно додаткового апаратного забезпечення, оновлення програмного забезпечення може вирішити описані проблеми.
- *Легкий вибір обчислювальних вузлів і балансування навантаження МЕС*: базова станція приймає рішення на основі набору обчислювальних вимог.

• *Підвищення спектральної ефективності*: зв'язок точка-точка, передбачений в 5G, відбувається без участі базової станції і зменшує навантаження на стільникову мережу.

Запропонований метод для розподілених периферійних обчислень зв'язку в 5G дозволяє ідентифікувати та автентифікувати учасників MEC, виділяти додаткові ресурси для MEC з мобільної мережі, включаючи підготовку зв'язку точка-точка, а також призначати обчислювальний блок і баланс навантаження для запиту MEC, за рахунок внесення змін в протокол обміну повідомленнями між базовою станцією та мобільними пристроями.

Науковою новизною методу є застосовані методи розподілу даних, перевірки даних, віддзеркалення та метод пошуку помилок для системи MEC, що дозволяє модулю MEC перевіряти результати обчислень та розподіляти ресурси на запит MEC.

3.7 Висновки

1. Вдосконалено модель класифікації трафіку шляхом визначення найкращого методу машинного навчання для класифікації трафіка та визначення його оптимальних параметрів за критеріями швидкості та точності класифікації.

Наукова новизна роботи полягає в визначенні оптимальних за критерієм точності параметрів алгоритмів машинного навчання для розв’язання задачі класифікації трафіка в мережах мобільного зв’язку 5-го та 6-го поколінь. Запропоновані параметри та алгоритми 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.

2. Вдосконалено набір ознак, за якими виконується класифікація трафіка.

Наукова новизна полягає у суттєвому скороченні кількості ознак, необхідних для класифікації трафіка без суттєвої втрати точності. Досягнуто зменшення набору ознак з 84 до 18 (на 79%), що призвело до погіршення точності з 0.707 до 0.638 (на 10%). Цей результат може бути використаний при налаштуванні класифікації трафіка для зменшення її складності і збільшення її швидкодії.

3. Запропоновано алгоритм управління кластерними промисловими IoT мережами, який дозволить клієнтам оптимізувати використання ресурсів при збереженні доступності та вхідної пропускної здатності кластера.

4. Запропонований метод для розподілених периферійних обчислень зв'язку в 5G дозволяє ідентифікувати та автентифікувати учасників MEC, виділяти додаткові ресурси для MEC з мобільної мережі, включаючи підготовку зв'язку точка-точка, а також призначати обчислювальний вузол і балансувати навантаження граничних обчислень, за рахунок внесення змін в протокол обміну повідомленнями між базовою станцією та мобільними пристроями.

Науковою новизною методу є застосовані методи розподілу даних, перевірки даних та пошуку помилок для системи MEC, що дозволяє модулю MEC перевіряти результати обчислень та розподіляти дані для обчислень.

4 ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ: ВДОСКОНАЛЕННЯ ЗАВАДОСТІЙКИХ КОДІВ

В даній дисертаційній роботі ставиться задача вдосконалення інформаційно-телекомунікаційної системи в цілому шляхом покращення якості надання послуг. Як було показано в розділі 1, для більшості послуг, що надаються в мережі важливу роль грають рівень помилок і відсоток втрат пакетів під час їх доставки, тому вдосконалення системи можна досягти вдосконаленням методів завадостійкого кодування, в тому числі застосуванням фонтанних кодів. Розглянемо математичні моделі та процедури кодування-декодування для описаних в підрозділі 1.5 методів завадостійкого кодування і підходи до їх вдосконалення.

4.1 Математичні моделі досліджуваних методів кодування

4.1.1 Математична модель коду RS

Коди Ріда-Соломона та засновані на них методи кодування, виявлення та виправлення помилок набули широкого поширення, після того, як Берлекемп та Мессі у 1968 році запропонували ефективний алгоритм виявлення та виправлення помилок [144], що знаходить розв'язок не більш ніж за $2t$ кроків. Саме цей момент можна вважати початком масового застосування кодів Ріда-Соломона для виявлення і виправлення помилок. До цього через достатню повільність і складність в апаратній реалізації наявних на той момент алгоритмів, здебільшого обходилися тільки обчисленням синдромів з метою виявлення помилки. У разі виявлення помилки робилася

спроба повторного запиту кадру, якщо це було можливо, в іншому разі видавалося повідомлення про помилку.

Кодування за допомогою коду Ріда-Соломона може бути реалізовано двома способами: систематичним і несистематичним [38,145].

При несистематичному кодуванні інформаційне слово множиться на обраний непривідний поліном у полі Галуа. Отримане закодоване слово повністю відрізняється від вихідного і для вилучення інформаційного слова потрібно виконати операцію декодування і вже потім можна перевірити дані на вміст помилок. Таке кодування вимагає великих витрат ресурсів тільки на витяг інформаційних даних, при цьому вони можуть бути без помилок.

При систематичному кодуванні до інформаційного блоку з k символів приписуються $2t$ перевірочних символів, при обчисленні кожного перевірочного символу використовуються всі k символів вихідного блоку. У цьому разі немає витрат ресурсів під час вилучення вихідного блоку, якщо інформаційне слово не містить помилок, але кодер/декодер має виконати $k*(n-k)$ операцій додавання і множення для генерації перевірочних символів. Крім того, оскільки всі операції проводяться в полі Галуа, то самі операції кодування/декодування вимагають багато ресурсів і часу.

Кодове слово Ріда-Соломона формується з залученням спеціального полінома. Усі коректні кодові слова мають ділитися без залишку на ці породжуючі поліноми. Загальна форма полінома, що породжує має вигляд:

$$g(x) = \prod_{i=1}^{2t}(x \oplus 2^i). \tag{4.1}$$

а кодове слово формується за допомогою операції:

$$F(x) = (x^r * M(x)) \oplus R(x), \tag{4.2}$$

де *g(x)* є поліномом, що породжує, *R(x)* є інформаційним блоком, F(x) – кодове слово, що називається простим елементом поля, *a* – примітивний елемент.

Кількість перевірочних символів може бути визначена з співвідношення:

$$R(x) = (x^r * M(x))mod(g(x)). \quad (4.3)$$

Рис. 4.1. Схема алгоритму кодування коду Ріда-Соломона (RS)

Нижче показана схема кодеру для версії RS(255,249):

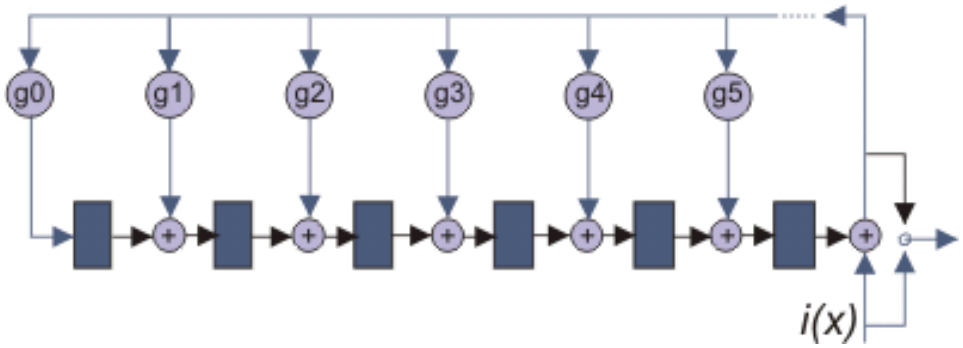


Рис. 4.2. Схема кодеру Ріда-Соломона

Кожен із 6 регістрів (рис. 4.2) містить у собі символ (8 біт). Арифметичні оператори виконують додавання або множення на символ як на елемент кінцевого поля. Під час передачі кадру мережею або під час зберігання кадру даних на носії, інформація може бути спотворена через ті чи інші фізичні причини: шуми в каналі передачі даних або пошкодження даних. У такому разі можна говорити, що на кадр *F* буде накладено деяке спотворення *E*, або іншими словами, поліном кадру *F(x)* буде складатися разом із деяким, так званим, поліномом спотворення *E(x)*, і в результаті матимемо спотворений поліном *C(x)=F(x)+E(x)* на момент приймання повідомлення з мережі або читання даних із носія. Спотворюватися можуть будь-які коефіцієнти полінома (байти кадру), як інформаційні, так і надлишкові. У підсумку матимемо, спотворений кадр *C*. Ступінь спотворення визначається за допомогою синдрому помилки *S(x)*:

$$S(x) = \sum_{j=1}^{r} C\left(2^j\right) * x^{j-1}. \quad (4.4)$$

Очевидно, що якщо поліном синдрому дорівнює нулю *S(x) = 0* (усі його коефіцієнти нульові), то можна говорити, що або помилок не було, або сталося спотворення, яке не виявляється за заданої кількості надлишкових

байтів через те, що кратність помилки, яка сталася, більша за кратність помилки, яку можна виявити, тобто $T > r = 2t$. В іншому разі, якщо синдром ненульовий, то можна декодувати його.

Кодове слово Ріда-Соломона має $2t$ синдромів, це залежить тільки від помилок (а не переданих кодових слів). Синдроми можна обчислити шляхом підстановки $2t$ коренів полінома, що породжує $g(x)$ у $C(x)$.

Знаходження позицій помилок у символах робиться шляхом розв'язання системи рівнянь з t невідомими. Існує кілька швидких алгоритмів для розв'язання цього завдання. Ці алгоритми використовують особливості структури матриці кодів Ріда-Соломона і сильно скорочують необхідну обчислювальну потужність. Наприклад, через визначення полінома локації помилок. Це може бути зроблено за допомогою алгоритму Berlekamp-Massey або алгоритму Евкліда [144]. Алгоритм Евкліда використовується частіше на практиці, тому що його легше реалізувати, однак, алгоритм Berlekamp-Massey дає змогу отримати ефективнішу реалізацію. Після чого виконується знаходження коренів цього полінома.

Принципи відновлення даних в кодах RS.

Нехай є три довільних цілих числа A,B,C, будь-які два з них можуть бути стерті у BEC, необхідно відновити стерті числа через ті, що залишилися. Для цього застосуємо "алгебраїчний" підхід. Він полягає в наступному. Складається матриця спеціального виду, розміру 5×3. Перші три рядки цієї матриці утворюють одиничну матрицю, а останні два – це деякі числа, вибір яких буде описаний нижче. В англомовній літературі цю матрицю зазвичай називають generator matrix (породжуюча матриця). Помножимо сконструйовану матрицю на вектор, складений з вихідних чисел A, B і C.

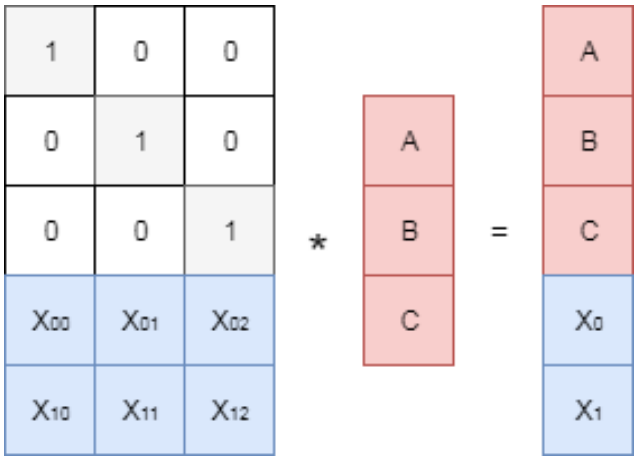


Рис. 4.3. Перетворення для відновлення даних – 1

У результаті множення матриці на вектор із даними отримуємо два "надлишкових" числа, позначених на рис.4.3 як X0 і X1, які будуть використані для відновлення стертих A і B.

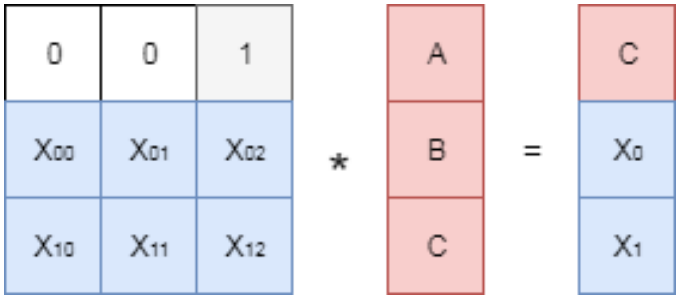


Рис. 4.4. Перетворення для відновлення даних – 2

Для відновлення A і B, викреслюють відповідні рядки з матриці, що породжує, і знаходять обернену до неї. На рис. 4.5 ця обернена матриця позначена як $\{Y_{ij}\}$. Тепер помножимо ліву і праву частини вихідного рівняння на цю обернену матрицю:

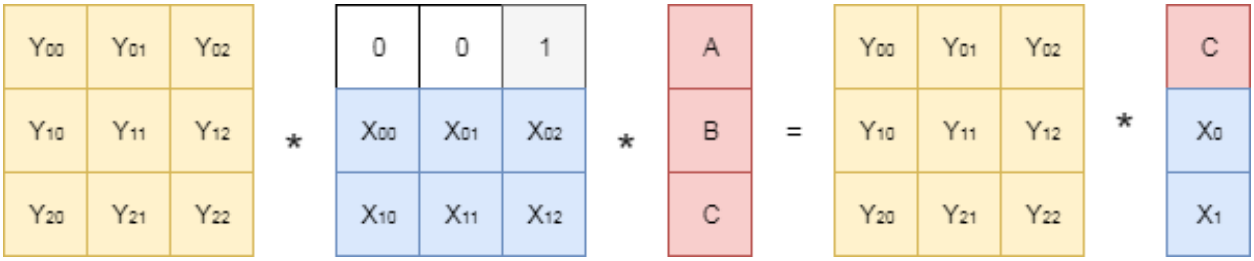


Рис. 4.5 – Перетворення для відновлення даних – 3

Скорочуючи матриці в лівій частині рівняння (добуток оберненої і прямої матриць є одинична матриця), і з огляду на той факт, що в правій частині рівняння немає невідомих параметрів, отримуємо вирази для шуканих A і B.

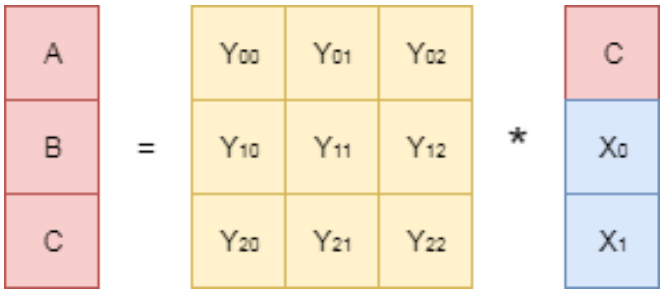


Рис. 4.6 – Перетворення для відновлення даних – 4

Процес кодування полягає в знаходженні "надлишкових" даних *X0, X1*, а процес декодування – у знаходженні оберненої матриці та множення її на вектор даних, що "збереглися". Розглянута схема може бути узагальнена на довільну кількість інформаційних і надлишкових даних. Інакше кажучи, за вихідними N числами можна побудувати K надлишкових, причому завжди можливо відновити втрату будь-яких K з $N+K$ чисел. У цьому разі матриця що породжує матиме розмір $(N+K)\times N$, а верхня частина матриці розміром $N\times N$ буде одиничною. При побудові породжувальної матриці вибір чисел X_{ij} потрібно здійснювати таким чином, щоб незалежно від рядків, що викреслюються, матриця залишалася оборотною. Приклад – матриця Коші. У

цьому випадку сам метод кодування часто називають методом Коші-Ріда-Соломона (Cauchy-Reed-Solomon). Іноді, для цих же цілей використовують матрицю Вандермонда, і відповідно, метод має назву Вандермонда-Ріда-Соломона (Vandermonde-Reed-Solomon).

4.1.2 Математична модель коду LDPC

Коди з малою щільністю перевірок на парність (Low Density Parity Check — LDPC) є лінійними блоковими кодами, перевірочні матриці яких в кожному стовпці і кожному рядку мають мале число одиниць в порівнянні з числом нулів в них [32]. Вперше LDPC коди були введені Р. Галлагером в 1963р.

Наддовгі LDPC коди застосовуються в сучасних телекомунікаційних стандартах, наприклад, в DVB-S2 [147]. При цьому в стандарті не вказані явним чином можливості виправлення бітових помилок наддовгими LDPC кодами. Тому важливою науковою і практичною задачею є визначення можливості виправлення помилок наддовгими LDPC кодами і визначення місця цих кодів серед відомих блокових кодів шляхом порівняння їх характеристик.

Формування регулярних LDPC кодів визначено послідовної процедурою [32]. Регулярний LDPC код з довжиною блоку n формується на основі перевірочної матриці H, яка характеризується постійним числом одиниць в рядку W_r і постійним числом одиниць в стовпці W_c. Перевірочна матриця H має низьку щільність одиниць (щільність одиниць вважається низькою, якщо питома частина одиниць становить менше 50% всіх елементів перевірочної матриці).

На підставі заданих параметрів n, W_r, W_c змінюються коригувальні властивості коду t, біт. При цьому, положення одиниць в перевірочної

матриці H формується на основі випадкових перестановок стовпців базової підматриці, що містить тільки одну одиницю в кожному стовпці. При цьому швидкість регулярного LDPC-коду, залежно від параметрів перевірочної матриці, визначається за формулою:

$$r_k = \frac{n - \left(n \cdot \frac{W_c}{W_r} - \left(W_c - 1 \right) \right)}{n} = 1 - \frac{W_c}{W_r} + \frac{W_c - 1}{n}. \qquad (4.5)$$

У той же час, матриці H LDPC коду однакового розміру і з однаковими параметрами можуть породжувати коди з різними кодовою відстанню d і виправлювальною здатністю t. Звідси випливає завдання пошуку найкращої перевірочної матриці LDPC коду із заданими параметрами n, W_r, W_c за критерієм максимальної виправлювальної здатності $t_{\max} \le \left(d_{\max} - 2 \right) / 2$.

Перевірочна матриця LDPC коду може бути представлена у вигляді:

$$H = \begin{bmatrix} H_1 \\ \hline \pi_1(H_1) \\ \hline \vdots \\ \hline \pi_{Wc-1}(H_1) \end{bmatrix}, \qquad (4.6)$$

де H_1 – базова підматриця, $\pi_i(H_1)$ – підматриці, отримані шляхом випадкової перестановки стовпців базової підматриці H_1, $i = 1, 2, \ldots, W_c - 1$.

Перевірочну матрицю H можна привести до вигляду:

$$H = \left[A \middle| I_{n-k} \right], \qquad (4.7)$$

де A – деяка фіксована $\left(\left(n-k\right)\times k\right)$ – матриця з 0 і 1, а I_{n-k} – одинична матриця розміру $\left(n-k\right)\times\left(n-k\right)$.

Матриця генерування кодових слів G слів має вигляд:

$$G=\left[I_k\middle|-A^T\right]. \tag{4.8}$$

Якщо матриця H представлена у вигляді (4.7), то матриця G (4.8) легко може бути знайдена з матриці H шляхом перетворень методом Гауса [150].

Матриця G також називається такою, що породжує (породжуюча), так як кодовими словами є всі можливі лінійні комбінації рядків матриці G. Матриці H і G зв'язані співвідношеннями:

$$GH^T=0, HG^T=0, \tag{4.9}$$

Формування кодового слова виконується на основі операцій множення і додавання інформаційних біт з рядками матриці що породжує G. Декодування інформації може проводитись різними ітераційними методами, що оперують прийнятим кодовим словом і перевірочною матрицею H.

Кодова відстань d для регулярного LDPC-коду визначається наступним чином: d рівне найменшому числу стовпців перевірочної матриці H, які в сумі дають 0. Для регулярних та нерегулярних LDPC кодів на сьогоднішній день не існує точного аналітичного виразу, який дає відповідь на питання щодо виправляючої здатності LDPC- коду. Однак, існують пряма і зворотна теореми про кодову відстань лінійного коду LDPC [32].

Теорема 1. Якщо будь-які $l \le d-1$ стовпців перевірочної матриці H лінійного коду лінійно незалежні, то мінімальна кодова відстань коду буде

щонайменше *d*. Якщо при цьому знайдуться *d* лінійно залежних стовпців, то кодова (мінімальна) відстань коду лише *d*.

Теорема 2. Якщо мінімальна кодова відстань лінійного коду рівна *d*, будь-які $l \leq d - 1$ стовбців перевірочної матриці H лінійно незалежні і буде знайдено *d* лінійно залежних стовбців.

Таким чином, з теорем 1, 2 можна зробити висновок, що кодова відстань коду LDPC, за матрицями *G* і *H* для LDPC-коду визначається наступним чином:

– *d* дорівнює найменшому числу стовпців матриці *H*, які в сумі дають 0;

– *d* дорівнює найменшій вазі рядку (числу одиниць в рядку) матриці *G*.

Ці властивості дають можливість визначити кодову відстань і виправлювальну здатність LDPC-коду з матриць H і G шляхом аналізу властивостей перевірочної або генеруючої матриць LDPC коду.

Важливо відзначити, що лінійний код з кодовою відстанню *d* може виправляти (*d*–1)/2 помилок. LDPC коди характеризуються парних значенням кодової відстані *d*, тому LDPC код може одночасно виправляти (*d*–2)/2 помилок, та виявляти *d* / 2 помилок.

4.1.3 Математичні моделі фонтанних кодів

Поняття "Цифровий фонтанний код" ввів Байєрс та ін. [150] в 1998 році. В рамках цього нового виду багатоадресних і широкомовних протоколів, приймач може відновити вихідні дані по кодованих символах, випадково взятих з каналу з великими втратами. Шаблон втрат каналу може бути невідомим і доступ до даних буде ініціюватися в довільний момент часу. Прикладом такого коду є код Торнадо, який заздалегідь повинен оцінити втрати в каналі і обов'язково мати фіксовану швидкість коду *R*, близьку до значення втрат [36,151]. До основних характеристик цифрових фонтанних

кодів відносять надійну доставку, відсутність повторної передачі, відсутність зворотного зв'язку, ефективне кодування і декодування, доступ до даних на вимогу.

Теоретично цифровий фонтанний код в каналі зі стираннями без пам'яті виглядає наступним чином. Запитаний файл розбивається на K блоків однакового розміру, і кожен блок інкапсулюється в пакет. Базуючись на цих K пакетах, фонтанний кодер може потенційно генерувати необмежений потік незалежних і однаково розподілених закодованих пакетів. Ці кодовані пакети передаються по каналу зі стираннями, але тільки частина пакетів приймається без помилок – всі інші будуть відкинуті. Потім фонтанний декодер, з високою ймовірністю, відновлює початкові пакети з будь-якої підмножини отриманих кодованих пакетів.

Фонтанні коди – це коди без фіксованої швидкості, так як на передавальній і приймальній стороні кодова швидкість не фіксована і може потенційно дорівнювати нулю. Тим не менш, на практиці необхідно розглянути усічені фонтані коди. В фонтанних кодах, може бути призначена мінімальна кількість прийнятих пакетів для задоволення вимог. Наприклад, це мінімальне число – n, і декодер відновлює дані з k/n усіченого фонтанного коду. Для ідеального або оптимального фонтанного коду, кодова швидкість повинна дорівнювати 1. При k трохи менше ніж n, фонтанний код не є оптимальним. На сьогоднішній день існує два основних класи практичних фонтанних кодів: Luby Transform (LT) коди і коди Raptor. Обидва коди квазі-оптимальні для кінцевої довжини даних.

4.1.3.1 Математична модель LT коду

Винайдені Лабі, коди LT [35,171] – це перший клас практичних фонтанних кодів. Як лінійний код, код LT може генерувати змінну кількість

незалежних і однаково розподілених кодованих символів. Використовуючи породжувальну матрицю, декодер LT може відновити вихідне повідомлення на льоту з довільно зібраних закодованих символів з невеликими витратами на декодування. Звичайні коди LT швидкі і ефективні з ітеративним алгоритмом декодування переданих повідомлень, при жорсткому декодуванні інформації. Вони можуть адаптуватися до багатоадресного і широкомовного середовища Інтернет тільки через розподіл ступеня для вихідних кодованих символів. У приймачі, інформація про сусідів кожного кодованого символу використовується для побудови графа Таннера породжувальної матриці.

Загальний метод генерації потоку кодованих символів задається як створення рядків породжувальної матриці G на льоту або заздалегідь. Після того, як рядок G_i визначається, відповідний кодований символ y_i стає скалярним добутком рядка і стовпчика вектору s для всіх k вхідних символів. Кодований символ задається

$$y_i = G_i s, \tag{4.10}$$

де $i = 1,2, \cdots$.

З цієї точки зору, вихідні символи є незалежними один від одного і порядок стовпців не має значення для продуктивності коду. Закодовані символи будуть передаватися по міру необхідності. Коли приймач збирає достатньо закодованих символів, він може повідомити передавач, що прийом завершений. Після того, як передавач отримує повідомлення про завершення від всіх терміналів, він може припинити відправку закодованих символів.

Оскільки декодер знає всіх сусідів кожного прийнятого кодованого символу, він відтворює всі відповідні стовпці в оригінальній породжувальній матриці. З цими відновленими колонками, декодер формує породжувальну матрицю A усіченого коду LT, розміром $m \times n$. Вихідні символи передаються каналом зі стираннями і деякі з них будуть видалені. На стороні приймача, з n прийнятих символів, декодер створює породжувальну матрицю G розміром $n \times k$ ($k \leq n \leq m$) яка відповідає матриці A, але без рядків, відповідних стертим символам. Тоді, як n отриманих символів – це випадкова підмножина m переданих символів.

Процес декодування. При опублікуванні винаходу кодів LT, Лабі [35] представив алгоритм декодування цих кодів для боротьби зі стираннями. Алгоритм переданих повідомлень представляє собою жорстку схему декодування, яка може бути дуже швидкою і ефективною. Існують два типи декодування переданих повідомлень з кодом LT: послідовне декодування та паралельне декодування.

Послідовна процедура декодування кодів LT [171]:

Крок 1: Знайти один v-вузол 1-го ступеня і призначити його значення сусідньому s-вузлу. v-вузол звільняється, далі відновлюються сусідні s-вузли. У той же час видаляється грань, яка з'єднує ці вузли.

Крок 2: значення відновленого s-вузла складається за допомогою операції XOR з усіма своїми сусідами (не включаючи тільки видалений) потім грані, які з'єднували ці вузли видаляються з графу, стовпчик, який відповідає відновленому символу, видаляється з породжувальної матриці

Крок 3: Якщо всі s-вузли відновлюються, декодування успішно завершується. В іншому випадку, повторюється процедура, починаючи з кроку 1. Якщо немає вузлів зі ступенем 1 і декодування не завершене – кадр відкидається.

Паралельне декодування може бути реалізоване так само легко, як послідовний метод, але працювати швидше. Приклад паралельного декодування переданих повідомлень коду LT наводиться на рис. 4.7. Розмірність коду – $k = 4$ і число прийнятих пакетів $n = 7$, так $(n, k) = (7,4)$ в приймачі реалізовано усічений код LT. Припустимо, що породжувальна матриця усіченого коду LT M задається рівнянням (4.11).

$$M = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}, \tag{4.11}$$

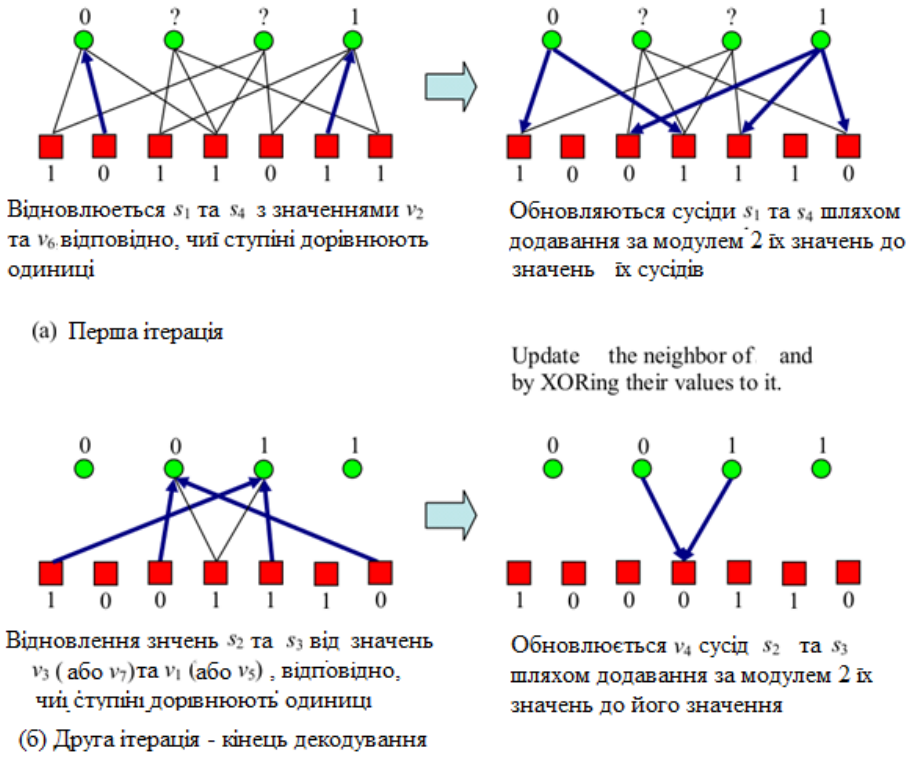


Рис. 4.7. Приклад паралельного жорсткого декодування LT коду [171]

Пакет передачі даних еквівалентний символу, який може бути представлений послідовністю значень, діапазони яких можуть бути від одного біта до кількох біт, для простоти розмір значення у прикладі дорівнює одному біту. Припускаємо, що отримані кодовані символи [1 0 1 1 0 1 1].

Відновлення чотирьох вихідних символів займає чотири ітерації [0 0 1 1] в послідовному декодуванні, але для паралельного декодування потрібно всього дві ітерації. Можна перевірити результат декодування з [0 0 1 1], M=[1 0 1 1 0 1 1].

Якщо повідомлення потрапляють до набору зупинки, кодування не може бути продовжене навіть якщо вихідна породжувальна матриця в декодері має повний ранг. Припустимо, що приймач створює породжувальну матрицю повного рангу з розмірністю 4, задану як

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}, \qquad (4.12)$$

Прийняті закодовані символи: [1 0 1 1 0 0 0]. Після завершення першої ітерації, декодування припиняється тому що немає v-вузла зі ступенем розподілу, який дорівнює 1 для другої ітерації. Декодування зупиняється набором зупинки (stopping set), що складається з v_1, v_3, v_4, v_5, v_6 і v_7. Всі ці наведені v-вузли мають ступінь розподілу 2 або більше.

Для того щоб дослідити складність кодів LT, спочатку потрібно розглянути роботи представлені Маккеєм [157]. Це експеримент ”м’ячі-і-контейнери”. В ідеальному випадку, кожний кодований символ являється сусідом з одним інформаційним символом від джерела повідомлень.

Випадково кинуті *n* ідентичних м’ячів в *k* рівних контейнери. Якщо м'яч кинутий – кожен контейнер має ймовірність того що він попаде – *1/K*. У цих умовах, враховуючи *n* кинутих м’ячів, ймовірність того, що певні контейнери не мають попадання $(1-(1/k))^n$. Якщо *k* велике, ця ймовірність наближається до $(1-(1/k))^n \approx e^{-n/k}$ через $\lim_{x\to\infty}(1+1/x)^x$. Для того, щоб попасти у всі *k* контейнери хоча б з імовірністю $1-\delta(0<\delta<1)$ має бути $(1-1/k)^n<1$, і, отже, $n > k\ln(k/\delta)$ при великих *k*. Це більш низька оцінка допомагає проаналізувати ступінь розподілу.

Хоча робасний розподіл полегшує практичні коди LT, вартість кодування залишається проблемою, складність обчислень в середньому має порядок *ln(k/δ)*. З $n = k\beta$ закодованих символів, середній ступінь закодованого символу

$$D_{e,avg} = \sum_{d=1}^{k} d\mu(d) = \sum_{d=1}^{k} \frac{d[\rho(d)+\tau(d)]}{\beta}, \tag{4.13}$$

Таким чином, отримуємо

$$D_{e,avg} \le \sum_{d=1}^{k} d[\rho(d)+\tau(d)], \tag{4.14}$$

Середній ступінь інформаційного символу від джерела є

$$D_{s,avg} = D_{e,avg} n/k = \sum_{d=1}^{k} d[\rho(d)+\tau(d)] =$$

$$= 1/k + \sum_{d=2}^{k} d/[d/(d-1)] + \sum_{d=1}^{k/r-1} dr/dk + (k/r)(r/k)\ln(r/\delta) \approx \approx H_k + 1 + \ln(r/\delta), \tag{4.15}$$

де H_k гармонічна сума до k.

Luby [35] визначив, що для великої довжини даних, складність обчислення кодів LT має в середньому значення $O\ (ln\ (k / \delta))$.

4.1.3.2 Математична модель коду Raptor

Raptor код [37] є розширенням коду LT, але можна домогтися лінійної складності при передачі декодованих повідомлень. В рамках 3GPP, коди Raptor використовуються для надійної доставки даних в мобільних бездротових мережах, широковіщальній і груповій доставці.

Raptor коди – каскадні коди. Символи даних по-перше попередньо кодуються зовнішнім кодом. Вихідні символи прекодеру називаються проміжними символами, і вони являються вхідними символами внутрішнього коду LT. Прекодер – код з фіксованими параметрами, як правило, з досить високою швидкістю. Прекодер може бути багатоступеневим, тобто попередньо код може бути сумою кількох кодів з фіксованими параметрами. Внутрішній код LT іноді називають ослабленим LT кодом [157].

Raptor код може позначатися $(k, C, \Omega\ (x))$, де k – кількість символів джерела і $\Omega(x)$ – поліном розподілу ступеню кодованих символів внутрішнього коду LT. $\Omega(x)$ описується через

$$\Omega(x) = \Sigma_d \Omega_d x^d, \tag{4.16}$$

де d обрана ступінь LT закодованого символу. Середній ступінь закодованих символів дорівнює $\Omega'(1)$, де $\Omega'(x)$ є похідною від $\Omega(x)$ відносно x.

Shokrollahi [37] ввів розподілення ступеня закодованих символів для ослабленого коду LT. Де ε – дійсне число більше нуля і $D = \lceil 4\ (1 + \varepsilon) / \varepsilon \rceil$, а поліном розподілу ступеня описується через

$$\Omega(x) = \frac{1}{1+\mu}\left[\mu x + \sum_{d=2}^{D} \frac{x^d}{(d-1)d} + \frac{x^{D+1}}{D}\right], \qquad (4.17)$$

де $\mu = (\varepsilon/2) + (\varepsilon/2)^2$.

Передача декодованих повідомлень. Ітераційний алгоритм переданих повідомлень працює з двома матрицями: з породжувальною матрицею внутрішнього коду LT і перевірочною матрицею зовнішнього коду. Проміжні символи не тільки *v*-вузли у графі Таннера з прекодеру перевірочної матриці, а й *s*-вузли породжувальної матриці LT коду. LT декодер оновлює декодоване повідомлення на предекодері і далі приймається рішення на виході декодера попереднього коду. Декодування вважається успішним коли максимальне число ітерацій закінчено і всі проміжні символи були отримані.

Є два типи алгоритмів відновлення переданих повідомлень для Raptor кодів [153]. В першому методі, декодер LT використовує алгоритм проходження повідомлення для відновлення проміжних символів стільки, скільки може, поки декодування LT не буде зупинене за допомогою набору зупинки. Тоді значення відновлених проміжних символів передаються на *v*-вузли графа Таннера матриці контролю парності прекодеру і зовнішній декодер відновлює інші проміжні символи. Цей метод являє собою схему локальних ітерацій. Другий спосіб – схема глобальних ітерацій. Кожна ітерація декодування складається з двох етапів: однієї ітерації за допомогою LT коду, а потім однієї ітерації за допомогою прекодеру. В кінці кожної стадії, оновлені значення проміжних символів передаються в інший декодер.

Винахідник кодів Raptor, Shokrollahi, встановив [37], що прекодери для хороших кодів Raptor, як правило, мають високу швидкість. Чим вище кодова швидкість на прекодері, тим менше проміжних символів

створюються. Таким чином, з тією ж швидкістю Raptor коду, більш значна частка проміжних символів може бути відновлена за допомогою одного і того ж або аналогічного внутрішнього LT коду і тому показники помилок відповідно кращі.

Складність кодування. Shokrollahi в [37] доводить, що, з ретельно розробленим солітонівським розподілом *Ω(x)* і відповідною R_c (4.18) прекодеру *C*, коди Raptor досягають лінійного кодування і декодування. Прекодер *C* повинен бути лінійним кодом довжини *n* з такими властивостями:

$$R_c = (1+\varepsilon/2)/(1+\varepsilon), \tag{4.18}$$

ймовірнісний декодер [32] може декодувати прекодер C у бітовому каналі зі стиранням (bit error channel, BEC) з імовірністю стирання

$$\delta = \frac{(\varepsilon/4)}{(1+\varepsilon)} = \frac{(1-R)}{2}, \tag{4.19}$$

з $O(\ln(1/\varepsilon))$ арифметичних операцій в середньому на кожен символ. У відповідності до рівняння (4.18), швидкість прекодеру обмежена

$$0.5 < R_c < 1, \tag{4.20}$$

Shokrollahi [37] також встановив, що *(k, C, Ω (x))* Raptor код має швидкість $1/R_c$, збирає $(1+\varepsilon)\,k$ Raptor кодованих символів для декодування, і вартість $O(\ln(1/\varepsilon))$ по відношенню до ймовірнісного декодування як прекоду

так і коду LT. Ймовірність помилки цього декодера лише поліноміально менше *k*. Для одноетапного прекодеру Raptor коду, Shokrollahi [37] визначає вартість кодування як $E(C)/K + \Omega'(1)$, де $E(C)$ число арифметичних операцій, необхідних для створення кодового слова в прекодері.

Для того, щоб проілюструвати кодер Raptor, припустимо, що прекодер – одноетапний LDPC код. Для кодів LDPC, є два найпоширеніші способи кодування. Один з них – прямолінійне кодування з допомогою породжувальної матриці, а інший швидке кодування за допомогою матриці перевірок на парність. Таким чином, доступні два типи ефективних і практичних кодерів Raptor.

Швидке кодування (рис. 4.8) можливе за допомогою матриці з низькою щільністю перевірок на парність, і це дуже корисно для кодування Raptor. Розглянемо два швидких методів кодування з матрицею перевірок на парність.

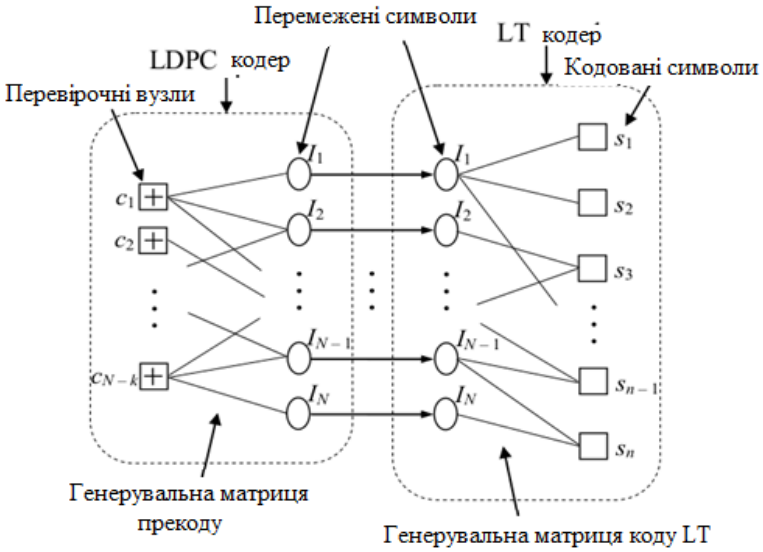


Рис. 4.8. Швидке кодування кодів Raptor [171]

Перший алгоритм швидкого кодування був введений Річардсоном і Урбанке [155], і знижує вартість кодування до $O(N + g^2)$. Ціле позитивне

число g має бути таким малим, наскільки це можливо. Цей швидкий алгоритм кодування спільний для всіх кодів LDPC [39,40,160]. Дається дуже рідка $(N - k) \times N$ матриця перевірок на парність H, T – нижня трикутна матриця, яка має всі 1 по головній діагоналі і все що вище головної діагоналі – нулі (рис. 4.9).

$$H = \begin{bmatrix} A & B & T \\ C & D & E \end{bmatrix}, \tag{4.21}$$

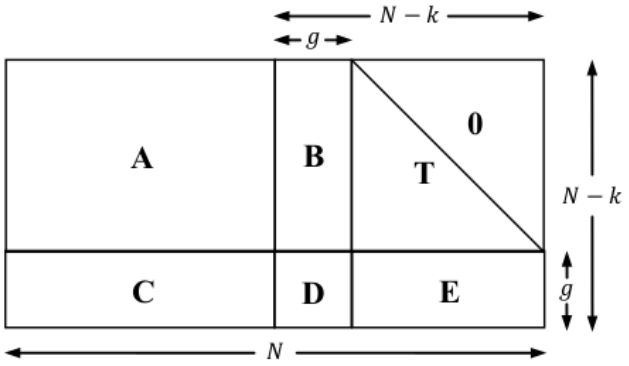


Рис. 4.9. Матриця перевірок на парність в приблизній нижнє-трикутній формі для швидкого кодування

Якщо оригінальна матриця H дуже рідка, переставлена матриця H буде також рідкою і це дозволяє отримати приблизно лінійну вартість кодування. Якщо ця матриця перевірок на парність має повний ранг n –k, розмірність коду буде дорівнювати k. Припустимо, H двійкова матриця і всі обчислення будуть виконуватись за модулем 2. Для будь-якого початкового блоку U (вектор-рядків), послідовність кодування v знаходиться в систематичній формі

$$v = [u \quad p_1^T \quad p_2^T]. \tag{4.22}$$

Частини парності p_1^T і p_2^T розроблені з наступними правилами:

1. Знаходиться верхній вектор синдрому U,

$$z_A = Au^T, \tag{4.23}$$

2. Обчислюється послідовність бітів контролю парності p_2^A, яка прирівнює верхній вектор синдрому до 0.

$$p_2^A = T^{-1} z_A, \tag{4.24}$$

3. Знаходиться нижній вектор синдрому *[U 0 p]*

$$z_B = Cu^T + Ep_2^A. \tag{4.25}$$

4. Визначається

$$F \equiv ET^{-1}B + D, \tag{4.26}$$

потім знаходиться перша частина рівняння

$$p_1 = F^{-1} z_B. \tag{4.27}$$

5. Розраховується новий верхній вектор синдрому

$$z_C = z_A + Bp_1 . \quad (4.28)$$

6. Нарешті інший набір бітів контролю парності, p_2^A, може бути отриманий, наприклад, таким що верхній синдром дорівнює нулю

$$p_2 = T^{-1} z_C . \quad (4.29)$$

Майже всі шість етапів можуть бути зроблені в лінійному часі. p_2^A в кроці 2 і p_2 в кроці 6 знаходяться в лінійному часі по зворотній підстановки. На кроці 4, обчислення F займає $O(g^3)$ але це робиться лише один раз, перед кодуванням будь-якого блоку джерела. Складність рівняння (4.29) – $O(g^2)$. Саме тому r вибирається, якомога меншим.

