Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Кваліфікаційна наукова
праця на правах рукопису

ЛЯШЕНКО ГАЛИНА ЄВГЕНІЇВНА

УДК 621.391
(індекс)

ДИСЕРТАЦІЯ

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ ВІДДАЛЕНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Спеціальність: 172 – Електронні комунікації та радіотехніка

Галузь знань: 17 – Телекомунікації та радіотехніка

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____Г.Є.Ляшенко

Науковий керівник
Астраханцев Андрій Анатолійович
кандидат технічних наук, доцент

Харків 2024

АНОТАЦІЯ

Ляшенко Г.Є. Методи підвищення ефективності систем віддаленої біометричної автентифікації в телекомунікаційних мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 172 Електронні комунікації та радіотехніка. – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2024.

В роботі розв’язано науково-практичну задачу вдосконалення систем віддаленої біометричної автентифікації в телекомунікаційних мережах шляхом застосування методів мережної стеганографії.

Мета дослідження – підвищення ефективності систем віддаленої біометричної автентифікації в телекомунікаційних мережах за рахунок застосування методів мережної стеганографії. Визначений метод біометричної автентифікації дозволяє підвищити завадостійкість та ефективність систем віддаленої автентифікації в телекомунікаційних мережах, а вдосконалений метод передачі інформації телекомунікаційними системами під час автентифікації дозволяє підвищити захищеність передачі інформації.

Задачі дослідження:

− Визначити переважний за набором ознак метод біометричної автентифікації.

− Визначити переважний метод формування біометричного шаблону та запропонувати рекомендації по його застосуванню і захисту.

− Визначити переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії. Вдосконалити метод

передачі біометричної інформації шляхом застосування мережної стеганографії для підвищення захищеності віддаленої автентифікації.

− Запропонувати методи підвищення завадостійкості під час передачі даних користувача.

Об’єкт дослідження – процес обробки, захисту та прихованої передачі біометричних даних в телекомунікаційних системах та мережах.

Предмет дослідження – математичні моделі, методи та засоби забезпечення ефективності системи віддаленої біометричної автентифікації в каналах зв’язку.

Методи дослідження – методи математичного моделювання; методи теоретико-множинного підходу; методи цифрової обробки сигналів – для підготовки інформаційного сигналу та сигналу-контейнера для вбудовування прихованих даних; методи багатокритеріальної оптимізації – для вибору оптимального за зазначеними критеріями методів.

Наукова новизна результатів досліджень:

− Вперше визначений переважний за критерієм завадозахищеності та ймовірності помилки метод біометричної автентифікації, відмінністю якого є врахування стійкості до завад. Це дало змогу підвищити завадостійкість та ефективність систем віддаленої автентифікації в телекомунікаційних мережах.

− Вдосконалено метод обробки біометричних даних користувача шляхом обрання оптимального методу захисту біометричного шаблону. Це дозволило підвищити точність автентифікації.

− Вперше визначений переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії. Це дало змогу покращити ефективність системи віддаленої автентифікації за рахунок застосування визначеного методу.

− Вдосконалено метод віддаленої біометричної автентифікації в телекомунікаційних мережах, відмінністю якого є послідовне застосування методів формування біометричного шаблону, узгодження параметрів передачі

з якістю каналу зв’язку, завадостійкого кодування та мережної стеганографії. Це дозволило підвищити захищеність передачі інформації та завадостійкість.

Практична значущість результатів дослідження.

Запропонований комплексний критерій оцінювання стеганографічних систем передачі інформації може бути використаний для вибору оптимального методу прихованої передачі інформації в залежності від умов передачі та сфери застосування системи. Рекомендації щодо вибору ефективного методу для побудови стеганографічної системи дозволяють підвищити ефективність роботи системи прихованої передачі інформації, зокрема надають можливості для більш раціонального використання пропускної здатності контейнерів. Використання запропонованих методів формування біометричного шаблону, завадостійкого кодування та адаптації системи передачі інформації до зовнішніх впливів дозволяє підвищити швидкість, завадостійкість та захищеність від атак системи віддаленої біометричної автентифікації.

Отримані результати впроваджені в навчальний процес Харківського національного університету радіоелектроніки, зокрема, на кафедрі інформаційно-мережної інженерії. Вдосконалений метод передачі автентифікаційної інформації телекомунікаційними мережами для підвищення захищеності передачі інформації та завадостійкості використано в лекційних та лабораторних заняттях з дисциплін «Безпека інфокомунікаційних мереж» та «Інформаційна безпека інноваційної діяльності». Дослідження переважного за критеріями завадозахищеності та ймовірності помилки методу біометричної автентифікації, відмінністю якого є стійкість до типових завад в каналах зв’язку, використано в лекційних та лабораторних заняттях з дисциплін «Інформаційна безпека електронного бізнесу» та «Електронні платіжні системи». Визначений в роботі переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії використано в дисциплінах «Безпека інфокомунікаційних мереж» та

«Програмування мережних послуг». Це підтверджено відповідним актом впровадження [додаток В].

Ключові слова: методи біометричної автентифікації, розпізнавання, стійкість, зображення, багатокритеріальна оптимізація, мережна стеганографія, завадостійкість, бездротові канали, мережі, системи передачі даних, показник якості, захист інформації, методи захисту, стеганографія, інформаційний канал.