Незалежно від того фонтанний код використовується на пакетному або бітовому рівні, алгоритм відновлення переданих повідомлень однаковий. Конфігурація декодеру Raptor також однакова для схем місцевих ітерацій і глобальних ітерацій декодування. Сивасубраманіан і Лейб [159] представили алгоритми для декодера місцевих ітерації. Сивасубраманіан і Лейб [153,159] і Хуанг та ін. в [41] описали загальну конфігурацію декодеру глобальних ітерацій для LDPC-кодів, кодів LT і кодів Raptor, і пояснили принцип роботи декодера Raptor.

Кожний код перетворюється у бінарну послідовність. Двійкові 0 і 1, як передбачається, з'являються з однаковою ймовірністю. У моделі пакетних стирань фонтанного коду, корисне навантаження пакета можна розглядати як один біт. Декодовані повідомлення в моделі – логарифмо-подібні співвідношення двійкової випадкової величини $X \in \{0,1\}$ в $GF(2)$, типу

$$L(x) = \ln \frac{P_X(x=0)}{P_X(x=1)}, \tag{4.30}$$

де $P_X\ (x)$ ймовірність того, що X приймає значення x. В системі моделей, описаних в цьому розділі, $P\ (S_i = 0) = P\ (S_i = 1)$. S_i еквівалентно фонтанному кодованому біту. Згідно висновку в [39], розглянуте ЛПС в каналі зі стираннями для прийнятого біту r_i задається як:

$$L(r_i) = \begin{cases} \infty, & r = 0 \\ -\infty, & r = 1 \\ 0, & r = e \end{cases}, \tag{4.31}$$

де e означає стирання. Під час всієї процедури декодування пакетів, вартість декодування повідомлення дорівнює $+\infty$, $-\infty$ або 0. Для випадку використання тільки коду LT, жорстке декодування може замінити м'яким декодуванням, тому що стирання не приймають участь в декодуванні і двійкові 0 і 1 представляють собою м'яку інформацію $+\infty$ і $-\infty$.

У моделі бітових корегуючих фонтанних кодів, передані біти у вигляді BPSK, тому декодована інформація є ЛПС бінарної випадкової величини $X \in \{\pm 1\}$ *в GF (2)* з «+1» – двійкова «1» і «-1» – двійковий «0»:

$$L_X(x) = \ln \frac{P_X(x=-1)}{P_X(x=+1)}. \tag{4.32}$$

Згідно висновку в [39], досліджуване логарифмо-правдоподібне співвідношення від АБГШ каналу для прийнятого біту r_i задається як

$$L(r_i) = -4r_i / N_0 = -4(h_i s_i + n_i / N_0), \tag{4.33}$$

де r_i вибірковий вихід приймача узгодженого фільтру, n_i – адитивний шум, і N_0 – однобічна спектральна щільність потужності білого гаусовського шуму.

Для безпомилкової передачі, в системній моделі пакетних стирань фонтанних кодів, приймач завжди має $n = 1$ $(r = 0)$ для $S_i = 1$ $(S_i = 0)$; в системній моделі бітового виправлення фонтанних кодів – $r_i = 1$ $(r_i = -1)$ для $s_i = 1$ $(s_i = 0)$.

4.2 Аналіз методів підвищення завадостійкості кодів за рахунок перемежіння

Зміну за певним правилом природного порядку проходження символів в деякій кодової послідовності називають процедурою перемежіння (Interleaving), зворотну перемежінню процедуру прийнято називати деперемежінням (deinterleaving). В результаті виконання процедури деперемежіння відновлюється природний порядок проходження символів.

Перемежіння і деперемежіння зазвичай використовуються для відновлення пакетів помилок, викликаних завмираннями рівня прийнятого сигналу і зменшення ступеня групування помилок у послідовності, що надходять на вхід канального декодера. При перемежінні передане кодове слово формується із символів різних кодових слів. Тому при деперемежінні виникаючий пакет помилок розбивається на окремі помилки, що належать різним кодовим словам. Інакше кажучи, при деперемежінні пакет помилок трансформується в послідовність незалежних помилок, для виправлення яких, як правило, можна використовувати менш потужний код. Збільшення глибини перемежіння поліпшує характеристик завадостійкості, оскільки при цьому відбувається ослаблення кореляції помилок. Але при цьому зростає затримка в доставці повідомлення, пов'язана з виконанням процедур

перемежіння і деперемежіння. Тому доводиться приймати компромісне рішення між ступенем поліпшення характеристик завадостійкості та можливою затримкою. Розглянемо найбільш ефективні методи перемежіння.

4.2.1 Блокове перемежіння

При блоковому перемежінні кодові слова довжиною n символів записуються у вигляді таблиці шириною W і глибиною D символів, як показано на рис. 4.10.

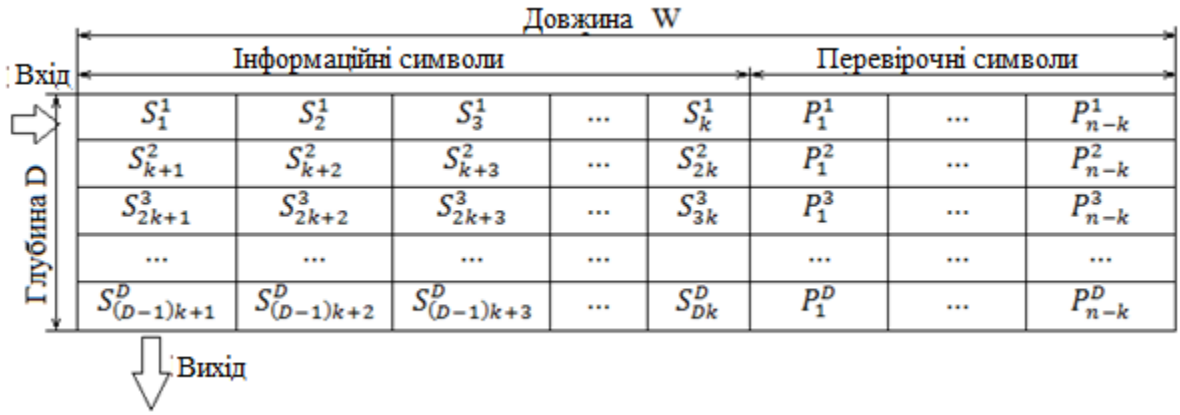


Рис. 4.10. Блокове перемежіння, строковий запис

Припустимо, що $W = n$. Тоді рядки таблиці являють собою кодові слова, що містять k інформаційних символів і $(u - k)$ перевірочних символів. Після заповнення таблиці здійснюється послідовне зчитування символів по стовпцях і їх передача по каналу зв'язку. У приймачі виконується зворотна процедура – послідовний запис символів по стовпцях до повного заповнення таблиці. Потім проводиться зчитування символів по рядках таблиці і їх декодування. Такий перемежувач дозволяє зруйнувати пакет помилок завдовжки W, в результаті чого в кожному кодовому слові буде не більше однієї помилки.

Однак, періодична послідовність одиночних помилок, віддалених один від одного на *D* символів, викликатиме повну поразку помилками деякого одного слова. Затримка при виконанні процедур перемежіння - деперемежіння дорівнює 2*WD* символів. Об'єм пам'яті і перемежувача і деперемежувача становить *WD* символів. Інший можливий варіант виконання перемежувача зображений на рис. 4.11.

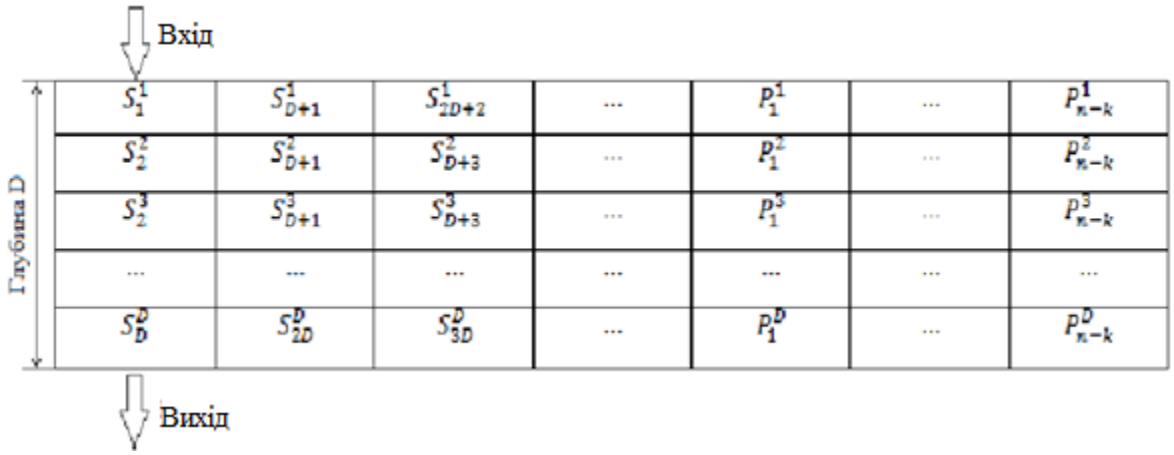


Рис. 4.11. Блокове перемежіння, запис по стовпцям

Тут інформаційні символи послідовно записуються по стовпцях. Причому перевірочні символи формуються з *k* інформаційних символів, рознесених один від одного у вихідній послідовності на *D* символів. Зчитування символів також здійснюється по стовпцях. Перевагою цього методу є передача інформаційних символів в природному порядку проходження і відсутність затримки в перемежувачі. Загальна затримка становить *WD* символів і обумовлена виконанням процедури деперемежіння. Параметри *D* і *W* перемежувача повинні вибиратися з таким розрахунком, щоб найбільш імовірні значення довжини пакетів помилок виявилися менше.

Однак цей тип перемежувача не володіє стійкістю по відношенню до періодичної послідовності одиночних помилок, рознесених на *D* символів. У

ції ситуації всі символи в рядку виявляються помилковими і канальний декодер переповнюється.

4.2.2 Міжблокове перемежіння

При міжблоковому переміщенні в якості вхідного блоку приймається блок з *NB* символів, і кожен блок з *N* символів розподіляється між наступними *y* вихідними блоками. Нехай *x* і *y* є відповідно вхідний і вихідний символи перемежувача. Приклад міжблокового перемежіння при $B = 3$ і $N = 2$ показаний на рис. 4.12 і описується через:

$$y(i + j, j + Bt) = x(i, m), \tag{4.34}$$

де символи *i*-го, *(i + 1)*-го і *(i + 2)*-го вхідних кодових блоків позначені відповідно *a, b, c*. Згідно з наведеним правилом відображення

$$y(i + j, j + 3t) = x(i, m), \tag{4.35}$$

для всіх *j* та при *j=m mod3, t=m mod2*

При *m=0* маємо $y(i,0) = x(i,0)$, *m=1* маємо $y(i+1,4) = x(i,1)$, *m=2* маємо $y(i+2,2) = x(i,2)$.

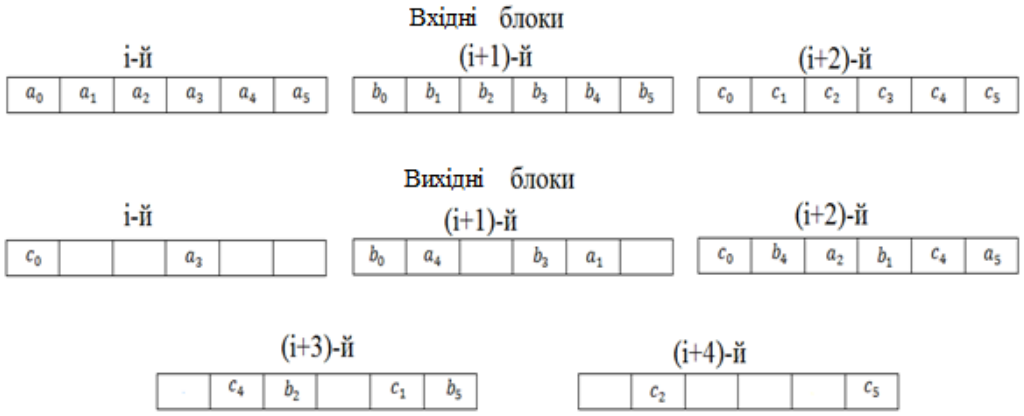


Рис. 4.12. Міжблокове перемежіння

4.2.3 Згорткове перемежіння

Передбачається, що є синхронізація мультиплексорів і демультіплексорів передавача і приймача. Демультиплексор здійснює послідовне підключення виходу кодеру до різних рядків пам'яті перемежувача. Мультиплексор відповідно підключає вхід декодера до різних рядках пам'яті деперемежувача. Кожен рядок пам'яті являє собою регістр зсуву, кількість елементів затримки якого зазначено відповідним числом, вписаним в прямокутник. Перший елемент кодованої послідовності записується у верхній рядок і відразу ж передається по каналу зв'язку. Записується він також в перший рядок пам'яті деперемежувача, що забезпечує затримку на *(B-1) m* символів. Другий елемент кодованої послідовності записується у другий рядок пам'яті перемежувача, що забезпечує затримку на *m* символів. Таким чином, суміжні символи кодованої послідовності виявляються рознесеними на *m* символів. Тому на них не впливають пакети помилок, довжина яких не перевищує *m*. При прийомі другий символ додатково затримується на *(B-2)*m* символів, так що загальна затримка символів становить *(B-1)*m* символів. Слід зазначити, що всі символи кодової послідовності після перемежіння і деперемежіння мають однакову затримку, тому порядок проходження символів на виході кодеру і вході декодеру зберігається.

4.3 Імітаційне моделювання та аналіз ефективності завадостійких кодів RS, LT, LDPC в каналах з пакетними завадами

Для дослідження ефективності процедури перемежіння в каналах передачі даних, була розроблена програмна модель на основі моделі рис.

4.13, що дозволяє досліджувати поведінку кодів на тлі основних помилок в каналах зв'язку.

Рис. 4.13. Системна модель фонтанних кодів з використанням блоку перемежіння [171]

Коротко охарактеризуємо розроблену модель. Перемежіння і деперемежіння здійснюється за допомогою:

• блокового перемежувача;

• міжблокового перемежувача.

Кодування і декодування здійснюється такими кодами як:

• код Ріда-Соломона, для якого реалізована можливість зміни надлишкової інформації, доданої до кінця закодованого повідомлення;

• LT код, для якого реалізована можливість зміни ймовірності помилки в каналі передачі даних і надмірність коду;

• LDPC код з використанням матриці перевірок на парність 1153x2304.

Створена програма дозволяє зробити імітацію каналу зв'язку з декількома змінними параметрами для конкретного файлу (txt або bmp). В якості моделей каналів передбачені 3 математичні моделі:

• канал з адитивним гаусовським шумом;

• канал з мультиплікативної перешкодою;

• канал зі стираннями.

Передбачено зміну дисперсії помилки для адитивної перешкоди і зміна ймовірності помилки для мультиплікативної завади і каналу зі стираннями.

У реалізованій моделі кращі завадостійкі характеристики забезпечують міжблокові перемежувачі – вони в середньому на 8% краще справляються з завадами, при інших однакових показниках. У зв'язку з цим надалі використовуватимуться міжблокові перемежувачі з показниками: глибина – 1024 біт, ширина – 2048 біт і довжина – 2048 біт.

Дослідження проводилися наступним чином. Спочатку пропускаємо файл (txt або bmp) через одну з моделей перемежіння, отримуємо перемежений файл. Далі за допомогою моделі завадостійкого кодування кодуємо файл одним з кодів, потім за допомогою моделі каналу передачі даних вносимо помилки, відповідні одному з реалізованих каналів, в закодований файл, далі декодуємо файл і пропускаємо через деперемежувач. Результати моделювання показані на рис. 4.14.

З отриманих результатів, можна зробити висновок, що кращі властивості декодування забезпечує LDPC-код. Він дозволяє виправляти передане повідомлення з дисперсією помилки 0.415 від амплітуди сигналу в каналі з АБГШ, з імовірністю помилки 0.390 в каналі з мультиплікативної помилкою і ймовірністю помилки 0.357 в каналі зі стираннями (з урахуванням використання перемежіння).

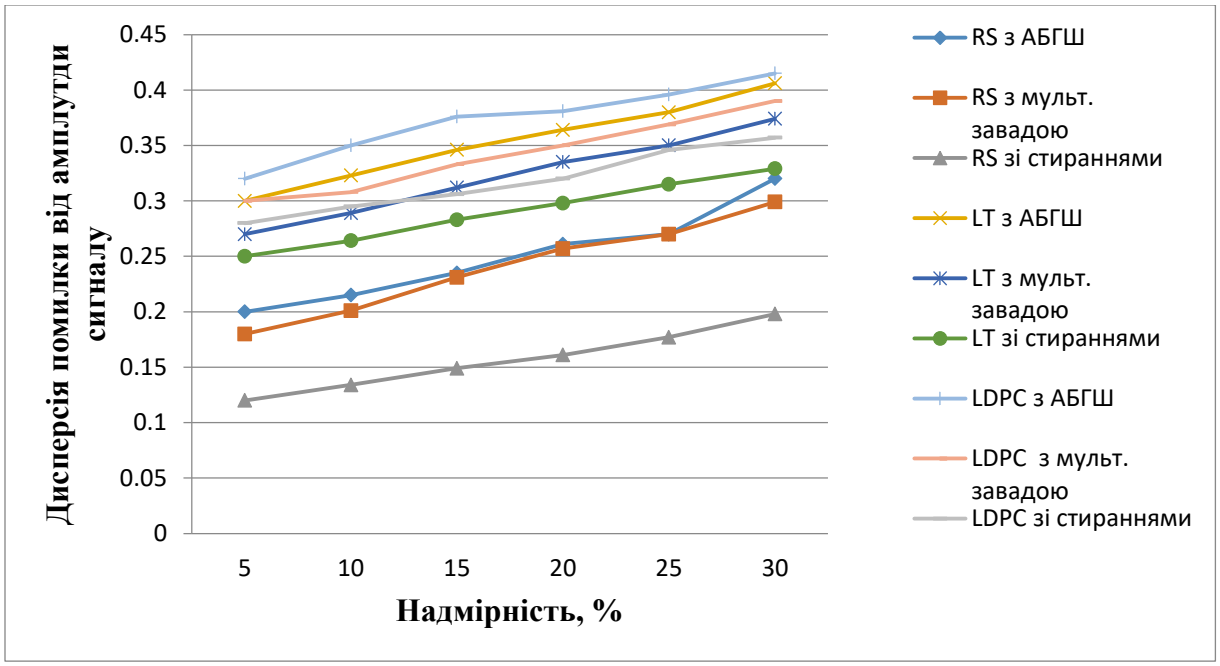


Рис. 4.14. Результати моделювання

Дані результати доводять, що в даних реалізаціях LDPC коди є більш надійними ніж коди Ріда-Соломона і LT, дозволяють виправляти більшу кількість помилок, що вносяться в передані повідомлення, при однаковій надмірності, а також володіють кращими характеристиками часу кодування і декодування повідомлень. Також з результатів моделювання можна зробити висновок, що використання методів перемежіння на 11% дозволяють поліпшити виправлення помилки в переданому повідомленні (у порівнянні з результатами, отриманими в [171]).

Моделювання проводилося з показником надмірності рівним 10%. Час витрачається на кодування і декодування повідомлень у LT-коду значно менше, ніж у кодів Ріда-Соломона і LDPC (табл. 4.1, 4.2).

Для кодування і декодування, а також перемежіння і деперемежіння повідомлень розміром 16 Мб LT-коди потребують 1.51с. і 1.34с. відповідно, у

той час коли для кодування і декодування кодом Ріда-Соломона необхідно затратити 6156.39 с. і 4212.37 с. відповідно.

Таблиця 4.1 – Час затрачений на перемежіння та деперемежіння залежно від розміру файлу

Розмір файлу, Мб	Час затрачений на перемежіння файлу, с.	Час затрачений на деперемежіння файлу, с.
0.25	0.02	0.015
0.5	0.0185	0.0176
1	0.0374	0.0362
2	0.069	0.061
4	0.12	0.112
8	0.202	0.196
16	0.389	0.37

Таблиця 4.2 – Залежність затрат часу від розміру файлу

Розмір файлу, МБ	Затрачений час, с.					
	Код Ріда-Соломона		LDPC код		LT код	
	Кодув. + перемеж.	Декодув. + деперемеж.	Кодув. + перемеж.	Декодув. + деперемеж.	Кодув. + перемеж.	Декодув. + деперемеж.
0.25	4.62	2.07	1.75	1.01	0.05	0.035
0.5	19.02	8.42	2.92	2.12	0.06	0.055
1	77.04	40.53	5.16	3.93	0.11	0.103
2	301.07	124.06	9.16	6.86	0.26	0.16
4	912.12	456.11	15.49	10.02	0.53	0.30
8	2546.2	1487.2	20.51	15.79	1.07	0.65
16	6156.39	4212.37	31.15	28.33	1.51	134

LDPC коди витрачають на дані дії 31.1с і 28.3с. Виходячи з отриманих результатів, кращі характеристики забезпечують LT-коди, які дозволяють виправляти більшу кількість помилок в мережі передачі даних, а також використовувати менше часу на кодування і декодування, з урахуванням перемежіння і деперемежіння (у порівнянні з кодами Ріда-Соломона і LDPC),

внаслідок чого рекомендується для зменшення рівня помилок і втрат пакетів в інтелектуальній інформаційно-телекомунікаційній системі використовувати LT-коди в якості основи для подальшого вдосконалення. При цьому налаштування коду мають обиратися інтелектуальною системою в залежності від параметрів каналу в конкретний момент часу.

4.4 Синтез програмної моделі Raptor кодів з процедурою перемежіння

Програмна модель була створена в середовищі Matlab для моделювання втрат в каналі BEC і перевірки працездатності конструктивних параметрів, матриць і розподілів. Канал BEC стирає випадково прийнятий вектор запису в отриманій LT кодової матриці, відповідно частині коду Raptor, що піддається впливу каналу. Синтезована модель наведена на рис. 4.15. В якості вхідних даних використовується довжина повідомлення k, довжина кодового слова n і фактор витрат на кодування ε. Синтезована модель дозволяє:

1. Проектування і оцінку параметрів коду LT;
2. Проектування H-матриці для зовнішнього коду LDPC;
3. Оцінку H-матриці LDPC-коду над каналом BEC ;
4. Оцінку повного коду Raptor при використанні каналу BEC.

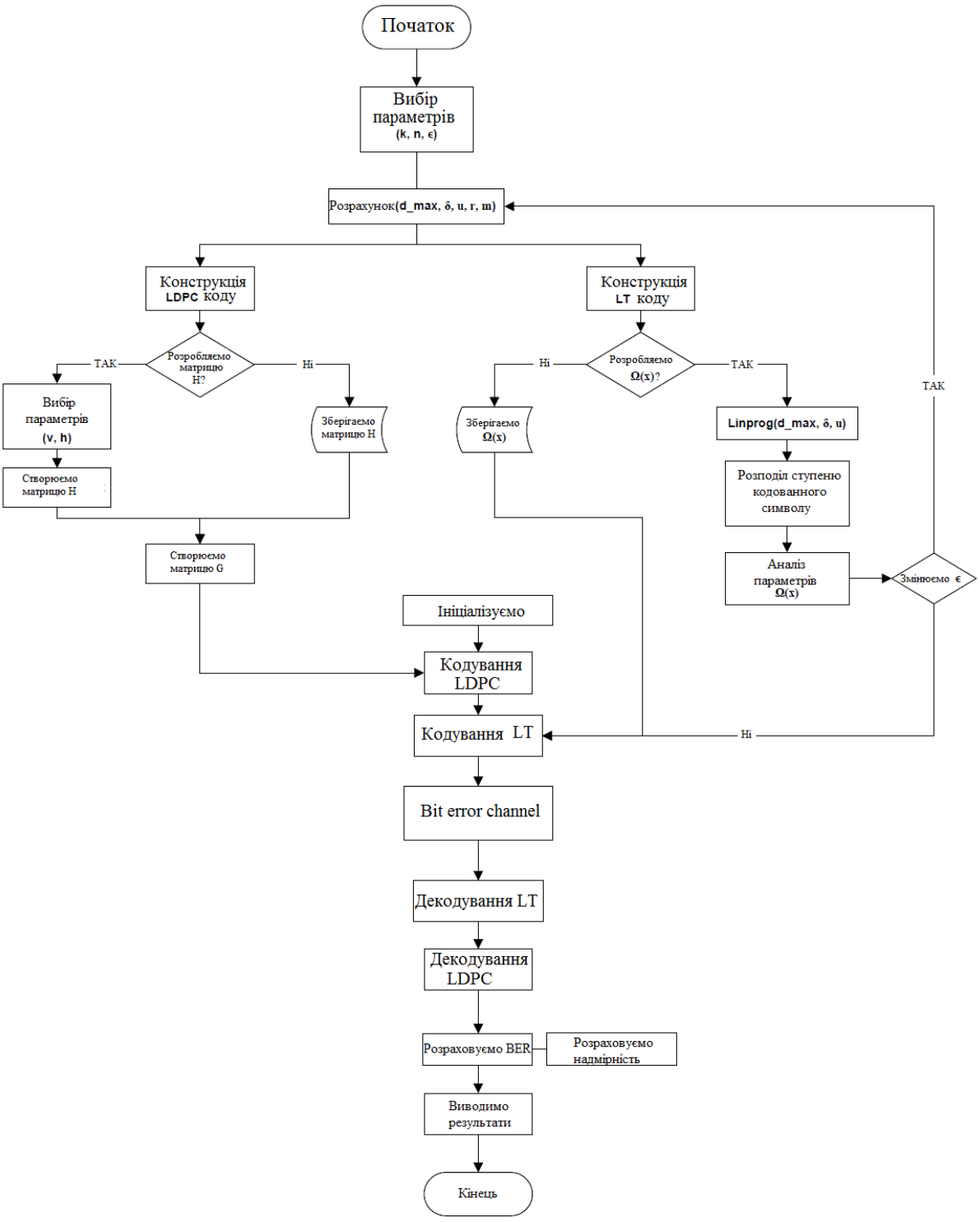


Рис. 4.15. Алгоритм запропонованої модифікації Raptor коду

Крім того, наступні параметри розраховуються перед обчисленням результатів кодових конструкцій:

- максимальна ступінь обмежень для Raptor розподілу ступеня *Dmax*;
- змінна μ, що використовується в конструкції розподілу ступенів;
- очікувана частка повідомлень, що не можуть бути декодовані символів ς;
- рекомендована швидкість LDPC коду *r*;
- число кодованих символів *m*, яке необхідно декодувати *(1 - ς) n* символів повідомлень.

Швидкість коду LDPC може бути обрана користувачем і програмна модель створить перевірочну матрицю *H*, яка буде використовуватися в прекоді LDPC. Матриця *H* буде генерована відповідно до описаної специфікації. Ця *H*-матриця може бути змінена (в межах *r*), для того щоб зробити більш надійні коди LDPC – особливо для невеликих довжин коду. Задана матриця може бути також вказана користувачем. Максимальне число ітерацій можна також регулювати. Породжуюча матриця *G* завершує етап проектування прекоду. Проектований код LDPC є масштабованим в межах від 100 до 1024 символів.

Випадкове двійкове повідомлення довжини *k* генерується і попередньо кодується LDPC-кодом, створюючи кодове слово довжини *n*. Це кодове слово потім передається на внутрішній код LT і кодується. Моделювання каналу відбувається через випадкові стирання, які вносяться в передані пакети. Модуляція і демодуляція не виконується. Всі алгоритми, використовувані в цієї програмній моделі, засновані на жорсткому рішенні декодування.

Приймач збирає кодовані пакети до тих пір, поки оцінена довжина *m* повідомлення *E* не буде отримана, потім декодер LT починає декодування. Алгоритм ймовірнісного декодування використовується в коді Raptor, який

потім декодує фракцію кодового слова, представлений в декодері LT коду. Коли більше немає символів (пакетів) ступеня «один», які можна декодувати, декодер зупиняється і передає кодове слово на декодер LDPC. Після максимального числа ітерацій, або наше повідомлення буде декодоване, або відкинуте через неможливість декодування.

Якщо стирання ще присутні в кодовому слові, симулятор може бути налаштований так, що приймач буде приймати кодовані пакети до тих пір поки декодування не буде завершене. Для таких реалізацій, канал зворотного зв'язку необхідний для того, щоб відправити повідомлення зупинки. Вхідні дані, необхідні для коду Raptor, наведені тут: 1. Довжина повідомлення – n; 2. Швидкість коду – r; 3. Перевірочна матриця – H ; 4. Породжувальна матриця – G; 5. Число символів, необхідних для декодування – m.

Кожна частина конструкції може бути створена в симуляторі, щоб проаналізувати різні аспекти продуктивності. Після отримання результатів в кожному тестовому блоці, коди можуть бути інтегровані і оцінені. Є багато різних способів тестування Raptor кодів. Найбільш актуальним, однак, є оцінка продуктивності і накладних витрат. Іншими словами, скільки вихідних символів необхідно для декодування повідомлення і як впливає дія завад на ці накладні вимоги.

4.5 Висновки

У даному розділі наведені результати дослідження фонтанних кодів і застосування методів перемежіння для виправлення помилок в каналах зі стиранням і білим гаусовського шумом.

Коди LT з робасним солітонівським розподілом може гарантувати повне відновлення даних з деякими накладними витратами на декодування. Проте,

цей розподіл має деякі недоліки: високий рівень порогу помилок, накладні витрати можуть бути великими (маленькими) при великих (малих) довжинах даних; складність зростає логарифмічно при зростанні коду. Код Raptor може досягти більш низького порога помилки, але це не обов'язково означає, що складність обчислення буде низькою, оскільки код Raptor є каскадним кодом.

Вдосконалено модель кодів Raptor, шляхом застосування міжблокової схеми перемежіння для системних моделей пакетних підчисток і виправлення бітової помилки. Новизна моделі полягає у використанні додаткового блоку перемежіння під час кодування переданих повідомлень та методу декодування за допомогою максимальної правдоподібності, що дозволило покращити показники виправлення помилок в каналах з затираннями та завмираннями.

Дані результати доводять, що в даних реалізаціях LDPC коди є більш надійними ніж коди Ріда-Соломона і LT, дозволяють виправляти більшу кількість помилок, що вносяться в передані повідомлення, при однаковій надмірності, а також володіють кращими характеристиками часу кодування і декодування повідомлень. Також з результатів моделювання можна зробити висновок, що використання методів перемежіння на 11% дозволяють поліпшити виправлення помилки в переданому повідомленні (у порівнянні з результатами, отриманими в [171]).

5 ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ ДАНИХ: ВДОСКОНАЛЕННЯ ПРОЦЕДУРИ АВТЕНТИФІКАЦІЇ ТА ДОСТУПУ ДО СЕРВІСІВ

Як було зазначено в розділі 1 та [60] до основних показників захищеності даних в мережі відносяться показники конфіденційності, цілісності, доступності і спостереженості.

В цьому розділі наводяться моделі і методи, які дозволяють підвищити захищеність системи в цілому за рахунок вдосконалення її окремих елементів.

В підрозділі 5.1 наводиться загальна постановка задачі забезпечення захищеності даних користувача. Підрозділ 5.2 описує загальні підходи до формування біометричного шаблону та проходження віддаленої автентифікації, на основі чого в підрозділі 5.3 пропонується вдосконалений метод формування біометричного шаблону і новий метод агрегації різних біометричних ознак. В підрозділі 5.4 наведено метод підвищення конфіденційності шляхом використання прихованого каналу для передачі біометричних шаблонів та описується впровадження запропонованого методу. В підрозділах 5.5 і 5.6 пропонуються методи автентифікації користувачів і захисту їх персональних даних під час дзвінка. В підрозділі 5.7 описані вдосконалення системи керування приватними даними користувача. Підрозділ 5.8 описує вдосконалення системи віддаленої ідентифікації людини за обличчям за допомогою штучних мереж та систем комп’ютерного зору. В підрозділі 5.9 наводиться розрахунок оцінки рівня покращення системи захисту даних в мобільній мережі 5G за рахунок використання запропонованих методів та перекриття певних атак.

5.1 Постановка задачі вдосконалення захищеності

Як було наведено в розділі 2, захищеність інформаційно-телекомунікаційної системи є загальною складовою її ефективності. Складова захищеності може бути оцінена через дві складові:

- співвідношення ступеня перекриття існуючих загроз до застосування запропонованих методів і після;
- підвищення рівня надання послуг із забезпечення захищеності, описаних в 1.5 [60].

Базуючись на цьому, відповідно до наданої в розділі 2 моделі, захищеність системи в даній роботі оцінюється через (5.1):

$$Sec(\%) = AttBlock + ServLevel, \tag{5.1}$$

де *AttBlock* відповідає ступеню перекриття існуючих загроз і оцінюється за формулою (5.2):

$$AttBlock = \forall Att(i): (AttP(i)*AttBlockB(i)) / (AttP(i)*AttBlockA(i)), \tag{5.2}$$

де *AttP(i)* – імовірність реалізації атаки; *AttBlockA(i)* – ступінь перекриття атаки після (After) впровадження запропонованих методів; *AttBlockB(i)* – ступінь перекриття атаки до (Before) впровадження запропонованих методів.

Підвищення рівня надання послуг (*ServLevel*) в свою чергу складається з рівня забезпечення конфіденційності (*ConfLev*), цілісності (*IntegrLev*), доступності (*AccessLev*) і спостереженості (*ObservLev*), (5.3):

$$ServLevel = ConfLev + AccessLev + IntegrLev + ObservLev. \quad (5.3)$$

Відповідно до [60] і (5.3), в даній дисертаційній роботі запропоновані моделі і методи підвищення захищеності через вдосконалення конфіденційності, цілісності, доступності і спостереженості. Так, показник конфіденційності вдосконалюється шляхом підвищення якості надання послуг «конфіденційність при обміні» (підрозділ 5.3, 5.6), «аналіз прихованих каналів» (підрозділ 5.4). Показник цілісність – шляхом підвищення якості надання послуги «цілісність при обміні» (підрозділ 5.3, 5.6). Показник доступність – шляхом розширення послуги «використання ресурсів» (підрозділ 5.7). Показник спостереженість – шляхом підвищення якості послуг «ідентифікація і автентифікація» (підрозділ 5.7), «ідентифікація і автентифікація при обміні», а також високорівневою реалізацією послуг «автентифікація відправника» та «автентифікація отримувача» (підрозділ 5.5).

5.2 Існуючи підходи до формування біометричного шаблону та проходження віддаленої автентифікації

Ідеальна біометрична схема захисту шаблону повинна мати наступні чотири властивості [73, 190, 247].

1) Різноманітність: безпечний шаблон не повинен дозволяти порівняльний пошук по базам даних, тим самим забезпечуючи конфіденційність користувача.

2) Можливість ануляції: вона повинна бути простою для відкликання скомпрометованого шаблону та перевипуску нового, заснованого на тих же біометричних даних.

3) Безпека: отримання оригінальної біометричної інформації із сформованого шаблону повинно бути обчислювально важким. Ця властивість перешкоджає відновленню біометричних ознак з викраденого шаблону.

4) Продуктивність: схема захисту біометричного шаблону не повинна погіршити продуктивність розпізнавання.

Основним викликом розробки біометричної схеми захисту шаблону, який задовольняє всім вищезгаданим вимогам, є необхідність обробки мінливих даних користувача.

Нагадаємо, що декілька зображень однієї біометричної ознаки не призводять до того ж набору значень. З цієї ж причини не можна зберігати біометричний шаблон у зашифрованій формі (наприклад, за допомогою стандартних методів шифрування, таких як RSA, AES та ін.), а потім оцінювати відповідність у зашифрованому домені.

Також варто звернути увагу на те, що шифрування не є гладкою функцією і невелика різниця у значеннях, що витягуються з початкових біометричних даних, призведе до дуже великої різниці в зашифрованому результаті. При цьому, варіант з розшифровуванням шаблону і оцінюванням відповідності між збереженим та розшифрованим шаблоном, не є безпечним, оскільки має зберігатися сам біометричний шаблон. Отже, стандартні методи шифрування не є корисними для забезпечення захисту біометричних шаблонів.

Розглянемо основні схеми захисту біометричного шаблону, що отримали поширення на цей час. Згідно [190, 195, 197], підходи до захисту можна поділити на 2 напрямки: підходи на основі перетворення властивостей та біометричні криптосистеми (рис. 5.1).

Також в декількох джерелах [197, 198] пропонуються додаткові методи, до яких відносять гомоморфну криптографію, гібридні методи, а також методи на основі стеганографії та ватермаркінгу.

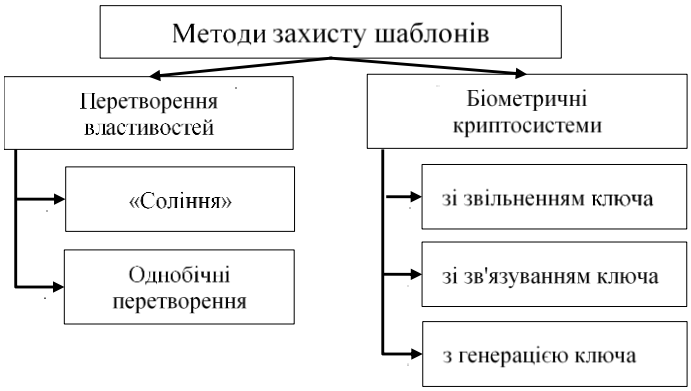


Рис. 5.1. Спрощена класифікація методів захисту шаблону

У підходах на основі перетворення властивостей біометричні дані обробляються за допомогою деякої функції-перетворення і далі зберігається лише вже трансформований шаблон. В залежності від типу функції-перетворення цей підхід поділяється на методи «соління» та однобічні перетворення.

В методах на основі «соління» функція-перетворення може бути оберненою [60], тобто, якщо ключ перетворення відомий по трансформованому шаблону, можна відтворити оригінальний. Безпека таких систем базується на захищеності ключа чи пароля. В методах на основі однобічних перетворень зазвичай обчислювально важко відновити оригінальний шаблон по трансформованому, навіть якщо ключ відомий [190].

Біометричні криптосистеми [184] в свою чергу поділяються на системи зі звільненням ключа (key release cryptosystems), системи зі зв'язуванням

ключа (key binding cryptosystems) та системи з генерацією ключа (key generation cryptosystems).

У біометричних криптосистемах користувачеві не потрібно запам'ятовування паролів та/або використовувати додаткові пристрої для зберігання, передачі та ін. Біометрична криптосистема в будь-який час і в будь-якому місці ініціалізується шляхом вилучення "на льоту" необхідних параметрів з наданих біометричних зображень (з можливими помилками, стиранням тощо) без шкоди для цих зображень.

Розглянемо перелічені вище методи і проведемо оцінку їх переваги та недоліків. За результатами аналізу сформуємо набір правил для вибору найкращого рішення в кожній окремій ситуації.

До основних методів захисту шаблону відносяться [190, 195, 196]:

А) Методи «Соління». Соління або біохеш – це підхід захисту шаблону, в якому біометричні ознаки перетворюються за допомогою функції, визначеної специфічним ключем або паролем користувача. Оскільки трансформація може бути обернена, то ключ повинен бути надійно збережений користувачем та представлений під час автентифікації. Ця потреба в додатковій інформації у вигляді ключа збільшує ентропію біометричного шаблону і, отже, ускладнює для противника вгадування шаблону.

Можна відзначити наступні переваги даного методу. По-перше це ефективний метод перетворення вхідних біометричних даних у високо-ентропійні за рахунок збільшення ентропії біометричних даних при накладенні на біометричні зразки псевдовипадкових послідовностей. По-друге використання ключа призводить до збільшення відстані Хемінга між даними біометричних зразків. Схема прийняття рішення при біометричній

ідентифікації повинна враховувати значення кількості бітів, які співпадають при порівнянні біометричних зразків.

Обмеження: 1) Якщо специфічний ключ користувача скомпрометований, шаблон більше не є безпечним, тобто, якщо противник отримує доступ до ключа та трансформованого шаблону, він може відновити оригінальний біометричний шаблон. 2) Оскільки порівняння відбувається у перетвореному вигляді, механізм соління повинен бути розроблений таким чином, щоб продуктивність розпізнавання не погіршувалася, навіть під час змін у біометричних даних користувача.

Використання нечітких контейнерів на основі застосування методів «соління» являється ефективним методом побудови множини представлень біометричних даних біометричного зразку.

Б) Методи на основі однобічних перетворень. У цьому підході біометричний шаблон шифрується за допомогою однобічної функції перетворення. Параметри функції перетворення визначаються ключем, який повинен бути доступним під час автентифікації. Основною характеристикою такого підходу є те, що навіть якщо ключ та/або трансформований шаблон відомі, то обчислювально важко (з точки зору складності грубої сили) для противника відновити оригінальний біометричний шаблон.

До переваг методу слід віднести те, що навіть якщо ключ скомпрометований, ця схема забезпечує кращу безпеку, ніж метод «соління». Заміна шаблону та ануляція можуть бути реалізовані за допомогою специфічних функцій.

Обмеження: Основним недоліком такого підходу є компроміс між невідповідністю та однобічністю функції перетворення. Функція перетворення з одного боку повинна зберігати подібність (функції одного користувача повинні мати високу подібність у перетвореному просторі та

функції різних користувачів повинні бути досить різнорідними після трансформації), а з іншого боку, повинна бути однобічною. Важко спроектувати функції перетворення, які одночасно задовольняють обом умовам. Крім того, функція перетворення також залежить від біометричних ознак, які потрібно використовувати у певному застосуванні.

В) Біометричні криптосистеми. Традиційно, біометричні криптосистеми на нечітких екстракторах, а також системи, що їм передують, на нечітких контейнерах [185, 196], будуються з використанням завадостійкого кодування. На початковому етапі біометричні дані в певному сенсі об'єднуються з елементами завадостійких кодів (наприклад, з кодовими словами або синдромними послідовностями). Для нечітких екстракторів додатково утворюється відкритий допоміжний рядок (helper data), який допомагає при вилученні секретного параметра на нечітких заданих біометричних даних. На етапі використання застосовується завадостійке декодування, що усуває можливу невизначеність (викликану завадами, стиранням тощо) у наданих біометричних шаблонах користувача. Якщо відмінності в наборах характеристик невеликі (не перевищують можливості коригувальних кодів), то нечіткі екстрактори (контейнери) дозволяють однозначно відновити секретний параметр (біометричний ключ).

До класу біометричних криптосистем відносяться три групи систем.

В1) Біометричні системи зі звільненням ключа [184, 197]. У режимі звільнення ключа біометрична автентифікація здійснюється незалежно від механізму звільнення ключа, біометричний еталон і ключ зберігаються окремо один від одного, сам ключ звільняється після успішної біометричної автентифікації.

В2) Біометричні системи зі зв'язуванням ключа [184, 197]. У криптографічних системах такого типу ключ і біометричний еталон

криптографічно пов'язані між собою. Ключ за певним алгоритмом пов’язується з біометричним еталоном користувача і зберігається в такому вигляді в базі даних, відповідно розкрити ключ представляється можливим тільки власникові біометричних параметрів. У таких системах передбачається, проте не є необхідним, використання допоміжних даних (helper data), для демаскування зашумлених біометричних даних.

До переваг криптосистем цього типу слід віднести те, що цей підхід є толерантним для змін (варіацій) даних користувача, і ця толерантність визначається здатністю коду по виправленню помилок.