СПИСОК ОПУБЛІКОВАНИХ РОБІТ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ляшенко Г. Є. Дослідження ефективності методів біометричної автентифікації / Г. Є. Ляшенко, А. А. Астраханцев // Системи обробки інформації. – 2017. – № 2(148). – С. 111–114. – Режим доступу: https://doi.org/10.30748/soi.2017.148.20. (Фахове видання. Належить до категорії Б)

2. Аналіз скритності та стійкості до шуму в каналах зв'язку методів мережної стеганографії / А. О. Щербак, А. А. Астраханцев, О.В. Щербак, Г.Є. Ляшенко // Проблеми телекомунікацій. – 2018. – No. 2(23). – P. 89–98. – Mode of access: https://doi.org/10.30837/pt.2018.2.07. (Фахове видання. Належить до категорії Б)

3. Чернікова В. Г. Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока / В. Г. Чернікова, А. А. Астраханцев, Г. Є. Ляшенко // Системи озброєння і військова техніка. – 2018. – № 1(53). – С. 195–202. – Режим доступу: https://doi.org/10.30748/soivt.2018.53.28. (Фахове видання. Належить до категорії Б)

4. G. Liashenko, A. Astrakhantsev and V. Chernikova, "Network steganography application for remote biometrie user authentication," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 326-330, doi: 10.1109/DESSERT.2018.8409153.(Scopus)

5. Ляшенко Г. Є. Дослідження методів розпізнавання облич / Г.Є. Ляшенко, О.І. Даниленко // НІСТ'2019 Міжнародна науково-практична конференція «Наукоємні технології в інфокомунікаціях»: Матеріали III Міжнародної науково-практичної конференції. - МАДРИД, Харків. - 2019. - С.85-86.

6. Liashenko, G., Astrakhantsev, A. (2021). Implementation Biometric Data Security in Remote Authentication Systems via Network Steganography. In:

Ilchenko, M., Uryvsky, L., Globa, L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-030-58359-0_14.(Scopus)

7. G. Liashenko and A. Astrakhantsev, "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&T), Kyiv, Ukraine, 2019, pp. 543-546, doi: 10.1109/PICST47496.2019.9061524.(Scopus)

8. Astrakhantsev A. Noise resistance of remote authentication via lte network / Andrii Astrakhantsev, Galyna Liashenko, Anna Shcherbak // Information and telecommunication sciences. – 2020. – No. 2. – P. 38–43. – Mode of access: https://doi.org/10.20535/2411-2976.22020.38-43 . (Фахове видання. Належить до категорії Б)

9. Дослідження завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами / А. О. Щербак, А. А. Астраханцев, О.В. Щербак, Г.Є. Ляшенко // Проблеми телекомунікацій.-2020. - Вып. №1(26). - С. 63-72. (Фахове видання. Належить до категорії Б)

10. Biometric templates noise immunity during transmission by mobile networks / Anna Shcherbak, Andrii Astrakhantsev, Oleg Shcherbak, Galyna Liashenko // Cybersecurity providing in information and telecommunication systems. – 2021. – P. 175–181.(Scopus)

11. Ляшенко Г. Є. Аналіз методів захисту біометричних шаблонів / Г. Є. Ляшенко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тез. доп. дванадцатої міжнародної науково-технічної конференції, 27–28 квітня 2022 р. – Т. 1. – Баку–Харків–Жиліна, 2022. – С. 77.

12. 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. – Mode of access:

https://doi.org/10.20535/SRIT.2308-8893.2022.3.05 (Фахове видання. Належить до категорії A. Scopus)

13. Ляшенко Г. Система для оцінки роботи методів формування біо-хешу / Галина Ляшенко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей десятої міжнародної науково-технічної конференції 9 – 10 квітня 2020 року. – 2020. – Т. 1. – С. 82.

14. Ляшенко Г. Моделювання методів мережної стеганографії для підвищення надійності віддаленої аутентифікації / Г. Ляшенко, А. Щербак // Проблеми інформатизації. Тези доповідей шостої міжнародної науково-технічної конференції 14 – 16 листопада 2018 року. – 2018. – С. 16.

15. Ляшенко Г. Є. Аналіз можливих атак на систему біометричної автентифікації / Г.Є. Ляшенко // Проблеми інформатизації : тези доп. 7-ї міжнар. наук.-техн. конф., 13-15 листопада 2019 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2019. – С. 90.

16. Маслакова Н. Забезпечення безпеки систем «розумного будинку» / Н. Маслакова, Г. Ляшенко // Проблеми інформатизації. Тези доповідей дев’ятої міжнародної науково-технічної конференції 18 – 19 листопада 2021 року. – 2021. – Т. 1. – С. 37.

17. Ляшенко Г. Модель впливу завад на біометричні шаблони при передачі мобільними мережами / Г.Ляшенко // Проблеми інформатизації. Тези доповідей восьмої міжнародної науково-технічної конференції. – 2020. – Т. 2. – С. 65.

18. Ляшенко Г. Ефективність методів біометричної автентифікації / Г. Ляшенко, А. Астраханцев // Тези доповідей міжнародної науково-практичної конференції "Проблеми і перспективи розвитку IT-індустрії" 20-21 квітня 2017 р. – 2017. – С. 53.

ABSTRACT

Liashenko G.Y. Methods of increasing the efficiency of the remote biometric authentication system in telecommunication networks. – Qualifying scientific work on manuscript rights.

The dissertation for the competition PhD scientific degree on a specialty 172 "Telecommunications and Radio Engineering". – Kharkiv National University of Radio Electronics, Ministry of Education and Science of Ukraine, Kharkiv, 2024.

The work solves the scientific and practical problem of improving remote biometric authentication systems in telecommunication networks by using network authentication methods.