Обмеження: 1) Відповідність необхідно виконати за допомогою схем корекції помилок, і це виключає використання складних схем порівняння. Це може призвести до зменшення точності порівняння. 2) Загалом, біометричні криптосистеми не призначені для забезпечення різноманітності та ануляції. Проте, намагаються ввести ці дві властивості в біометричні криптосистеми, головним чином, використовуючи їх у поєднанні з іншими підходами, такими як «соління». 3) Допоміжні дані повинні бути ретельно розроблені.

В3) Біометричні системи з генерацією ключа [184]. У такій біометричній криптосистемі ключ формується безпосередньо з біометричних даних користувача і не зберігається в базі даних. Варто звернути увагу на те, що якщо схема генерує той самий ключ, незалежно від шаблону вхідних даних, він має високу основну стабільність, але нульову ентропію, що призводить до високого значення FAR. З іншого боку, якщо схема створює різні ключі для різних шаблонів того ж користувача, схема має високу ентропію, але відсутність стабільності і це призводить до високого значення FRR. Можна вивести ключ безпосередньо з біометричних ознак, однак важко одночасно досягти високої ентропії та високої стабільності.

До переваг методу слід віднести пряму генерацію ключа з біометрії.

Обмеження: Важко генерувати ключ з високою стабільністю та ентропією.

Сценарій та початкові дані відіграють важливу роль у виборі схеми захисту шаблону [190]. Наприклад, у застосуванні біометричної верифікації, такої як банкомат банку, проста схема соління, заснована на PIN-коді користувача, може бути достатньою для забезпечення захисту біометричного шаблону. З іншого боку, при проходженні процедур аеропорту, однобічне перетворення є більш придатним підходом, оскільки він забезпечує як захист шаблону, так і можливість ануляції (відкликання), не покладаючись на будь-які інші вхідні дані від користувача. Біометричні криптосистеми є більш доцільними у додатках з порівняннями на карті.

Іншим основним чинником, що впливає на вибір схеми захисту шаблону, є вибрана біометрична ознака, її набір функцій та ступінь варіацій даних користувачів. Дизайн схеми захисту шаблону залежить від конкретного типу біометрії, що використовується. Так однобічні функції були запропоновані для відбитків пальців але важко спроектувати відповідне перетворення для райдужної оболонки ока (iris-code). Навпаки, може бути простішим розробити біометричну криптосистему для райдужної оболонки ока, оскільки вона представлена як бінарний рядок фіксованої довжини, де можна легко застосувати стандартні методи кодування з корекцією помилок. Крім того, якщо варіації всередині даних одного типу для одного користувача досить великі, то неможливо застосувати однобічне перетворення або створити біометричну криптосистему. Тому навіть у конкретному сценарії, більш ніж одна схема захисту шаблону може бути прийнятною, а вибір відповідного підходу може базуватися на ряді таких факторів, як продуктивність розпізнавання, обчислювальна складність, вимоги до пам'яті.

Наведемо принципи оцінки основних характеристик системи за умови використання наведених методів формування біометричного шаблону. В якості характеристик системи біометричної автентифікації будемо використовувати помилки першого роду, коли визначається ймовірність помилкової відмови в доступі клієнту, який має право доступу FRR (False Rejection Rate) та помилки другого роду, як ймовірність помилкового доступу, коли система помилково пізнає чужого клієнта як свого FAR (False Acceptance Rate) [73].

Нехай на шаблон S довжиною l_s біт накладаються кодові слова двійкового коду (n,k,d), що корегує помилки. При цьому під n будемо розуміти загальну довжину кодових слів, k – довжина інформаційних слів та d – кодова відстань. Таких слів буде

$$N = l_s/n, \tag{5.4}$$

при цьому кількість кодових слів $N_c = 2^k$.

Перетворення визначається операцією побітового складання слів шаблону S_iта коду C_i:

$$S_i \oplus C_i = SC_i,\ i = \overline{1,N}. \tag{5.5}$$

Кодова відстань визначає можливості коректувати та визначати помилки. Код може при декодуванні гарантовано виправити помилки кратністю $t = (d-1)/2$ та виявити помилки кратністю $d-1$.

Кодові слова генеруються за випадковими значеннями інформаційних слів k_i, $i = 1, N$. Таким чином ключова послідовність, за якою генеруються кодові слова повинна бути випадковою і мати довжину

$$K = kN = \frac{k}{n} l_s \text{ біт}, \tag{5.6}$$

де співвідношення $R = k/n$ визначає швидкість коду.

Схема прийняття рішення порівнює зашумлені образи, які зберігаються на сервері з прийнятими з каналу зв'язку. Порівняння виконується згідно виразу (5.7):

$$SC_i^C \oplus SC_i^{\text{К}} = SC_i^{\text{Р}}, i = \overline{1, N} \tag{5.7}$$

де N – кількість кодових слів, що зашумлять біометричні образи; $SC_i^{\text{С}}$ – зашумлений біометричний образ, що зберігається на сервері; $SC_i^{\text{К}}$ – зашумлений біометричний образ, що перевіряється на сервері;

При порівнянні отримаємо результат (5.8):

$$SC_i^P = S_i^K \oplus C_i^K \oplus S_i^C \oplus C_i^{\text{С}} = \left(S_i^K \oplus S_i^C\right) \oplus \left(C_i^K \oplus C_i^{\text{С}}\right) \tag{5.8}$$

де $C_i^{\text{С}}$ – кодова послідовність, що додає шум до біометричного образу, який зберігається на сервері;

C_i^K – кодова послідовність, що додає шум до біометричного образу, який перевіряється на сервері;

Сума кодових слів, які прийшли з каналу зв'язку та зашумлені в біометричних шаблонах на сервері дає кодові слова лінійного блокового коду (*n*,*k*,*d*). Отримаємо

$$SC_i^P = (S_i^K \oplus S_i^C) \oplus C_i^{\mathrm{P}},\ i = \overline{1,N}\ , \tag{5.9}$$

де $C_i^{\mathrm{P}} = C_i^K \oplus C_i^{\mathrm{C}}$- кодові слова лінійного блокового коду (*n*,*k*,*d*).

Ймовірність того, що при декодуванні виникнуть помилки (які будуть визначатися як розбіжність S_i^K та S_i^C) визначається через (5.10):

$$p_e = 1 - \frac{N_c}{N_b}\ . \tag{5.10}$$

При автентифікації кількість помилкових кодових слів не повинна перевищувати значення порогу T (дозволена для коректної роботи кількість помилок). В такому випадку отримаємо оцінку FAR ймовірності помилкового доступу, коли система помилково пізнає чужого як свого

$$FAR = \sum_{j=0}^{T} C_N^j p_e^j (1 - p_e)^{N-j}. \tag{5.11}$$

Декодування кодових слів коду (*n, k, d*) дозволяє гарантовано виявити помилки кратністю $d - 1$. Таким чином код виявляє помилки з ймовірністю

$$p_{\text{ід}} = \sum_{j=1}^{d-1} C_n^j\, p_{\text{д}}^j (1 - p_{\text{д}})^{n-j}\ . \tag{5.12}$$

Використовуючи цей вираз, отримаємо оцінку помилки першого роду FRR:

$$FRR = 1 - \sum_{j=0}^{T} C_N^j p_{\text{ід}}^j \left(1 - p_{\text{ід}}\right)^{N-1}. \quad (5.13)$$

Базуючись на вищенаведеному, в роботі був запропонований вдосконалений метод формування біометричного шаблону на основі групи В (біометричні криптосистеми), а саме В3 – біометричні криптосистеми з генерацією ключа. Розглянемо запропонований метод більш детально.

5.3 Вдосконалений метод формування біометричного шаблону

Запропонований метод [284] дозволяє використовувати біометричні ознаки для віддаленої автентифікації та формування криптографічного ключа без ризику їх компрометації. Також на основі інформації о наявних біометричних ознаках користувача обрати найкращий за заданими критеріями спосіб їх перетворення в захищений біометричний шаблон.

Метод (рис. 5.2) поєднує відомі елементи і вперше запропоновані. До відомих блоків відносяться блок попередньої обробки, блок отримання ознак, блок формування вектору ознак.

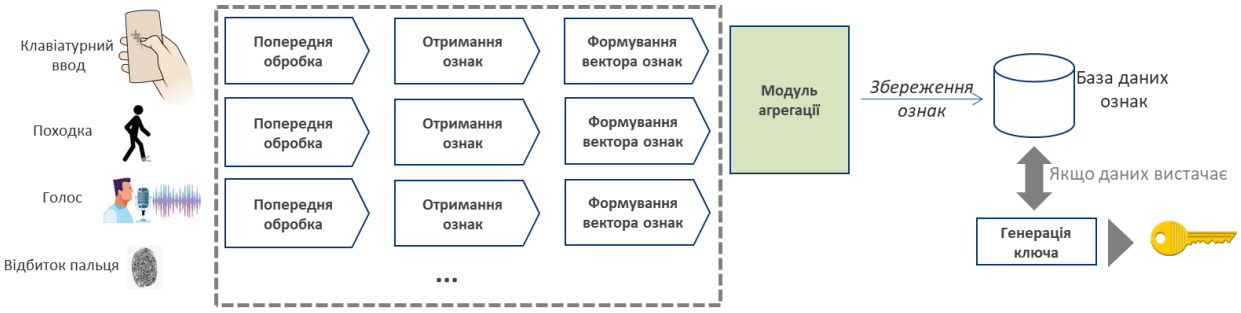


Рис. 5.2. Узагальнена схема генерації ключа на основі біометричної автентифікації із запропонованим модулем агрегації біометричних ознак

Після цього дані з різних біометричних сенсорів потрапляють на запропонований модуль агрегації і за результатами його роботи формується криптографічний ключ. Розглянемо принцип роботи методу та основні перетворення більш детально.

5.3.1 Модуль формування вектору ознак окремого виду біометрії

Попередня обробка даних включає вибір необхідного типу біометрії і отримання інформації від потрібних сенсорів. Під час отримання ознак, дані з сенсорів трансформуються в набір ознак, відповідно до алгоритму обробки даного типу біометрії. Після отримання набору ознак він перетворюється на вектор ознак, що буде мати фіксований розмір (рис. 5.3).

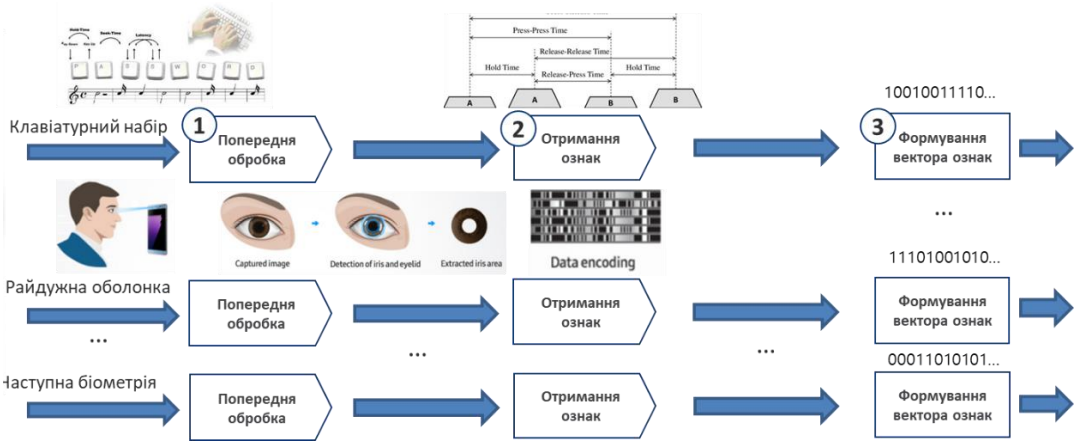


Рис. 5.3. Основні перетворення модуля формування вектору ознак

Опишемо процес обробки даних від сенсорів, отримання ознак і формування вектору ознак більш детально на прикладі обробки біометричних ознак райдужної оболонки ока [199].

У якості біометричного шаблону для ідентифікації на основі райдужною оболонки виступає тканина «trabecular meshwork», яка робить видимими

поділи райдужної оболонки на радіальні сектора. Інші видимі характеристики включають кільця, борозни, веснянки, і область "корони". Процес формування біометричного шаблону з райдужної оболонки ока поєднує в собі декілька етапів починається з попередньої обробки зображення ока і наведений на рис. 5.4.

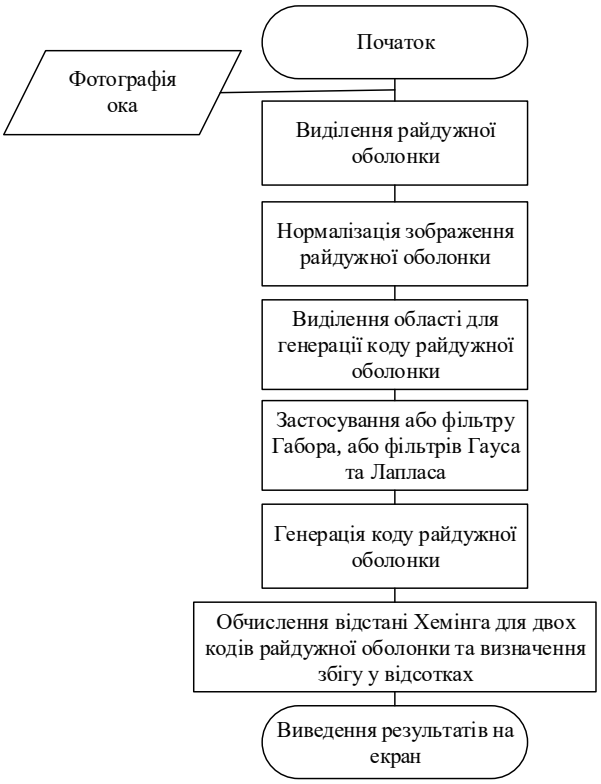


Рис. 5.4. Алгоритм розпізнавання по райдужній оболонці ока

Попередня обробка зображення включає в себе [204,207,208,211,257] перетворення зображення у градації сірого, виділення контуру зіниці, виділення контуру райдужної оболонки, нормалізацію зображення та виділення правої верхньої чверті нормалізованого зображення, до якої далі буде застосовуватися фільтр Габора або Лапласа. В якості тестових зображень були обрані фотографії очей розміром 320x280 пікселів з бази

даних CASIA-Iris-Interval [202, 203]. Ці зображення вже представлені в градаціях сірого. На прикладі одного з них (рис. 5.5) буде продемонстровано весь процес обробки райдужної оболонки ока [199].

Для отримання окремого зображення райдужної оболонки необхідно виділити її зовнішні та внутрішні кордони. Виділення внутрішніх кордонів здійснюється за допомогою виділення контуру зіниці.

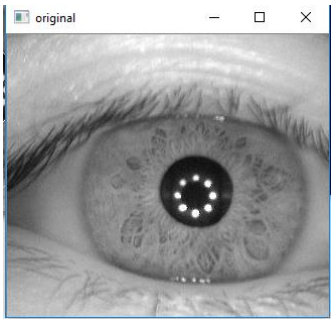


Рис. 5.5. Приклад досліджуваного зображення

Для уникнення виділення зайвих контурів потрібно зробити очищення зображення. Під очищенням зображення мається на увазі розширення всіх знайдених кордонів. Збільшення розміру ліній навколо знайдених компонентів допомагає об'єднати їх у великі лінійні сегменти. Таким чином, лінії, які були в повному обсязі визначені під час детектування кордонів, придбають форму. Завдяки цьому, ймовірність, що периметр зіниці прийме форму замкнутому колу, збільшується. Для цього використовується фільтр розмиття по Гаусу (рис. 5.6).

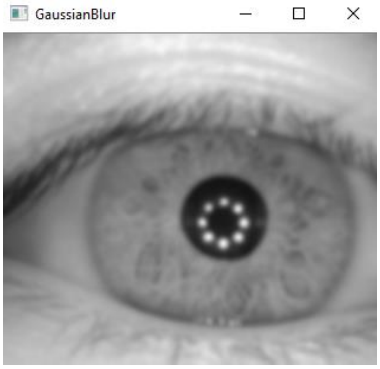


Рис. 5.6. Зображення після застосування фільтра Гауса

Для виділення контуру зіниці використовується детектор Canny. Детектор використовує фільтр на основі першої похідної від Гаусіана. Так як він сприйнятливий до шумів, краще не застосовувати даний метод на необроблених фотографіях, тому було виконане очищення зображення.

Детектор Canny здійснює виділення пікселів, що знаходяться на кордонах, оператором Собеля на матриці з розмірами 3x3. Оператор виділяє в якості пікселів ті з них, на яких дискретний аналог градієнта досягає локального максимуму. Після цього детектор робить зв’язку окремих пікселів, виділених оператором Собеля, в нерозривні фрагменти кордону. З цією метою здійснюється простежування виділених фрагментів з обробкою двопороговою процедурою. Піксель відноситься до граничних, якщо зафіксований на ньому локальний максимум градієнта перевищує встановлений верхній поріг, що забезпечує подальше зниження чутливості до шумів. Крім того оператор простеження володіє консервативністю, формує зв'язкові ділянки кордону. Консервативність полягає в тому, що після виявлення граничного пікселя до фрагменту кордону відносяться сусідні з ним до тих пір, поки значення градієнта не опиниться нижче нижнього порога. Застосування детектора Canny зображене на рис. 5.7.

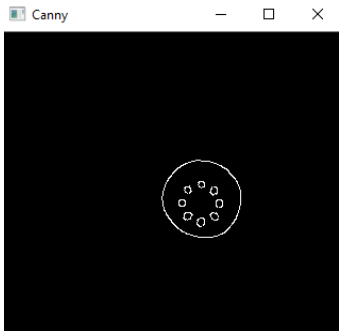


Рис. 5.7. Зображення після застосування детектора Canny

Детектувати круги можна за допомогою перетворення Хафа. Суть роботи перетворення Хафа полягає в наступному. У зображенні, що містить пікселі, віднесені до кордону за результатами роботи детектора Canny, послідовно аналізуються всі точки кордонів на приналежність до шуканого об'єкту. Для випробуваної точки розраховуються параметри кола і в параметричному просторі Хафа фіксується факт отримання цих значень. Після випробування всіх точок зображення в цьому просторі реалізується процедура голосування: виділяються і фіксуються в якості справжніх значення параметрів, отримані в результаті найбільшої кількості випробувань. Завдяки перетворенню Хафа можна виявити радіус так координати центру окружності зіниці (рис. 5.8).

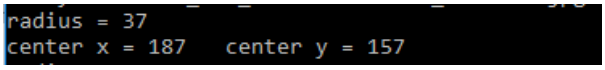


Рис. 5.8. Радіуси центру окружності після перетворення Хафа

Райдужна оболонка має діаметр приблизно 10-13мм. Відповідно до цієї інформації було виділено зовнішній контур райдужної оболонки. Для зображень з бази даних CASIA-Iris-Interval радіус райдужної оболонки

становить приблизно 100 пікселів. Таким чином, було виділено її зовнішні та внутрішні межі (рис. 5.9).

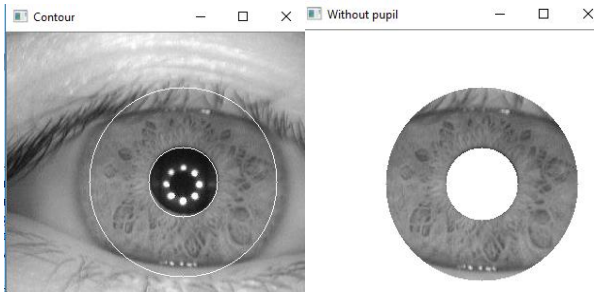


Рис. 5.9. Виділення зовнішнього контуру райдужної оболонки

Оскільки необхідно врахувати здатність зіниці зменшуватися та збільшуватися та зміну зображення ока за рахунок зміни фізичного положення людини стосовно камери, слід привести кільцеподібний малюнок райдужки до стандартизованого виду. Це виконується за допомогою перетворення зображення в полярну систему координат. Для знаходження координат x та y полярної системи координат використовуються формули (5.14) та (5.15) відповідно:

$$x = r \cdot (x_0 + R \cdot \cos(\alpha)), \tag{5.14}$$

$$y = r \cdot (y_0 + R \cdot \sin(\alpha)), \tag{5.15}$$

де x_0 та y_0 – координати центру райдужної оболонки;

R – радіус райдужної оболонки;

r – розраховується за формулою (5.16);

α – кутова координата, що розраховується за формулою (5.17).

$$r = \sum_{j=0}^{n} \frac{j}{n}, \tag{5.16}$$

де n – висота нормалізованого зображення; j – значення координати ординати у пікселях нормалізованого зображення.

$$\sum_{i=0}^{\theta} \alpha = \frac{2 \cdot \pi \cdot i}{\theta}, \tag{5.17}$$

де θ – ширина нормалізованого зображення; i – значення координати абсциси у пікселях нормалізованого зображення.

При перетворенні зображення у полярну систему координат слід врахувати виключення зіниці із перетворення за вище названими формулами. За допомогою вказаних цих формул було перетворено у полярну систему координат райдужну оболонку (рис. 5.10).

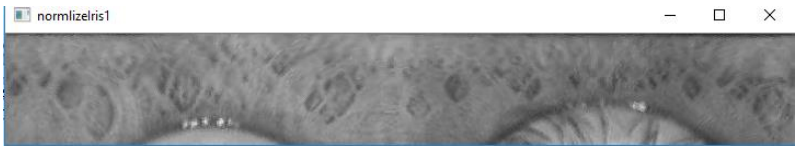


Рис. 5.10. Контур райдужної оболонки у полярних координатах

Попередні дослідження [204-209] показали, що найбільша частина важливої інформації райдужної оболонки знаходиться у правій верхній чверті райдужної оболонки, тому для подальшої обробки необхідно вирізати цю ділянку з нормалізованого зображення. У деяких випадках верхня або нижня повіки можуть потрапити в нормалізоване зображення. Оскільки, вони не несуть інформації для ідентифікації, їх також необхідно видалити. На рис.

5.11 продемонстроване зображення ділянки райдужної оболонки із врахованими вище зазначеними критеріями.

Рис. 5.11. Досліджувана частина контуру райдужної оболонки

Після цього зображення вважається готовим для того, щоб з нього можна було вилучити важливі данні. Для отримання біометричних ознак із зображення на рис. 5.11 застосовується або фільтр Габора або комбінація фільтрів Гауса та Лапласа.

Фільтр Габора був запропонований Джоном Даугманом [205,211] і діє наступним чином. Для вилучення фазової інформації до кожній точки обраної області застосовуються двомірні хвилі Габора. На відміну від амплітудної інформації, фазова складова не залежить від контрасту зображення і освітлення, що є значною перевагою. В основу фільтра Габора покладена гармонічна функція помножена на Гаусіан. Це відображено у формулі (5.18):

$$g(x, y, \lambda, \theta, \sigma, \psi, \gamma) = e^{-\frac{x'^2+\gamma^2 y'^2}{2\sigma^2}} \cdot \cos\left(2\pi \frac{x'}{\lambda} + \psi\right), \qquad (5.18)$$

де λ – довжина хвилі множника косинуса;

ψ – зсув фаз в градусах;

γ – коефіцієнт стиснення, що характеризує еліптичність функції Габора;

σ – параметр, від якого залежать розміри ядра;

x' – визначається за формулою (5.19);

y' – визначається за формулою (5.20).

$$x' = xcos\theta + ysin\theta, \quad (5.19)$$

$$y' = -xsin\theta + ycos\theta, \quad (5.20)$$

де x – рядок у матриці ядра;

y – стовпець у матриці ядра;

θ – орієнтація нормалі паралельних смуг функції Габора в градусах.

Наступний механізм представляє комбінацію фільтрів Гауса та Лапласа [205]. Гаусова фільтрація виконується шляхом згортання кожної точки вхідного масиву з гаусовим ядром та їх подальшого складання для створення вихідного масиву. Фільтр Гауса застосовується для видалення шуму і базується на наступній формулі (5.21):

$$G_0(x, y) = Ae^{\frac{-(x-\mu_x)^2}{2\sigma_x^2} + \frac{-(y-\mu_y)^2}{2\sigma_y^2}}, \quad (5.21)$$

де x – рядок у матриці ядра;

y – стовпець у матриці ядра;

μ – пік функції;

σ – дисперсія.

Фільтр Лапласа базується на операторі Лапласа, дія якого полягає в наступному. В крайовій області інтенсивність пікселя показує "стрибок" або високу різницю інтенсивності. При отриманні першої похідної від інтенсивності можна спостерігати, що край характеризується максимумом. Друга похідна буде дорівнювати нулю. Таким чином за цим критерієм можна виявити краї на зображенні. В основу оператора Лапласа покладена формула (5.22):

$$L(f) = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}, \quad (5.22)$$

де x – рядок у матриці ядра;

y – стовпець у матриці ядра.

Застосовуються ці фільтри на попередньо виділену область райдужної оболонки. Результати застосування фільтрів Габора (рис. 5.12) та фільтрів Гауса та Лапласа (рис. 5.13) показані нижче.

Рис. 5.12. Застосування фільтру Габора

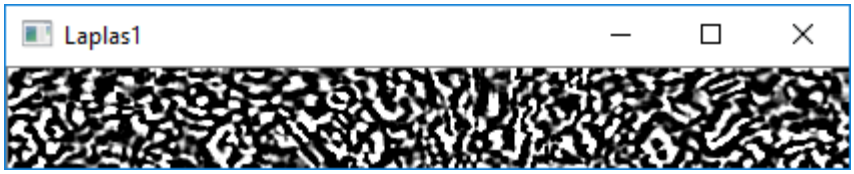


Рис. 5.13. Застосування комбінації фільтрів Гауса та Лапласа

Після застосування одного з фільтрів виконується створення коду райдужної оболонки. Для кодування використовуються 0 та 1, які встановлюються в залежності від значення пікселю зображення, до якого був застосований фільтр Габора. Оскільки, значення пікселів може бути, в даному випадку, лише 0 – для чорного та 255 – для білого, то відповідно 0 та 1 будуть записуватися IrisCode. Таким чином, підсумкова довжина вектору ознак райдужної оболонки залежить від кількості точок, в яких знаходять фазову інформацію, тобто кількості пікселів зображення.

5.3.2 Оцінка ефективності фільтрів під час формування вектору ознак з райдужної оболонки ока

Для перевірки ефективності та стійкості алгоритмів з різними фільтрами було виконано накладання шуму Перліна на тестові зображення [199]. Результати виявлення порогу шуму для обох фільтрів наведено у гістограмі на рис. 5.14.

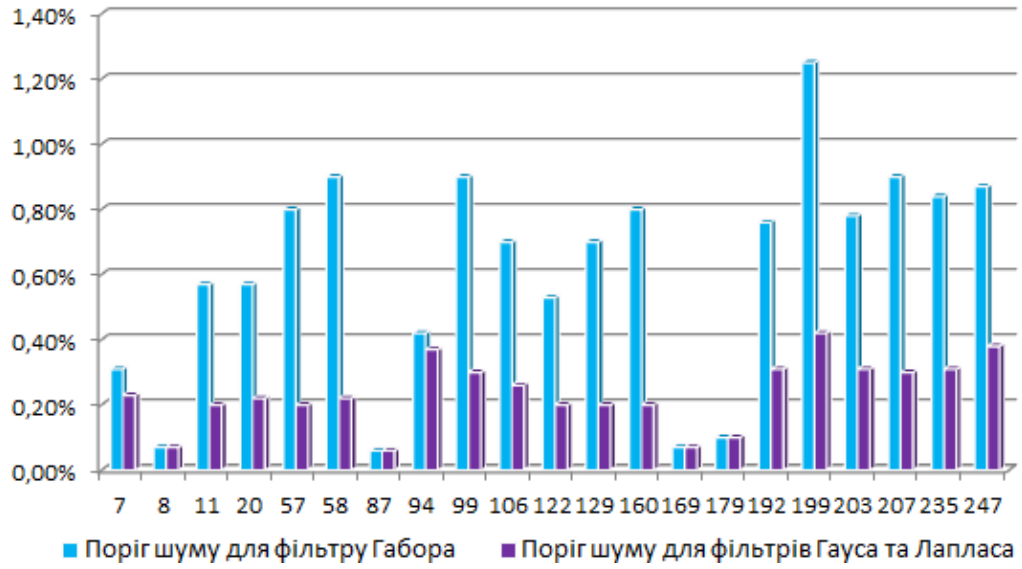


Рис. 5.14. Гістограма значень порогів шуму для досліджуваних фільтрів

Для аналізу рівня завад, що був внесений пороговим значенням шуму для кожного із зображень, було підраховано значення «сигнал/шум» (SNR) за формулою (5.23):

$$SNR = \sum_{x,y}(C_{x,y})^2 / \sum_{x,y}(C_{x,y} - S_{x,y})^2, \quad (5.23)$$

де: x – номер рядка у зображенні;

y – номер стовпця у зображенні;

$C_{x,y}$ – значення пікселя оригінального зображення;

$S_{x,y}$ – значення пікселя зображення, на яке був накладений шум.

Результати значень SNR для кожного із зображень, що тестуються, при використанні різних фільтрів занесені у таблицю 5.1.

В результаті розрахунків було виявлено досить велике значення SNR для більшості зображень, що характеризує низьку кількість завад на зображеннях, що були зашумлені. На основі цього можна зробити висновок, що обидва фільтри є чутливими до накладання шуму, що свідчить про їх стійкість.

Таблиця 5.1 – Значення SNR при певному порозі шуму

Номер досліджуваного зображення	Поріг шуму для фільтру Габора	Поріг шуму для фільтрів Гауса та Лапласа	SNR для фільтру Габора	SNR для фільтрів Гауса та Лапласа
007	0.31%	0.23%	4320.8	4465.19
008	0.07%	0.07%	47919.1	47919.1
011	0.57%	0.2%	527.537	63806.1
020	0.57%	0.22%	426.97	446.643
057	0.8%	0.2%	309	13074.9
058	0.9%	0.22%	658.513	12828.9
087	0.06%	0.06%	347622	347622.0
094	0.42%	0.37%	18841.4	31602.9
099	0.9%	0.3%	376.715	494.807
106	0.7%	0.26%	151.149	36006.1
122	0.53%	0.2%	486.07	19163.0
129	0.7%	0.2%	5906	12915.9
160	0.8%	0.2%	165.388	47764.7
169	0.07%	0.07%	22170	22170.0
179	0.1%	0.1%	126523	126523.0
192	0.76%	0.31%	435.51	764.507
199	1.25%	0.42%	271.935	4657.28
203	0.78%	0.31%	598.919	36831.5
207	0.9%	0.3%	2327.61	2733.02
235	0.84%	0.31%	4131.17	12803.4
247	0.87%	0.38%	315.399	2778.89

Як видно з табл. 5.1 результати порогів шуму у фільтрах Гауса та Лапласа для зображень менші ніж для порогів шуму у фільтрі Габора, а показники SNR навпаки більші. З цього можна зробити висновок, що комбінація фільтрів Гауса та Лапласа є більш стійкою до шумів.

Також для кількісної оцінки величини спотворень оригінального зображення було підраховане середньоквадратичне відхилення (MSE), що представляє відносний показник розсіювання значень. MSE було розраховано за формулою (5.24):

$$MSE = \frac{1}{XY} \cdot \sum_{x,y}(C_{x,y} - S_{x,y})^2, \tag{5.24}$$

де: X – кількість рядків пікселів;

Y – кількість стовпців пікселів;

x – номер рядка у зображенні;

y – номер стовпця у зображенні;

$C_{x,y}$ – значення пікселя оригінального зображення;

$S_{x,y}$ – значення пікселя зображення, на яке був накладений шум.

Результати значень MSE для кожного із зображень, що тестуються, при використанні різних фільтрів занесені у табл. 5.2.

Враховуючі результати таблиць 5.1 та 5.2 можна зазначити, що кореляція між значеннями SNR та MSE полягає у наступному: чим більше відношення сигнал / шум, тим менше різниця MSE.

Таблиця 5.2 – Значення MSE при певному порозі шуму

Назва зображення	Поріг шуму для фільтру Габора	Поріг шуму для фільтрів Гауса та Лапласа	MSE для фільтру Габора	MSE для фільтрів Гауса та Лапласа
007	0.31%	0.23%	0.078	0.075
008	0.07%	0.07%	0.007	0.007
011	0.57%	0.2%	0.587	0.004
020	0.57%	0.22%	1.242	1.187
057	0.8%	0.2%	1.303	0.030
058	0.9%	0.22%	0.658	0.033
087	0.06%	0.06%	0.0001	0.001
094	0.42%	0.37%	0.023	0.013
099	0.9%	0.3%	1.321	1.005
106	0.7%	0.26%	2.257	0.009
122	0.53%	0.2%	0.907	0.023
129	0.7%	0.2%	0.067	0.030
160	0.8%	0.2%	3.301	0.011
169	0.07%	0.07%	0.021	0.020
179	0.1%	0.1%	0.005	0.004
192	0.76%	0.31%	1.029	0.586
199	1.25%	0.42%	1.761	0.102
203	0.78%	0.31%	0.896	0.014
207	0.9%	0.3%	0.233	0.198
235	0.84%	0.31%	0.076	0.024
247	0.87%	0.38%	1.434	0.162

Для оцінки ймовірності виникнення помилок при роботі алгоритмів були розраховані показники FAR (5.11) та FRR (5.13).

Зашумлення зображення може призводити до неспрацьовуванні сканера (FRR), а не до прийняття зображення за інше з бази (FAR), оскільки мінімальні значення відмінностей (MSE) між оригінальними зображеннями складають 3.5-3.6, а максимальне значення MSE при впливі шумів при використанні фільтру Габора досягає 3.3. Враховуючи максимальне значення MSE при впливі шумів при використанні фільтру Габора було визначено, що майже 50% зображень мають ймовірність FAR близьку до нуля. Для усієї бази ймовірність FAR при використанні фільтру Габора дорівнює 0.162.

Також була підрахована кількість зображень різних очей, MSE яких має менш ніж десятикратну відмінність від порогу шуму. В результаті цього було визначено FRR всіх досліджуваних зображень. Воно дорівнює 0.312 при використанні фільтру Габора та 0.064 при використанні комбінації фільтрів Гауса та Лапласа. Таким чином, показники ймовірності виникнення помилок свідчать, що використання в алгоритмі фільтрів Гауса та Лапласа є більш безпечним та стійким до шумів.

5.3.3 Модуль агрегації біометричних ознак

Агрегація біометричних ознак дуже важлива і для користувача і для всієї системи безпеки, оскільки вона дозволяє використовувати саме ті біометричні ознаки в даний момент часу, які є найбільш зручними для користувача і при цьому вони мають забезпечити заданий рівень захищеності (конфіденційності).

Запропонований модуль агрегації отримує на вхід вектори ознак з виходу модулів формування вектору ознак (рис. 5.15). До задач модуля агрегації входить поєднання різних типів біометричних даних в єдину структуру (рис. 5.16), забезпечення конфіденційності та цілісності даних користувача при обміні, а також забезпечення стійкості до завад під час передачі відкритими каналами.

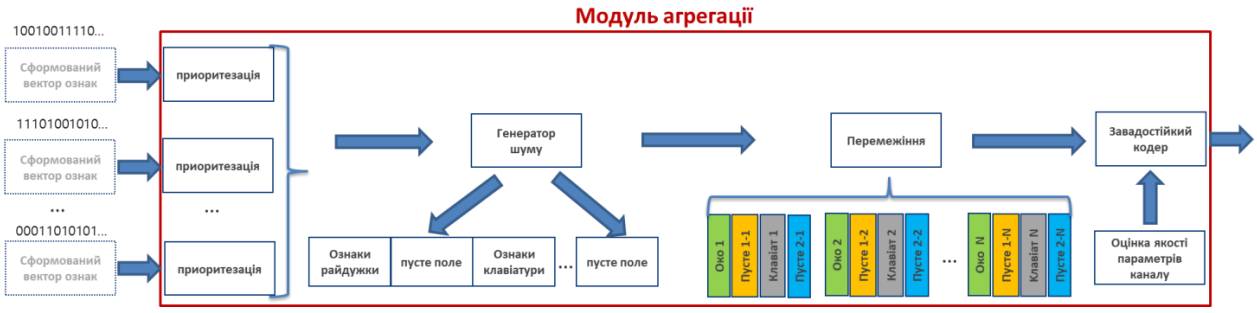


Рис. 5.15. Запропонована структура модуля агрегації біометричних ознак

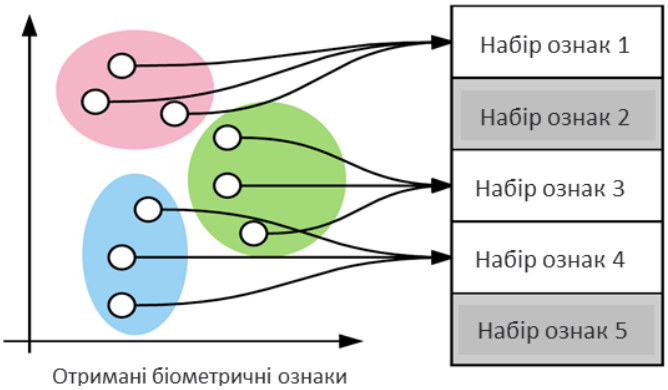


Рис. 5.16. Спрощена схема роботи модуля агрегації біометричних ознак

Принцип роботи модуля агрегації полягає в наступному (рис. 5.15):

1) *Отримання сформованих векторів ознак* від модулів формування вектору ознак.

2) Визначення наявних типів біометричних даних.

3) Для формування криптографічного ключа чи проходження автентифікації необхідно перевищити порогове значення. Кожен тип біометрії має власний пріоритет (рівень довіри) і відповідну вагу. Застосування *вектору пріоритетів* дозволяє визначити важливість певного методу біометричної автентифікації і його вплив на підсумковий результат.

4) Вибір тих біометричних даних, які мають забезпечити перевищення порогового значення необхідного для певного додатку користувача, відповідно до заздалегідь заданого набору правил [213,257], які будуть детально описані нижче, в підрозділі 5.7.

5) Застосування *генератора шуму* для зашумлення тих полів, що не використовуються під час даної сесії (але за умови використання іншої біометрії наступного разу – можуть бути заповнені). Це не дозволяє злонамірнику винайти зв’язок між полями.

6) Оскільки криптографічний ключ має передаватися по відкритим каналам мобільного зв'язку для виконання віддаленої автентифікації, то необхідно забезпечити його стійкість до завад в каналі. Цю задачу вирішує *блок перемежіння*. Додатковою його задачею є підвищення прихованості.

7) Використання *завадостійкого коду* після перемежіння також має на меті підвищити стійкість до завад. На цьому етапі пропонується використовувати модифікований варіант коду Raptor, який був описаний в розділі 4.

8) Параметри завадостійкого коду залежать від параметрів каналу зв'язку, які через петлю зворотного зв'язку потрапляють на кодер (*блок оцінка параметрів каналу зв'язку*). Запропонована інтелектуальна система прийняття рішень, яка дозволяє налаштовувати параметри завадостійкого кодування та обирати тип біометричної системи для формування шаблону (підрозділ 5.3.4).

Наукова новизна методу формування модуля агрегації полягає в застосуванні набору правил (додаток / необхідний пороговий рівень), застосуванні пріоритезації біометричних ознак, використанні генератору шуму для зашумлення невикористовуваних полів, застосуванні перемежувача та завадостійкого кодування для підвищення стійкості до завад і конфіденційності під час передачі каналами зв'язку, а також застосуванні інтелектуальної системи прийняття рішень для оцінки параметрів каналу зв'язку і налаштування параметрів завадостійкого кодування.

5.3.4 Інтелектуальна система прийняття рішень

Розглянемо запропоновану систему прийняття рішень (рис. 5.17) [73]. Нехай на її вхід подається набір початкових даних (блок «Вхідні дані», рис.

5.17), який для досліджуваного випадку містить інформацію про стан каналу зв’язку та інформацію про характер отриманих біометричних ознак користувача.

Рис. 5.17. Узагальнена схема інтелектуальної системи прийняття рішень

Інформація про стан каналу [193] включає наступні параметри (дослідження проводилися на прикладі LTE/5G мережі):

- параметри потужності сигналу та якості: потужність сигналу RSRP (Reference Signal Receive Power), якість сигналу RSRQ (Reference Signal Received Quality), співвідношення сигнал/шум SINR (Signal-to-Interference-plus-Noise Ratio), доступна пропускна здатність Cell Bandwidth, використовувана схема модуляції та кодування MCS (Modulation and Coding Scheme);

- наявність фонових сесій за протоколами IP, TCP, RTP, SCTP та ін.

На основі пропускної здатності, співвідношення сигнал/шум та параметрів якості/потужності визначаються рекомендовані параметри завадостійкого кодування, а також гранична кількість повторно переданих пакетів.

Наявність активних сесій аналізується за допомогою програмного забезпечення на пристрої користувача і може впливати на вибір методу, що використовує заміну певних полів в заголовку.

Для навчання штучної мережі була підготовлена вибірка мережних станів, отримана з телефонів Samsung Galaxy S21, яка містить стани каналу від RSRP = –60 дБм до –120 дБм, якість RSRQ змінюється в діапазоні від –5 до -18 дБ, пропускна здатність: 10-15МГц.

Перед початком роботи інтелектуальної системи мають бути сформовані всі дозволені сценарії роботи (рис. 5.17). Множина сценаріїв має зберігатися у спеціальній базі знань. Архітектура бази даних включає всі зазначені поля стану каналу і поле, що містить сформовані біометричні ознаки користувача. Також до неї включені поле з переліком можливих методів захисту та поле з набором дозволених алгоритмів. Обрання того чи іншого сценарію буде відбуватися на основі навчання відповідної нейронної мережі. Для недопущення випадку DoS (denial of service) атаки в базі знань має бути прописаний «найгірший» сценарій, який буде працювати у будь-яких умовах, але можливо з гіршими характеристиками (нижча швидкість та прихованість, більша надмірність шаблону).

Використовуючи вхідні дані, система (рис. 5.17), обирає згідно заданих заздалегідь критеріїв відповідності сценарій, що максимально відповідає поточному стану. Після цього з бази знань обирається набір доступних для цього сценарію методів захисту.

Приклад роботи системи і формування рішення наведено на рис. 5.18. У наведеному прикладі маємо низький рівень потужності при низькій якості, що згідно [200] буде відповідати параметру якості каналу (CQI) 7-9. Це призведе до обрання алгоритму модуляції 16QAM і швидкості кодування 1/3, також немає інформації про додаткові сесії, відповідно має бути обраний

стійкий до завад алгоритм захисту – біометрична система зі зв’язуванням ключа.

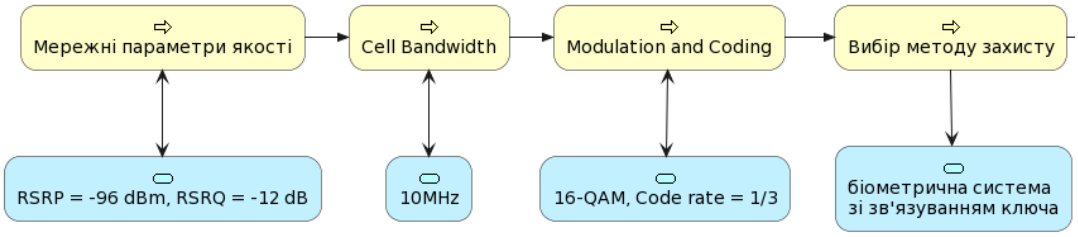


Рис. 5.18. Приклади роботи інтелектуальної системи прийняття рішень

5.3.5 Модуль генерації ключа

На вхід блоку формування ключа приходить пріоритезований вектор біометричних ознак $⟦w=w⟧\_1, w\_2, …w\_n$ після процедур завадостійкого кодування та перемежіння. До нього застосовується хешування, наприклад [214], після чого результат потрапляє на блок симетричного шифрування [215].