The purpose of this research is to improve the effectiveness of remote biometric authentication systems in telecommunication systems. This can be done through the use of network steganography methods. The specified method of biometric authentication allows to increase the immunity and efficiency of remote authentication systems in telecommunication systems. The improved method of information transmission by telecommunication systems during authentication allows us to increase the security of information transmission.

Objectives of the study:

− Determine the preferred biometric authentication method based on the set of features.

− Determine the preferred method for generating a biometric template and offer recommendations for its application and protection.

− Determine the preferred method for network steganography based on the criteria of speed, secrecy, and bandwidth. Improve the method for transmitting biometric information by using network steganography to increase the security of remote authentication.

− Propose methods for increasing noise immunity during the transmission of user data.

The object of research is the process of processing, protection and covert transmission of biometric data in telecommunication systems and networks.

The subject of the research is mathematical models, methods and means of ensuring the effectiveness of the remote biometric authentication system in communication channels.

Research methods – mathematical modeling methods; methods of the theoretical-multiple approach; methods of digital signal processing - for preparing an information signal and a container signal for embedding hidden data; multi-criteria optimization methods - for choosing the optimal methods according to the specified criteria.

Scientific novelty of research results:

For the first time, a biometric authentication method has been determined that is preferable in terms of interference immunity and error probability, the difference of which is the consideration of interference resistance. This made it possible to increase the interference resistance and efficiency of remote authentication systems in telecommunication networks.

The method of processing user biometric data has been improved by choosing the optimal method of protecting the biometric template. This made it possible to increase the accuracy of authentication.

For the first time, a network steganography method has been determined that is preferable in terms of speed, secrecy, and bandwidth. This made it possible to improve the efficiency of the remote authentication system by using the specified method.

The method of remote biometric authentication in telecommunication networks has been improved, the difference of which is the consistent application of methods for forming a biometric template, matching transmission parameters with the quality

of the communication channel, noise-resistant coding, and network steganography. This allowed to increase the security of information transmission and noise immunity.

Practical significance of the research results:

The proposed comprehensive criterion for evaluating steganographic information transmission systems can be used to select the optimal method of hidden information transmission. Depending on the conditions of transmission and the field of application system. Recommendations for choosing an effective method for building a steganographic system allow to increase the efficiency of the system of hidden transmission of information, in particular, provide opportunities for more rational use of the capacity of containers. The use of the proposed methods of biometric template formation, interference-resistant coding and adaptation of the information transmission system to external influences allows to increase the speed, immunity and protection against attacks of the remote biometric authentication system.

Keywords: biometric authentication methods, recognition, vulnerability, image, multi-criteria optimization, network steganography, noise immunity, wireless channels, networks, data transmission networks, quality indicator, information protection, protection methods, steganography, information channel.

List of publications of the applicant

Ляшенко Г. Є. Дослідження ефективності методів біометричної автентифікації / Г. Є. Ляшенко, А. А. Астраханцев // Системи обробки інформації. – 2017. – № 2(148). – С. 111–114. – Режим доступу: https://doi.org/10.30748/soi.2017.148.20. (Фахове видання. Належить до категорії Б)

2. Аналіз скритності та стійкості до шуму в каналах зв'язку методів мережної стеганографії / А. О. Щербак, А. А. Астраханцев, О.В. Щербак, Г.Є. Ляшенко // Проблеми телекомунікацій. – 2018. – No. 2(23). – P. 89–98. – Mode of access: https://doi.org/10.30837/pt.2018.2.07. (Фахове видання. Належить до категорії Б)

3. Чернікова В. Г. Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока / В. Г. Чернікова, А. А. Астраханцев, Г. Є. Ляшенко // Системи озброєння і військова техніка. – 2018. – № 1(53). – С. 195–202. – Режим доступу: https://doi.org/10.30748/soivt.2018.53.28. (Фахове видання. Належить до категорії Б)

4. G. Liashenko, A. Astrakhantsev and V. Chernikova, Network steganography application for remote biometrie user authentication, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 326-330, doi: 10.1109/DESSERT.2018.8409153.(Scopus)

5. Ляшенко Г. Є. Дослідження методів розпізнавання облич / Г.Є. Ляшенко, О.І. Даниленко // НІСТ'2019 Міжнародна науково-практична конференція «Наукоємні технології в інфокомунікаціях»: Матеріали III Міжнародної науково-практичної конференції. - МАДРИД, Харьков. - 2019. - С.85-86.

6. Liashenko, G., Astrakhantsev, A. (2021). Implementation Biometric Data Security in Remote Authentication Systems via Network Steganography. In:

Ilchenko, M., Uryvsky, L., Globa, L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-030-58359-0_14.(Scopus)

7. G. Liashenko and A. Astrakhantsev, "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&T), Kyiv, Ukraine, 2019, pp. 543-546, doi: 10.1109/PICST47496.2019.9061524.(Scopus)

8. Astrakhantsev A. Noise resistance of remote authentication via lte network / Andrii Astrakhantsev, Galyna Liashenko, Anna Shcherbak // Information and telecommunication sciences. – 2020. – No. 2. – P. 38–43. – Mode of access: https://doi.org/10.20535/2411-2976.22020.38-43 . (Фахове видання. Належить до категорії Б)

9. Дослідження завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами / А. О. Щербак, А. А. Астраханцев, О.В. Щербак, Г.Є. Ляшенко // Проблеми телекомунікацій.-2020. - Вып. №1(26). - С. 63-72. (Фахове видання. Належить до категорії Б)

10. Biometric templates noise immunity during transmission by mobile networks / Anna Shcherbak, Andrii Astrakhantsev, Oleg Shcherbak, Galyna Liashenko // Cybersecurity providing in information and telecommunication systems. – 2021. – P. 175–181.(Scopus)

11. Ляшенко Г. Є. Аналіз методів захисту біометричних шаблонів / Г. Є. Ляшенко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тез. доп. дванадцатої міжнародної науково-технічної конференції, 27–28 квітня 2022 р. – Т. 1. – Баку–Харків–Жиліна, 2022. – С. 77.

12. 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. (Фахове видання. Належить до категорії A. Scopus)

13. Ляшенко Г. Система для оцінки роботи методів формування біо-хешу / Галина Ляшенко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей десятої міжнародної науково-технічної конференції 9 – 10 квітня 2020 року. – 2020. – Т. 1. – С. 82.

14. Ляшенко Г. Моделювання методів мережної стеганографії для підвищення надійності віддаленої аутентифікації / Галина Ляшенко, Анна Щербак // Проблеми інформатизації. Тези доповідей шостої міжнародної науково-технічної конференції 14 – 16 листопада 2018 року. – 2018. – С. 16.

15. Ляшенко Г. Є. Аналіз можливих атак на систему біометричної автентифікації / Г. Є. Ляшенко // Проблеми інформатизації : тези доп. 7-ї міжнар. наук.-техн. конф., 13-15 листопада 2019 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2019. – С. 90.

16. Маслакова Н. Забезпечення безпеки систем «розумного будинку» / Н. Маслакова, Г.Ляшенко // Проблеми інформатизації. Тези доповідей дев’ятої міжнародної науково-технічної конференції 18 – 19 листопада 2021 року. – 2021. – Т. 1. – С. 37.

17. Ляшенко Г. Модель впливу завад на біометричні шаблони при передачі мобільними мережами / Галина Ляшенко // Проблеми інформатизації. Тези доповідей восьмої міжнародної науково-технічної конференції. – 2020. – Т. 2. – С. 65.

18. Ляшенко Г. Ефективність методів біометричної автентифікації / Галина Ляшенко, Андрій Астраханцев // Тези доповідей міжнародної науково-практичної конференції "Проблеми і перспективи розвитку IT-індустрії" 20-21 квітня 2017 р. – 2017. – С. 53.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ITU – International Telecommunication Union

LTE – Long Term Evolution

UMTS – Universal Mobile Telecommunications System

E-UTRAN– Evolved UMTS Terrestrial Radio Access

IMT – International Mobile Telecommunications

IOT – Internet Of Things

eMBB – Enhanced Mobile Broadband

URLLC – Ultra Reliable Low Latency Communications

mMTC – Massive Machine-Type Communications

URLLC ULTRA – Reliable Low Latency Communications

EPC – Evolved Packet Core

OFDM – Orthogonal Frequency-Division Multiplexing

MIMO – Multiple Input Multiple Output

MME – Mobility Management Entity

SGW – Serving Gateway

PGW – Packet Data Network Gateway

HSS – Home Subscriber Server

PCRF – Policy And Charging Rules Function

UE –User Equipment

HSS – Home Subscriber Service

PCRF – Policy Control Function

NF – Network Function

NG-RAN – The Next Generation Radio Access Network

USIM – User Services Identity Module Domain

MS – Mobile Station

5GC – 5G Core Network

SBA – Service-Based Architecture

AMF – Access And Mobility Management Function

UPF – User Plane Function

CUPS – Control And User Plane Separation

ВСТУП

Актуальність теми дослідження.

За останній час системи біометричної автентифікації набули значної популярності, оскільки вони дозволяють користувачам не запам’ятовувати пароль. Також їх значному поширенню сприяє розвиток мобільних пристроїв для розв’язання найрізноманітніших завдань, включаючи віддалені платежі та віддалений доступ до робочого місця.

Зазвичай робота біометричних систем полягає у перетворенні біометричних характеристик людини у біометричний шаблон, який представляє собою набір даних у двійковому форматі. Вилучення та перетворення у двійковий код унікальних характеристик людини не є фінальним етапом. Аналогічно збереженню паролю у відкритому вигляді, не хешуючи його, зберігання біометричного коду є небезпечним. Використання звичайних хеш-функцій для біометричного коду є неможливими, адже необхідно забезпечити можливість розпізнавати різні зразки однієї й тієї ж унікальної характеристики людини. При зміні одного елементу звичайна хеш-функція буде повністю змінена, що перешкодить розпізнаванню власника біометричного зразка. Таким чином, для вирішення цієї проблеми використовуються алгоритми біохешу, проблема вибору якого є актуальною на сьогоднішій день.

Актуальною є потреба в підвищенні ефективності систем віддаленої біометричної автентифікації шляхом покращення методу формування біометричного шаблону, підвищення прихованості та завадозахищеності.

Об’єкт дослідження – процес обробки, захисту та прихованої передачі біометричних даних в телекомунікаційних системах та мережах.

Предмет дослідження – математичні моделі, методи та засоби забезпечення ефективності системи віддаленої біометричної автентифікації в каналах зв'язку.

Методи дослідження – методи математичного моделювання; методи теоретико-множинного підходу; методи цифрової обробки сигналів – для підготовки інформаційного сигналу та сигналу-контейнера для вбудовування прихованих даних; методи багатокритеріальної оптимізації – для вибору оптимального за зазначеними критеріями методів.