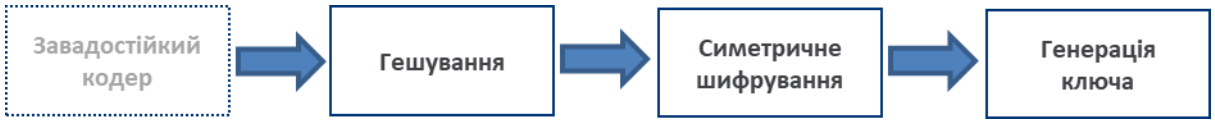


Рисунок 5.19. Модулі генерації криптографічного ключа та захисту біометричного шаблону

Після формування ключа і підготовки шаблона до передачі відкритими каналами зв’язку можна підвищити рівень конфіденційності шляхом застосування методів мережної стеганографії (прихованих каналів).

5.4 Застосування прихованих каналів для передачі інформації під час віддаленої автентифікації

5.4.1 Застосування методів мережної стеганографії для підвищення прихованості віддаленої автентифікації

Для підвищення захищеності (шляхом збільшення прихованості) біометричних даних можливе використання різних методів стеганографії [243,244], які дозволяють скрити сам факт передачі даних, необхідних для автентифікації мережею. Інформація, факт передачі якої потрібно приховати, розміщується в стегоконтейнері, в якості якого можуть виступати аудіо та відео файли, зображення та інша інформація, яка має надмірність. Модифікація таких контейнерів незначна і факт приховування в них даних складно виявити.

Для методів приховування в нерухомих зображеннях та відео автором були запропоновані вдосконалені методи, які дозволяють забезпечити більш високі значення надійності та захищеності [246, 255, 260].

У мережній стеганографії в ролі стегоконтейнера використовуються мережні протоколи моделі OSI. Модифікація деяких заголовків пакетів, полів корисного навантаження, порядку передачі пакетів дозволяє приховувати інформацію не порушуючи звичайну роботу мережі [217].

У даній роботі обґрунтовується можливість використання для підвищення захищеності (прихованості) методів мережної стеганографії з порівняльною оцінкою їх ефективності [194,201,249,259,263]. За останні роки було отримано ряд результатів, які спрямовані на створення нових методів мережної стеганографії. Так, в роботі [250] було розроблено метод мережної стеганографії, який не можна виявити. В роботі [251] запропоновано його застосування для встановлення прихованого зв’язку між зловмисником і

активним шкідливим додатком на стороні зараженого терміналу. В свою чергу, в роботі [252] запропоновано новий метод мережної стеганографії – «метод опцій», та описано теоретичну основу на прикладі опцій «запис маршруту» та «тимчасовий штамп». Щодо досліджень впливу стеганографічних характеристик, у роботі [253] проводились дослідження важливості впливу такої характеристики як стеганографічна вартість на ймовірність виявлення методів мережної стеганографії.

В [216] наведено класифікацію існуючих методів мережної стеганографії. Відповідно до неї існують методи модифікації пакетів (модифікація заголовків пакетів, полів корисного навантаження), методи модифікації структури передачі пакетів (зміна послідовності передачі, внесення навмисних затримок), а також гібридні методи.

До методів мережної стеганографії з модифікацією пакетів відносять методи модифікації полів заголовків IP і TCP, що не використовуються [218], SCTP протоколів [219] і методи, які модифікують корисне навантаження пакета, наприклад Transcoding Steganography [220].

Заголовок IP пакета зазвичай використовує поля, що мають деяку надмірність або не використовуються під час передачі. Ці поля можна використовувати для прихованої передачі даних (наприклад, поля «ідентифікатор» і «прапори» при відсутності фрагментації пакетів під час передачі).

Transcoding Steganography використовується для приховування даних в IP телефонії а також при передачі потокового відео. IP телефонія дозволяє користувачам здійснювати телефонні дзвінки через дані мереж, що використовують протокол IP. Для приховування інформації даний метод стискає корисне навантаження мережного пакету за рахунок перекодування голосових даних з мінімальною втратою якості голосу і на місце, що

звільнилось в область корисного навантаження пакета вносять стеганограму [220].

До гібридних методів відносять методи LACK, HICCUPS, RSTEG [194].

LACK (Lost audio packets steganography) – це стеганографічний метод, який модифікує як RTP пакети, так і їх тимчасові залежності. Для того, щоб приховати інформацію використовується той факт, що надмірно затримані пакети не використовуються для відновлення даних і відкидаються. У передавачі один RTP пакет вибирається з голосового потоку і його корисне навантаження замінюється бітами секретного повідомлення. Потім цей пакет навмисно затримується перед передачею. Якщо приймальна сторона не знає про факт передачі прихованої інформації то пакет відкидається. Але якщо одержувач знає про приховану передачу, то замість відкидання він приймає цей пакет і вилучає корисне навантаження. Дізнатися про навмисну затримку пакета допомагають затримка обробки кодеку мови, затримка пакетування, затримка буфера тремтіння. Спроба приховати великий обсяг даних призведе до того, що велика кількість пакетів будуть приходити з підозріло великими затримками [221].

Метод HICCUPS (Hidden Communication System for Corrupted Networks) використовує той факт, що бездротові мережі сприйнятливі до спотворення даних тому використання перешкод і шуму в середовищі зв'язку в продуктивності системи представляється дуже привабливим. HICCUPS – це стеганографічна система з розподілом смуги пропускання для мереж загального користування. Цей метод включає використання захищеної телекомунікаційної мережі з криптографічними механізмами для забезпечення роботи стеганографічної системи і пропонує новий протокол з розподілом пропускної спроможності для стеганографічних цілей, заснованих на пошкоджених пакетах (кадрах) [222].

Метод RSTEG (Retransmission steganography) ґрунтується на повторному пересиланні пакетів. Отримувач не повинен визнавати пакет успішно прийнятим для того, щоб навмисне викликати повторну передачу. Пакет, що ретранслюється, є носієм стеганограми замість призначених для користувача даних у полі корисного навантаження [217].

Для визначення переважного методу приховання, використаємо основні показники стеганографічних систем: пропускну здатність, стійкість до атак і завад, прихованість та складність реалізації [221, 248].

Стеганографічна пропускна здатність еквівалентна корисному навантаженню водяного знаку. Це максимальна кількість бітів, яку можна заховати в даному об'єкті прикриття так, щоб ймовірність виявлення зловмисником була незначною.

Стійкість до атак і завад – це здатність виявляти водяний знак після звичайних операцій обробки сигналу. Прикладами поширених операцій над зображеннями є просторова фільтрація, друк і сканування, а також геометричні спотворення (поворот, масштабування).

Прихованість полягає в неможливості виявити водяний знак на конкретному носії. Найпопулярнішим способом виявлення водяного знаку є аналіз статистичних характеристик перехоплених даних і порівняння їх з типовими характеристиками.

Побудуємо ієрархію для вибору оптимального методу мережної стеганографії (рисунок 5.20). На першому рівні цієї ієрархії мета – вибір оптимального методу, на другому рівні – критерії що характеризують стеганографічні методи, на третьому – методи, що розглядаються.

Ієрархія відображає проведений аналіз важливих елементів та їх взаємовідношення. Для прийняття рішень про те, які методи є кращими потрібно визначити з якою силою елементи одного рівня впливають на

елементи попереднього рівня для того, щоб було можливо розрахувати величину впливу елементів самого нижчого рівня на загальну мету [193].

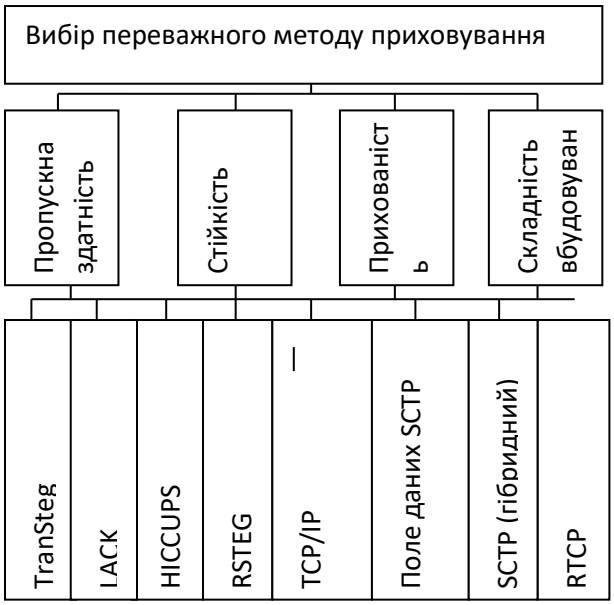


Рис. 5.20. Ієрархія методів мережної стеганографії та критеріїв важливості

Використовуючи існуючі характеристики методів наведені в [218-222], а також порівняння методів мережної стеганографії наведених у [194], всім елементам присвоєні оцінки за 9-бальною шкалою, які відповідають шкалі відносної важливості що приведена у табл. 5.3 [223,245].

Після встановлення рівнів ієрархії формуються матриці попарних порівнянь (5.25) між елементами відносно кожного елемента більш високого рівня, який виступає критерієм для порівняння.

Таблиця 5.3 – Таблиця відносної важливості

Ступінь переваги	Визначення
1	Еквівалентність критеріїв
3	Помірна перевага одного критерія над іншим
5	Істотна перевага одного критерія над іншим
7	Очевидна перевага одного критерія над іншим
9	Абсолютна перевага одного критерія над іншим
2, 4, 6, 8	Проміжні значення

$$A = \begin{pmatrix} 1 a_{12} \ldots a_{1j} \\ a_{21} 1 \ldots a_{2j} \\ \ldots \\ a_{i1} a_{i2} \ldots 1 \end{pmatrix}, \tag{5.25}$$

де $a_{ij} = \frac{w_з}{w_j}$ – значення, що відображає ступінь переваги одного показника над іншим.

На основі (5.25), оцінимо власні вектори V_i показників (5.26) і глобальний вектор пріоритетів P_i (5.27):

$$V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}}, \quad j = \overline{1,n}, \tag{5.26}$$

де n – кількість показників.

$$P_j = \frac{V_j}{S}, \quad j = \overline{1,n}, \text{ де } S = \sum_{j=1}^{n} V_j. \tag{5.27}$$

Далі виконані попарні порівняння обраних методів мережної стеганографії по відношенню до показників якості мережної стеганографії [248].

В табл. 5.4 зведені глобальні вектори пріоритетів методів мережної стеганографії, оцінені відносно можливості застосування в системі віддаленої автентифікації.

Аналіз табл. 5.4 показав, що кращими за сукупністю критеріїв є метод модифікації заголовків (TCP, IP, RTP), а також гібридний стеганографічний метод HICCUPS. Також високий пріоритет у методу TranSteg. Ці методи можуть бути використані для підвищення конфіденційності шляхом

використання прихованого каналу для передачі біометричних шаблонів під час віддаленої автентифікації.

Таблиця 5.4 – Вектори пріоритетів методів мережної стеганографії

№	Метод	Глобальний вектор пріоритету
1	**TranSteg**	**0,162**
2	LACK	0,116
3	**HICCUPS**	**0,165**
4	RSTEG	0,059
5	**Модифікація заголовків TCP/IP/RTP**	**0,171**
6	Модифікація блоків даних SCTP	0,082
7	SCTP (гібрид)	0,114
8	SCTP multi-homing	0,129

5.4.2 Аналіз завадостійкості методів мережної стеганографії під час проведення віддаленої автентифікації

Враховуючи специфіку віддаленої біометричної автентифікації, для вказаних методів була оцінена стійкість до завад та прихованість [248,249,254,264]. У ході дослідження використовувався адитивний білий гаусів шум (Additive White Gaussian Noise, AWGN). Даний тип шуму характеризувався двома параметрами: середнім значенням μ і дисперсією $\sigma=2$ і мав рівномірну потужність у всієї смузі частот. Випадковий характер шуму у часовій області в окремих випадках спричиняв передачу символу, який був спотворений таким чином, що приймач інтерпретував його як інший символ. Якщо в передані дані вносились помилки, цілісність системи могла порушуватись. Для оцінки ефективності системи було використано коефіцієнт бітових помилок (Bit Error Ratio, BER). В табл. 5.5 представлено результати розрахунку коефіцієнту бітових помилок відносно одного контейнеру.

Таблиця 5.5 – Результати розрахунку BER для реалізованих методів стеганографії

Дисперсія	BER для методу HTTP	BER для методу ICMP	BER для методу TCP
0.1	0	0	0
0.2	0	0	0
0.3	0.0030	0.004	0.0023
0.4	0.0034	0.016	0.0093
0.5	0.0038	0.041	0.03

З табл. 5.5 видно, що метод ICMP є менш стійким до шумів, так як забезпечував більші значення коефіцієнту бітових помилок у порівнянні з іншими методами. В методі HTTP при значеннях дисперсії менш ніж 0.3 приховані данні відновлювались без змін. Проте при збільшенні значення дисперсії повідомлення не відновлювалось. В методі ICMP повідомлення не відновлювалось при значенні дисперсії більш ніж 0.3, а в методі TCP данні можна відновити з невеликими спотвореннями при значенні дисперсії 0.4. В результаті даного порівняння методів можна зробити висновок, що найбільш стійким до шуму виявився метод мережної стеганографії, що приховує дані у TCP-заголовках.

Для дослідження стійкості до виявлення реалізованих методів мережної стеганографії було проведено аналіз впливу передачі вбудованого прихованого повідомлення на характеристики трафіка в цілому. Трафік перехоплювався та аналізувався за допомогою програми Wireshark: при включеному браузері після початку перехоплення трафіка за хвилину часу було завантажено дві http-сторінки та дві https-сторінки. Також було використано клієнтську програму YateClient, за допомогою якої було виконано п’ятисекундний дзвінок за допомогою технології Voice over Internet Protocol (VoIP). Для забезпечення цих двох сервісів було використано протокол доменної системи імен (Domain Name System, DNS), протокол

захисту транспортного рівня (Transport Layer Security, TLS), протокол встановлення сесії (Session Initiation Protocol, SIP) / протокол опису сеансу зв'язку (Session Description Protocol, SDP), SIP, протокол датаграм користувача (User Datagram Protocol, UDP), протокол передачі даних у реальному часі (Real-time Transport Protocol, RTP), протокол управління передачею в реальному часі (Real-time Transport Control Protocol, RTCP). На рис. 5.21 зображена гістограма, на якій представлено динаміку зміни характеристик трафіка при використанні методу HTTP.

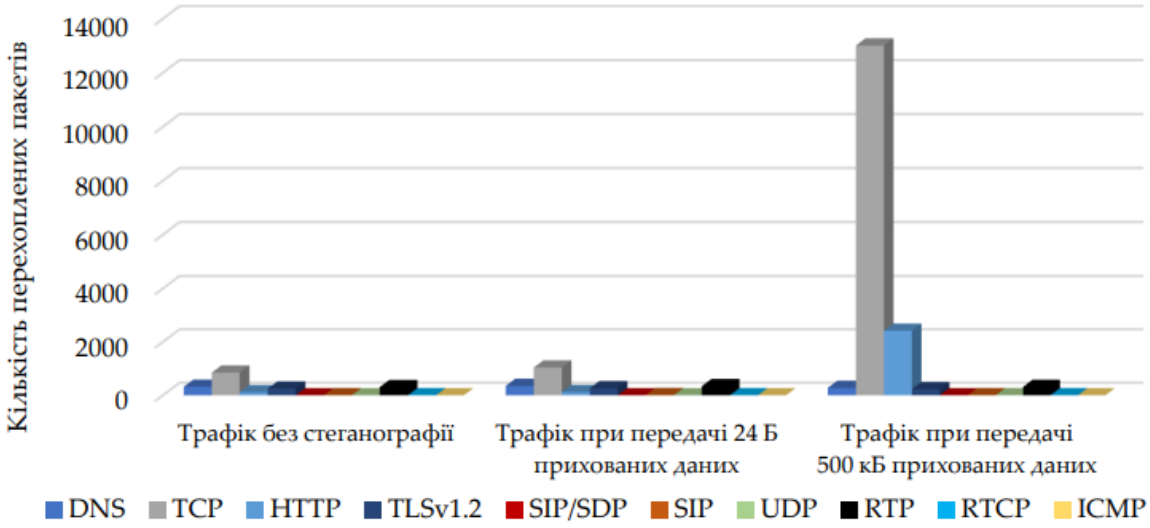


Рис. 5.21. Дослідження статистичних характеристик трафіка при використанні методу HTTP

Можна побачити, що у разі передачі невеликої кількості прихованих даних (24 байти) статистичні характеристики трафіка майже не змінилися, але при передачі більшої кількості даних, значно збільшується об'єм TCP і HTTP трафіка. Кількість TCP-сегментів зростає з тієї причини, що при надсиланні кожного нового HTTP-заголовку встановлюється нове з'єднання, при якому кожний раз відбувається початок сеансу TCP.

На рис. 5.22 представлено отримані результати аналізу характеристик трафіка, коли використовувався метод TCP. Як і очікувалось, при невеликому розмірі прихованих даних, що передаються, об’єм TCP-трафіка збільшився незначно. В свою чергу, при зростанні об’єму прихованих даних (500 кб) об’єм TCP-трафіка зростає майже в два рази, що робить даний метод мережної стеганографії досить помітним.

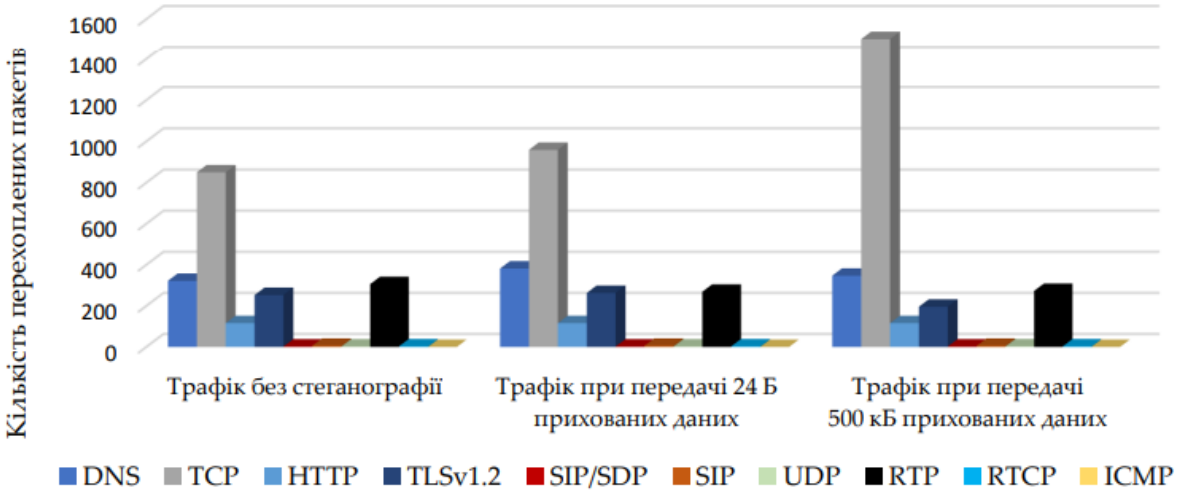


Рис. 5.22. Дослідження статистичних характеристик трафіка при використанні методу TCP

Метод ICMP досліджувався за умови вбудовування інформації у двох режимах. На рис. 5.23 та рис. 5.24 представлено статистичні характеристики трафіка, що були досліджені для режимів «Безпечний» і «Швидкий» відповідно.

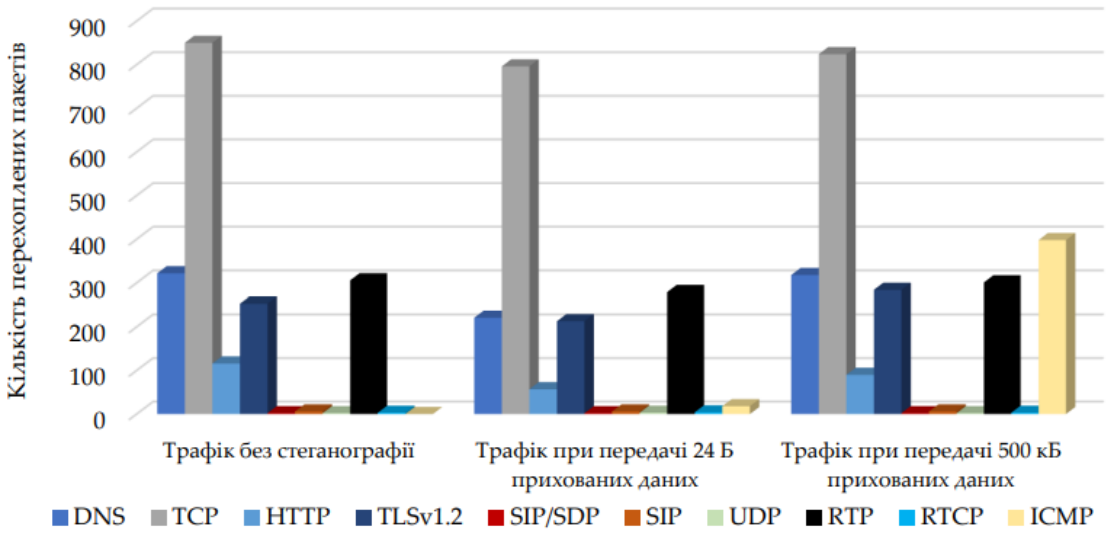


Рис. 6. Дослідження статистичних характеристик трафіка при використанні режиму «Безпечний» методу MC-ICMP

Рис. 5.23. Дослідження статистичних характеристик трафіка при використанні “безпечного” методу ICMP

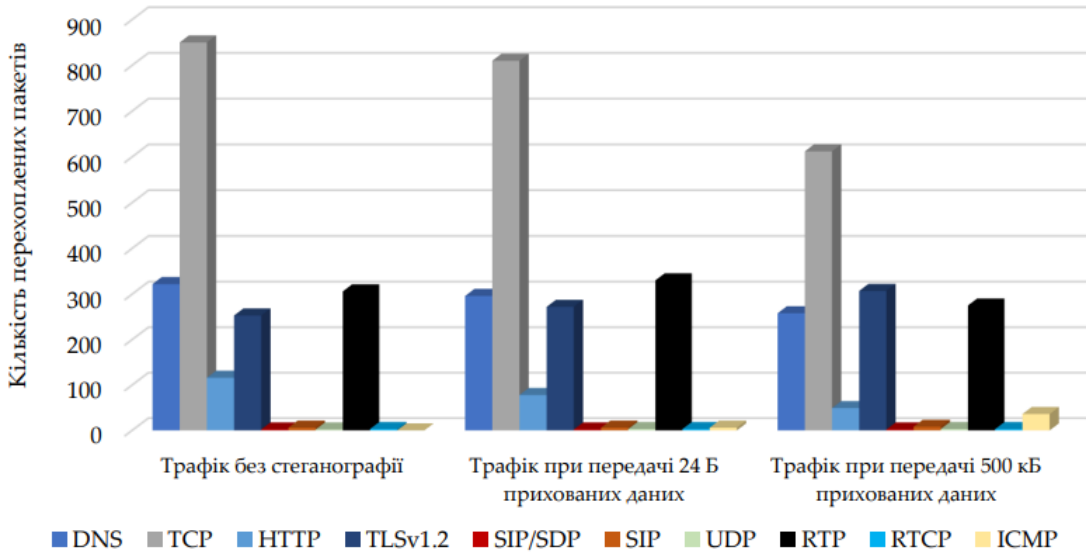


Рис. 5.24. Дослідження статистичних характеристик трафіка при використанні “швидкого” методу ICMP

Результати показують, що кількість ICMP-пакетів значно зросла при передачі даних розміром 500 кб в режимі «Безпечний», що не можна сказати

про режим «Швидкий». У разі використання режиму «Швидкий» кількість нових ICMP-пакетів значно менша, що вказує на те, що, використовуючи даний метод для створення прихованого каналу передачі даних, можливість його виявлення значно менша.

Найгіршим виявився метод HTTP, який мав низьку стійкість до шуму, через те що при значенні дисперсії менше 0.3 приховане повідомлення не відновлювалось. Крім того, у разі застосування методів HTTP та TCP трафік різко збільшувався в декілька разів. У свою чергу, метод TCP є найбільш ефективним за умови роботи каналами зв'язку з шумами: він дає можливість відновити приховане повідомлення з невеликими спотвореннями при значенні дисперсії 0.4. Проте даний метод мережної стеганографії значно програє режиму «Швидкий» методу ICMP за критерієм прихованості. З огляду на специфіку застосування розглянутих методів мережної стеганографії для віддаленої автентифікації за сукупністю критеріїв стійкість до шумів / прихованість, рекомендується для використання режим «Швидкий» методу MC-ICMP.

При цьому слід зазначити, що метод HICCUPS забезпечує найвищий рівень прихованості у зашумлених каналах [248, 249], оскільки виконує маскування інформації під «природні» завади. Метод TranSteg використовується для приховування даних в IP телефонії а також при передачі потокового відео. Для приховування інформації даний метод стискає корисне навантаження мережного пакету за рахунок перекодування голосових даних з мінімальною втратою якості голосу і на місце, що звільнилось в область корисного навантаження пакета вносять стеганограму, відповідно цей метод ефективний під час активної голосової чи відео сесії. Метод LACK також використовує активну RTP сесію, але його принцип дії заснований на внесенні затримки при відправці певних голосових пакетів,

корисне навантаження яких замінено. Метод RSTEG ґрунтується на повторному пересиланні пакетів і його використання для найбільшої прихованості також рекомендовано в каналах зв’язку з низьким співвідношенням сигнал/шум.

На основі визначеного переважного методу мережної стеганографії, була запропонована схема захисту процесу віддаленої біометричної автентифікації з додаванням етапів приховування та завадостійкого кодування (рис. 5.25). Блоки, що відрізняють її від існуючої системи (рис. 1.20 б) наведені зеленим кольором.

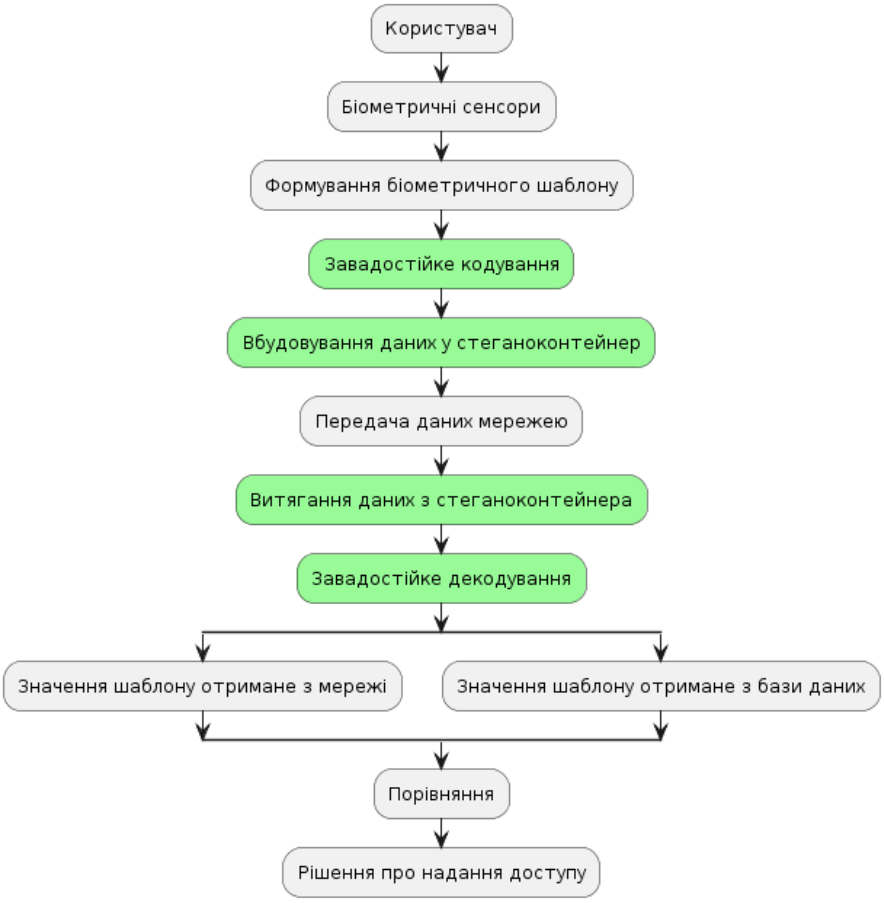


Рис. 5.25. Модифікована схема захисту віддаленої біометричної автентифікації [259]

Оскільки маємо декілька методів мережної стеганографії зі схожим значенням глобального вектору пріоритетів, вибір може бути оптимізований в певний момент часу, в залежності від стану каналу зв'язку і наявності активних сесій. Застосуємо і вдосконалимо інтелектуальну систему (рис. 5.17), описану в 5.3.4. Вдосконалення буде полягати у виборі набору методів захисту, на основі ідентифікації умов на вході і визначенні поточного сценарію [73, 259].

Як було вказано в 5.3.3, інтелектуальна система аналізує наявність фонових сесій за протоколами IP, TCP, RTP, SCTP, що дозволяє обрати під наявну сесію переважний метод мережної стеганографії. Також на основі пропускної здатності, співвідношення сигнал/шум та параметрів якості/потужності визначаються рекомендовані параметри завадостійкого кодування, а також гранична кількість повторно переданих пакетів, що дозволяє задати пропускну здатність стеганографічних методів, які використовують повторну передачу (RSTEG, HICCUPS).

Приклад роботи інтелектуальної системи, адаптованої під вибір методу приховування (методу мережної стеганографії) показаний на рис. 5.26.

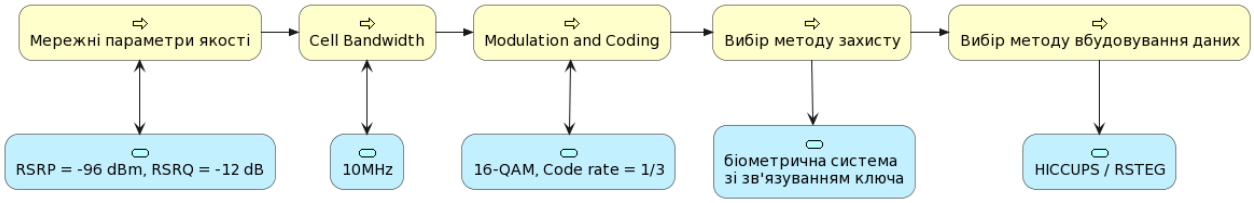


Рис. 5.26. Приклади роботи інтелектуальної системи прийняття рішень

Застосування наведеного методу дозволяє вдосконалити показник конфіденційності шляхом застосування і аналізу використання прихованих каналів передачі.

5.4.3 Впровадження стеганографічної системи приховання біометричних даних користувача

Вказаний підхід був впроваджений в систему приховання біометричних даних користувача у зображеннях за допомогою цифрових водяних знаків [213, 265]. Згідно патентів [213, 265] (рис. 5.27), пропонується на зображеннях користувача знаходити біометричні ознаки методами комп'ютерного зору (наприклад, дослідженими в розділі 3), кодувати винайдені біометричні ознаки і генерувати нове зображення з модифікованими біометричними ознаками та цифровим водяним знаком (watermark). Після цього у соціальних мережах або відкритих публікаціях початкове фото замінюється на синтезоване.

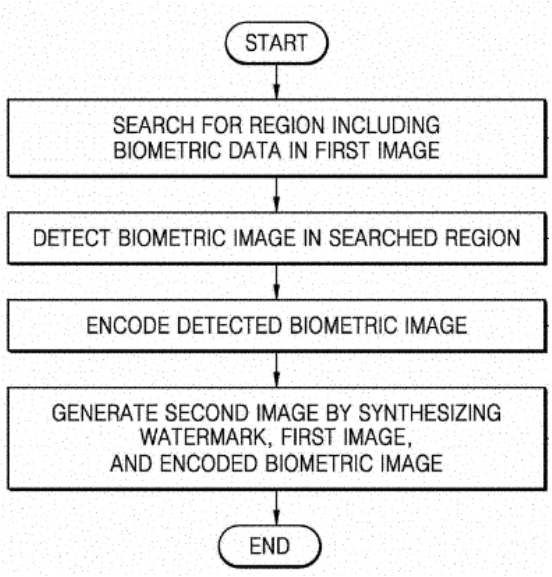


Рис. 5.27. Алгоритм виявлення біометричних ознак користувача у зображенні

Водяний знак може містити оригінальну карту глибини або модифікацію параметрів інтелектуальної карти глибини [213]. Він також може включати параметри навколишніх спотворень. Водяний знак може бути вбудований в

просторову область (наприклад, через зміну співвідношення яскравості) або область перетворення (наприклад, у вейвлет-область або дискретні коефіцієнти косинусного перетворення).

Для шифрування водяного знаку використовується секретний ключ пристрою. Цей ключ зберігається в довірчій зоні і не може бути викрадений. Процедура шифрування та дешифрування також виконується в довірчій зоні ("безпечному світі").

Послідовність (рис. 5.27) має виконуватися окремо для кожного типу біометричних даних, описаних вище. В якості ілюстрації (рис. 5.28), наведемо більш детально цю послідовність на прикладі приховування райдужної оболонки користувача з відкритого зображення.

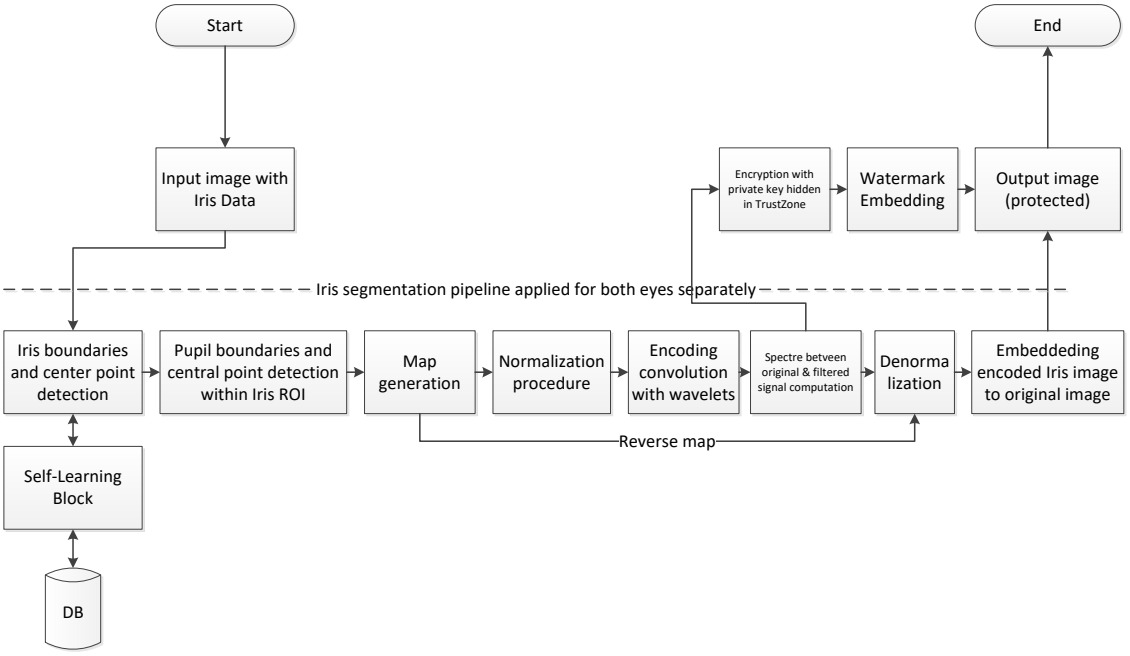


Рис. 5.28. Процес приховування приватних даних з райдужної оболонки користувача [213]

Для відтворення початкового зображення і використання біометричної інформації наявної в ньому використовується цифровий водяний знак і наступна послідовність, рис. 5.29.

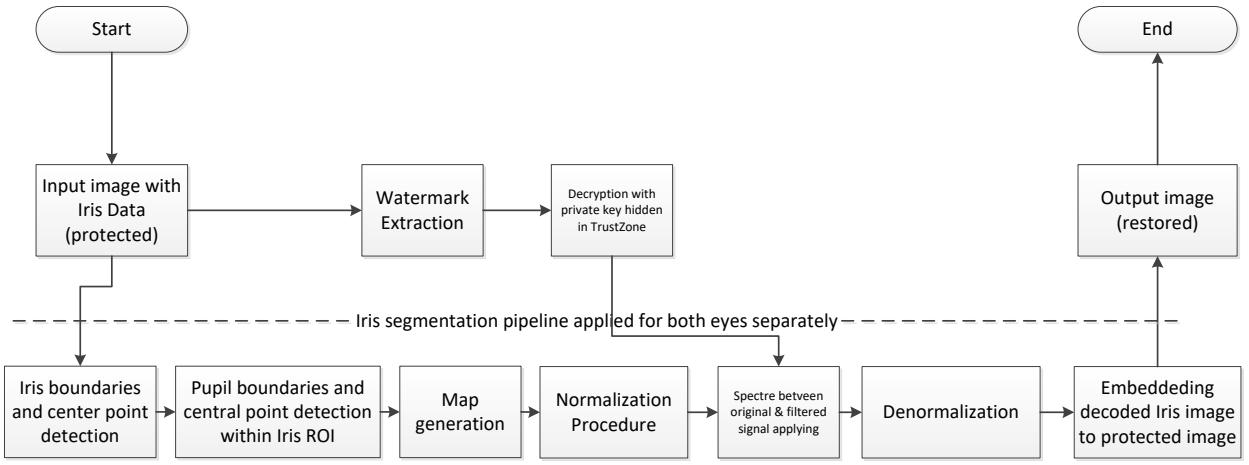


Рис. 5.29. Процес відтворення приватних даних з райдужної оболонки користувача [213]

Відтворення райдужної оболонки включає витягання водяного знаку із захищеного зображення та розшифрування за допомогою закритого ключа, що зберігається в TrustZone на пристрої. Після цього застосовується спектральна різниці до нормалізованого зображення райдужної оболонки ока та вбудовування в захищене зображення. В результаті зображення буде містити оригінальні (відновлені) біометричні дані.

5.5 Забезпечення безпечної відповіді на дзвінки шляхом взаємної автентифікації користувачів під час дзвінка

5.5.1 Вішинг та спам-дзвінки: сучасний стан проблеми

Багато людей отримують телефонні дзвінки від невідомих абонентів, і це стає серйозною проблемою. Спам-дзвінки продовжують ошукувати людей у всьому світі, незважаючи на зусилля операторів, представників телекомунікаційних компаній, розробників мобільних операційних систем, виробників смартфонів та глобальну пандемію (рис. 5.30). Truecaller

повідомляє про 31,3 мільярда спам-дзвінків по всьому світу з січня по жовтень 2022 року [224]. Згідно зі звітом [224], у 2021 році середньостатистичний американець втратив близько 502 доларів США через вішинг (також відомий як "голосовий фішинг") і це більше, ніж 351 долар США у 2020 році. 2021 рік також став рекордним за кількістю втрачених грошей через голосовий фішинг.

Спам-дзвінки, як правило, є шахрайством, спрямованим на отримання конфіденційної особистої інформації, такої як: інформація про соціальне страхування, ідентифікаційний номер, дані кредитної картки. Зловмисники використовують спам-дзвінки для незаконного отримання даних, щоб отримати доступ до ваших банківських рахунків та облікових записів у соціальних мережах. Лише в США це сталося з 27 мільйонами людей, які стали жертвами цих шахрайських дій.

Одним з найпопулярніших видів голосового фішингу є рободзвінок [225]. Рободзвінок – це переадресація на дзвінок, який передає заздалегідь записані повідомлення за допомогою програмного забезпечення для автоматичного набору. Його можна використовувати для таких речей, як офіційні оголошення та телемаркетингові кампанії. Він також може стати ідеальною платформою для шахрайства та спам-дзвінків.

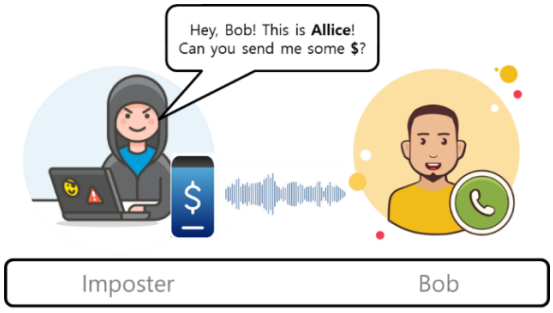


Рис. 5.30. Хакер видає себе за Алісу і дзвонить Бобу, використовуючи її номер телефону

Одна з трьох жертв шахрайських дзвінків піднімає слухавку, бо номер був знайомий. Невідомі номери є найпоширенішими, і люди не відповідають на них. Це призвело до того, що шахраї прийняли нову стратегію, щоб отримати відповідь на свої дзвінки. Щоб завоювати довіру одержувача, вони почали підробляти номери телефонів реальних компаній і діяти як вони. Це називається "корпоративний спуфінг" [225].

Для захисту від спаму та фішинг-спаму необхідно бути впевненим у тому, що співрозмовник підтверджений, для чого підробляють ідентифікатор абонента різними методами та за допомогою різних технологій [227]. Зловмисник може використовувати ідентифікатор абонента для жартівливих дзвінків і крадіжки телефону. Щоб захистити користувачів, необхідно застосовувати ефективні методи автентифікації, сумісні з існуючими телекомунікаційними протоколами.

5.5.2 Аналіз існуючих рішень по автентифікації дзвінків

Автентифікація дзвінків – це процес, який перевіряє особу абонента і ускладнює нелегальну підробку. Сучасні рішення в основному базуються на наявності довіреної третьої сторони («контакт-центру»), в якості якого має виступати провайдер послуг, що додає додаткові складності при організації безпеки – необхідність створення і підтримки контакт-центру. Найбільше розповсюдження зараз отримали рішення на основі фреймворку STIR/SHAKEN [226].

Відповідно до протоколу STIR/SHAKEN, до кожного дзвінка потрібно додати сертифікат про справжність, щоб постачальники послуг могли диференціювати законні дзвінки від шахрайських дзвінків, таких як незаконна підробка, рободзвінки або спам-дзвінки. Якщо дзвінок не

відповідає сертифікату, то клієнт побачить попередження про "спам-ризик" на ідентифікаторі абонента.

Фактично STIR/SHAKEN – це дві технології, які розшифровуються як безпечна телефонія з повторною перевіркою ідентичності (STIR) та безпечна обробка підтвердженої інформації за допомогою токенів (SHAKEN). Простіше кажучи, технологія STIR дозволяє краще ідентифікувати абонента, оскільки вона перевіряє, звідки надходить дзвінок у різних точках. Замість того, щоб перешкоджати абонентам змінювати свій ідентифікатор, вона підказує кінцевим користувачам, чи варто довіряти дзвінку, чи ні.

Хоча технологія STIR була розроблена для сумісності з VoIP-дзвінками, ця система не сумісна зі звичайними телефонними мережами. Це призвело до розробки технології SHAKEN, яка виконує аналогічну функцію, що й STIR, але сумісна з телефонними мережами, які не залежать від інтернет-з'єднання.

Розглянемо більш детально, що відбувається на кожному етапі дзвінка при використанні технології STIR/SHAKEN [228].

1. Отримання запрошення

Коли хтось здійснює телефонний дзвінок, SIP-INVITE (запрошення) надсилається на мобільний телефон абонента, який телефонує. Це перший крок у процесі верифікації, і він важливий, оскільки запускає серію подій STIR/SHAKEN, призначених для перевірки особи абонента.

2. Визначення рівня атестації

Коли оператор зв'язку отримує запрошення від абонента, довірена третя сторона (провайдер) перевіряє запит, перш ніж прийняти його. Провайдер перевіряє джерело дзвінка та номер телефону, який використовується, щоб визначити, який рівень атестації надати дзвінку. Це важливо, оскільки ці дані також будуть передані в мережу одержувача, навіть якщо вона не збігається з мережею абонента.

В STIR/SHAKEN передбачено три рівні атестації – це повна атестація, часткова атестація і атестація шлюзу, які в мережі позначаються як A, B і C відповідно. Рівні атестації відіграють важливу роль у вирішенні того, як дзвінок відображатиметься на телефоні клієнта.

2.1 Повна атестація (A) – найкращий рівень атестації, який можна отримати від STIR/SHAKEN. Це означає, що оператор зв'язку перевірив особу абонента, який телефонує, і що абонент, який телефонує, має дозвіл на використання номера.

2.2 Часткова атестація (B) надається, коли оператор може підтвердити, що виклик надходить з місця, вказаного на мітці STIR. Однак часткова атестація також означає, що оператор не може перевірити, чи має абонент дозвіл на використання номера. Така атестація іноді надається новим внутрішнім номерам компаній, які не зареєстровані у оператора.

2.3 Атестація шлюзу (C) надається тоді, коли оператор може підтвердити, звідки надійшов виклик, але не його початкове місцезнаходження. Атестація шлюзу, яка відображається у вигляді літери C на пристрої абонента, зазвичай надається міжнародним дзвінкам.

3. Створення заголовка ідентифікації

Після отримання атестації та належної перевірки телефонного дзвінка оператор створює SIP-заголовок, який містить ідентифікаційну інформацію. Ідентифікаційний заголовок містить такі дані, як номер абонента, основна історія дзвінків, позначка часу, оцінка атестації та ідентифікатор походження.

4. Перевірка токену

Після створення ідентифікаційного заголовка вихідний дзвінок готовий до відправки. На наступному етапі оператор зв'язку абонента надсилає SIP-запрошення та інформацію в заголовку ідентифікатора оператору зв'язку

абонента. У деяких випадках ідентифікаційний маркер також надсилається до служби розміщення викликів телекомунікаційної компанії одержувача. Це додатковий запобіжний захід, який допомагає уникнути фальсифікації та підвищити точність даних.

5. Ініціювання верифікації

Після того, як оператор зв'язку приймаючої сторони отримає запит-запрошення і заголовну інформацію, він передає її до служби верифікації.

6. Отримання сертифіката та автентифікація

Коли служба верифікації отримує запит на автентифікацію, вона виконує кілька перевірок, щоб переконатися, що дзвінок не є підробленим. На цьому етапі постачальник послуг верифікації отримує цифровий сертифікат від оператора абонента і починає виконувати різні тести. Якщо всі етапи перевірки пройдено належним чином, дзвінок не був підроблений.

На цьому етапі служба верифікації оператора на стороні одержувача може перевірити такі речі, як ідентифікаційний заголовок, дійсність підпису SIP за допомогою відкритих ключів і ланцюжок довіри сертифіката.

7. Фінальна верифікація та з'єднання дзвінків

Нарешті, процес верифікації повертає свої результати оператору. Якщо результат виявився успішним і дзвінок не був підроблений, він передається до оператора-одержувача. Якщо процес завершено, але здається, що дзвінок був підроблений, він надсилається абоненту разом із попередженням про те, що він може бути підробленим.

Недоліками описаного вище підходу є те, що він потребує додаткового часу на перевірку на боці «довіреної сторони», в літературі відсутній опис процедури автентифікації у випадку CS дзвінка, а також існуючий підхід не захищає від випадків коли:

- з довіреного номера дзвонить інша людина (в існуючих рішеннях виконується автентифікація пристрою а не користувача);
- на приймальному боці трубку знімає не власник телефону, що може привести до витоку конфіденційної інформації;
- відбувається спуфінг (підміна) номера;
- відбувається витік даних на боці «контакт-центру» - довіреної третьої сторони.

Для перекриття цих недоліків був запропонований метод забезпечення взаємної автентифікації без зберігання конфіденційної інформації на боці «довіреної третьої сторони». В якості вимог до методу запобігання спам-дзвінків, рободзвінків та вішингу, були обрані:

- взаємна автентифікація користувачів під час дзвінка;

- сумісність з дзвінками 3G/2G (CS-дзвінки) і VoIP/SIP (PS-дзвінки);

- автентифікація повинна виконуватися природно, без додаткових дій з боку користувача;

- неможливість прийняти дзвінок без проходження автентифікації користувача.

5.5.3 Метод безпечної відповіді на дзвінки шляхом забезпечення взаємної автентифікації

В даній роботі, виходячи з наведених вище вимог був запропонований простий метод безпечної відповіді на дзвінки [289] через взаємну автентифікацію користувачів під час телефонного (CS) або пакетного (VoIP) дзвінка, що дозволяє користувачам бути впевненими в особі абонента (фізичної чи юридичної особи) і не боятися ділитися конфіденційною інформацією.

Сутність методу безпечної відповіді на дзвінки [289] полягає в (рис. 5.31):

1. отриманні біометричних даних користувача, що підлягає автентифікації (фаза реєстрації);
2. ідентифікації користувача ПІД ЧАС ДЗВІНКУ (без додаткових дій з боку користувача), як конкретного авторизованого користувача на основі біометричних даних (взаємна автентифікація під час дзвінка);
3. у разі позитивної ідентифікації:
   a. повідомлення з результатом автентифікації буде надіслано обом сторонам;
   b. на екрані з'являється підтвердження абонента, що викликає, та абонента, якому здійснюється виклик;
   c. виклик може бути прийнятий або відхилений відповідно до рішення авторизованого користувача;
4. у разі негативної ідентифікації:
   a. вхідний дзвінок буде відхилений;
   b. або може бути запитано додаткову автентифікацію.

Описану вище послідовність реалізує метод, зображений на рис. 5.31.

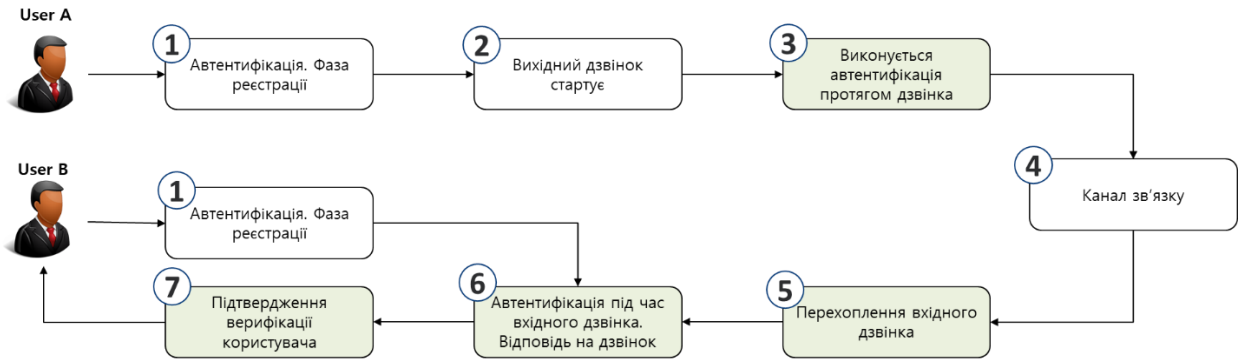


Рис. 5.31. Запропонований метод безпечної відповіді на дзвінки шляхом забезпечення взаємної автентифікації

Зеленим кольором позначені вдосконалені чи вперше запропоновані елементи.

Відповідно до рис. 5.31 процедура використання запропонованого методу [284, 289] складається з наступних етапів:

1. *Автентифікація: фаза реєстрації* полягає в тому, що користувачу потрібно вперше пройти процедуру реєстрації для автентифікації вуха. Щоб це зробити, користувач робить запит на процедуру автентифікації в додатку. Після чого бере телефон і декілька разів прикладає його до вуха, під час чого виконується наведений на рис. 5.32 алгоритм.

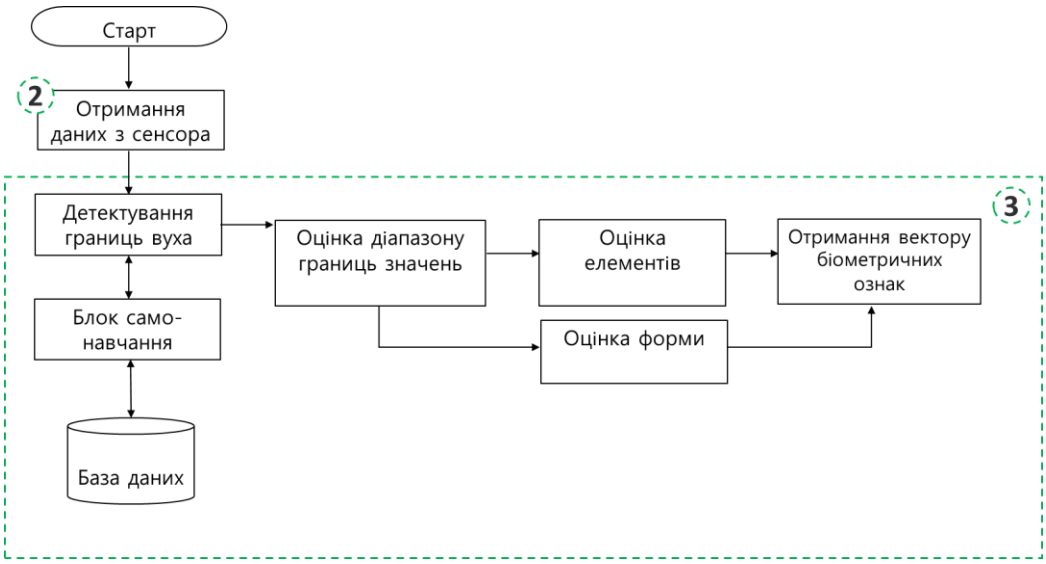


Рис. 5.32. Первинна автентифікація (фаза реєстрації користувача)

2. Початок вихідного дзвінка (рис. 5.31). Після успішної фази реєстрації, користувач починає дзвінок через стандартний додаток.

3. Автентифікація протягом вихідного дзвінка (рис. 5.31). Новий запропонований елемент алгоритму, полягає у застосуванні автентифікації по малюнку вуха під час набору номера. Автентифікація по малюнку вуха була обрана базуючись на перевагах, наведених на рис. 5.33. У випадку її

неуспішності може застосовуватись автентифікація через акустичний відгук [284] або відбиток пальця (рис. 5.34).

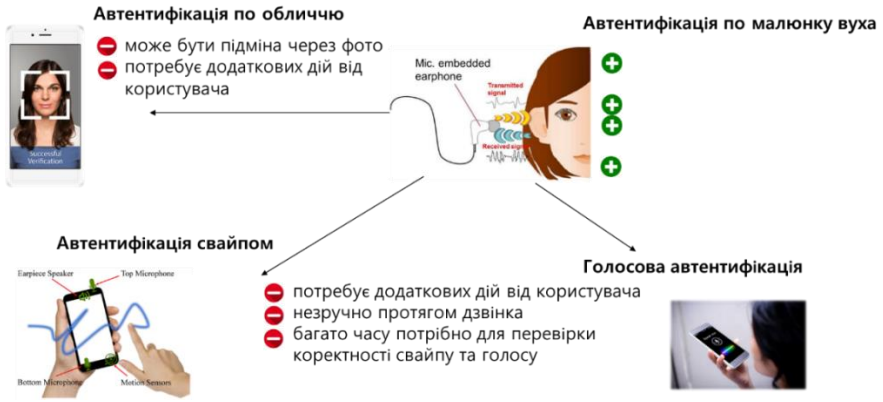


Рис. 5.33. Переваги видів автентифікації по малюнку вуха / акустичному відгуку вушної раковини

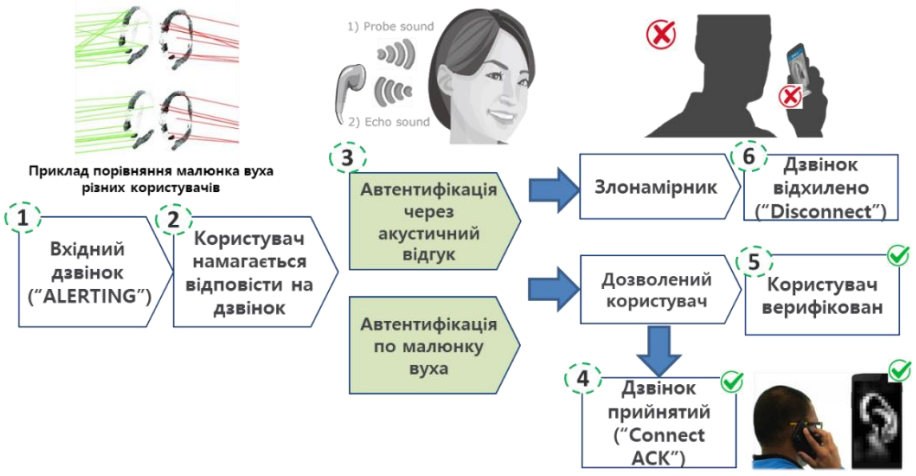


Рис. 5.34. Послідовність дій під час верифікації користувача при відповіді на дзвінок за допомогою телефону

4. Канал зв'язку (рис. 5.31). Виконується типові мережні процедури, пов'язані з передачею інформації від користувача *A* до користувача *B* і у зворотному боці.

5. Перехоплення вхідного дзвінка (рис. 5.31). Новий запропонований елемент алгоритму. Відповідає за автентифікацію користувача, що приймає

дзвінок, відповідно до одного з двох наведених нижче сценаріїв (рис. 5.34, у випадку відповіді на дзвінок за допомогою телефона і рис. 5.35 у випадку відповіді на дзвінок за допомогою смарт-годинника).

Рис. 5.35. Послідовність дій під час верифікації користувача при відповіді на дзвінок за допомогою смарт-годинника

Повідомлення про успішне проходження автентифікації включається до повідомлення "*CONNECT*" і відправляється на сторону абонента, що дзвонить. У випадку неуспішної автентифікації користувачу пропонується інший спосіб верифікації (наприклад відбиток пальця). До успішної автентифікації дзвінок не може бути прийнятий і буде відхилений.

6. *Відповідь на вхідний дзвінок* дозволяється тільки після успішної автентифікації.

7. *Підтвердження про верифікацію користувача* відбувається після успішної автентифікації під час дзвінка. Підтвердження для обох користувачів будуть доставлені за допомогою повідомлень "*SETUP*" і "*CONNECT ACK*". Приклад початкового і модифікованого повідомлення "*CONNECT ACK*" наведений на рис. 5.36.

CONNECT ACK
Вигляд повідомлення на цей час:

08:25:12.381 [18] UMTS DSDS NAS Signaling Messages --
CONNECT_ACKNOWLEDGE
Subscription ID = 2
Message Direction = From UE
chan_type = 0 (0x0)
prot_disc_check = 3 (0x3)
trans_id_or_skip_ind = 0 (0x0)
prot_disc = 3 (0x3) (GSM_CALL_CONTROL)
msg_type = 15 (0xf)

CONNECT ACK
Приклад модифікації повідомлення:

08:25:12.381 [18] UMTS DSDS NAS Signaling Messages --
CONNECT_ACKNOWLEDGE
Subscription ID = 2
Message Direction = From UE
chan_type = 0 (0x0)
prot_disc_check = 3 (0x3)
trans_id_or_skip_ind = 0 (0x0)
prot_disc = 3 (0x3) (GSM_CALL_CONTROL)
msg_type = 15 (0xf)
mt_verification = 1

Рис. 5.36. Приклад початкового і модифікованого повідомлення "*CONNECT ACKNOLEDGEMENT*"

Підсумкова call flow діаграма, що відображає весь процес дзвінка з вказанням модифікованих елементів (зелений колір) наведена на рис. 5.37. Для захищеної передачі повідомлень взаємної автентифікації використовується короткий автентифікаційний рядок, описаний в 5.6.3. Запропонований метод дозволяє забезпечити високорівневу реалізацією послуг «автентифікація відправника» та «автентифікація отримувача», згідно [60].

Рис. 5.37. Модифікований протокол обміну повідомленнями під час проходження голосового дзвінка через мережу

5.6 Метод забезпечення конфіденційності користувачів під час дзвінка

5.6.1 Аналіз сучасного стану проблеми

Окрім задачі взаємної автентифікації користувачів, під час дзвінка користувачі стикаються ще з рядом проблем, до яких відносяться:

- наскрізне шифрування в мобільній мережі відсутнє;
- голосові дані користувача (включаючи паролі) можуть бути перехоплені;
- абоненти мобільної мережі не захищені від сніфінг-атаки з боку оператора;
- абоненти мобільної мережі не захищені від атаки створення фейкової базової станції і інших атак, описаних в розділі 1.

5.6.2 Аналіз існуючих рішень з автентифікації та шифрування в мережі

Нагадаємо архітектуру безпеки мереж, наведену в розділі 1. В 2G/3G мережах, куди в Україні на деяких операторах виконується переадресація виклик під час хендоверу використовується протокол виклику та відповіді (рис. 5.38), в якому обладнання користувача (UE) має доводити знання ключа і лише в окремих випадках UE автентифікує домашню мережу, через що за допомогою маленьких стільників все ще можна створити підроблене з'єднання (фейкову базову станцію) [229].

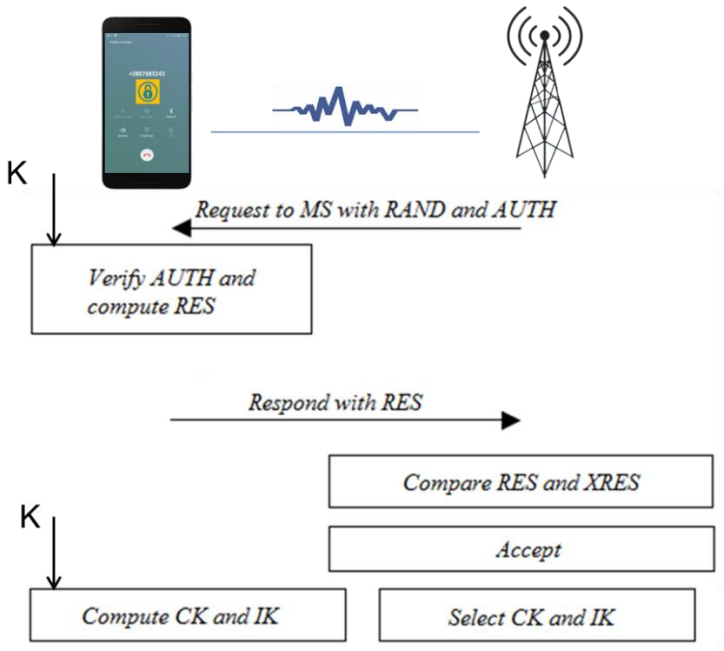


Рис. 5.38. Процедури автентифікації абонента в мережі 2G/3G перед початком дзвінка і вибір схеми шифрування

5.6.3 Забезпечення конфіденційності користувачів шляхом впровадження безпечного обміну ключами і наскрізного шифрування

Перекриття наведених в 5.6.1 атак досягається шляхом реалізації наступних запропонованих [289] під час дзвінка відмінностей (рис. 5.39):

- протоколу Діффі-Хелмана для безпечного обміну ключами;
- короткого автентифікаційного рядка (SAS) для протидії атаці "зловмисника посередині";
- використанні хешу попереднього дзвінка для протидії спуфінгу телефонних номерів;
- використанні сучасного симетричного шифрування мови алгоритмом AES(256) для протидії прослуховуванню і підвищенню конфіденційності при обміні [60].

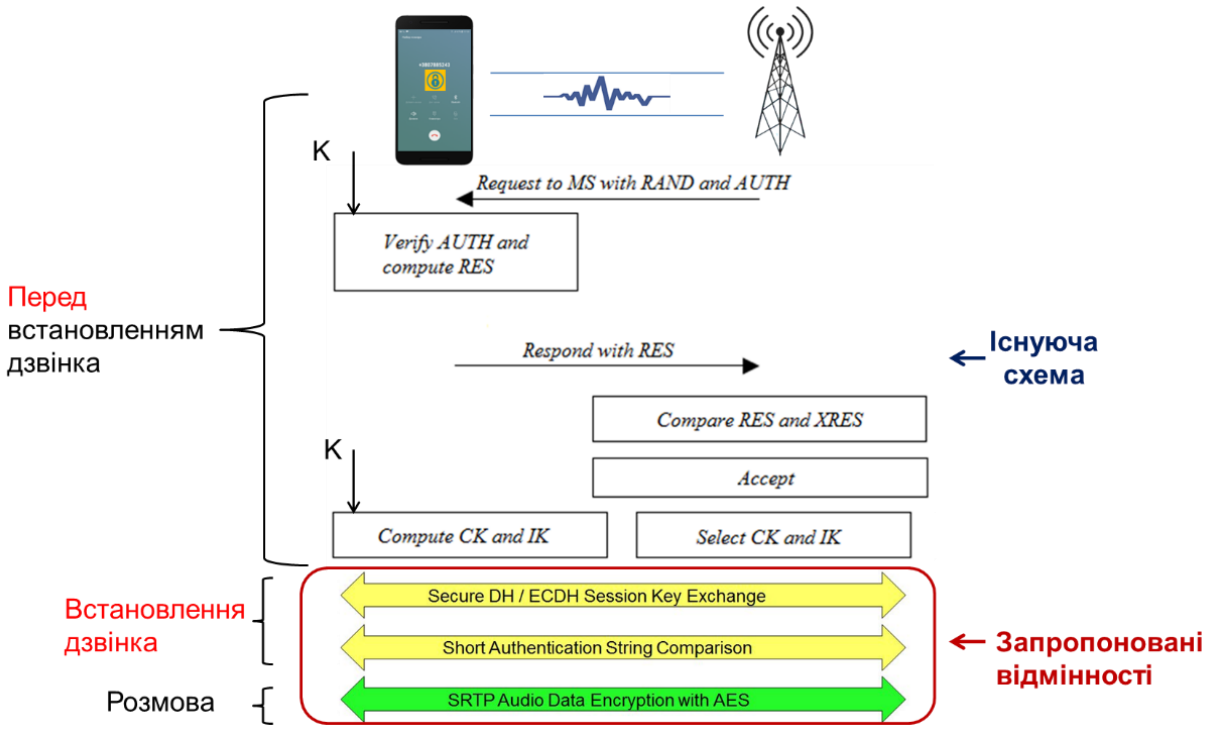


Рис. 5.39. Вдосконалена процедура забезпечення конфіденційності абонента [289]

Розглянемо протоколу обміну ключами Діффі-Хелмана (DH) (рис. 5.40).

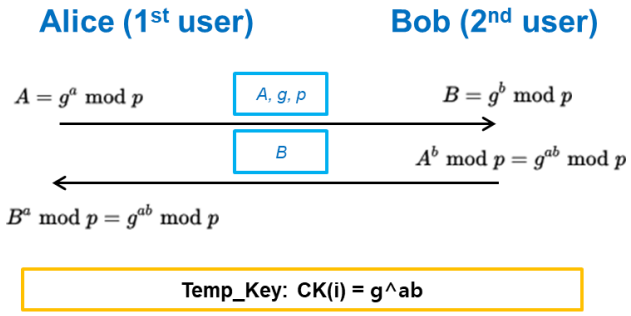


Рис. 5.40. Протокол обміну ключами DH

Згідно рис. 5.40:

Аліса вибирає a, відправляє

$$A = g^a, \tag{5.25}$$

Боб вибирає b, відправляє

$$B = g^b, \tag{5.26}$$

Обидві сторони обчислюють g^{ab} і формують код перевірки справжності повідомлення (HMAC) на основі цього значення, разом з багатьма іншими параметрами, щоб отримати тимчасовий ключ сеансу CK(i). Далі сторони обчислюють 32-бітове значення короткого автентифікаційного рядка (SAS) як функцію CK(i) і порівнюють їх.

Обчислення нового сеансового ключа *Total_key* виконується як значення g^{ab} і хеш-функції хешу попереднього виклику (зі старої сесії). Також можуть бути використані підписані сертифікати або перевірений SAS.

Для реалізації наведеного вище протоколу була запропонована модифікація повідомлень "*SETUP*" і "*CONNECT*" в традиційній послідовності повідомлень (call flow) під час встановлення дзвінка. Модифікована послідовність call flow наведена на рис. 5.41.

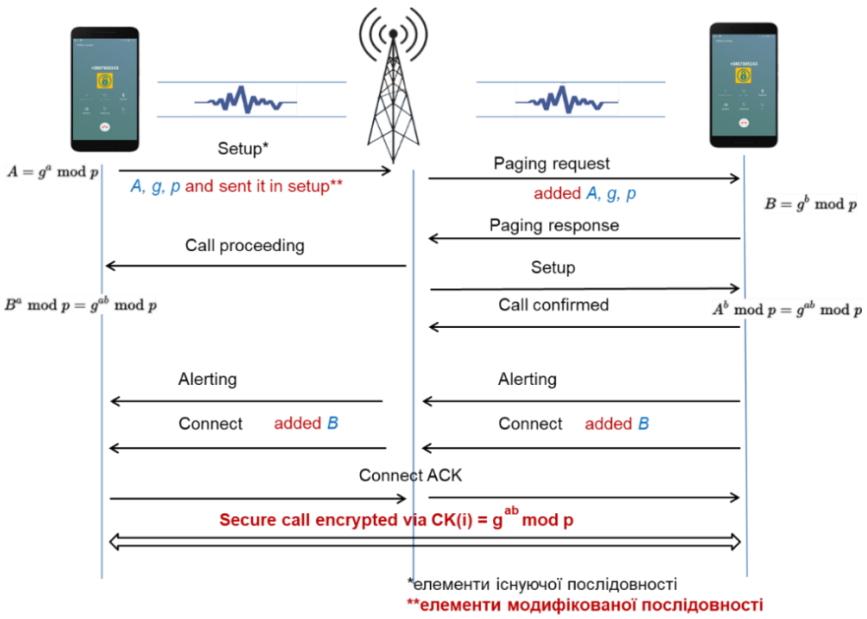


Рис. 5.41. Імплементація протоколу обміну ключами Діффі-Хелмана в протокол обміну повідомленнями

Сам по собі обмін ключами Діффі-Хеллмана не забезпечує захист від атаки "зловмисника посередині". Щоб переконатися, що зловмисник дійсно не присутній в першій сесії (коли немає спільних секретів), використовується метод короткого автентифікаційного рядка (SAS) (рис. 5.42).

До переваг короткого автентифікаційного рядка відноситься відсутність необхідності «довіреної третьої сторони». Найбільш ефективними випадками, коли застосування короткого автентифікаційного рядка необхідно, є:

- сертифікати користувачів відсутні, відізвані або у них вийшов термін придатності;
- відсутній хеш попереднього дзвінка;
- використовується непідписаний протокол Діффі-Хелмана.

Послідовність дій під час розрахунку і використання SAS, наведена на рис. 5.42. Запропоновані відмінності позначені червоним кольором.

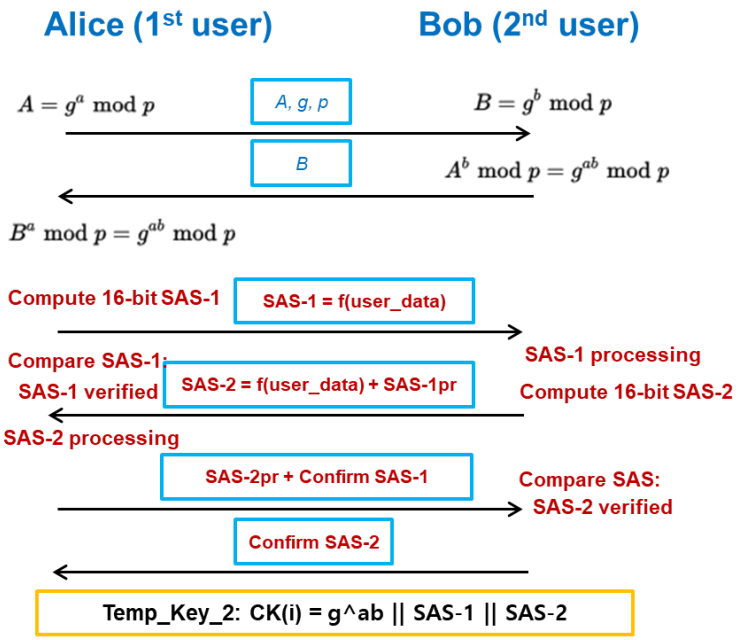


Рис. 5.42. Послідовність дій під час розрахунку і використання SAS

Також короткий автентифікаційний рядок SAS дозволяє передати повідомлення взаємної автентифікації, описані в розділі 5.5.3.

Ефективність протидії MitM-атакам досягається впровадженням другого рівня автентифікації, заснованому на певній формі безперервності ключа. Для цього зберігаємо в TrustZone деяку хешовану ключову інформацію для використання в наступному виклику, яка буде змішана з загальним секретом DH наступного виклику, що надає йому властивості безперервності ключа, аналогічні протоколу SSH (рис. 5.43).

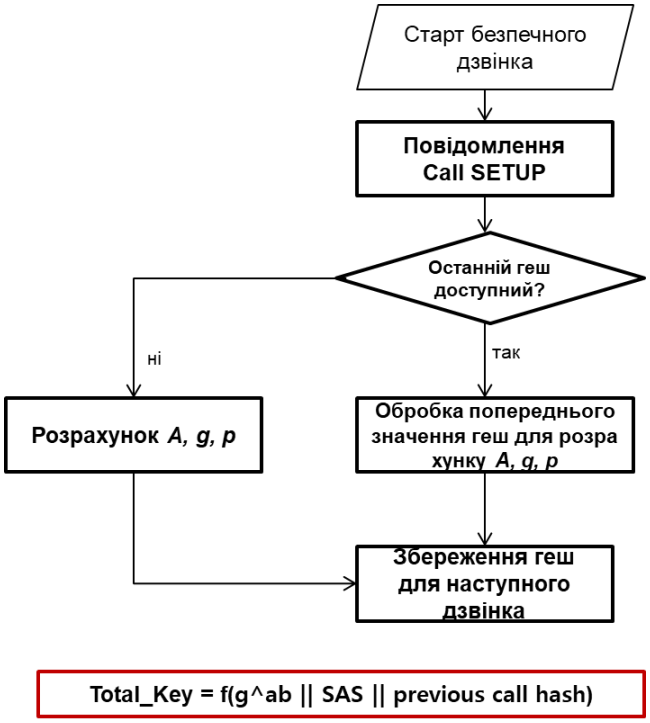


Рис. 5.43. Алгоритм обчислення ключових даних

Таким чином сутність запропонованого методу [289] може бути описана у вигляді наступної послідовності кроків:

- обчислення тимчасового ключа для першого користувача з ключового матеріалу першого користувача та випадкових криптографічних даних через TrustZone для безпечного мобільного дзвінка;

- надсилання ключового матеріалу другому користувачу;

- генерування сеансового ключа з тимчасових ключів першого користувача та другого користувача для шифрування мобільного голосового дзвінка між першим користувачем та другим користувачем;

- використання короткого автентифікаційного рядка (SAS) для захисту від атак типу "зловмисник посередині" (MitM);

- зберігання в пам'яті хеш-значення для минулих захищених викликів;

- доповнення матеріалу криптографічного ключа під час другого сеансу зв'язку між першим користувачем і другим користувачем матеріалом криптографічного ключа з першого сеансу зв'язку.

Впровадження описаного методу реалізує на вищому рівні послуги «конфіденційність при обміні» і «цілісність при обміні» [60], що забезпечує підвищення загального рівня конфіденційності.

5.7 Методи управління приватними даними користувача

5.7.1 Постановка задачі управління приватними даними користувача

Останнім часом мобільні пристрої міцно увійшли в повсякдення і дозволяють вирішувати найрізноманітніші задачі, такі як електронні платежі, віддалене управління об’єктами, розподілені обчислення. Більшість цих задач базується на використанні збережених в телефоні приватних даних користувача.

В даній роботі запропоновано 2 методи [256, 257, 283], що дозволяють надавати користувачу додаткові можливості без зниження рівня захищеності.

Патент [257] пропонує використання біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об’єктами.

Патенти [256, 283] пропонують методи зберігання приватних даних користувача в захищеному ієрархічному вигляді, що дозволяють надавати доступ до них різного рівня у надзвичайних випадках для збереження життя користувача.

Опишемо обидва рішення більш детально.

5.7.2 Захищений метод віддаленого управління об’єктами

5.7.2.1 Аналіз проблеми дистанційного управління та відмінності від існуючих рішень

За останній час використання мобільних пристроїв значно змінило своє призначення і зараз потрібним користувачам є застосування, коли за допомогою поєднання алгоритмів розпізнавання зображень та збережених в мобільному пристрої біометричних даних можна керувати віддаленими пристроями. Прикладами таких застосувань є відкривання вхідних дверей будинку або машини, керування пристроями розумного будинку та інше (рис. 5.44). Необхідна вимога – підключення до мережі 5G або WiFi обох пристроїв та можливість гарантованої верифікації користувача на мобільному пристрої.

З іншого боку, немає рішень для поєднання розпізнавання зображень та доступу до особистої інформації користувача, що зберігається в електронному пристрої [257]. Загальним методом захисту особистої інформації від розкриття є використання механізмів автентифікації, наприклад біометрична автентифікація. Запропоноване рішення поєднує розпізнавання зображень та автентифікацію користувача, щоб надати доступ

до уповноваженої людини до своїх особистих даних, що зберігаються в електронному пристрої.

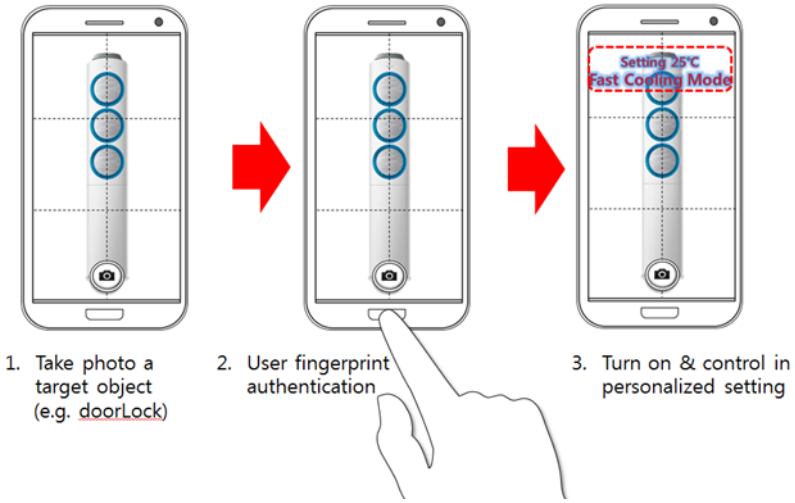


Рис. 5.44. Процедура розпізнавання об’єктів та надання доступу [257]

Одним з ключових компонентів запропонованого рішення [257] є система оптичного розпізнавання. Задача може бути сформульована так: проаналізувати растрове зображення та оцінити, чи присутні на ньому відомі об'єкти. Це задача розпізнавання об'єктів з навчанням під наглядом. Існує багато підходів для виконання розпізнавання об'єктів.

Процедура розпізнавання складається з двох фаз: фази навчання (класифікатор навчається на навчальному наборі даних) і фази розпізнавання (класифікатор розпізнає об'єкти).

На етапі навчання користувач асоціює зразки зображень об'єктів, які потрібно розпізнати, з конфіденційною інформацією. Наприклад, він/вона фотографує форму входу в обліковий запис Google і навчає класифікатор на цьому зображенні, позначаючи його конфіденційною інформацією. Це можна зробити опосередковано: об'єкт асоціюється з міткою, а мітка асоціюється з конфіденційною інформацією. У цьому випадку база даних ключ-значення

може бути зашифрована з метою безпеки. Для навчання класифікатора можна використовувати декілька зображень об'єкта.

На етапі розпізнавання блок розпізнавання об'єктів аналізує вхідне зображення (зняте камерою або зчитане з пам'яті електронного пристрою) і приймає рішення, чи присутній на зображенні відомий об'єкт.

З міркувань безпеки обидві фази повинні виконуватися на електронному пристрої. Саме тому обчислювальні можливості обмежені.

Існує ряд алгоритмів, які можуть бути використані в даному винаході для розпізнавання, наприклад, розпізнавання Віоли-Джонс, архітектура згорткової нейронної мережі. Огляд існуючих методів наведено в [232].

5.7.2.2 Існуючі рішення по розпізнаванню об’єктів. Алгоритм Віоли-Джонс

Великі компанії, такі як Google та Microsoft, використовують розпізнавання об'єктів для різних цілей, однак вони не використовують цю технологію для чутливого управління інформацією (рис. 5.45).

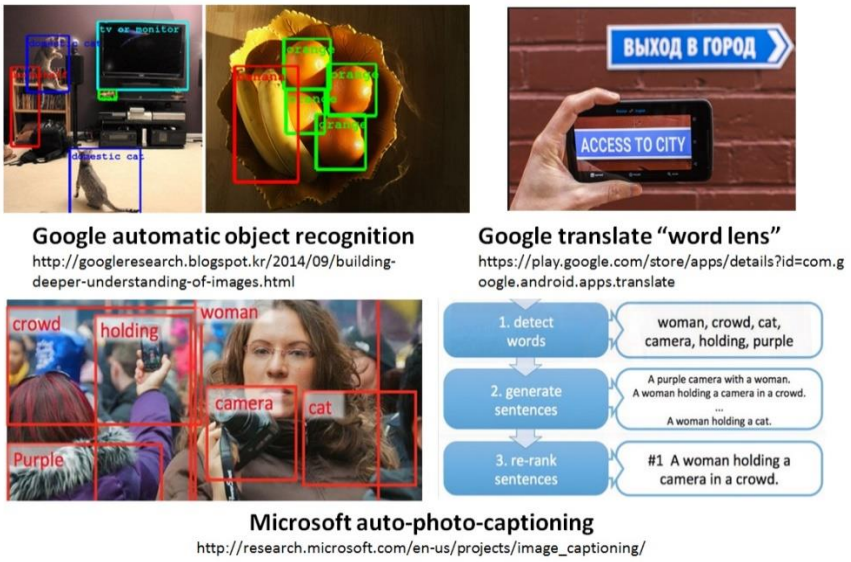


Рис. 5.45. Досягнення Google та Microsoft в розпізнаванні об’єктів [257]

Одним з перших обчислювально ефективних та швидких алгоритмів розпізнавання об'єктів є алгоритм Віоли-Джонс (Viola-Jones) для виявлення об'єктів [233]. Цей алгоритм має чотири етапи: вибір ознак (на основі вейвлетів Хаара), створення інтегрального зображення, алгоритм навчання (наприклад, Adaboost або RF, досліджені і описані в розділі 3), каскадні класифікатори.

На попередньому етапі зображення обробляється додатковою фільтрацією / нормалізацією тощо, а потім перетворюється у формат відтінків сірого.

На першому етапі вибір ознак зображення трактується як суперпозиція вейвлетів Хаара (Haar). Ці двовимірні вейвлети показані на рис. 5.46. Ці ознаки спочатку використовувались для проблеми виявлення обличчя, але також працюють з іншими типами об'єктів і можуть використовуватися у якості каскадних класифікаторів.

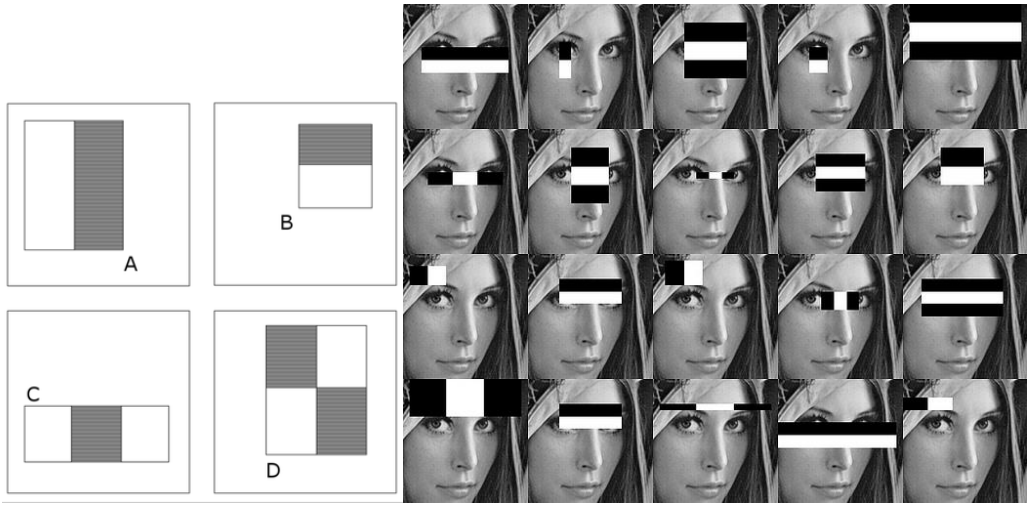


Рис. 5.46. Каскадні класифікатори Хаара та типи ознак алгоритму Віоли-Джонс. Зображення взяте з [235]

На наступному етапі застосовується один з алгоритмів навчання моделі. Приклад реалізації алгоритму навчання наведений на рис. 5.47 [235].

Вхід: Набір із N позитивних і негативних тренувальних зображень із їхніми мітками $(\mathbf{x}^i, y^i)$. Якщо зображення i є обличчям, $y^i = 1$, якщо ні, $y^i = -1$.