Мета та задачі дослідження.

Метою даної роботи є підвищення ефективності систем віддаленої біометричної автентифікації в телекомунікаційних мережах за рахунок застосування методів мережної стеганографії.

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

− Визначити переважний за набором ознак метод біометричної автентифікації.

− Визначити переважний метод формування біометричного шаблону та запропонувати рекомендації по його застосуванню і захисту.

− Визначити переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії. Вдосконалити метод передачі біометричної інформації шляхом застосування мережної стеганографії для підвищення захищеності віддаленої автентифікації.

− Запропонувати методи підвищення завадостійкості під час передачі даних користувача.

Наукова новизна результатів

При розв'язанні сформульованої наукової задачі в роботі отримано нові наукові результати:

− Вперше визначений переважний за критерієм завадозахищеності та ймовірності помилки метод біометричної автентифікації, відмінністю якого є

врахування стійкості до завад. Це дало змогу підвищити завадостійкість та ефективність систем віддаленої автентифікації в телекомунікаційних мережах.

− Вдосконалено метод обробки біометричних даних користувача шляхом обрання оптимального методу захисту біометричного шаблону. Це дозволило підвищити точність автентифікації.

− Вперше визначений переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії. Це дало змогу покращити ефективність системи віддаленої автентифікації за рахунок застосування визначеного методу.

− Вдосконалено метод віддаленої біометричної автентифікації в телекомунікаційних мережах, відмінністю якого є послідовне застосування методів формування біометричного шаблону, узгодження параметрів передачі з якістю каналу зв'язку, завадостійкого кодування та мережної стеганографії. Це дозволило підвищити захищеність передачі інформації та завадостійкість.

Практична значущіть результатів

Запропонований комплексний критерій оцінювання стеганографічних систем передачі інформації може бути використаний для вибору оптимального методу прихованої передачі інформації в залежності від умов передачі та сфери застосування системи.

Рекомендації щодо вибору ефективного методу для побудови стеганографічної системи дозволяють підвищити ефективність роботи системи прихованої передачі інформації, зокрема надають можливості для більш раціонального використання пропускної здатності контейнерів.

Використання запропонованих методів формування біометричного шаблону, завадостійкого кодування та адаптації системи передачі інформації до зовнішніх впливів, дозволяє підвищити швидкість, завадостійкість та захищеність від атак системи віддаленої біометричної автентифікації.

Отримані результати впроваджені в навчальний процес Харківського національного університету радіоелектроніки, зокрема, на кафедрі

інформаційно-мережної інженерії. Вдосконалений метод передачі автентифікаційної інформації телекомунікаційними мережами для підвищення захищеності передачі інформації та завадостійкості використано в лекційних та лабораторних заняттях з дисциплін «Безпека інфокомунікаційних мереж» та «Інформаційна безпека інноваційної діяльності». Дослідження переважного за критеріями завадозахищеності та ймовірності помилки методу біометричної автентифікації, відмінністю якого є стійкість до типових завад в каналах зв'язку використано в лекційних та лабораторних заняттях з дисциплін «Інформаційна безпека електронного бізнесу» та «Електронні платіжні системи». Визначений в роботі переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії використано в дисциплінах «Безпека інфокомунікаційних мереж» та «Програмування мережних послуг». Це підтверджено відповідним актом впровадження [додаток В].

Апробація результатів дисертації.

Основні результати дисертаційного дослідження пройшли апробацію в ході 11 наукових конференцій, серед яких:

- 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT);
- 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T);
- HICT'2019 Міжнародна науково-практична конференція «Наукоємні технології в інфокомунікаціях (Харків, 2019);
- Дванадцята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Баку–Харків–Жиліна, 27–28 квітня 2022 р);
- Десята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Харків, 9 – 10 квітня 2020 року);
- 6 міжнародна науково-технічна конференція «Проблеми Інформатизації» (14 – 16 листопада 2018 року);

- 7 міжнародна науково-технічна конференція «Проблеми Інформатизації» (13-15 листопада 2019 р);
- 8 міжнародна науково-технічна конференція «Проблеми Інформатизації» (2020 р.);
- 9 міжнародна науково-технічна конференція «Проблеми Інформатизації» (18 – 19 листопада 2021 року);
- Міжнародна науково-практична конференція "Проблеми і перспективи розвитку IT-індустрії (2017 р.)
- Conference on Mathematical Control Theory, 2019р;

Публікації

Результати дисертаційної роботи відображені у 18 друкованих працях, серед яких 1 розділ у закордонній монографії, що індексується Scopus, 6 – у наукових журналах, включених до «Переліку наукових фахових видань України», з них 1 – категорії А, що входить до наукометричної бази Scopus; а також 11 тез доповідей у матеріалах міжнародних наукових конференцій, з них 3 входять до наукометричної бази Scopus.

Структура дисертації

Дисертація складається із вступу, 4 розділів, висновку, списку використаних джерел та 3 додатків. Загальний обсяг дисертації складає 156 стор. (з них 119 сторінок основного тексту), 70 рисунків (з них 0 на окремих сторінках), 28 таблиць і 3 додатки на 5 сторінках, список використаних джерел з 97 найменувань на 13 сторінках.