1. Ініціалізація: призначити вагу $w_1^i = \frac{1}{N}$ кожному зображенню i.
2. Для кожної ознаки f_j з $j = 1, \ldots, M$
    1. Перенормувати ваги так, щоб вони давали в сумі одиницю.
    2. Застосувати ознаку до кожного зображення в тренувальному наборі, а потім знайти оптимальні поріг та полярність θ_j, s_j, які мінімізують зважену похибку класифікування. Тобто, $\theta_j, s_j = \arg\min_{\theta,s} \sum_{i=1}^{N} w_j^i \varepsilon_j^i$, де $\varepsilon_j^i = \begin{cases} 0 & \text{if } y^i = h_j(\mathbf{x}^i, \theta_j, s_j) \\ 1 & \text{інакше} \end{cases}$
    3. Призначити вагу α_j пороговій функції h_j, що обернено пропорційно частоті помилок. Таким чином на найкращі класифікатори зважають більше.
    4. Ваги для наступної ітерації, тобто w_{j+1}^i, зменшують для зображень i, які було класифіковано правильно.
3. Встановити остаточний класифікатор в $h(\mathbf{x}) = \operatorname{sgn}\left(\sum_{j=1}^{M} \alpha_j h_j(\mathbf{x})\right)$

Рис. 5.47. Алгоритм навчання Віоли-Джонс [235]

У каскадному методі кожен етап складається з сильного класифікатора. Тобто всі ознаки згруповані в кілька етапів, де кожен етап має певну кількість ознак. Завданням кожного етапу є визначення того, чи дане під-вікно точно не є обличчям, чи може бути обличчям. Якщо вікно не є обличчям, то воно негайно відкидається як таке, що не є обличчям, якщо воно не пройшло жодного з етапів. Каскадування здійснюється за допомогою псевдо-алгоритму наведеного на рис. 5.48:

```
  • Користувач вибирає значення для f, максимально прийнятну
    кількість помилок на шар і d, мінімальну прийнятну швидкість
    виявлення на шар
  • Користувач вибирає цільову загальну помилкову позитивну
    швидкість Ftarget
  • P = набір позитивних прикладів
  • N = набір негативних прикладів
  • F(0) = 1.0; D(0) = 1.0; i = 0

while F(i) > Ftarget

     i++

     n(i) = 0; F(i)= F(i-1)
```

```
     while F(I) > f x F(i-1)

      - n(i) ++

      - використати P та N для тренування класифікатора з n(I)
ознаками використовуючи AdaBoost

      - оцінити ефективність поточного класифікатора, використовуючи
метрики F(i) та D(i)

      - зменшити поріг для i-го класифікатора поки поточний
класифікатор не досягне швидкості виявлення щонайменше d x D(i-1)
(аналогічно для F(i))

      - N = ∅

      - If F(i) > Ftarget потім оцінити поточний каскадний детектор
на наборі зображень без обличь і оцінити помилкові детектування.
```

Рис. 5.48. Псевдо-алгоритм каскадування [235]

Цей алгоритм швидкий та ефективний, тому він буде використаний в запропонованому рішенні.

Після обробки зображень важливим етапом є детектування спеціальних точок. Для їх знаходження може бути використаний наприклад FAST Corner Detector [236].

На етапі пошуку дескриптори з фіксованих фреймів зберігаються в базі даних. З ними зіставляються дескриптори з фрейму запиту. Для зіставлення використовується пошук найближчого сусіда [237] (який був детально описаний в розділі 1 і досліджений в розділі 3). У цьому випадку ми можемо використовувати алгоритм *k*-середніх для визначення найкращого кадру та *kd*-дерево [238] для прямого зіставлення базового кадру та кадру запиту (рис. 5.49).

Нарешті, при розрахунку геометричної моделі:

- після співставлення ми маємо деяку кількість збігів. Ми можемо обчислити геометричну модель, щоб перевірити, чи дійсно ці кадри мають один і той самий об'єкт [239], (рис 5.49).

- за кількістю збігів та якістю геометричної моделі можна вирішити, чи містить кадр запиту той самий об'єкт, що і базовий кадр.

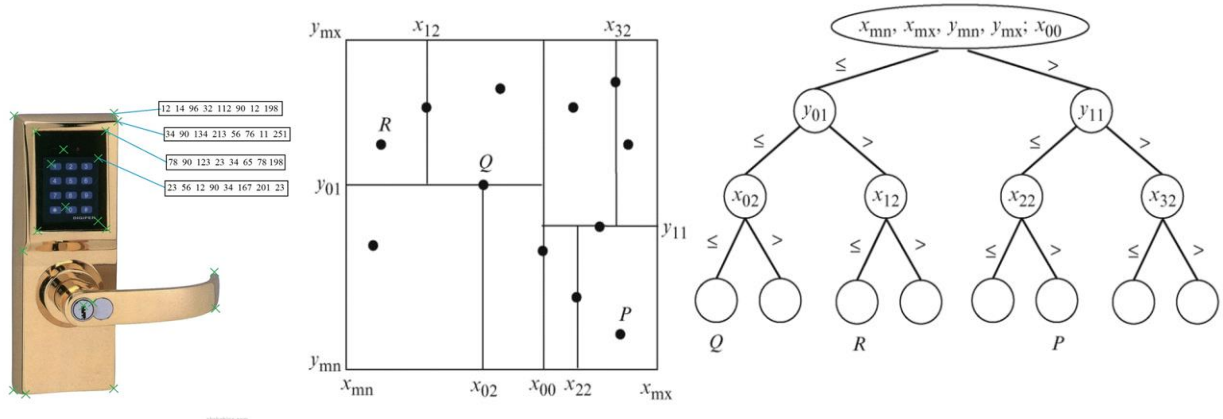


Рис. 5.49. Виявлення спеціальних точок та розрахунок геометричної моделі [257]

Проаналізуємо існуючі рішення і їх особливості.

В [240] запропонований наступний метод. Користувач генерує шаблон у матриці (або двовимірній сітці) і вводить ім'я користувача та пов'язаний з ним пароль. Ім'я користувача, пароль і шаблон зберігаються локально на комп'ютерному пристрої або передаються на віддалений комп'ютерний сервер для подальшої автентифікації. Після автентифікації на екрані з'являється матриця введення. Користувач вводить пароль у матрицю у вигляді шаблону, а також вводить ім'я користувача. Комп'ютер отримує раніше збережений шаблон і пароль з ім'ям користувача. Недоліками такого підходу є те, що не використовується жодних процедур розпізнавання

зображень, автентифікації за відбитками пальців, а також існує необхідність запам'ятовувати пароль.

В [241] запропонована портативна система безпеки, яка містить модуль захоплення зображень для захоплення одного або більше зображень та модуль аналізу зображень, що знаходиться в робочому зв'язку з модулем захоплення зображень, причому модуль аналізу зображень конфігурований для (i) розпізнавання, з одного або більше захоплених зображень, однієї або більше подій, пов'язаних з виявленням рухомих об'єктів, (ii) вибірково ідентифікувати скінченну кількість просторових взаємозв'язків рухомих об'єктів, та (iii) аналізувати одне або більше зображень у портативному охоронному пристрої для класифікації скінченної кількості просторових взаємозв'язків рухомих об'єктів, що відповідають попередньо визначеним даним про рухомі об'єкти, які зберігаються на блоці зберігання даних, розташованому в портативному охоронному пристрої. До її недоліків відноситься відсутність автентифікації і також необхідність запам'ятовувати пароль.

З комерційних рішень, доступних на ринку, варто відмітити рішення від Mozilla [242], як приклад розширення для запам'ятовування облікових даних під час веб-серфінгу. Після введення облікових даних на сторінці входу в систему інформація про обліковий запис зберігається. Викликавши контекстне меню, можна відобразити пароль або скопіювати його в буфер обміну. Але ця система також має ряд недоліків, таких як:

а) обмежується лише браузером на одному комп'ютері (неможливо нагадати інформацію про обліковий запис на іншому комп'ютері).

б) інформація про обліковий запис зберігається локально на комп'ютері і може бути скомпрометована шкідливим програмним забезпеченням або іншим користувачем.

5.7.2.3 Впровадження запропонованого методу управління приватними даними

В патенті [257] описано винахід, який являє собою спосіб і пристрій для збору, зберігання і представлення конфіденційної інформації користувача, пов'язаної з візуально розпізнаними об'єктами (наприклад, сторінками інтернет-сервісів, дверними замками, системами кондиціонування повітря і іншими пристроями розумного будинку, які можуть працювати в мережі 5G. Основний спосіб включає етапи ідентифікації користувача на пристрої, розпізнавання певного об'єкта з використанням алгоритмів розпізнавання об'єктів, зберігання розпізнаних об'єктів та секретної інформації, порівняння збережених розпізнаних об'єктів з вхідними, пошук інформації, пов'язаної з розпізнаним об'єктом, та виконання дії, пов'язаної з об'єктом (наприклад, відображення пароля, PIN-коду, реквізитів облікового запису, налаштувань керування, вбудовування інформації в додатки для охорони здоров'я тощо). Винахід може бути використаний у будь-яких електронних пристроях, що мають камеру та дисплей.

Винахід, що пропонується, вирішує:

- проблему необхідності запам'ятовування користувачем інформації про декілька облікових записів;

- проблему потенційного порушення конфіденційності (у випадку, коли конфіденційна інформація зберігається на хмарі);

- проблему управління профілями користувачів, прив'язаними до певних електронних пристроїв (декілька користувачів можуть мати декілька профілів/налаштувань);

Запропоноване рішення дає нові можливості застосування розпізнавання зображень, тобто доступ до певних даних, пов'язаних з розпізнаними

об'єктами. З іншого боку, користувачеві не потрібно запам'ятовувати специфічну інформацію для пошуку.

Основні переваги запропонованого рішення полягають у наступному:

а) не потрібно запам'ятовувати багато секретної інформації (наприклад, ідентифікатор, номер рахунку, пароль і т.п.)

б) відсутність сервера, секретна інформація користувача зберігається лише на його пристрої.

с) можна надавати персоналізоване обслуговування.

Структурна схема системи показана на рис. 5.50. Зображення або відео знімається за допомогою камери. Крім того, зображення/відео можуть зберігатися на блоці репозиторію, наприклад, з додатку галереї на смартфоні або бути частиною програми, запущеної на електронному пристрої, наприклад, програми електронної пошти із зображенням як вкладенням. Блок оптичного розпізнавання виконує розпізнавання об'єктів.

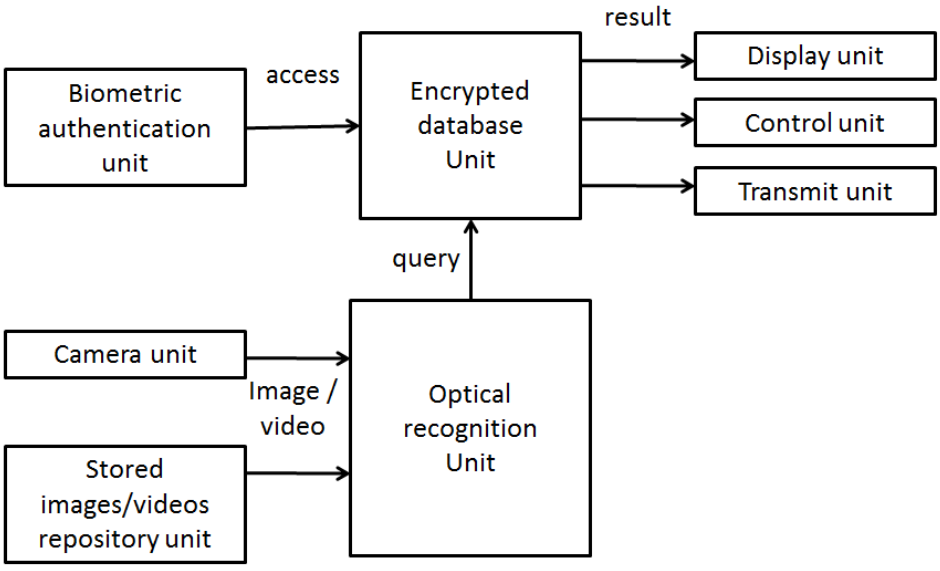


Рис. 5.50. Дизайн запропонованої системи [257]

Користувач виконує автентифікацію на блоці біометричної автентифікації. Отриманий хеш розшифровує база даних. Виконується запит на пошук об'єктів у базі даних. Результати пошукового запиту представляються користувачеві. У деяких варіантах реалізації це просто дія відображення: відображення результату пошуку користувачеві. В інших варіантах реалізації дії можуть виконуватися для управління або обміну інформацією з додатками, що працюють на електронному пристрої. У третіх варіантах результат пошукового запиту виводиться за допомогою передавального пристрою. Пристрій передачі може бути будь-яким з WiFi, NFC, RFID, BLE, Bluetooth, ZigBee тощо.

Суть розкритого винаходу полягає у способі безпечного управління конфіденційною інформацією користувача. Основна формула винаходу:

1. Спосіб управління конфіденційними даними користувача, який включає:

a) авторизацію користувача на електронному пристрої,

b) розпізнавання одного або більше об'єктів у полі зору камери електронного пристрою або на зображенні чи відео, що зберігається на електронному пристрої,

c) отримання чутливої інформації, пов'язаної з одним або кількома об'єктами, при цьому чутлива інформація отримується з бази даних, що зберігається на електронному пристрої, або чутлива інформація розпізнається із зображення або відеозапису одного або декількох об'єктів, та

d) виконання будь-якої комбінації дій, пов'язаних з типом розпізнаних об'єктів, вибраних з групи, що складається з aa) відображення чутливої інформації, bb) відображення пультів дистанційного керування, cc) передавання чутливої інформації за допомогою електромагнітних або

акустичних хвиль; та dd) передавання чутливої інформації до певних програм, що працюють на електронному пристрої.

Діаграми роботи запропонованого рішення наведені на рис. 5.51 та рис. 5.52 і описують процеси зберігання та відтворення конфіденційної інформації користувача.

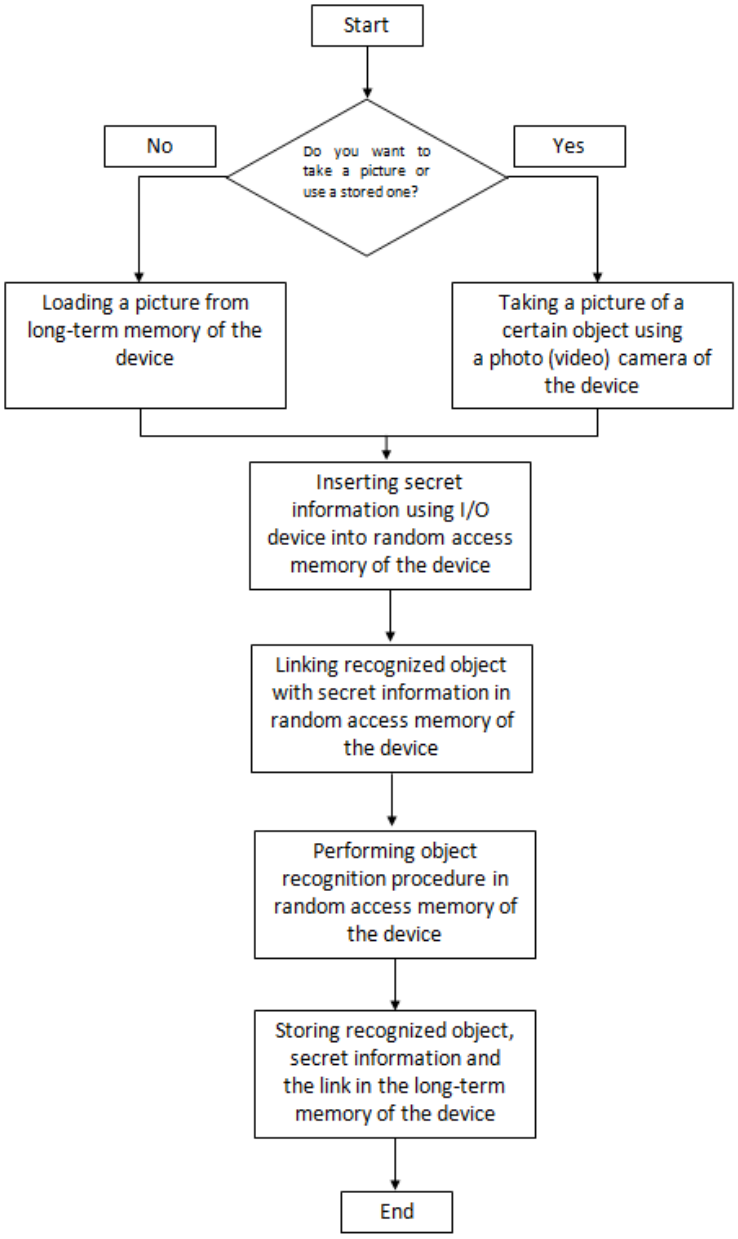


Рис. 5.51 Етап 1. Збір сутностей, секретної інформації та збереження їх на пристрої [257]

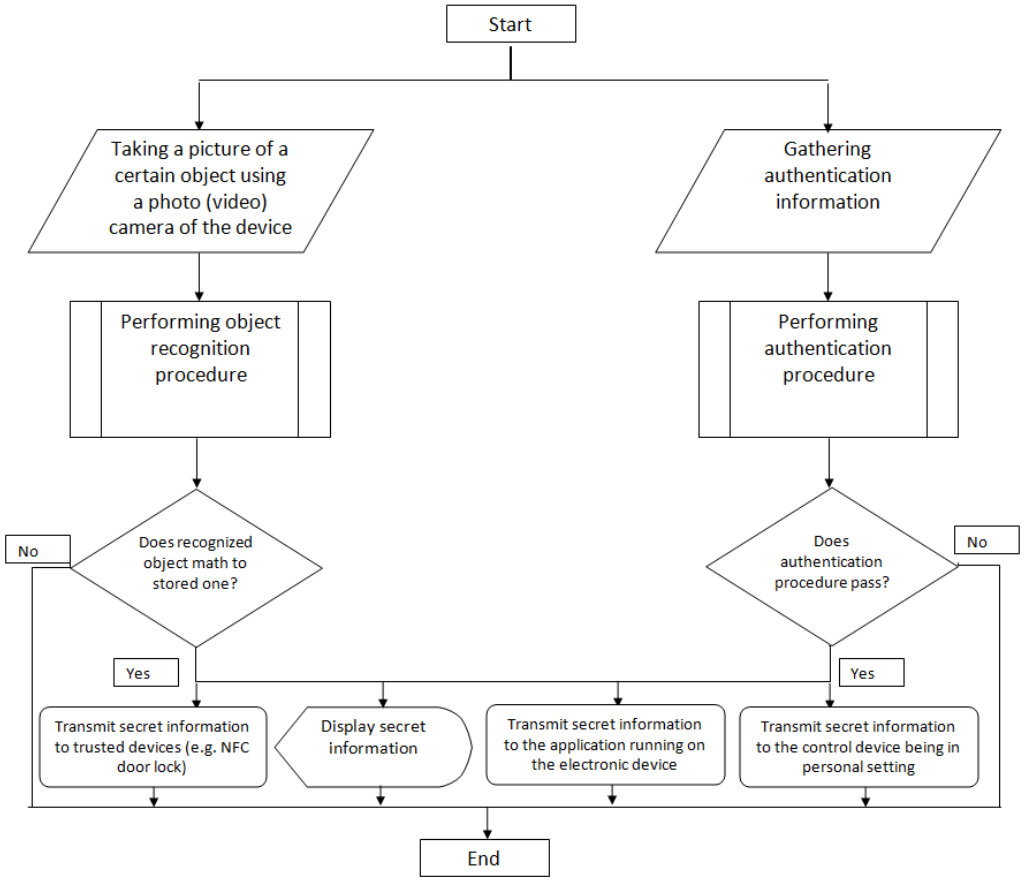


Рис. 5.52. Етап 2. Обробка даних та представлення секретної інформації [257]

5.7.3 Захищений метод зберігання приватних даних користувача

5.7.3.1 Огляд проблеми зберігання та надання приватних даних користувача та відмінності від існуючих рішень

Як було описано вище, мобільні пристрої користувача зберігають багато приватної інформації, до якої окрім біометричних даних, паролів, адрес/контактів також відноситься медична інформація. Останнім часом, особливо під час глобальної пандемії, а тим більш під час війни, гостро стає проблема швидкого доступу до певних медичних даних, які можуть в екстрених випадках зберегти життя користувачу (наприклад, група крові). Це

може бути необхідно, наприклад коли користувач втратив свідомість внаслідок травмування або приступу хвороби (рис. 5.53). При цьому, доступ до повних даних мають отримувати лише лікарі в спеціалізованому закладі, який буде акредитований для надання спеціалізованої допомоги.

На цей час в мобільних пристроях є лише підтримка екстреного номеру, на який можна зробити дзвінок у надзвичайному випадку, без розблокування телефону.

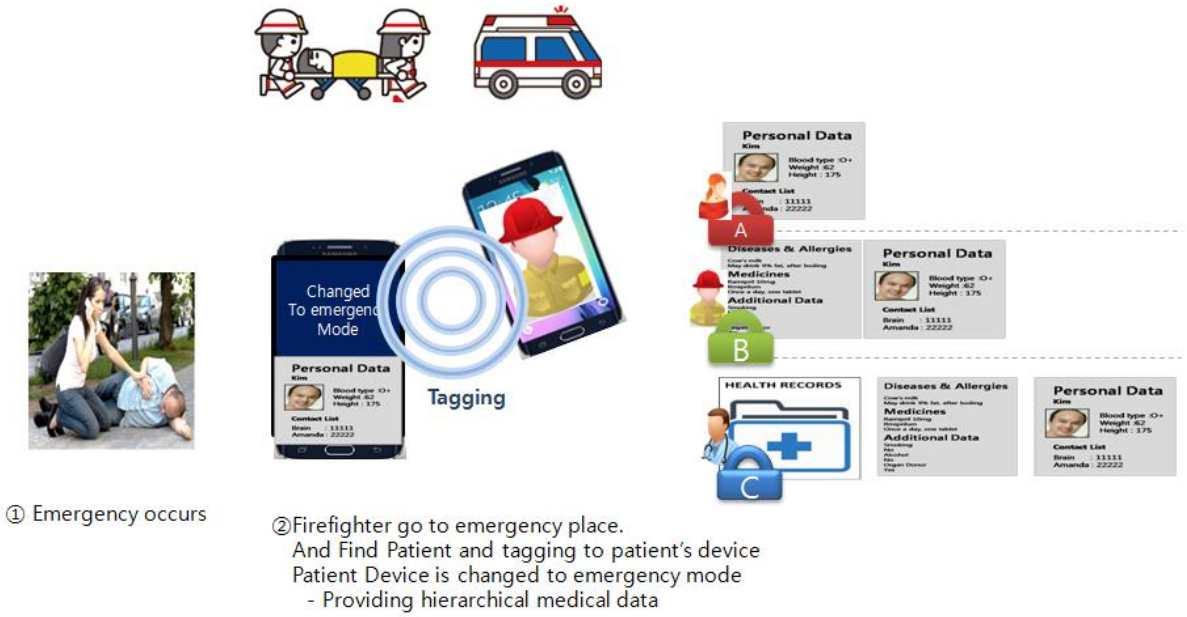


Рис. 5.53. Блок-схема проблемної ситуації

В патенті [256] пропонується метод ієрархічної організації приватних даних з різними рівнями доступу, який дозволяє вирішити описану вище проблему надання первинного доступу користувачу без зайвого розповсюдження особистих даних.

Для надання ієрархічних медичних даних шляхом переведення смартфона в екстрений режим є кілька проблем, які необхідно вирішити. По-перше, це проблема створення надійного сховища для персональних

медичних даних. По-друге, є проблема перевірки "екстреного випадку" та увімкнення "екстреного режиму". По-третє, проблема передачі інформації про місцезнаходження, рятувальника та пацієнта родині та медичному персоналу. По-четверте, проблема автентифікації особи рятувальника. По-п'яте, проблема реєстрації випадків доступу. Обговоримо ці проблеми більш детально.

Проблема створення надійного сховища для персональних медичних даних. Медичні персональні дані повинні оброблятися тільки в "Безпечному світі", оскільки шкідливе програмне забезпечення та системи вторгнення можуть отримати доступ до цих даних, коли вони обробляються і представлені у відкритому вигляді. Запропоноване в [256] рішення пропонує використовувати TrustZone і вирішує цю проблему. Інші рішення [266-269] пропонують лише зберігати медичні дані в зашифрованому вигляді і не описують, як вони обробляються.

Проблема перевірки "екстреного випадку" та ввімкнення "екстреного режиму". Проблема розпізнавання "невідкладного стану" не вирішена в жодному з відомих рішень. В існуючих рішеннях "аварійний випадок" не визначається автоматично, "аварійний режим" може бути ввімкнений вручну. У запропонованому сценарії [256] цей режим може бути ввімкнений через мережеве повідомлення або натільних пристроїв користувача. Особливістю запропонованого рішення є можливість увімкнення "екстреного режиму" шляхом включення додаткового медичного обладнання, такого як розкладачка швидкої допомоги або допоміжні ноші.

Проблема передачі інформації родині та медичному персоналу. Інформація про місцезнаходження користувача, рятувальника та пацієнта повинна надсилатися в зашифрованому вигляді лише довіреній особі. Наприклад, в деяких роботах [266, 267] інформація не надсилається, але

довірена особа може мати доступ до цих даних, знаючи секретний ключ. У деяких роботах пропонується використання 2-ключової системи шифрування [269], де один ключ використовується до мобільного терміналу, а другий – до терміналу уповноваженої особи, при цьому ключ дозволяє уповноваженій особі отримати доступ до медичних даних.

Проблеми автентифікації рятувальника та протоколювання випадків доступу. Проблеми автентифікації рятувальника та реєстрації випадків доступу не вирішені в жодному з відомих рішень. Проблема автентифікації власника смартфону вирішується біометричною автентифікацією користувача [266], але в екстрених випадках це не зручно.

Підсумкове порівняння запропонованого рішення з аналогами наведено в табл. 5.6.

Таблиця 5.6. Порівняння зі схожими рішеннями

Номер патенту	**Відмінність**
US 20100179831 A1 [266]	Підтвердження дозволу на доступ до даних користувачів
US 8837718 B2 [277]	Підтвердження дозволу на доступ до даних користувачів
WO 2007031955 A2 [268]	1. Використовувати спеціальне обладнання (наприклад, смартфон) та сценарій для доступу до медичних даних користувача 2. Використовувати спеціальний режим "здоров'я" для дозволу доступу до медичних даних користувача 3. Пристрій надсилає різні ключі для різних людей в групі
US 8874067 B2 [269]	1. Довірена особа після отримання повідомлення може дозволити доступ до персональних медичних даних. 2. Ієрархічна структура медичних даних користувача.

5.7.3.2 Запропонована структура зберігання приватних та медичних даних

В даний час можуть існувати індивідуальні медичні бази даних, які в екстрених випадках можуть бути негайно передані довіреним особам, таким як медичний персонал (рятувальники), друзі, сім'я та державні установи. Але

індивідуальна медична база даних не є однорідною і складається з різної інформації з різним рівнем безпеки [256]. Наприклад, особиста інформація користувача, така як ім'я, адреса, група крові, не є дуже секретною, але вона не повинна бути доступною для всіх. Інші типи інформації – хронічні захворювання та алергії – можуть бути доступними лише для спеціальних осіб, коли це дійсно необхідно. Третій тип медичної інформації, такий як історія хвороби, може бути наданий лише безпосередньо довіреному медичному центру. Відповідно до цих різних типів інформації можуть застосовуватися різні типи безпеки та різні ключі шифрування/розшифрування. Пристрої користувача можуть визначати, кому і яку інформацію надавати.

Структура для зберігання медичних даних.

Запропоноване рішення реалізує ієрархічну систему зберігання медичних даних. Особливості такого зберігання полягають у наступному:

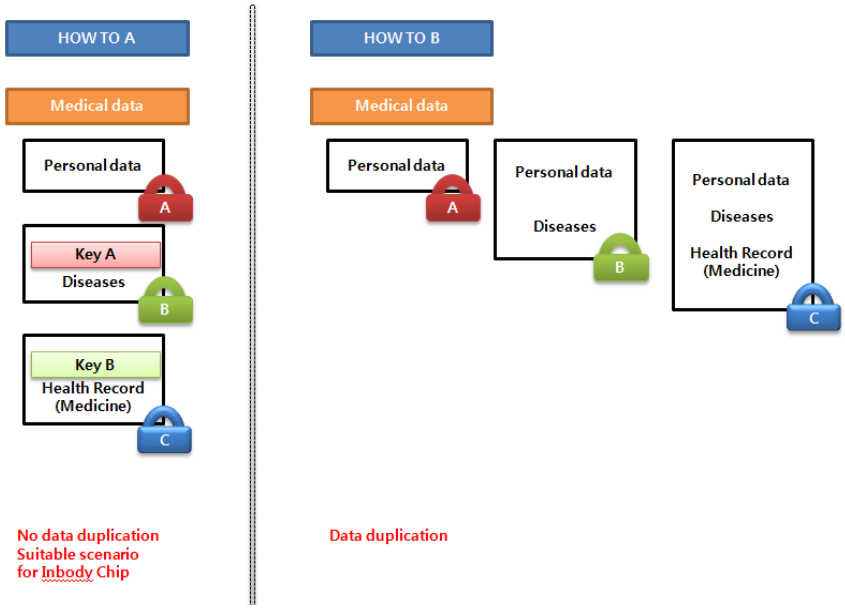


Рис. 5.54. Запропонований метод зберігання та відображення ієрархічних медичних даних [256]

Персональні дані класифікуються відповідно до одного з трьох рівнів даних і не дублюються. Кожен з рівнів даних шифрується власним ключем, відповідно до рівня доступу. На кожному рівні даних зберігається ключ нижчого рівня (рис. 5.54).

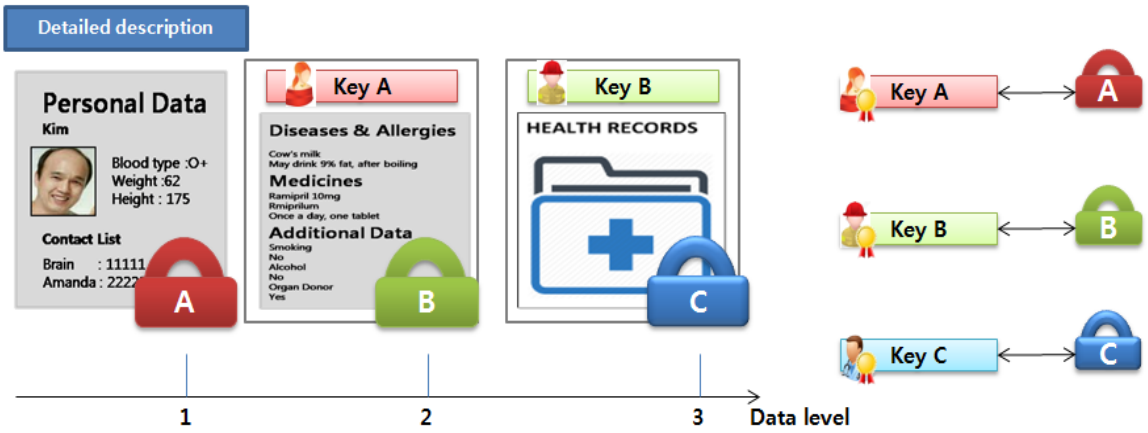


Рис. 5.55. Запропонований метод обміну приватними даними [256]

У цьому випадку "Ключ А", який використовується для шифрування Персональних даних (Рівень даних 1), зберігається разом з даними Хронічних захворювань та алергій (Рівень даних 2) і шифрується "Ключем В" (рис. 5.55). Дані про стан здоров'я (Рівень даних 3) зберігаються з "Ключем В" і шифруються "Ключем С". Якщо особа отримує "Ключ А", вона може прочитати лише рівень даних 1. Якщо особа отримує "Ключ В", вона може прочитати дані рівня 2 і отримати "Ключ А" і відповідно дані рівня 1.

5.7.3.3 Принцип роботи запропонованого методу

У разі надзвичайних ситуацій, таких як автомобільна аварія, напад хвороби, коли власник смартфона знаходиться без свідомості або його можливості обмежені, користувач потребує негайної допомоги. Для надання

першої допомоги необхідна інформація про пацієнта. Також необхідно повідомити родину (друзів) пацієнта.

Коли стався нещасний випадок, хтось, хто став свідком події (власник смартфона впав), повідомляє про це в службу 911. Тоді рятувальник виїжджає на місце події. Рятувальник кладе пацієнта на ноші, щоб доставити його до карети швидкої допомоги. У смартфоні пацієнта можна натиснути "екстрену кнопку". Інший випадок – натиснути "екстрений виклик", потім вибрати "введення користувача" і, нарешті, ввести певний код для активації NFC-модуля для отримання інформації від рятувальника. Після цього смартфон генерує три ієрархічні ключі ("Ключ A", "Ключ B", "Ключ C").

Смартфон пацієнта отримує запит від смартфона рятувальників. Він містить ідентифікатор рятувальника та Public_Key. Смартфон пацієнта автоматично зв'язується з сервером третьої сторони (медичним центром) і пересилає ідентифікатор рятувальника. Якщо ідентифікатор рятувальника та публічний ключ підтверджено, рятувальник отримує доступ до "Ключа B" та двох типів даних (Data Level 1, Data Level 2). Смартфон надсилає рятувальнику медичну карту (рівень даних 3), зашифровану "Ключем C", і відправляє "Ключ C" до довіреного медичного центру (рис. 5.56).

У випадку, коли мобільна мережа недоступна для надсилання "інформації про стан", зв'язок може бути встановлений за допомогою інших каналів (бездротова мережа, прямий вхід тощо) [286].

Коли смартфон пацієнта знаходиться поза зоною покриття, "рятувальник" змушує мобільну мережу передати спеціальний запит (наприклад, увімкнути NFC або Bluetooth для пристроїв, що знаходяться в зоні інтересу). Отримавши цей запит, смартфони, що знаходяться в цій зоні, можуть на короткий час почати вібрувати.

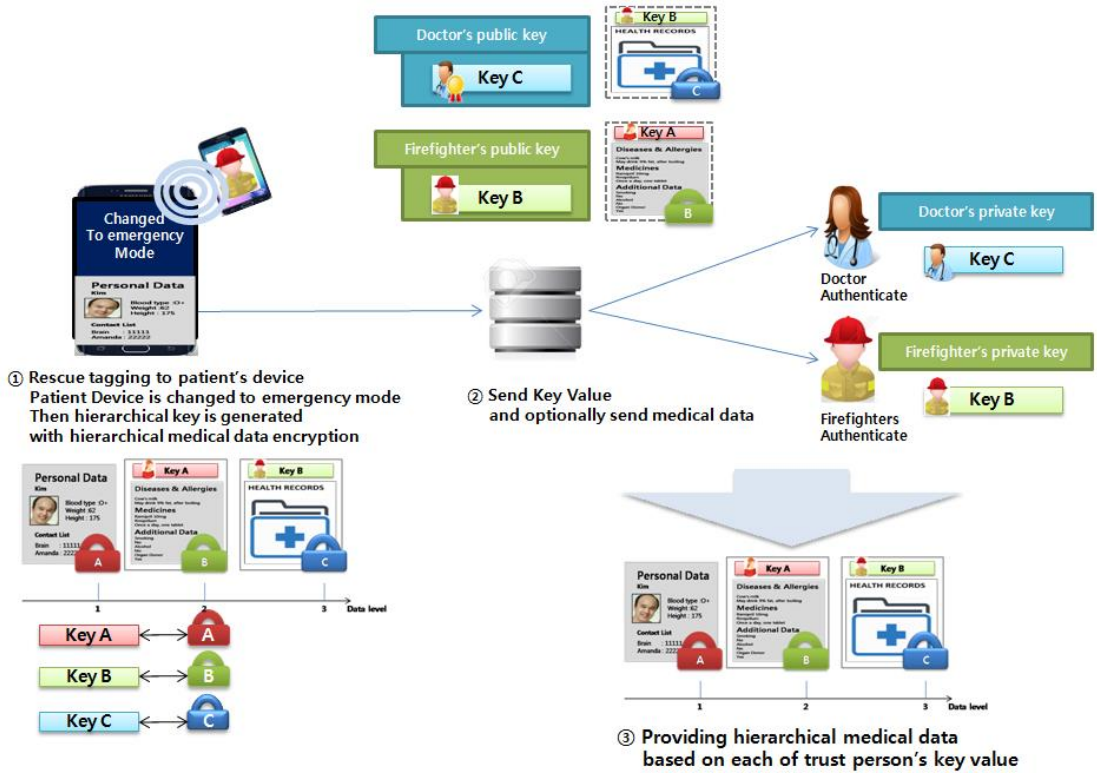


Рис. 5.56. Ілюстрація принципу роботи запропонованого рішення [256]

Ця вібрація потрібна для тих людей, яким не потрібне автоматичне ввімкнення бездротового з'єднання. Після виконання цих кроків ситуація подібна до першого випадку, коли смартфон пацієнта стає видимим.

Розширений сценарій застосування.

1. Інший випадок розглядається, коли власник використовує додаткове обладнання, наприклад, натільний пристрій (наприклад, розумний годинник, перстень, браслет тощо). Існує два можливих випадки, коли стан здоров'я швидко погіршується: по-перше, коли власник розумного пристрою знаходиться при свідомості і може застосовувати деякі жести, і по-друге, коли власник розумного пристрою падає (втрачає свідомість або перебуває в подібному стані).

а) У першому випадку власник пристрою може застосувати спеціальний жест (або натиснути "спеціальну кнопку") для переведення пристрою в

"аварійний режим". Цей жест може бути застосований і рятувальником, якщо власник пристрою знаходиться без свідомості або його можливості обмежені.

При виконанні спеціального жесту пристрій пацієнта надсилає підписане повідомлення на смартфон пацієнта (рис. 5.57). Після отримання підписаного повідомлення смартфон вмикає "екстрений режим", готує повідомлення "інформація про стан" та надсилає його рідним. Інформація про стан також може бути надіслана до центру порятунку.

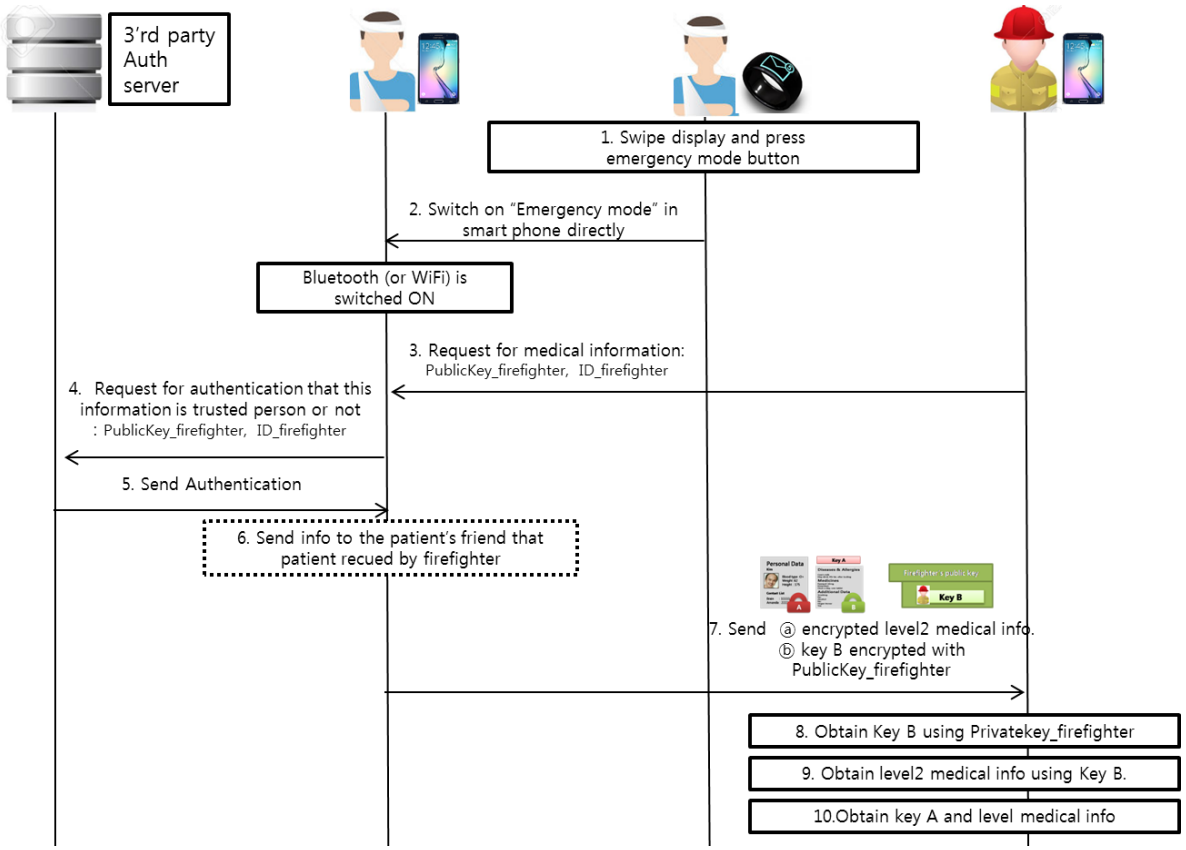


Рис. 5.57. Розширений сценарій: використання носимого пристрою або спеціального жесту [256]

б) У другому випадку смартфон перевіряє, чи змінився стан здоров'я пацієнта (наприклад, падіння супроводжується стрибкоподібними змінами медичних параметрів користувача, наприклад, стрибком артеріального

тиску). Тоді розумний пристрій автоматично перемикає свій режим в "екстрений режим" і надсилає підписане повідомлення на смартфон користувача. Після отримання підписаного повідомлення смартфон вмикає "екстрений режим", готує повідомлення "інформація про стан" та надсилає його рідним. Інформація про стан і дані про стан здоров'я також можуть бути надіслані в рятувальний центр. Якщо рятувальник виїжджає на місце події, розширений сценарій схожий на основний.

2. Розглянемо інший випадок, коли власник має вбудований в тіло чіп. Чіп містить ідентифікаційну інформацію. У цьому випадку, якщо власник пристрою знаходиться без свідомості або його можливості обмежені, використовується пристрій "рятувальник" (наприклад, карета швидкої допомоги, допоміжні ноші тощо), який виявляє чіп, отримує публічну інформацію (ідентифікатор пацієнта) та надсилає її на смартфон рятувальника.

5.7.3.4 Новизна та переваги запропонованого методу

До новизни запропонованого рішення [256] відносять наступне:

а) *Пропонується нове надійне сховище для персональних медичних даних* з використанням TrustZone. Персональні дані користувачів класифікуються в ієрархічній структурі, відповідно до одного з трьох рівнів даних, і не дублюються. Кожен рівень даних шифрується власним ключем, відповідно до рівнів доступу, де ключ, необхідний для розшифрування даних нижчого рівня, міститься в полі даних вищого рівня.

б) *Перевірка "екстреного режиму".* Для зміни режиму смартфону на "екстрений режим" можуть бути використані наступні методи: окремий додатковий пристрій, переносний пристрій у поєднанні зі смартфоном, явне

натискання "екстреної кнопки" на смартфоні та повідомлення з мобільної мережі.

в) *Використання додаткового екстреного обладнання для отримання доступу* до медичних даних користувачів. Використання обладнання швидкої допомоги (наприклад, карети швидкої допомоги, допоміжних нош тощо) для пошуку чіпу, вбудованого в тіло пацієнта, та ввімкнення режиму екстреної допомоги.

г) *Отримання інформації про рятувальника та автентифікація рятувальника*. Надання методу обміну даними між довіреною особою та смартфоном пацієнта для підвищення рівня безпеки. Смартфон пацієнта отримує запит від рятувальника з його інформацією та надсилає запит на автентифікацію на сервер третьої сторони ("медичний центр"). Після підтвердження доступ до медичних даних користувача буде надано.

д) *Забезпечення системи безпечного обміну даними*. Якщо медичний центр підтверджує ідентифікаційну інформацію рятувальника, смартфон користувача надсилає медичні дані на смартфон рятувальника. Тільки підтверджена особа може мати доступ до персональних медичних даних.