1 ОГЛЯД ОСОБЛИВОСТЕЙ ПОБУДОВИ СУЧАСНИХ МОБІЛЬНИХ МЕРЕЖ

На сьогоднішній день мобільні технології надають широкі можливості завдяки створенню нових способів обміну даними. Вони використовуються практично у всіх сферах повсякденного життя, дозволяють залишатись на зв’язку та користуватись різними послугами дистанційно, незалежно від місця знаходження. Поява нових послуг, які можуть бути надані через Інтернет, а також збільшення кількості користувачів ставлять нові задачі для розвитку можливостей мобільних мереж завдяки розвитку нових технологій, які здатні підтримувати зростання об’єму трафіка та широкий спектр пристроїв користувачів.

За даними International Telecommunication Union (ITU) кількість користувачів мереж активного широкосмугового мобільного зв’язку, які є важливою частиною комунікаційної інфраструктури, активно зростає. За останні два десятиріччя розвиток технологій мобільного зв’язку призвів до розвитку нових поколінь мобільних мереж (рис.1.1).

Еволюція мобільних технологій почалась у 1980-х роках з аналогового зв’язку (1G). У 1990-х роках з’явилась можливість надсилання текстових повідомлень (2G). З початку 2000-х років активно розвивався мобільний зв’язок та Інтернет (3G), з 2008 року (4G) хмарні технології, IP та сучасний мобільний зв’язок, які набувають подальшого розвитку у передачі необмеженого обсягу даних (5G) [1-2].

На сьогоднішній день активно використовуються мережі LTE та впроваджуютсья технології 5G.

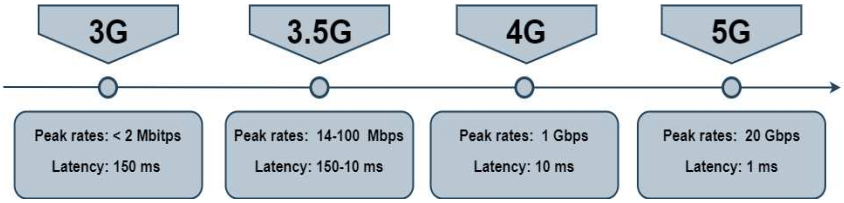

Рисунок 1.1 – Еволюція розвитку мобільних мереж

Вимоги до LTE охоплюють два фундаментальні компоненти архітектури системи UMTS: розвинену універсальну наземну мережу радіодоступу (E-UTRAN) і розширене пакетне ядро. Впровадження таких систем було спрямоване на покращення ємності системи та покриття, підвищення пікової швидкості передачі даних, низьку затримку (як на рівні користувача, так і на рівні керування), зниження експлуатаційних витрат, підтримку кількох антен та інтеграцію з існуючими системами (UMTS, WiFi тощо) [3].

З 2020 року активно розвиваються мережі п’ятого покоління мобільних технологій. До цілей розробки цієї технології відноситься створення більш гнучкої архітектури мережі, що дозволяє легше впроваджувати нові послуги, забезпечувати передачу не лише голосу та мультимедійних даних, а й зосередитись на міжмашинному зв’язку та забезпеченні низької затримки. Також розвиток спрямований на передачу великих обсягів даних на високій швидкості. ITU було розроблено стандарт IMT (International Mobile Telecommunications)-2020. У ньому описано основні вимоги до технології 5G. До них належать підтримка високої швидкості передачі даних користувача, підтримка широкого спектру послуг, таких як розумні будинки, інтелектуальні мережі, віддалена медична допомога, додатки віртуальної реальності, хмарні технології та інші.

Технологія 5G дозволяє пристроям під час руху зі швидкістю до 500 км/год залишатися підключеними до мережі. Також 5G дозволяє підключати до 1 мільйона пристроїв на квадратний кілометр, що сприяє розвитку інтернету речей (IoT) (рис.1.2).

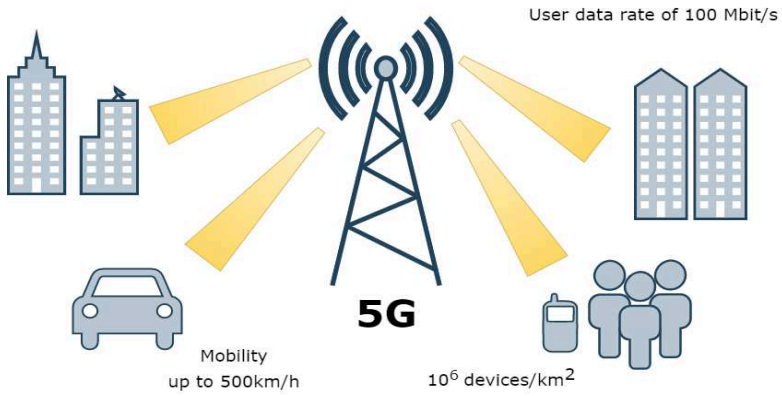

Рисунок 1.2 – Мережі 5G

Різні послуги та додатки мають різні вимоги до функціональності та продуктивності. Наприклад, послуги з надання відео у форматі 4K HD і 8K HD, управління безпілотними автомобілями, дистанційна медицина та інтернет речей можуть потребувати різних вимог до безпеки, мобільності, підтримки швидкості передачі даних й інших параметрів.

Типи послуг 5G, які використовуються для оптимізованої обробки трафіку, включають такі категорії, як розширений мобільний широкополосний зв'язок (eMBB), критичний зв'язок і сверхнадійний зв'язок із малою затримкою (URLLC), massive Machine Type Communications (mMTC) (рис. 1.3) [4].