е) *Передача інформації про місцезнаходження, рятувальника та пацієнта родині* ("інформація про стан"). Після запуску екстреного режиму, смартфон пацієнта робить одночасно 2 фотографії з фронтальної та тильної камер і надсилає екстрене повідомлення ("інформація про стан") з цими 2 фотографіями (рятувальника, пацієнта) та інформацією про місцезнаходження довіреній особі (родині, другу). Таким чином повідомляється про надзвичайний випадок.

ж) *Забезпечення системи реєстрації випадків доступу до персональних та медичних даних*. Інформація про випадки доступу до медичних даних користувача зберігається в пам'яті смартфона. Інформація, що реєструється,

включає в себе ідентифікатор рятувальника та контактну інформацію. Інформація також може бути передана в медичний центр.

5.8 Вдосконалення системи ідентифікації людей на основі машинного навчання і комп’ютерного зору

Підсумком матеріалів, наведених в розділах 3 та 5 є поєднання методів машинного навчання з методами біометричної автентифікації, за рахунок чого була вирішена задача вдосконалення ідентифікації людини [270].

5.8.1 Постановка задачі

Системи ідентифікації людей на основі комп'ютерного зору це технологія, яка дозволяє ідентифікувати або верифікувати особу на зображенні або у відеопотоці. Існує кілька основних класів систем ідентифікації, загалом всі вони базуються на порівнянні обраних ознак або генерованих векторів обличчя із зображеннями або дескрипторами, які вже є в базі даних. Також системи ідентифікації описуються як біометричний додаток на основі штучного інтелекту, вони можуть однозначно ідентифікувати особу, аналізуючи особливості на основі особистих текстур і розмірів обличчя.

Система комп'ютерного зору для ідентифікації обличчя часто використовується в системах контролю доступу і може бути порівняна з іншими біометричними протоколами, такими як розпізнавання відбитків пальців і сканування сітківки ока [270]. Точність розпізнавання за допомогою комп'ютерного зору є меншою через більш доступну можливість обману системи, а також через те, що система чутлива до умов навколишнього середовища.

5.8.2 Структура системи ідентифікації людей на основі комп’ютерного зору

Будь-яка система на основі комп'ютерного зору критично залежить від умов навколишнього середовища, тому спочатку зосередимося на них, а потім опишемо саму систему.

5.8.2.1 Вимоги до системи

Системи комп'ютерного зору залежать від факторів навколишнього середовища, серед яких основними є положення камери, фон та освітлення.

Якість розпізнавання обличчя залежить від положення камери і від того, наскільки вона статична. Камеру слід розміщувати таким чином, щоб таким чином, щоб можна було виділити основні риси об'єкта на вихідному зображенні. Крім того, роздільна здатність зображення і розмір рамки об'єкта на всьому зображенні. також важлива роздільна здатність зображення та межа об'єкта до всього зображення. Таким чином, можна буде виділити основні риси обличчя. Це дуже важливо для розпізнавання, оскільки основна метою вбудовування моделей є забезпечення відмінності для об'єктів різних класів об'єктів і розмірної схожості для об'єктів в межах об'єктів в межах одного класу. Для запобігання малих відхилень об'єкта і камери і камери, можна використовувати стабілізацію обличчя в ключових точках.

Фон навколишнього середовища може впливати як позитивно, так і негативно як позитивно, так і негативно, тому його необхідно враховувати і якщо можливо, змінювати для досягнення максимальної ефективності.

Негативний вплив фону на якість виявлення полягає у збільшенні кількості хибних спрацьовувань через високу неоднорідності фону та великої кількості різних текстур. Також слід уникати поверхонь, що відбивають світло оскільки вони призводять до того, що об'єкти виявляються кілька разів

і одночасно. Позитивний вплив фону на виявлення та розпізнавання відбувається, коли фон однорідний і має високий рівень контрасту з можливими цілям.

При виборі освітлення в приміщенні слід враховувати наступні параметри повинні бути враховані:

1. Розмірне положення джерела світла. Джерело світла повинно бути встановлене так, щоб уникнути засвічень і тіней на об'єкті.

2. Інтенсивність світла. Вона повинна бути достатньою, щоб показати всі деталі на можливих мішенях.

3. Розсіювання світла. Має бути рівномірно розсіяне по всьому приміщенню.

Якщо не врахувати ці фактори, то зменшиться кількість видимих деталей об'єкта і, як наслідок, генероване зображення матиме низьку репрезентативну здатність, що, в свою чергу, знижує якість розпізнавання.

При незначних відхиленнях від бажаних значень освітленості, застосовуються методи цифрової обробки зображень, щоб покращити якість зображення та виділити ціль. Часто використовується вирівнювання зображення гістограми для підвищення його контрастності, варіації гаусових фільтрів для придушення шумів і виділення контурів об'єктів. Одним з найефективніших є двосторонній фільтр.

Основною вимогою до камери є забезпечення достатньої роздільної здатності зображення, його контрастність і частота кадрів в секунду. Обчислювальні ресурси слід підбирати залежно від того, яку частоту кадрів можна забезпечити.

5.8.2.2 Структура системи

Основна ідея системи повторної ідентифікації за допомогою комп'ютерного зору полягає в тому, щоб описати унікальну людину за унікальним зображенням і прийняти рішення про ідентифікацію, порівнюючи зображення. Загалом система складається з наступних частин: детектор, модель відстеження, дескриптор об'єкта модель пошуку, модель пошуку на основі даних та модель авторизації та прийняття рішень. На рис. 5.58 показано структуру системи.

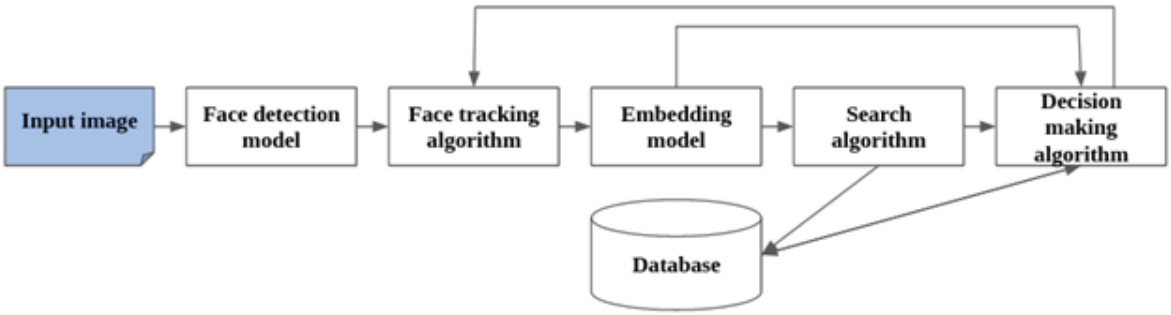


Рис. 5.58. Структура запропонованої системи ідентифікації на основі комп'ютерного зору

Окремі зображення з потоку камери подаються на модель виявлення модель розпізнавання. Вона виявляє обличчя на вхідних зображеннях, а вихідні дані складаються з координат обмежувальних рамок навколо обличчя.

Потім для кожного виявленого обличчя траєкторія руху ініціалізується алгоритмом відстеження. Кожне зображення кожної траєкторії зберігається. Якщо для одного обличчя є більше 5 кадрів (гіперпараметр) для одного обличчя, то всі зображення траєкторій подаються на модель для отримання унікального зображення обличчя.

Модель генерації вбудовування генерує унікальний вектор дескрипторів з 512 дескрипторів (гіперпараметр) для кожного вхідного зображення обличчя.

Кожне з отриманих вбудовувань запитується для пошуку п'яти близьких сусідів (гіперпараметр) з бази даних. Після цього кожне вхідне зображення порівнюється з відповідним з бази даних, в результаті цих порівнянь для кожного зображення визначається клас, до якого воно належить. Початкове передбачення класу отримується шляхом вибору класу, який найчастіше зустрічається серед прогнозів для кожного вхідного вбудовування, якщо всі класи різні, то траєкторія присвоюється класу найближчому до кожного з вхідних вкладок, але якщо відстань менше порогової, то ініціалізується новий клас.

Потім система називає відповідну траєкторію ім'я отриманого класу для неї, і продовжує відстежувати об'єкт між кадрами, але більше не надсилає його зображення до моделі розпізнавання обличчя.

5.8.3 Вибір алгоритмів для забезпечення роботи системи

5.8.3.1 Порівняння алгоритмів виявлення

Детектори YOLO [273] та SSD [274] схожі за структурою блоків передбачення і відрізняються лише базовою мережею та кількістю блоків передбачення. Детектор YOLO має один блок для виявлення об'єктів, що забезпечує швидкість, але втрачає але втрачає в якості, якщо порівнювати з SSD. SSD має кілька додаткових шарів для уточнення виявлення об'єктів різного розміру, а потім після чого блок агрегації всіх прогнозів видає остаточні прогнози.

В результаті запропонованих удосконалень SSD алгоритму виявлення SSD (описані нижче), був отриманий детектор, який є достатньо швидким та

має достатньо високу якість виявлення, що задовольняє критеріям оптимальності, тому він буде використовуватиметься у запропонованій системі (табл. 5.7).

Таблиця 5.7. Порівняння алгоритмів детектування

Назва алгоритму	FPS (frame per second)	mAP	Датасет
YOLO	40	48.1	COCO test-dev
SSD	8	50.4	COCO test-dev
Improved SSD	15	54.1	COCO test-dev

5.8.3.2 Порівняння алгоритмів відстеження

Порівняння алгоритмів стеження з метрикою якості MOTA (Multiple object tracking accuracy) наведено в табл. 5.8.

Трекер на основі кореляційних фільтрів доцільно використовувати в умовах наявності та відсутності об'єкта детектора. Крім того, трекер на основі кореляційних фільтрів є більш цінний відносно обчислювального ресурсу, ніж IOU-трекер [275]. Якщо частота кадрів низька, то IOU між виявленням одного об'єкта на сусідніх кадрах стає низьким і якість відстеження значно знижується.

Таблиця 5.8. Порівняння алгоритмів трекінга

Назва алгоритму	FPS (frame per second)	MOTA	Датасет
IOU tracker	100 000	76.5	DETRAC
Background aware CF [276]	156	77.8	DETRAC

Оскільки фон об'єкта незмінний, а обраний детектор обраний детектор досить швидкий і має високу якість виявлення, система буде використовувати IOU-трекер.

5.8.3.3 Порівняння алгоритмів розпізнавання обличчя

Після порівняння в якості архітектури для системи було обрано модель ArcFace [278]. До уваги було взято швидку збіжність моделі, що оптимізує функцію помилки. Вона не потребує складної процедура генерації партій в межах однієї епохи навчання при використанні моделі ResNet50 [271] досягає найвищих результатів на стандартизованих наборах даних (табл. 5.9). Покращення будуть зроблені будуть зроблені вдосконалення для підвищення репрезентативності моделі.

Таблиця 5.9. Порівняння алгоритмів розпізнавання

Назва алгоритму	Точність (accuracy), фаза ідентифікації	Точність (accuracy), фаза верифікації	Датасет
YOLO	65.49	80.14	MEGA FACE
SSD	81.72	96.98	MEGA FACE
Improved SSD	84.16	95.34	MEGA FACE

5.8.3.4 Порівняння алгоритмів пошуку

Наївний метод k-найближчих сусідів є найточнішим, його результати є стандартними, але зі зростанням бази даних його використання стає неможливим через велику кількість часу, що витрачається на обчислення відстаней між вхідними вкладенням та всіма вкладеннями з бази даних. Тому було вирішено використати наближений метод *k*-найближчих сусідів. Було обрано HNSW [279]. Основними перевагами алгоритму HNSW є швидкість, висока наближеність до результатів методу *k*-найближчих сусідів та ефективна реалізація в бібліотеці nmslib.

5.8.3.5 Алгоритм прийняття рішень

Порівняння порогових значень відстані між вбудовуваннями буде будуть використовуватися для прийняття рішень про авторизацію в системі. Як метрика відстані метрики відстані буде використано косинусну відстань між

векторами оскільки функція помилки ArcFace оперує косинусом відстані між векторами відстанню під час навчання.

5.8.4 Опис удосконалень моделей виявлення та розпізнавання

Ключовими елементами, які найбільше впливають на якість системи повторної ідентифікації є модель виявлення та модель розпізнавання. Модель виявлення залежить від того, чи буде кожна окрема ціль буде виявлена у відеопотоці для подальшої обробки. Модель розпізнавання залежить від унікальності представлення окремих об'єктів у багатовимірному просторі вбудовування багатовимірному просторі вбудовування, а також можливість розрізняти об'єкти окремих класів. Тому було вирішено вдосконалити та оптимізувати існуючі моделі виявлення моделі виявлення та отримати дескриптори.

5.8.4.1 Опис покращення моделі виявлення SSD

Описані вище моделі виявлення YOLO та SSD мають кілька важливих особливостей, які дозволяють потенційне покращення якості виявлення та швидкості.

Детектори YOLO та SSD за своєю структурою схожі на блоками передбачення, але відрізняються базовою мережею та кількістю блоків передбачення. Детектор YOLO має один додатковий шар для прогнозування положення об'єктів на зображенні, що забезпечуючи швидкість, але втрачає якість порівняно з SSD. Детектор SSD має кілька додаткових шарів для покращення виявлення об'єктів різного розміру різних розмірів, за яким слідує додатковий шар, який об'єднує прогнози всіх додаткових шарів і виробляє остаточні прогнози. Така складність призводить до нижчої швидкості виявлення, ніж у YOLO.

Метою вдосконалення алгоритму виявлення SSD було покращення якості його роботи без значних втрат у швидкості виявлення.

Крім того, заміна мережі VGG16 на мережу MobileNet [272] дозволить зменшити кількість мережевих параметрів і підвищити швидкість роботи. Покращений SSD використовує мережу MobileNet як базову нейронну мережу. Прогностичні виходи, які відносяться до базової мережі, приєднуються до одинадцятого шару та тринадцятого, а також додаються вісім додаткових шарів до мережі після тринадцятого шару. Прогнозування здійснюється з кожного додаткового шару.

Крім того, для покращення якості виявлення та зменшення кількості помилкових спрацьовувань у кожен додатковий шар було додано блок уваги – CBAM (Constitution block attention module) [280]. Модуль CBAM використовується для збільшення репрезентативності згорткових нейронних мереж. Він не вимагає великої кількості обчислень, тому може ефективно використовуватися без особливих втрат у швидкості. Модуль канальної уваги використовує міжканальну взаємодію ознак і намагається виділити більш важливі з них з більшою вагою. Модуль канальної уваги можна вважати детектором важливих ознак; він концентрується на тому, що є важливим.

Модуль просторової уваги враховує просторову взаємодію ознак і фокусується на розташуванні ознак.

Комбінація двох модулів уваги дозволяє відокремлювати канальну та просторову інформацію з вхідних даних.

Деталі навчання. Спочатку було взято SSD-детектор з базовою мережею MobileNet. Він пройшов попередню підготовку на датасеті WIDER Face [261]. Після додавання блоків уваги CBAM всі шари до десятого включно були заморожені і не брали участі в навчанні для оптимізації функції втрат,

щоб уникнути проблеми надмірної підгонки. Для навчання та тестування використовувалися набори даних WIDER Face.

Навчання проводилося протягом 35 000 ітерацій з розміром партії 16. Початкова швидкість навчання була встановлена на 0.01 і змінювалася з кожною ітерацією. Для оптимізації моделі було використано алгоритм оптимізації Адама [262] з наступними значеннями спаду імпульсу та ваги 0.9 та 0.0001, відповідно. Розширення навчальної вибірки було використано для збільшення кількості навчальних вибірок та зменшення ймовірність надмірної підгонки. Було використано такі методи доповнення: випадкове віддзеркалення, випадкове масштабування з коефіцієнтом масштабування від 0,2 до 2, випадкове обертання між –30 і 30 градусів та гаусівський шум.

Таким чином, змінивши базову модель з VGG16 на MobileNet, було отримано збільшення швидкості та точності завдяки більшій потужності представлення мережі MobileNet.

Додавши модуль особливої уваги CBAM, була зменшена кількість хибних спрацьовувань. Результати навчання наведені вище в таблиці 5.7.

5.8.4.2 Опис моделі розпізнавання та її покращення

Після огляду та аналізу моделей розпізнавання обличчя, було вирішено використовувати моделі на основі ArcFace як архітектуру розпізнавання обличчя архітектури розпізнавання обличчя. Недоліком моделей навчання з функцією втрат ArcFace є чутливість до викидів у навчальних даних, тому навчальний набір даних повинен бути перевірений.

Метою модифікацій моделі на основі помилок ArcFace є збільшення швидкості навчання моделі, збільшення репрезентативності моделі репрезентативності моделі та зменшити чутливість до аномалій даних.

Опис опорної мережі:

Мережа SE-ResNet буде використовуватися як базова нейронна мережі для покращення репрезентативності мережі та швидкості збіжності навчання моделі. Нещодавні дослідження в галузі в області згорткових нейронних мереж (convolutional neural networks, CNN) показали, що їх репрезентативність може бути покращена шляхом інтеграції спеціалізованих механізмів навчання, які допомагають звернути увагу на особливості та параметри самої мережі.

Автори статті Squeeze-and-Excitation Networks [183] пропонують новий блок для CNN – блок Squeeze-and- Excitation (SE) блок, який виконує завдання нелінійної взаємодії між каналами одного шару. Блок адаптивно калібрує міжканальну взаємодію та їхні реакції на вхідні дані та моделює взаємозалежність між каналів. В результаті блок SE вчиться фокусуватися на важливих характеристиках, одночасно стискаючи менш важливі.

Блок є загальним, і він виконує різні ролі залежно від того, на якому шарі нейронної мережі він знаходиться. На ранніх шарах блок звертає увагу на особливості ігнорування класів зображень, посилюючи низькорівневу репрезентативність мережі. В останніх шарах SE блоки стають більш залежними від вхідних класів: кожен клас має власну реакцію. Встановлюючи блоки SE на всіх шарах, зважені ознаки можуть бути накопичені по всій мережі.

Перевагою SE-блоку над аналогічними блоками є простота інтеграції в будь-яку мережу, зменшення схильність до надмірної підгонки, збільшення репрезентативної здатності мережі, а також використання невеликої кількості обчислювальних ресурсів порівняно з усією мережею.

Деталі навчання. Для навчання використовувалися набори даних CASIA [281], VGGFace2 [230], MegaFace [231] та LFW [234] були використані для навчання мережі. Для отримання дескрипторів використано мережу SE-

ResNet-50. Розмір вихідного вектору дескрипторів становить 512. Вектор ознак отримується шляхом передачі вихідних даних з останнього шару згортки до шару пакетної нормалізації а потім до шару повністю зв'язаних нейронів і виведення вектору вихідного дескриптора вхідних даних.

Масштабування вектору дескрипторів здійснюється за допомогою масштабного коефіцієнту масштабування *s*, він дорівнює 64, а параметр кутового відступу функції помилки ArcFace *m* дорівнює 0.5, як було показано в оригінальній статті [183]. Розмір вибірки (*batch size*) було взято рівним 64 (відповідно до результатів наведених в розділі 3, в табл. 3.10).

Початкова швидкість навчання, як і для детектора, була встановлена на 0.01 і змінювалася на кожній ітерації. Процес навчання тривав протягом 150 000 ітерацій. Для оптимізації було взято алгоритм Адама з значеннями імпульсу 0.9 та ваги розпаду 0.0005. Було використано наступні методи доповнення: випадкове відображення, випадкове масштабування з коефіцієнтом масштабування від 0,2 до 2, випадковий поворот між -30 і 30 градусами та гаусівський шум.

Таким чином, встановивши базовою моделлю SE-ResNet-50, було отримано незначне падіння швидкості, але значне покращення якості за рахунок більшої потужності представлення за рахунок SE-блоків. Результати навчання наведені в таблиці 5.9.

5.8.4.3 Новизна та переваги запропонованої моделі

В роботі [270] запропоновано нову систему ідентифікації на основі комп'ютерного зору. В дослідженні були зроблені наступні вдосконалення:

1. Проведено ретельний аналіз та порівняння компонентів системи комп'ютерного зору для ідентифікації людей: виявлення, відстеження, розпізнавання, пошук, прийняття рішень. В результаті аналізу виявлено

існуючі недоліки алгоритмів та визначено можливості їх вдосконалення для підвищення якості їх роботи.

2. Вдосконалено моделі виявлення та розпізнавання обличчя. Для моделі виявлення було додано MobileNet як базову мережу, а блоки прогнозування об'єднано з блоком уваги CBAM.

3. Покращено швидкість та якість ідентифікації людей шляхом розробки системи ідентифікації на основі комп'ютерного зору, яка дозволяє виконувати її в реальному часі та з гарантованою якістю. В результаті якість виявлення було підвищено до 54,1 mAP, а точність ідентифікації за моделлю розпізнавання зросла до 84,16%.

4. Система може бути використана для ідентифікації в середовищах, де можливо задовольнити вимоги до навколишнього середовища, наприклад, в офісах або на кордоні.

5.9 Оцінювання ступеня вдосконалення захищеності системи мобільного зв’язку

Показник захищеності як було зазначено вище оцінюється за формулою (5.1), а його складові – за формулами (5.2, 5.3). Розрахуємо ступінь вдосконалення захищеності інформаційно-телекомунікаційної системи за рахунок впровадження запропонованих змін. Для спрощення будемо вважати їх вплив взаємно незалежним.

Як було зазначено в п.5.1, формула 5.1 має вигляд:

$$Sec(\%) = AttBlock + ServLevel,$$

Підвищення рівня надання послуг (*ServLevel*) складається з рівня забезпечення конфіденційності (*ConfLev*), цілісності (*IntegrLev*), доступності (*AccessLev*) і спостереженості (*ObservLev*), (5.3):

$$ServLevel(\%) = ConfLev + AccessLev + IntegrLev + ObservLev.$$

Запропонований в підрозділі 5.3 метод агрегації біометричних ознак і інтелектуальна системи прийняття рішень, згідно [60] дозволяє підвищити показник конфіденційності шляхом підвищення якості надання послуг «конфіденційність при обміні» (з другого рівня до третього). Також наведений метод разом з запропонованими в підрозділі 5.6 методами шифрування та захищеного обміну ключами підвищує якість надання послуги «цілісність при обміні» з першого до другого рівня.

$ConfLev = ConfExchang(1 \rightarrow 3),$

$IntegrLev = IntegExchang(1 \rightarrow 2)$

Запропонований в підрозділі 5.4 метод приховування даних під час передачі вдосконалює рівень послуги «аналіз прихованих каналів» показника конфіденційності, з нульового рівня до рівня 2.

$ConfLev = AnalizCanal(0 \rightarrow 2)$

Впровадження взаємної автентифікації користувачів під час дзвінків, з підрозділу 5.5, згідно [60], підвищує якість послуги «ідентифікація і автентифікація при обміні», у порівнянні з існуючим протоколом STIR/SHAKEN з другого рівня до третього, забезпечує 3 рівень послуги «ідентифікація-автентифікація» (разом з наведеною в підрозділі 5.7 системою керування даними), а також впроваджує найвищий другий рівень послуг «автентифікація відправника» та «автентифікація отримувача» критерія спостереженості.

ObservLev = {IdAuth(1→3), IdAuthExchang(1→3), SenderAuth(1→2), ReceivAuth(1→2)}

Показник доступність вдосконалюється шляхом розширення послуги «використання ресурсів» (підрозділ 5.7) з другого до третього рівня.

Таким чином, відповідно до (5.3):

$$ServLevelBefore = ConfLevB + AccessLevB + IntegrLevB + ObservLevB. \quad (5.4)$$

$$ServLevelAfter = ConfLevA + AccessLevA + IntegrLevA + ObservLevA. \quad (5.5)$$

де:

ConfLevBefore = TrustConf(1) + AdminConf(1) + RepConf(1) + AnalizChannel(0)+ ConfObmin(1) = 4;

ConfLevAfter = TrustConf(1) + AdminConf(1) + RepConf(1)+ AnalizChannel(2)+ ConfExchang(3) = 8;

AccessLevBefore = ResourseUse(2) + ResistRefuse(2) + HotSwap(2) + Recov(2) = 8;

AccessLevAfter = ResourseUse(3) + ResistRefuse(2) + HotSwap(2) + Recov(2) = 9;

IntegrLevBefore = TrustIntegr(1) +AdminIntegr(2) + Revoke(2) + IntegExchang(1) = 6;

IntegrLevAfter = TrustIntegr(1) +AdminIntegr(2) + Revoke(2) + IntegExchang(2) = 7;

ObservLevB = Audit(5) + *IdAuth(2) + ReliableChannel(1) + DistribResponsib(2) + IntegSec(2) + SelfTest(1) + IdAuth(2) + IdAuthExchang(2) + SenderAuth(1) + ReceivAuth(1) = 19;*

ObservLevA = Audit(5) + *IdAuth(3)* + *ReliableChannel(1)* + *DistribResponsib(2)* + *IntegSec(2)* + *SelfTest(1)* + *IdAuth(3)* + *IdAuthExchang(3)* + *SenderAuth(2)* + *ReceivAuth(2) = 24.*

Згідно вищенаведеного та (5.4)-(5.5), формула (5.3) набуває вигляду:

ServLevelBefore = ConfLevB(4) +AccessLevB(8) + IntegrLevB(6) + ObservLevB(19) = 37,
ServLevelAfter = ConfLevA(8) +AccessLevA(9) + IntegrLevA(7) + ObservLevA(24) =48,

і відповідно вдосконалення рівня надання послуг:

ServLevel = (ServLevelAfter-ServLevelBefore)/ ServLevelBefore
ServLevel = (48-37)/37 = 29.7%.

Згідно рис. 1.20 і наведеного в п.1.8 загроз мережі 5G, в роботі оцінювався рівень перекриття вказаних загроз розробленими методами. Так, запропоновані в п.5.5 і п.5.6 методи наскрізного шифрування під час дзвінка і взаємної автентифікації користувачів з підтвердженням дозволяють унеможливити такі загрози Rogue Base Station, також перехоплення дзвінків атаками «злонамірник посередині» (MitM) і Jamming. Таким чином, буде перекрито 3 атаки з можливих 11, що надає виграш по коефіцієнту перекриття атак (5.2) 27%.

5.10 Висновки

Таким чином за результатами досліджень із вдосконалення захищеності інформаційно-телекомунікаційної системи, досягнуто наступних результатів:

1. Вдосконалено метод формування вектору ознак біометричних характеристик користувача шляхом вдосконалення модуля агрегації за рахунок застосування пріоритезації біометричних ознак, зашумлення невикористовуваних ознак, проріджування, завадостійкого кодування та врахування стану каналу зв’язку.

Наукова новизна полягає в захищеному методі поєднання різних біометричних ознак користувача для формування криптографічного ключа підпису або шифрування, застосуванні пріоритезації, зашумлення, проріджування та кодування. Запропонований метод дозволяє використовувати біометричні ознаки для віддаленої автентифікації та формування криптографічного ключа без ризику їх компрометації. Також на основі інформації о наявних біометричних ознаках користувача обрати найкращий за заданими критеріями спосіб їх перетворення в захищений біометричний шаблон. Вдосконалений метод впроваджено в патент, який знаходиться на реєстрації.

Елементи запропонованої системи впроваджені в патенті [213].

2. Вдосконалено процес підготовки біометричних даних користувача до передачі мережею зв’язку, шляхом додавання завадостійкого кодування і методів прихованої передачі інформації.

Наукова новизна полягає у внесенні додаткової надмірності у біометричні дані, шляхом використання завадостійкого кодування. Вперше застосовано методи мережної стеганографії для приховання процесу передачі біометричних даних користувача. Запропоноване рішення дозволяє на 10% зменшити рівень FRR, шляхом підвищення порогу спрацьовування системи у

зашумлених каналах зв’язку, а також підвищити стійкість до атак, шляхом приховання сеансу віддаленої автентифікації в заголовках мережних протоколів.

Елементи запропонованої системи впроваджені в патенті [265].

3. Запропоновано інтелектуальну систему прийняття рішень для вибору методу приховування даних користувача під час віддаленої автентифікації, в залежності від наявності активних сесій, доступної смуги пропускання та параметрів каналу зв’язку.

Наукова новизна полягає в тому, що вперше запропоновано інтелектуальну систему, що дозволяє обирати метод приховування інформації враховуючи сценарії застосування та параметри каналу зв’язку. Запропонована система дозволяє обрати метод підвищення прихованості шляхом використання мережної стеганографії на основі інформації про параметри каналу зв’язку та потреби сценарію застосування, що дозволяє підвищити завадостійкість приватних даних користувача та захищеність від атак.

4. Вперше запропоновано метод протидії шахрайським дзвінкам шляхом взаємної автентифікації користувачів під час дзвінка. Взаємна автентифікація реалізується шляхом модифікації певних полів повідомлень (SETUP, CONNECT ACK).

Наукова новизна полягає в тому, що автентифікація користувачів відбувається безпосередньо під час дзвінка і не потребує додаткових дій від користувача. Це досягається застосуванням Continuous Authentication або біометричної автентифікації за малюнком вуха/акустичним відгуком. Запропонований метод дозволяє уникнути підміни користувача на іншому боці і отримати доступ до сервісів (відповідати на дзвінок) лише авторизованому користувачу.

5. Вдосконалено систему управління приватними даними користувача, яка дозволяє надавати доступ до керування оточенням за рахунок розпізнавання об’єктів та застосування біометричної автентифікації.

Наукова новизна полягає в поєднані розпізнавання зображень та автентифікації користувача, щоб надати доступ уповноваженій людини до своїх особистих даних, що зберігаються в електронному пристрої. Запропонована система впроваджена в патенті [257].

6. Вдосконалено систему управління приватними даними користувача, яка дозволяє забезпечити ієрархічний доступ до особистих даних і захищену сертифікатами схему доступу до приватних даних лікарями.

Наукову новизну складає метод ієрархічного відображення даних користувача, який дозволяє при переведенні телефону в emergency mode відображати різний рівень доступу до даних користувача стороннім особам, особам для надання первинної допомоги та лікарям.

Запропонований метод впроваджено в патенті [256].

7. Вдосконалено систему ідентифікації людини на зображеннях або у відеопотоці за рахунок використання MobileNet в якості базової мережі, а також об'єднання блоку прогнозування з блоком уваги CBAM.

Наукова новизна полягає в покращенні швидкості та якості ідентифікації людей шляхом розробки системи ідентифікації на основі комп'ютерного зору, яка дозволяє виконувати її в реальному часі та з гарантованою якістю. В результаті якість виявлення було підвищено до 54,1 mAP, а точність ідентифікації за моделлю розпізнавання зросла до 84,16%.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну проблему створення і наукового обґрунтування комплексної методології управління процесом обслуговування у інформаційно-комунікаційній мережі мобільного зв’язку з метою підвищення рівня захищеності та якості зберігання, обробки й передачі даних.

За підсумками вирішення проблеми можна зробити наступні висновки:

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 класифікація 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 вибірки 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 часу 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 ACK 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 моделі 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%.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 3GPP 5G System Overview https://www.3gpp.org/technologies/5g-system-overview

2. 3GPP The "Release 17 Description; Summary of Rel-17 Work Items" (TR21.917) https://www.3gpp.org/specifications-technologies/releases/release-17

3. 3GPP TSG Rel-18 Description https://www.3gpp.org/specifications-technologies/releases/release-18

4. NR and NG-RAN Overall description; Stage-2 (TS 38.300).

5. Service requirements for the 5G system (TS 22.261)

6. What is Service Based Architecture for 5G System https://www.tucana.com/news/blog-what-is-service-based-architecture-for-5g-system/

7. A. Al-Dulaimi, X. Wang, and I. Chih-Lin, “5G Networks: fundamental requirements, enabling technologies, and operations management,” Wiley, New Jersey, 2018.

8. Технологія MIMO. Вікіпедія. Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/MIMO

9. Скляр Б. “Цифровий зв’язок. Теоретичні основи і практичне застосування” / Б. Скляр; пер. с англ. – М.: «Вильямс», 2003 – 1104 с.

10. P. Elias, “Coding for two noisy channels,” *Information Theory, Third London Symposium*, Butterswort’s Scientific Publications, pp. 61-76, 1955.

11. Moon, Todd K. "Error correction coding", Mathematical Methods and Algorithms. J. Wiley and Son (2005). – p. 508.

12. Адитивний білий гаусовський шум. Вікіпедія. Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/Additive_white_Gaussian_noise

13. Кузьмін І. В., Кедрус В. А. “Основи теорії інформації і кодування”, 2-е видання, Вища школа 1986. – 286 с.

14. C. E. Shannon, “Communication in the presence of noise,” in *Proc. Institute of Radio Engineers 1949*, vol. 37 (1), pp. 10–21.

15. Mustafa Hamdi, Mohammed Jabbar Mohammed. “BER Vs E b /N 0 BPSK Modulation over Different Types of Channel”, Australian journal of basic and applied sciences 12(5):31-38, DOI:10.22587/ajbas.2018.12.5.7.

16. ДСТУ ETSI EG 202 057-4:2015 Аспекти оброблення, передавання сигналів мовної інформації та забезпечення їхньої якості (STQ). Визначення і вимірювання важливих для споживача параметрів QoS. Частина 4. Доступ до «Інтернету» (ETSI EG 202 057-4:2008, IDT).

17. Методика вимірювань параметрів якості послуг рухомого (мобільного) зв'язку, затверджено Рішенням Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації 02 березня 2021 року № 80; Зареєстровано в Міністерстві юстиції України 28 квітня 2021 р. за № 580/36202.

18. ДСТУ 8861:2019 Системи рухомого зв’язку. Показники якості послуг. Методика визначення параметрів.

19. Зміни до Положення про якість телекомунікаційних послуг, затвердженого рішенням Національної комісії з питань регулювання зв'язку України від 15 квітня 2010 року № 174, зареєстрованого в Міністерстві юстиції України 23 червня 2010 року за № 429/17724.

20. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT).

21. СОУ 64.2-00017584-005:2009 Телекомунікаційні мережі рухомого (мобільного) зв’язку загального користування. Система показників якості послуг рухомого (мобільного) зв’язку. Загальні положення.

22. СОУ 64.2-00017584-006:2009 Телекомунікаційні мережі рухомого (мобільного) зв’язку загального користування. Телекомунікаційні послуги. Показники якості. Методи випробування.

23. ДСТУ ETSI EG 202 057-1:2015 Аспекти оброблення, передавання сигналів мовної інформації та забезпечення їхньої якості (STQ). Визначення і вимірювання важливих для споживача параметрів QoS. Частина 1. Загальні положення (ETSI EG 202 057-1:2013, IDT).

24. ДСТУ ETSI EG 202 057-2:2015 Аспекти оброблення, передавання сигналів мовної інформації та забезпечення їхньої якості (STQ). Визначення і вимірювання важливих для споживача параметрів QoS. Частина 2. Послуги голосової телефонії, факсу групи 3 та передавання даних та коротких повідомлень (SMS) за допомогою модему» (ETSI EG 202 057-2:2011, IDT).

25. ДСТУ ETSI EG 202 057-3:2015 Аспекти оброблення, передавання сигналів мовної інформації та забезпечення їхньої якості (STQ). Визначення і вимірювання важливих для споживача параметрів QoS. Частина 3. Спеціальні параметри якості послуг для суходільних мереж рухомого зв'язку загального користування (PLMN) (ETSI EG 202 057-3:2005, IDT).

26. Son Hoang Dau, Han Mao Kiah, Wentu Song, Chau Yuen. "Locally Encodable and Decodable Codes for Distributed Storage Systems" https://doi.org/10.48550/arXiv.1504.04926

27. Robert H. Morelos-Zaragoza. "The art of Error Correcting Coding". First Edition. John Wiley & Sons, 2002. – 221p.

28. Код Ріда-Соломона. Вікіпедія. Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/Код_Ріда_-_Соломона

29. Richard E. Blahut. "Theory and Practice of Error Control Codes". Addison-Wesley Publishing Company, Massachusetts, 1984. – 576p.

30. R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Information Theory*, Vol. 27, pp. 533-547, September 1981.

31. I. S. Reed, and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, Vol. 8, No.2, pp. 300-304, June 1960.

32. R. G. Gallager, “Low-density parity-check codes,” Ph.D. diss., Massachusetts Institute of Technology, 1963.

33. M. Luby, M. Mitzenmacher, A. Shokrollahi, D. Spielman, and V. Stemann, “Practical loss-resilient codes,” in *Proc. ACM Symposium on Theory of Computing* 1997.

34. D. J. C. MacKay, “Good error-correcting codes based on very sparse matrices,” *IEEE Trans. Information Theory*, vol. 45, pp. 399–431, March 1999.

35. M. Luby, “LT codes,” in *Proceedings of The 43rd Annual IEEE Symposium on Fountations of Computer Science*, pp. 271-282, November 16-19, 2002.

36. O. Etesami, and A. Shokrollahi, “Raptor codes on binary memoryless symmetric channels,” *IEEE Trans. Inf. Theory*, Vol. 52, No. 5, May 2006.

37. A. Shokrollahi, “Raptor codes,”, *IEEE Trans. Inf. Theory*, Vol. 52, No. 6, pp. 2551– 2567, June 2006.

38. James S. Plank. “A Tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems”, Technical Report UT-CS-96-332, University of Tennessee, July, 1996. http://www.cs.utk.edu/~plank/plank/papers/CS-96-332.html

39. W. E. Ryan, “An introduction to LDPC codes,” in *CRC Handbook for Coding and Signal Processing for Recoding Systems* (B. Vasic, ed.), CRC Press, 2004.

40. A. Shokrollahi, “LDPC codes: An introduction,” Digital Fountain, Inc., April 2003.

41. W. Huang, H. Li and J. Dill, “Digital fountain codes system model and performance over AWGN and Rayleigh fading channels,” *Int’l Conf. Computing, Communications and Control Technologies*, Apr 6 - 9, 2010, Orlando, Florida, USA.

42. D. MacKay, “Fountain Codes”, Talk (presentation) for Thames Valley IEE, England, Oct. 27, 2005.

43. Заборовский В.С. “Анализ трафика в сетях коммутации пакетов” – СПб.: СПбГПУ, 2010. – 90с.

44. А.С. Довбиш. Звіт про науково-дослідну роботу «Інтелектуальна система керування навантаженням і ресурсами розподіленого обчислювального середовища з підвищеною інформаційною безпекою», СумДУ, 2016. – 166 с.

45. M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn and F. Abdessamia, "Network Traffic Classification techniques and comparative analysis using Machine Learning algorithms," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2016, pp. 2451-2455.

46. Meenaxi Raikar, Meena S M, Mohammed Moin Mulla, Nagashree Shetti, Meghana Karanandi. “Data Traffic Classification in Software Defined Networks (SDN) using supervised-learning”. Procedia Computer Science, Volume 171, 2020, https://www.sciencedirect.com/science/article/pii/S1877050920312928

47. AlZoman, R.M., Alenazi, M.J.F. “A Comparative Study of Traffic Classification Techniques for Smart City Networks”. Sensors 2020, 21, 4677. https://doi.org/10.3390/s21144677

48. Salman, O., Elhajj, I., Kayssi, A., Chehab, A. “A Review on Machine Learning Based Approaches for Internet Traffic Classification”. Ann. Telecommun. 2020, 673–710.

49. Alqudah, N., Yaseen, Q. “Machine Learning for Traffic Analysis: A Review”. Procedia Comput. Sci. 2020, 170, 911–916.

50. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Wang, C.; Liu, Y. “A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges”. IEEE Commun. Surv. Tutor. 2019, 21, 393–430.

51. Aureli D., Cianfrani A., Diamanti A., Sanchez Vilchez J.M., Secci S. “Going Beyond DiffServ in IP Traffic Classification”. In Proceedings of the NOMS 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, April 2020; pp. 1–6.

52. Tomasz Bujlow, Valentín Carela-Español, Pere Barlet-Ros: "Independent Comparison of Popular DPI Tools for Traffic Classification", Computer Networks 76 (2015), pp. 75-89. Internet: https://cba.upc.edu/monitoring/traffic-classification#independent-comparison-of-popular-dpi-tools-for-traffic-classification-dataset.

53. Gurney, Kevin. “An introduction to neural networks”. UCL Press Limited, eBook 1997.

54. Bhadeshia H. ”Neural Networks in Materials Science”. ISIJ International (10): 1999, pp. 966–979.

55. Штучна нейронна мережа. Вікіпедія. Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/Штучна_нейронна_мережа

56. Метод k-найближчих сусідів. Вікіпедія. Електронний ресурс. Режим доступу: https://wikipedia.org/wiki/Метод_k-ближайших_соседей

57. Breiman, Leo. “Random Forests”. Machine Learning (1): 2001, pp. 5–32.

58. Trevor Hastie, Robert Tibshirani, Jerome Friedman. “Random Forests” Chapter 15, The Elements of Statistical Learning. – 2009. – p. 587-623.

59. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 04.07.2008 N 112; Зареєстровано в Міністерстві юстиції України 25 липня 2008 р. за N 690/15381)

60. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. https://tzi.com.ua/downloads/2.5-004-99.pdf

61. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

62. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

63. Moazzam Tiwana. “3GPP 5G security architecture”, https://drmoazzam.com/3gpp-5g-security-architecture

64. The evolution of security in 5G / 5G Americas Whitepaper, 2018. https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf

65. The Evolution of Security in 5G. – 2019. – URL: https://www.5gamericas.org/the-evolution-of-security-in-5g-2/

66. Одарченко Р. С., Григоренко Д. К., Фесенко В. О., Дрофа Т. С. “Удосконалення ядра мережі 5g з метою підвищення рівня захищеності зв’язку”, Наукоємні технології № 1(57), 2023, с.47-57.

67. 3GPP TS 33.310 release 6 (2018-09) Network Domain Security (NDS); Authentication Framework (AF) https://www.3gpp.org/DynaReport/33310.htm

68. Marco Lourenço, Louis Marinos. “ENISA Threat assessment for the fifth generation of mobile telecommunications networks (5G)”, ENISA threat landscape for 5G networks, 2019.

69. Craig Gibson. “Securing 5G Through Cyber-Telecom Identity Federation”, Trend Micro Research. 2019.

70. Lichtman M. L. “5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation”. – 2018. DOI: 10.1109/ICCW.2018.8403769.

71. Jover R.P. “5G protocol vulnerabilities and exploits”, 2020. – URL: http://rogerpiquerasjover.net/5G_ShmooCon_FINAL.pdf.

72. Cedex S. A. “5G Security architecture and procedures for 5G System”, 2020. URL: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf

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

74. A. Sarkar, Binod K. Singh. “A Review on Different Biometric Template Protection Methods, Recent Advances in Computer Science and Communications”, Volume 14, Issue 5, 2021, pages: 1551 – 1572.

75. Poongodi P, Betty P. “A Study on Biometric Template Protection Techniques”, International Journal of Engineering Trends and Technology (IJETT) – Volume 7 Number 4, 2014.

76. M.S. Lutsenko, O.O. Kuznetsov, D.I. Prokopovich-Tkachenko, V.P. Zverev, “Comparative analysis of biometric cryptosystems” [rus], Kharkiv: Applied radio electronics. – 2018. – Volume 17, № 3, 4. – p. 182-191.

77. Ijaz Ahmad. Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov “5G security: Analysis of threats and solutions”, 2017 IEEE Conference on Standards for Communications and Networking (CSCN). Helsinki, Finland: 2017.