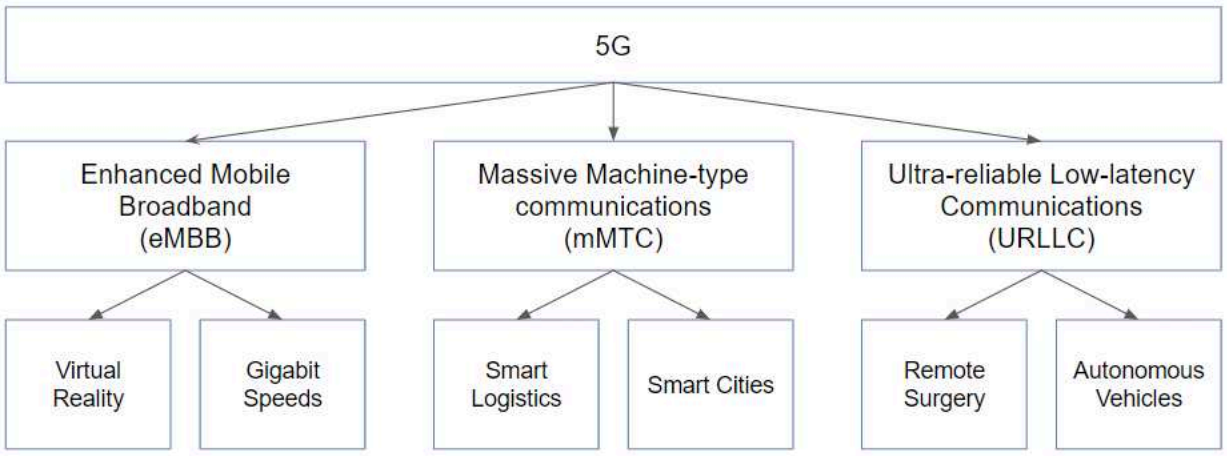

Рисунок 1.3 – Сфери застосування 5G

Розширений мобільний широкополосний зв’язок (eMBB) використовується для додатків, які вимагають доступу до мультимедійного вмісту та високої швидкості передачі даних (пікова швидкість до 20 Гбіт/с і швидкість отримання користувачем до 100 Мбіт/с), підтримки мобільності до 500 км/год і спектральної ефективності, втричі вищої, ніж у 4G. Для обробки таких послуг eMBB, як, наприклад, послуги корпоративних сервісів, віртуальної та доповненої реальності, передачі відео, важливими є швидкість передачі даних та ефективність використання спектра.

Для сверхнадійного зв’язку із малою затримкою (URLLC) велике значення має низька затримка та високий рівень мобільності. Це важливо, так як до послуг управління такого типу відносяться дистанційна хірургія, управління дорожнім трафіком та безпілотними автомобілями тощо.

Для mMTC необхідні висока щільність з’єднань і можливість функціонування великої кількості пристроїв в мережі, так як такі послуги забезпечують роботу інтернету речей, розумних будинків, різних сенсорів в сільському господарстві – пристроїв, які передають невеликий обсяг даних з невеликою чутливістю до затримки та мають низьке споживання енергії. Для надання таких послуг використовується пропускна спроможність 10 Мбіт/с/м2.

Одними з ключових принципів мереж 5G є можливість забезпечення сумісності у всьому світі, міжнародний роумінг і доступ до високошвидкісних послуг передачі даних [5].

1.1 Архітектура та основні елементи мереж 4G LTE та 5G

LTE (Long Term Evolution) і LTE-Advanced були розроблені для покращення пропускної здатності систем та покриття, спектральної ефективності, досягнення низької затримки, зниження експлуатаційних витрат, підтримки декількох антен і інтеграції з мережею Інтернет та існуючими системами мобільного зв’язку.

Вимоги до LTE охоплюють вдосконалену універсальну наземну мережу радіодоступу (E-UTRAN) та розширене пакетне ядро (EPC). Цілі загальної системи включають:

- покращену ємність системи та покриття;
- високу пікову швидкість передачі даних;
- низьку затримку (як на рівні користувача, так і на рівні керування);
- зниження експлуатаційних витрат;
- підтримку кількох антен;
- операції з гнучкою пропускною здатністю;
- повну інтеграцію з існуючими системами (UMTS, Wi-Fi тощо) [3].

До основних технологій LTE відносяться Orthogonal Frequency-Division Multiplexing (OFDM), багатоантенні системи Multiple Input Multiple Output (MIMO), Turbo Channel Coding та Link Adaptation.

На рисунку 1.4 наведено архітектуру мережі 4G LTE.