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

79. Різник О.Я. “Завадостійке перетворення даних”. ІІ Міжнародна науково-практична конференція “Інформаційна безпека та інформаційні технології”, Кропивницький, с.51, 2020 https://www.kntu.kr.ua/doc/zbirnyki/teachers/2020/3.pdf

80. Пятін І., Бойко Ю. “Методика полярного кодування в 5G мобільних засобах телекомунікацій багатопозиційною модуляцією”, Вимірювальна та обчислювальна техніка в технологічних процесах, 2020. №1, с. 67-76.

81. Пятін І., Бойко Ю. “Дослідження енергетичної ефективності канального кодування даних користувача кодами LDPC для систем зв’язку

5G", Вісник Хмельницького національного університету, тех. науки. 2020. №3. с. 174-185.

82. Василенко В.М. "Дослідження ефективності детермінованих та псевдовипадкових перемежувачів турбокодів", Математичне моделювання в економіці, 2018. Том. 2 (11). с. 40-49.

83. Зайцев С.В., Приступа В.В., Василенко В.М. "Оцінювання завадозахищеності безпровідних мереж із сигналами OFDM з внутрібітовою псевдовипадковою перебудовою піднесучих частот", Вісник Чернігівського державного технологічного університету, 2013. №. 2(65). с. 192-202.

84. Потий А., Пилипенко Д. "Классификация показателей безопасности информации", Системи обробки інформації, Вип. 3(84), с.53-56, 2010.

85. Bao-Shuh Paul Lin, Fuchun Joseph Lin, Li-Ping Tung. "The Roles of 5G Mobile Broadband in the Development of IoT, Big Data, Cloud and SDN", 2016, Communications and Network 08(01): pp. 9-21. https://www.researchgate.net/publication/305805805_The_Roles_of_5G_Mobile_Broadband_in_the_Development_of_IoT_Big_Data_Cloud_and_SDN

86. Luong Vy Le, Do Sinh, Bao-Shuh Paul Lin, Li-Ping Tung. "SDN/NFV, Machine Learning, and Big Data Driven Network Slicing for 5G", 2018 IEEE 5G World Forum (5GWF) At: Silicon Valley, CA, USA, USA https://www.researchgate.net/publication/328730635_SDNNFV_Machine_Learning_and_Big_Data_Driven_Network_Slicing_for_5G

87. TS 23.501 "System Architecture for the 5G System" 3GPP Release 17. https://www.tech-invite.com/3m23/tinv-3gpp-23-501.html

88. Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie Young. "ETSI White Paper No. 11: Mobile Edge Computing A key technology towards 5G", First edition – September 2015. ISBN No. 979-10-92620-08-5

89. View on 5G Architecture [Online]. https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf

90. A.P Singh, S. Nigam, andAs N.K Gupta, “A study of next generation wireless network 6G,” Int.J. Innovative Res. Computer Commun. Eng., vol. 4, no. 1, pp. 871–874, 2007.

91. A. Mourad, R. Yang, P.H. Lehne, and A. De La Oliva, “A baseline roadmap for advanced wireless research beyond 5G,” Electronics, vol. 9, no. 2, pp. 351, 2020.

92. A. Pouttu, “Genesis-taking the first steps towards 6G,” in: Proc. IEEE Conf. Standards Communications and Networking, 2018

93. H. Viswanathan, “Mogensen Communications in the 6G era,” IEEE, Access 8:57063–57074, 2020.

94. J. Gozalvez, “Tentative 3GPP timeline for 5G [mobile radio],” IEEE Vehicular Technol Magazine, vol. 10, no. 3, pp. 12–18, 2015.

95. M.W. Akhtar, S.A. Hassan, R. Ghaffar, H. Jung, S. Garg, and M.S. Hossain, “The shift to 6G communications: vision and requirements,” Human-centric Computing and Information Sciences, vol. 10, no 1, pp. 1-27, 2020.

96. L. Globa, M. Skulysh, and E. Siemens, “Conditionally Infinite Telecommunication Resource for Subscribers,” In M. Ilchenko et al., Advances in Information and Communication Technology and Systems. MCT 2019, LNNS 152, 2021, Springer, pp. 206–216, https://doi.org/10.1007/978-3-030-58359-0_11.

97. L. Globa, S. Sulima, M. Skulysh, and A. Zhuravel, “An approach for virtualized network slices planning in multiservice communication environment,” Information and Telecommunication Sciences, vol. 1, pp. 37–44, 2019.

98. ETSI: Network Functions Virtualisation (NFV); Infrastructure Overview. (ETSI GS NFV-INF 001 V1.1.1 (2015-01)). [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf

99. R. Russell, J. Stuart, and P. Norvig, “Artificial Intelligence: A Modern Approach,” 34-rd ed., New Jersey: Prentice Hall, 2020.

100. L. Globa and N. Gvozdetska, "Comprehensive Energy Efficient Approach to Workload Processing in Distributed Computing Environment," 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 2020, pp. 1-6, doi: 10.1109/BlackSeaCom48709.2020.9235010.

101. L.S. Globa, R.L. Novogrudska, and A.V. Koval, “Ontology Model of Telecom Operator Big Data,” in Proceedings of IEEE International Black Sea Conference on Communication and Netwoorking (BlackSeaCom), June 2018, pp. 1-5, doi:10.1109/BlackSeaCom.2018.8433710.

102. L. Globa, I. Svetsynska, and E. Volvach, “Computation of providing services integral quality index,” Information and Telecommunication Sciences, no. 1, pp. 34-42, 2018.

103. P. Tanwar, T. Prasad, and K. Dutt, “A Tour Towards the Various Knowledge Representation Techniques for Cognitive Hybrid Sentence Modeling and Analyzer,” International Journal of Informatics and Communication Technology (IJ-ICT, vol. 7, no. 3, pp. 124-134, 2018, DOI:10.11591/ijict.v7i3.pp124-134.

104. M. Rosing, W. Laurier, and S. Polovina, “The Value of Ontology,” The Complete Business Process Handbook, vol. 1, pp.91-100, 2018.

105. L. Globa, R. Novogrudska and O. Oriekhov, "Method of heterogeneous information resources structuring and systematizing for Internet portals development," in Eurocon 2013, July 2013, pp. 319-326, DOI: https://doi.org/10.1109/EUROCON.2013.6625003

106. M. Uschold, J. Bateman, M. Bennett, R. Brooks, M. Davis, A. Dima, at al., “Making the case for ontology,” Applied ontology, vol. 7, pp. 373-373, 2012,doi:10.3233/AO-2012-0110.

107. 5G security for transformed industries by Ericsson. 2018 [Online]. Available: https://www.ericsson.com/en/security

108. 3GPP TS 33.401, “3GPP System Architecture Evolution (SAE); Security architecture”. [Online]. Available: https://itectec.com/archive/3gpp-specification-ts-33-401

109. UMTS Security Awareness. 3GPP/PCG#13 Meeting. Seoul, Korea. 2004. [Online]: http://www.3gpp.org/ftp/PCG/PCG_13/DOCS/PDF/PCG13_19.pdf

110. L. Globa, N. Gvozdetska. “Experimental analysis of PCPB-2: Comprehensive Energy-Efficient Approach to Distributed Workload Processing in Communication Networks”, 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), DOI:10.1109/BlackSeaCom52164.2021.9527759

111. Globa L., Skulysh M., Romanov O., Nesterenko M. “Quality Control of Mobile Communication Management Services in a Hybrid Environment”, Advances in Information and Communication Technologies, 2019, pp.76-100. DOI:10.1007/978-3-030-16770-7_4.

112. Saeed, M.M., Alsharidah, M. “Enhancing the quality of communication of cellular networks using big data applications”. JBig Data 8, 143 (2021). https://doi.org/10.1186/s40537-021-00533-8

113. Arinze S., Alor M.O. “Determination of Quality of Service (QOS) in Mobile Network”, Scholars Journal of Engineering and Technology (SJET), October 2018, pp.288-292.

114. Sachan, S., Sharma, R., Sehgal, A. (2023). “Energy Efficiency and Scalability of 5G Networks for IoT in Mobile Wireless Sensor Networks”. In: Bhushan, B., Sharma, S.K., Kumar, R., Priyadarshini, I. (eds) 5G and Beyond. Springer Tracts in Electrical and Electronics Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-99-3668-7_8

115. Ciavaglia, L., Chemouil, P. & Maggs, B. “Techniques for smart and secure 5G softwarized networks”. Ann. Telecommun. 74, 543–544 (2019). https://doi.org/10.1007/s12243-019-00732-8

116. Priya, B., Malhotra, J. “iMnet: Intelligent RAT Selection Framework for 5G Enabled IoMT Network”. Wireless Pers Commun 129, 911–932 (2023). https://doi.org/10.1007/s11277-022-10163-9

117. Liu, Z., Liu, Q., Shea, R. et al. “Intelligent resource management for 5G”. Wireless Netw 26, 1535–1536 (2020). https://doi.org/10.1007/s11276-020-02270-x

118. Hernández-Chulde, C., Cervelló-Pastor, C. (2019). “Intelligent Optimization and Machine Learning for 5G Network Control and Management”. The PAAMS Collection. PAAMS 2019. Communications in Computer and Information Science, vol 1047. Springer, Cham. https://doi.org/10.1007/978-3-030-24299-2_33

119. Astrakhantsev A., Globa L, Novogrudska R, Skulysh M, Stryzhak O. “Improving resource allocation system for 5G networks”, 2021 International Conference on Information and Digital Technologies (IDT) – 2021. – P. 182-188.

120. Астраханцев А.А., Турута О.П., Турута О.В., Євдокименко М.О., Даніель Я.Д. 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)», Авторське право на твір №116973 від 10.03.2023

121. Astrakhantsev A.A., Davydiuk A. “Improved cluster management method for industrial “Internet Of Things” network”, Information and Telecommunication Sciences. – 2020. – №2. – P. 81-85.

122. 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.

123. Astrakhantsev A., Globa L, Sushko O., Davydiuk A. “Adjusting the parameters of machine learning algorithms to improve the accuracy of traffic classification”, Проблеми телекомунікацій. – 2023. – №1.

124. Astrakhantsev A., Globa L, Sushko O., Davydiuk A. “Feature set optimization for machine learning traffic classification in mobile networks”, BlackSeaCom 2023, July 2023.

125. “IP Network Traffic Flows Labeled with 75 Apps” (Internet: https://www.kaggle.com/jsrojas/ip-network-traffic-flows-labeled-with-87-apps).

126. S.A. Hinai and A.V. Singh, “Internet of things: Architecture, security challenges and solutions”, 2017 International Conference on Infocom Technologies and Unmanned Systems (ICTUS), Dubai, 2017, pp. 1-4.

127. H. Handoko, S.M. Isa. “High Availability Analysis with Database Cluster, Load Balancer and Virtual Router Redundancy Protocol”, 2018 3rd International Conference on Computer and Communication Systems.

128. “Database cluster and load balancing”, Link to resource: https://stackoverflow.com/questions/1163216/database-cluster-and-load-balancing

129. “Sharded Cluster Components”, Link to resource: https://docs.mongodb.com/manual/core/sharded-cluster-components/

130. “Failover Clustering and Always On Availability Groups (SQL Server)” – Link to resource: https://docs.microsoft.com/ru-ru/sql/database-engine/availability-groups/windows/failover-clustering-and-always-on-availability-groups-sql-server?view=sql-server- 2017

131. “Testing the productivity of NoSQL DBs” Internet: https://xakep.ru/2014/01/11/nosql-bd-test/

132. “The Radio Access Network and its resource allocation method calculated based on mixing fog”, Patent App. CN108243245A, 2020.

133. Debashish Purkayastha, Xavier De Foy, Robert G. Gazda. “Systems and methods to create slices at a cell edge to provide computing services”, Patent App. WO2018089417A1.

134. “Resource allocation methods based on mobile edge calculations”, Patent App. CN109041130A, 2021.

135. “A kind of data distribution method based on MEC auxiliary in 5G networks”, Patent App. CN108174421A, 2020.

136. “A kind of edge calculations method for 5G super-intensive networking scenes”, Patent App. CN107333267A, 2019.

137. “A kind of 5G method of mobile communication and system based on MEC and layering SDN”, Patent App. CN107404733A, 2020.

138. John Juha Antero Rasanen, Pekka Kuure. “Method and apparatus for implementing mobile edge application session connectivity and mobility”, - US Patent App. US16/072,901 (US 2019/0045409 A1)

139. Mehran Moshfeghi. “System and method for discount deal referral and reward sharing”, - US Patent App. US13/484,261 (US20120316939A1)

140. Willem Jacobus van Niekerk, Marc van Niekerk, Brendon van Niekerk, Ernst Kleinhans. “Method and system for online redistribution of data and rewards”, - US Patent App. US15/464,934 (US20170255981A1)

141. Dennis Detwiller, Robert Sparks. “Rewarding Users for Sharing Digital Content”, - US Patent App. US13/106,716 (US20120290308A1)

142. Pavel Mach, Zdenek Becvar. “Mobile Edge Computing: A Survey on Architecture and Computation Offloading”, https://arxiv.org/abs/1702.05309

143. Pham, Q. V., Fang, F., Ha, V. N., Piran, M. J., Le, M., Le, L. B., Hwang, W. J., & Ding, Z. (2020). “A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art”. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3001277

144. Canteaut, A. “Berlekamp-Massey algorithm”. In: van Tilborg, H.C.A. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, 2005. https://doi.org/10.1007/0-387-23483-7_24

145. “Reed Solomon Codes: A Classical Explanation”, 2022. https://xord.com/research/reed-solomon-codes-a-classical-explanation/

146. C. Wang, Sanjeev R. Kulkarni, “Exhausting Error-Prone Patterns in LDPC Codes”, Cornell University, 2006. https://doi.org/10.48550/arXiv.cs/0609046

147. Cédric Marchand, Emmanuel Boutillon. “LDPC decoder architecture for DVB-S2 and DVB-S2X standards”, 2015 IEEE International Workshop on Signal Processing Systems, SIPS 2015, IEEE, Oct 2015, Hangzhou, China.

148. Астраханцев А.А., Новіков Р.С. “Аналіз характеристик завадостійких кодів” [in rus], Системи обробки інформації. – Х.: ХУПС – 2013. – №9 (116). – С. 164-167.

149. Астраханцев А.А., Новіков Р.С. “Вибір параметрів LDPC кодів для каналів з АБГШ” [in rus], Системи обробки інформації. – Х.: ХУПС – 2014. – №1 (117). – С. 195-199.

150. J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, “A digital fountain approach to reliable distribution of bulk data,” in Proc. SIGCOMM, 1998.

151. M. Mitzenmacher, “Digital fountains: A survey and look forward,” in Proc. IEEE Information Theory Workshop, 24-29 Oct. 2004, pp. 271-276.

152. J. Byers, M. Luby, and M. Mitzenmacher, “Access multiple mirror sites in parallel: Using Tornado codes to A. S. Tanenbaum, *Computer Networks*, 3rd Ed., Prentice Hall PTR, New Jersey, 1996.

153. B. Sivasubramanian and H. Leib, “Fixed-rate Raptor codes over Rician fading channels,” *IEEE Trans. Vehicular Tech.*, Vol. 57, №6, November 2008, pp. 3905-3911.

154. E. Paolini, M. Varrella, M. Chiani, B. Matuz, and G. Liva, “Low-complexity LDPC codes with near-optimum performance over the BEC,” *ASMS 2008 4th*, pp. 274–282, 26–28 Aug. 2008.

155. T. Richardson and R. Urbanke, “Efficient encoding of low-density parity-check codes,” *IEEE Trans. Info. Theory* 47 (2), 2001, pp. 638-656.

156. X.-Y. Hu, E. Eleftheriou, D.-M. Arnold, and A. Dholakia, “Efficient implementations of the sum-product algorithm for decoding LDPC codes,” *Proc.IEEE Globecom Conf.* 2001, pp. 1036–1036E, Nov. 2001.

157. D. J. C. MacKay, “Fountain codes”, in *Proceedings of IEE Communications*, Vol. 152, Issue 6, December 2005, pp 1062-1068.

158. T. Stockhammer, H. Jenkac, T. Mayer, and W. Xu, “Soft decoding of LT-codes for wireless broadcast,” in *Proc. IST Mobile*, Dresden, Germany, 2005.

159. B. Sivasubramanian and H. Leib, “Fixed-rate Raptor code performance over correlated Rayleigh fading channels,” *Canadian Conference on Electrical and Computer Engineering*, 22-26 April 2007, pp. 912-915.

160. T. Richardson, “Error-floors of LDPC codes,” *Proceedings of the 41st Annual Conference on Communication, Control and Computing*, pp. 1426–1435, September 2003.

161. C. Di, D. Proietti, E. Telatar, T. Richardson, and R. Urbanke, “Finite length analysis of low-density parity-check codes on the binary erasure channel”, *IEEE Trans.Inform. Theory*, vol. 48, pp. 1570–1579, June 2002.

162. A. Orlitsky, K. Viswanathan, and J. Zhang, “Stopping Set Distribution of LDPC Code Ensembles,” *IEEE Trans. on Info. Theory*, Vol. 51, No. 3, pp. 929-953, March 2005.

163. O. Milenkovic, E. Soljanin, P. Whiting, “Asymptotic spectra of trapping sets in regular and irregular LDPC code ensemble,” *IEEE Trans. on Info. Theory*, Vol. 53, No. 1, pp. 38-55, Jan 2007.

164. M. Schwartz and A. Vardy, “On the stopping distance and the stopping redundancy of codes,” *IEEE Trans. on Info. Theory*, Vol. 52, No. 3, pp. 922-932, March 2006.

165. T. Tian, C. Jones, J. Villasenor, and R. D. Wesel, “Construction of irregular ldpc codes with low error floors,” in *Proceedings IEEE International Conference on Communications*, 2003.

166. V. Rathi. “On the asymptotic weight and stopping set distribution of regular LDPC ensembles,” *IEEE Trans. on Info. Theory*, Vol. 52, No. 9, pp. 4212-4218, Sep 2006.

167. K. Abdel-Ghaffar and J. Weber, “Stopping set enumerators of full-rank parity check matrices of Hamming codes,” in *Proc. IEEE Int’l Symp. Inform. Theory*, Seattle, WA, July 2006, pp. 1544–1548.

168. K.A.S. Abdel-Ghaffar and J.H. Weber, “Complete enumeration of stopping sets of full-rank parity-check matrices of hamming codes”, *IEEE Trans. Info. Theory*, vol. 53, no. 9, Sep. 2007.

169. M. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices,” *IEEE Trans. Inform. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2000.

170. H. Li, W. Huang and J. Dill, “A new approach to enumerating the smallest stopping sets in LDPC codes,” *Int’l Conf. Computing, Communications and Control*

171. Weizheng Huang. “Investigation on Digital Fountain Codes over Erasure Channels and Additive White Gaussian Noise Channels”, [Doctoral dissertation, Ohio University], June 2012. OhioLINK Electronic Theses and Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=ohiou1336067205

172. J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, “Construction of regular and irregular LDPC codes: geometry decomposition and masking,” *IEEE Trans. Inform. Theory*, vol. 53, Jan 2007, pp. 121–134.

173. Y. Kou, S. Lin, and M. P. C. Fossorier, “Low-density parity-check codes based on finite geometries: a rediscovery and new results,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, Nov. 2001, pp. 2711–2736.

174. IEEE Standard 802.16: A Technical Overview https://www.ieee802.org/16/docs/02/C80216-02_05.pdf

175. Gabriel Falcao, Vitor Silva, Jose Marinho. “LDPC Decoders for the WiMAX (IEEE 802.16e) Based on Multicore Architectures”, DOI: 10.5772/8265, December 2009

176. Hasani, Alireza. “High-throughput QC-LDPC codes for next-generation wireless communication systems”, DOI: 10.26127/BTUOpen-5819, February 2022

177. S. Kim, S. Lee, and S.-Y. Chung, “An efficient algorithm for ML Decoding of Raptor codes over the binary erasure channel,” IEEE Commun. Lett., vol. 12, Aug. 2008.

178. G. Liva, E. Paolini, and M. Chiani, “Performance versus overhead for fountain codes over $\mathbb{F}q$,” IEEE Commun. Lett., vol. 14, Feb. 2010.

179. Avani U Pandya and Sameer D. Trapasiya and Santhi S Chinnam. “AL-FEC Raptor Code Implementation Over 3GPP eMBMS Network”, 2013 https://api.semanticscholar.org/CorpusID:1947075

180. 3GPP TS 26.346 V10.4.0., ”Technical Specification Group Services and System Aspects: MBMS, Protocols and codecs”, 2012.

181. M. Cunche and V. Roca, “Improving the decoding of LDPC codes for the packet erasure channel with a hybrid Zyablov iterative decoding/Gaussian elimination scheme,” Centre de recherché INRIA Grenoble – Rhone-Alpes, March 2008.

182. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. https://tzi.com.ua/downloads/2.5-004-99.pdf

183. Jie Hu, Li Shen, Samuel Albanie, Gang Sun, Enhua Wu “Squeeze-and-Excitation Networks” arXiv:1709.01507, 2017.

184. M.S. Lutsenko, O.O. Kuznetsov, D.I. Prokopovich-Tkachenko, V.P. Zverev, “Comparative analysis of biometric cryptosystems” [in rus]. Kharkiv: Applied radio electronics. – 2018. – Volume 17, № 3, 4 - p.182-191.

185. A.A. Kuznetsov, R.V. Sergienko, A.A. Uvarova, “Fuzzy extractor on noise-tolerant codes for biometric cryptography” [in rus]. Kharkiv: Radio engineering. – 208 – Issue. 195 –c.224-234.

186. Y. Dodis. R. Ostrovsky, L. Reyzin, A. D. Smith., “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data”. SIAM J. Comput. – 2008. – Vol. 38, no. 1. – pp. 97-139.

187. Y. Dodis, L. Reyzin, A. Smith. “Fuzzy Extractors. A Brief Survey of Results from 2004 to 2006”. https://api.semanticscholar.org/CorpusID:62260600

188. A. Juels, M. Sudan., “A fuzzy vault scheme”. Des. Codes Cryptography. – 2006. – Vol. 38, no. 2. – P. 237-257.

189. Jain A.K., Ross A, Prabhakar S, “An introduction to biometric recognition”. IEEE Trans Circ Syst Video Technol – 2004, – 14:4 – 20.

190. Jain AK., Jain AK, Nandakumar K, “Biometric template security”. EURASIP J Adv Signal Process – 2008, – P. 1-17.

191. Upmanyu M, Namboodiri AM, Srinathan K, Jawahar CV. “Efficient biometric verification in encrypted domain”. ICB ‘09: Proc of the Third Int Conf on Biometrics – 2009, – p. 899-908.

192. Uludag U, Pankanti S, Prabhakar S, Jain AK, “Biometric cryptosystems: issues and challenges”. Proc IEEE 2004, –92(6) – P. 948-960.

193. Astrakhantsev A., G. Liashenko, A. Shcherbak, “Noise resistance of remote authentication via LTE network”, Information and Telecommunication Sciences – 2020 – Vol. 2, – P. 38-43.

194. G. Liashenko, A. Astrakhantsev, V. Chernikova, “Network steganography application for remote biometrie user authentication”, IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), – 2018, – pp.326-330.

195. Jayapriya P., Manimegalai R. R., Lakshmana Kumar R., “A Survey on Different Techniques for Biometric Template Protection”, Journal of Internet Technology Volume 21 (2020) No.5.

196. Poongodi P, Betty P, “A Study on Biometric Template Protection Techniques”, International Journal of Engineering Trends and Technology (IJETT) – Volume 7 Number 4, 2014

197. Edwin T. L. Rampine, Cynthia H. Ngejane, “A Brief Overview of Hybrid Schemes for Biometric Fingerprint Template Security”, In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), pages 340-346.

198. A. Sarkar, Binod K. Singh, “A Review on Different Biometric Template Protection Methods”, Recent Advances in Computer Science and Communications, Volume 14, Issue 5, 2021, pages: 1551 – 1572.

199. Чернікова В.Г., Астраханцев А.А., Ляшенко Г.Є. “Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока”, Системи озброєння і військова техніка, №1 (53), 2018, ст.195-202.

200. 3GPP [TS 38.214]: NR; Physical layer procedures for data (Internet: https://www.tech-invite.com/3m38/tinv-3gpp-38-214.html).

201. 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. – P. 543-546.

202. Iris Image Dataset “CASIA Iris Image Databases”, http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp

203. SIR-Smart Iris Recognition Dataset https://hycasia.github.io/dataset/casia-irisv4/

204. Tisse C., Martin L., Torres L., Robert M. “Person identification technique using human iris recognition” Proceedings ICASSP’05. V. 2. P. 949–952, 2005.

205. D. Dunn, W. Higgins “Optimal Gabor Filters for Texture Segmentation” IEEE Transactions On Image Processing,. Vol. 4, P. 947-964, 1995.

206. Yu L., Wang K., Zhang D. “Coarse Iris Classification Based on Box-Counting Method” Proc. IEEE Int. Conf. Image Processing, V.3. P.301–304, 2005.

207. Gui F., Qiwei L. “Iris localization scheme based on morphology and Gaussian filtering” IEEE Conf. on Signal-Image Technologies and Internet-Based System. Shanghai, China. P.798-803, 2007.

208. Silva-Mata F., Llano E.G., Alvarez Morales E.M. “A fast adaboosting based method for iris and pupil contour detection” CIARP’06. Cancun, Mexico. V.4225. P.127-136, 2006.

209. Shamsi M., Saad P., Ibrahim S., Rasouli A., Abdulrahim N. “A New Accurate Technique for Iris Boundary Detection” WSEAS Trans. Computers. V.9. N.6. P.654–663, 2010.

210. Gite H.R., Mahender C.N. “Iris code generation and recognition”, International Journal of Machine Intelligence, Volume 3, Issue 3, 2011, pp-103-107.

211. Noise resistance J. “Biometric personal identification system based on iris analysis.” United States Patent, Patent Number: 5,291,560, 1994.

212. Dipti.S.Randive, “Iris and Fingerprint Fusion for Biometric Identification”, International Journal of Computer Applications (0975 – 8887), Volume 77 – No.11, September 2013.

213. Andrii Astrakhantsev, Artem Popov, Oleksandr Popov, Aleksey Kulakov, “Method for securing image and electronic device performing same”, US Patent App. US17/378,032, 2021 (US20210342967A1). https://patents.google.com/patent/US20210342967A1/en

214. Locality Sensitive Hashing. Вікіпедія. Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/Locality-sensitive_hashing

215. Y.-L. Lai, J.Y. Hwang, Zhe Jin, S. Kim, “Symmetric keyring encryption scheme for biometric cryptosystem”, Information Sciences, Vol. 502, 2019, p. 492-509, https://www.sciencedirect.com/science/article/pii/S0020025519304815

216. Mazurczyk, W., Smolarczyk, M. & Szczypiorski, K. “Retransmission steganography and its detection”. Soft Comput 15, 505–515 (2011). https://doi.org/10.1007/s00500-009-0530-1

217. Handel, T.G., Sandford, M.T. “Hiding data in the OSI network model”. In: Anderson, R. (eds) Information Hiding. IH 1996. Lecture Notes in Computer Science, vol 1174. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-61996-8_29

218. Cauich, E., Gómez Cárdenas, R., Watanabe, R. “Data Hiding in Identification and Offset IP Fields”, In: Ramos, F.F., Larios Rosillo, V., Unger, H. (eds) Advanced Distributed Systems. ISSADS 2005. Lecture Notes in Computer Science, vol 3563. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11533962_11

219. W. Fraczek, W. Mazurczyk, K. Szczypiorski “Hiding Information in a Stream Control Transmission Protocol”, April 2011, Computer Communications 35(2), https://doi.org/10.48550/arXiv.1104.3333

220. Mazurczyk, W., Szaga, P. & Szczypiorski, K. “Using transcoding for hidden communication in IP telephony”, Multimed Tools Appl 70, 2139–2165 (2014). https://doi.org/10.1007/s11042-012-1224-8

221. W. Mazurczyk, “Lost Audio Packets Steganography: The First Practical Evaluation”, Security and Communication Networks, 2012, https://doi.org/10.48550/arXiv.1107.4076

222. Szczypiorski, K. “HICCUPS: Hidden communication system for corrupted networks”, In: International Multi-Conference on Advanced Computer Systems, pp. 31–40 (2003) https://www.researchgate.net/publication/228957814_HICCUPS_Hidden_communication_system_for_corrupted_networks

223. T. Saaty, "Decision making with the analytic hierarchy process", International Journal of Services Sciences, vol. 1, no. 1, pp. 83-98, 2008.

224. New Study Reveals Alarming Increase in Spam Call Statistics. https://techjury.net/blog/spam-call-statistics/ .

225. “20+ Surprising Robocalls Statistics That You Need To Know For 2022”, https://www.enterpriseappstoday.com/stats/robocalls-statistics.html .

226. “Basics to Know About Call Authentication”, https://blog.hiya.com/call-authentication

227. “8 Popular Prank Call Websites and How They Work”, https://www.makeuseof.com/tag/popular-prank-call-websites-how-they-work/

228. “Understanding STIR/SHAKEN and Call Spoofing”, https://blog.hiya.com/stir/shaken-does-it-reduce-illegal-call-spoofing

229. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 version 11.5.1 Release 11) https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/11.05.01_60/ts_133102v110501p.pdf

[230] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman. “Vggface2: A dataset for recognising faces across pose and age”, 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018).

[231] Ira Kemelmacher-Shlizerman, Steve Seitz, Daniel Miller, Evan Brossard “The MegaFace Benchmark: 1 Million Faces for Recognition at Scale”. arXiv:1512.00596, 2015.

232. Rupesh Kumar Rout, “A Survey on Object Detection and Tracking Algorithms”, National Institute of Technology Rourkela http://ethesis.nitrkl.ac.in/4836/1/211CS1049.pdf

233. Paul Viola, Michael Jones. “Rapid object detection using a boosted cascade of simple features”, Accepted conference on computer vision and pattern recognition 2001 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.6807

[234] G. B. Huang, M. Ramesh, T. Berg, E. Learned-Miller. “Labelled faces in the wild: A database for studying face recognition in unconstrained environments”, Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition, Erik Learned-Miller and Andras Ferencz and Frédéric Jurie, Oct 2008, Marseille, France.

235. Алгоритм Віоли-Джонс. Вікіпедія. Електронний ресурс. Режим доступу:https://en.wikipedia.org/wiki/Viola%E2%80%93Jones_object_detection_framework#cite_note-1

236. Feature detection. Вікіпедія. Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/Feature_detection_%28computer_vision%29

237. K-means_clustering. Вікіпедія. Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/K-means_clustering

238. k-dimensional tree. Вікіпедія. Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/K-d_tree

239. Random sample consensus. Вікіпедія. Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/RANSAC

240. Juliang Jiang, Jing Cao, Xiangdong Ruan, “Password protection using pattern”, https://patents.google.com/patent/US9111073B1/en (US 9111073 B1).

241. Eugene Evanitsky “Portable security system built into cell phones”, https://patents.google.com/patent/US8744522B2/en (US 8744522 B2).

242. Mozilla Firefox extension “Saved Password Editor”, Internet: https://addons.mozilla.org/en-US/firefox/addon/saved-password-editor

243. Астраханцев А.А., Дорожан А.В., Вовк О.О. “Дослідження характеристик методів приховування з використанням НЗБ на тлі адитивного шуму”, Вісник НТУ «ХПІ». – 2012. – №18. – С. 37-40.

244. Астраханцев А.А., Дорожан А.В., Вовк О.О. “Дослідження стійкості методів приховування інформації в нерухомих зображеннях” [in rus], Системи обробки інформації. – Х.: ХУПС – 2012. – №2. – С. 104-109.

245. 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.

246. 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.

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

248. 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.

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

250. Frączek W., Szczypiorski K. “StegBlocks: Ensuring perfect undetectability of network steganography”, Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference. Toulouse, France, 24-27 August, 2015. – IEEE, 2015. – P. 436-441. – DOI: 10.1109/ARES.2015.22.

251. Bąk P., Bieniasz J., Krzemiński M., Szczypiorski K. “Application of Perfectly Undetectable Network Steganography Method for Malware Hidden Communication”, Frontiers of Signal Processing (ICFSP): Proceedings of the 4th International Conference. Poitiers, France, 24-27 September, 2018 – IEEE, 2018. – P. 34-38. – DOI: 10.1109/ICFSP.2018.8552057.

252. Рубан І.В., Смирнов А.А. “Можливості використання заголовків пакетів мережного рівня базової моделі мережної взаємодії OSI/ISO в якості

стегоконтейнера" [in rus], Системи озброєння і військова техніка. – 2014. – № 3(39). – С. 138-141.

253. Mazurczyk W., Wendzel S., Villares I.A., Szczypiorski K. "On Importance of Steganographic Cost For Network Steganography", Security and Communication Networks. – 2016. – Vol. 9., No.8. – P. 781-790. – DOI: 10.1002/sec.1085.

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

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

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

257. Astrakhantsev A., Shchur O., Korobov M., Oliynyk A. "Electronic device and method for providing user information", US Patent App. US15/778,818, 2018, (EP3367277A1). https://patents.google.com/patent/EP3367277A1/en

258. Astrakhantsev A., Vovk O. "The concept of steganographic algorithm which has high performance of characteristics defined as significant", 2014 1st International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2015 – Conference Proceedings. –P. 177-179.

259. Astrakhantsev A., Liashenko, G. "Data protection management process during remote biometric authentication", System Research and Information Technologies, 2022, 2022(3), pp. 71–85.

260. Astrakhantsev A., Vovk O. “New steganographic method: Development and comparison with the most relevant”, 2015 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2015 – Conference Proceedings. – P. 237-240.

261. Yang, Shuo and Luo, Ping and Loy, Chen Change and Tang, Xiaoou. “Wider face: A Face Detection Benchmark”, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.

262. Diederik P. Kingma, Jimmy Ba “Adam: A Method for Stochastic Optimization”, Cornell University, 2014, arXiv:1412.6980.

263. 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, P. 257–273.

264. Astrakhantsev A., Shcherbak A., Shcherbak O., Liashenko G. “Biometric templates noise immunity during transmission by mobile networks”, CEUR Workshop Proceedings, 2021, v.2923, c. 175–181.

265. Astrakhantsev A., Popov A., Popov O., Pedan S., Shapoval I., Konoval O. “Electronic device and method of operating the same”, - US Patent App. US18/163,589, 2023, https://patents.google.com/patent/US20230259652A1/en

266. Theresa Brown, Nedlaya Francisco. “Universal personal medical database access control”, - US Patent App. US12/354,739, https://patents.google.com/patent/US20100179831A1/en (US20100179831 A1)

267. Kristin Estella, Lauter Mihir, Bellare Josh Benaloh, Melissa E. Chase. “User-specified sharing of data via policy and/or inference from a hierarchical cryptographic store”, - US Patent App. US12/413,445, https://patents.google.com/patent/US8837718B2/en (US8837718 B2)

268. Malik Hammoutene, Milan Petkovic, Claudine V. Conrado. “Cryptographic role-based access control”, - PCT/IB2006/053283, https://patents.google.com/patent/WO2007031955A2/en (WO2007031955 A2)

269. Abdelkrim HebbarAbderrahmane Maaradji. “Medical data access system”, - US Patent App. US13/379,414, (US 8874067 B2) https://patents.google.com/patent/US8874067B2/en

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

271. Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun “Deep 1Residual Learning for Image Recognition”. arXiv:1512.03385, 2015.

272. A. Howard, M. Zhu, Bo Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, H. Adam “MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications”, arXiv:1704.04861, 2017.

273. Joseph Redmon, Santosh Divvala, Ross Girshick, Ali Farhadi “You Only Look Once: Unified, Real-Time Object Detection”, arXiv:1506.02640, 2015.

274. W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C-Y Fu, A. Berg “SSD: Single Shot MultiBox Detector”, arXiv:1512.02325, 2016.

275. E. Bochinski, V. Eiselein, T. Sikora. “High-Speed Tracking-by-Detection Without Using Image Information”, In International Workshop on Traffic and Street Surveillance for Safety and Security at IEEE AVSS 2017.

276. Hamed Kiani Galoogahi, Ashton Fagg, Simon Lucey “Learning Background-Aware Correlation Filters for Visual Tracking”, arXiv:1703.04590, 2017.

277. Yandong Wen, Kaipeng Zhang, Zhifeng Li and Yu Qiao. “A Discriminative Feature Learning Approach for DeepFace Recognition”. The Chinese University of Hong Kong, ShaTin, Hong Kong, 2016.

278. Jiankang Deng, Jia Guo, Niannan Xue, Stefanos Zafeiriou “ArcFace: Additive Angular Margin Loss for Deep Face Recognition”, Cornell University arXiv:1801.07698, 2018.

279. Yu. A. Malkov, D. A. Yashunin “Efficient and robust approximate nearest neighbour search using hierarchical navigable small world graphs”, IEEE Trans. Pattern Anal. Mach. Intell. 2018, 42, 824–836 arXiv:1603.09320, 2016.

280. Sanghyun Woo, Jongchan Park, Joon-Young Lee, In So Kweon “CBAM: Convolutional Block Attention Module”, Sanghyun Woo, Jongchan Park, Joon-Young Lee, In So Kweon “CBAM: Convolutional Block Attention Module, arXiv:1807.06521, 2018.

281. D. Yi, Z. Lei, S. Liao, and S. Z. Li. “Learning face representation from scratch”, Center for Biometrics and Security Research & National Laboratory of Pattern Recognition Institute of Automation, Chinese Academy of Sciences arXiv:1411.7923, 2014.

282. M. Shafiq, X. Yu, Asif Ali Laghari, D. Wang. “Effective Feature Selection for 5G IM Applications Traffic Classification”. Mobile Inf. Syst. (2017), https://doi.org/10.1155/2017/6805056.

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

284. Progonov D., Popov O., Astrakhantsev A., Motchanyi A. “Device and method for acquiring biosignal”, WO2024096391A1.

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

286. Astrakhantsev 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.

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

288. 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.

289. Astrakhantsev A., Pedan S. “Improving user security during a call”, Radioelectronic and Computer Systems, 2024, no. 2(110), pp.173-185.

290. 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.

291. 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.

292. Globa, L., Novogrudska, R., Koval, A., & Senchenko, V. (2018). Examples of ontology model usage in engineering fields. Ontology in Information Science. DOI: 10.5772/intechopen.74369.

293. Nguyen, G. T., & Rieu, D. (1989). Schema evolution in object-oriented database systems. Data & Knowledge Engineering, 4(1), pp. 43-67. DOI: https://doi.org/10.1016/0169-023x(89)90004-9.

294. Guarino, N., Oberle, D., & Staab, S. (2009). What is an ontology?. In Handbook on ontologies (pp. 1-17). Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-540-92673- 3_0.

ДОДАТОК А. Акти впровадження

Товариство з обмеженою відповідальністю «лайфселл»
вул. Солом'янська, 11, літера "А", м. Київ, 03110, Україна
тел.: +380 (44) 233-31-31, e-mail: reception@lifecell.com.ua,
web: www.lifecell.ua
Код ЄДРПОУ: 22859846

«Затверджую»
Начальник відділу пакетної та IP мереж
ТОВ "lifecell"
Кобиляцький Сергій
_____
«05» березня 2024р.

АКТ

Впровадження удосконаленої технології обробки даних у вузлі інфокомунікаційної мережі

Ми, що нижче підписалися, представники Національного технічного університету України «Київський політехнічний інститут» – зав. каф. Інформаційних технологій в телекомунікаціях (ІТТ), д.т.н. проф. Скуліш М.А. , проф. каф. ІТТ, д.т.н. Глоба Л.С., доц. каф. ІТТ, к.т.н. Астраханцев А.А. та представники ТОВ "Lifecell" – склали цей акт про те, що розроблену співробітниками НТУУ «КПІ» технологію обробки даних у вузлі мережі (програмне забезпечення, протоколи), було випробувано на підприємстві ТОВ "Lifecell" (фрагмент тестової мережі) для підвищення ефективності обробки даних на тестовому вузлі мережі підприємства.

Технологія використовує розроблені Астраханцев А.А. результати дисертаційної роботи на здобуття ступеня доктора наук на тему: МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТА ЯКОСТІ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ».

На основі розроблених методу, програмного забезпечення, протоколів проведено апробацію засобів удосконаленої класифікації трафіка та розподілу навантаження для мобільних периферійних обчислень (МЕС).

Вдосконалені методи класифікації трафіка та розподілу навантаження з використанням апаратних засобів 5G мережі компанії використано в тестовому пілот-проекті модернізації системи надання мобільних периферійних обчислень.

Запропоновані рішення виявилися ефективними і надали можливість зменшити на 15% обсяг мережних ресурсів, необхідних для організації мобільних периферійних обчислень.

Адреса для листування:
м. Київ, 03110,
вул. Солом'янська, 11, літера "А"

Товариство з обмеженою відповідальністю «лайфселл»
вул. Солом'янська, 11, літера "А", м. Київ, 03110, Україна
тел.: +380 (44) 233-31-31, e-mail: reception@lifecell.com.ua,
web: www.lifecell.ua
Код ЄДРПОУ: 22859846

Від компанії:
ТОВ "Lifecell"

_____ Є. Олійник

_____ І. Іванов

Від НТУУ «КПІ»

_____ проф. Скуліш М.А.

_____ проф. Глоба Л.С.

_____ доц. Астраханцев А.А.

Адреса для листування:
м. Київ, 03110,
вул. Солом'янська, 11, літера "А"

ЗАТВЕРДЖУЮ

Проректор з навчальної роботи
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Тетяна ЖЕЛЯСКОВА
"__" _____ 2024 р.

АКТ

впровадження результатів дисертаційної роботи Астраханцева Андрія Анатолійовича
на тему "Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв'язку" у навчальний процес кафедри Інформаційних технологій в телекомунікаціях

Ми, що нижче підписалися, представники Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» – завідувач кафедри Інформаційних технологій в телекомунікаціях, д.т.н., проф. Скулиш М.А., проф. каф. Інформаційних технологій в телекомунікаціях, д.т.н. проф. Глоба Л.С., голова методичної комісії НН ІТС, доц. каф. Інформаційних технологій в телекомунікаціях, к.т.н., доц. Правило В.В. – склали цей акт про те, що ряд наукових та практичних результатів дисертаційної роботи к.т.н., доц. Астраханцева А.А. впроваджені в навчальному процесі кафедри Інформаційних технологій в телекомунікаціях, зокрема:

- досліджувані та вдосконалений методи завадостійкого кодування пакетів в мобільній мережі використані в лекційних заняттях та комп'ютерних практикумах з дисципліни «Завадостійке кодування в інформаційно-комунікаційних мережах».
- нові методи управління приватними даними користувача для забезпечення захищеності даних під час реалізації нових сервісів використані в лекційних заняттях та комп'ютерних практикумах з дисципліни «Основи побудови захищених банківських інформаційно-телекомунікаційних систем».

- запропонований метод взаємної автентифікації користувачів під час дзвінка, метод наскрізного шифрування під час дзвінка та метод формування вектору ознак біометричних характеристик користувача в лекційних заняттях та комп'ютерних практикумах з дисципліни «Основи криптографічного захисту інформації»

Це дозволило підвищити рівень підготовки бакалаврів та магістрів за напрямком 172 «Електронні комунікації та радіотехніка», освітньо-професійної програми «Інформаційно-комунікаційні технології».

д.т.н., проф.,
завідувач кафедри ІТТ _____ Скулиш М.А.

д.т.н., проф., _____ Глоба Л.С.

к.т.н., доц., _____ Правило В.В.