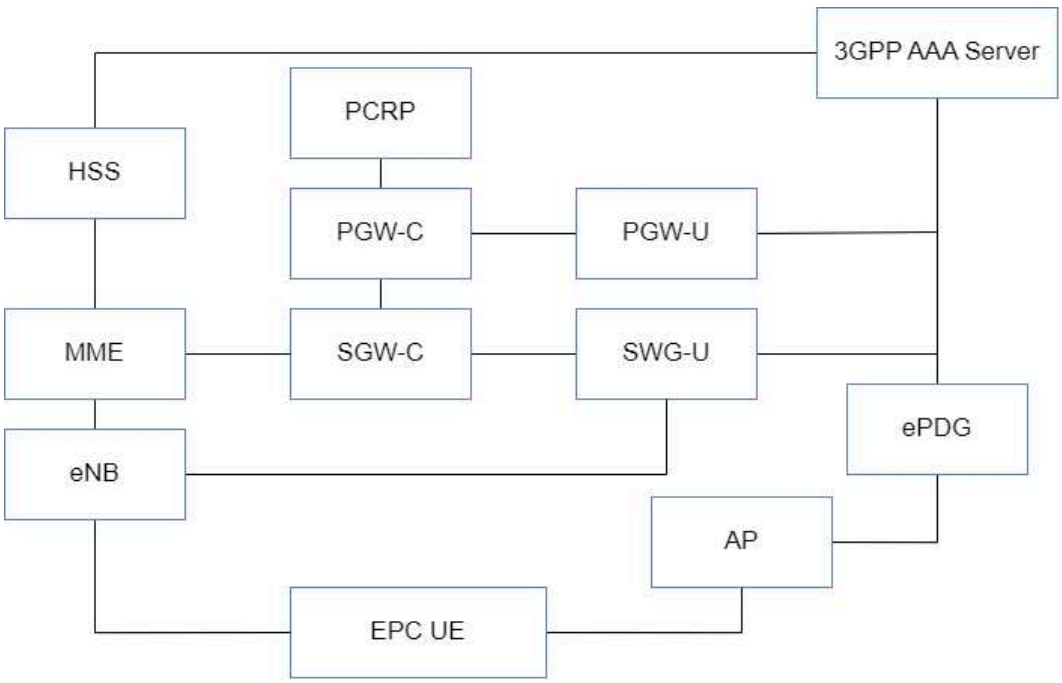

Рисунок 1.4 – Архітектура мережі 4G LTE

В архітектурі 4G LTE важливим компонентом є EPC, призначений для структурованої обробки трафіку даних і контролю мобільних пристроїв. До його ключових компонентів відносяться MME (Mobility Management Entity), SGW, PGW (PDN Gateway), HSS (Home Subscriber Server), PCRF (Policy and Charging Rules Function).

MME відповідає за управління сеансами та мобільність, керує сигналізацією між UE (обладнанням користувача) та базовою мережею.

SGW відповідає за маршрутизацію пакетів даних.

PGW керує IP з'єднаннями даних і призначає IP адреси UE.

HSS являє собою центральну базу даних для інформації про користувачів та підписки.

PCRF відповідає за політику та правила стягнення плати.

На відміну від 4G LTE, 5G базується на архітектурі на основі послуг (SBA) і вводить концепцію мережевих функцій (NF).

Мережна архітектура мобільної технології 5G має значні переваги у порівнянні з попередніми технологіями. Мережі 5G мають співіснувати з мережами попередніх поколінь. Розробка та розгортання нових мережних технологій потребує часу та співпраці організацій та операторів [6]. Перехід від 4G до 5G призводить до змін в мережній архітектурі.

До основних переваг технології 5G відносяться підвищена швидкість передачі даних, забезпечення меншої затримки, більша ємність.

Мережі 5G підтримують наступні діапазони частот:

- високочастотний діапазон (міліметрові хвилі): 24 ГГц – 40 ГГц. Такі сигнали мають досить обмежену дальність поширення;
- середній частотний діапазон: 3,5 ГГц – 6 ГГц забезпечує передачу великої кількості даних на значні відстані;
- низькочастотний діапазон: 1ГГц – 2.6 ГГц дозволяє забезпечити більше покриття [6, 7].

В загальному вигляді архітектура 5G складається з трьох основних компонентів, як і мережі попередніх поколінь: обладнання користувача (UE), мережі радіодоступу (NG-RAN) та базової мережі (5G Core) (рис. 1.5).

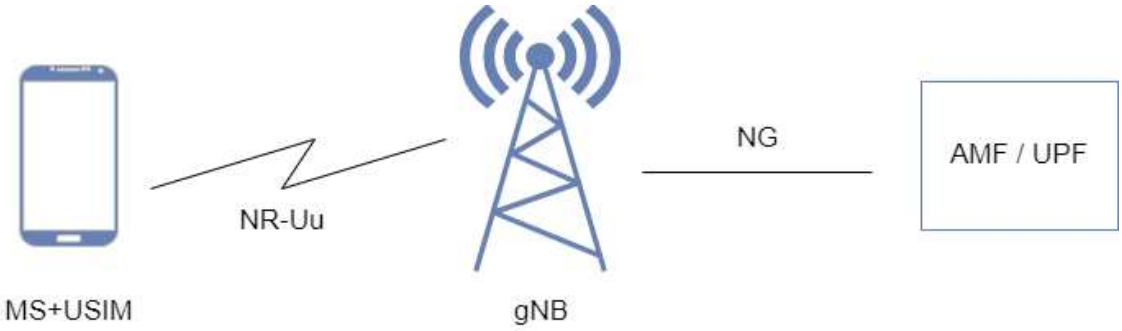

Рисунок 1.5 – Загальна архітектура 5G

Обладнання користувача складається з USIM (User Services Identity Module Domain) і MS (Mobile Station). MS представляє собою пристрій, який безпосередньо використовується кінцевим користувачем для комунікації [8]. Це може бути смартфон, планшет, ноутбук або інший бездротовий пристрій, який використовується для отримання доступу до мережевих послуг [9,10]. Обладнання користувача підключається до базової станції gNB для отримання доступу до мережі. Архітектура мережі радіодоступу наступного покоління NG-RAN (The Next Generation Radio Access Network) забезпечує підтримку розширених мобільних широкосмугових послуг, підтримку URLLC (Ultra-Reliable Low Latency Communications), єдину архітектуру для централізованого, розподіленого та монолітного розгортання; робить можливим повне відокремлення площини керування (CP) від площини користувача (UP) централізованого блоку для максимальної гнучкості розгортання, а також спільне використання ресурсів з існуючими мережами LTE [11].

Архітектура 5GC (5G core network) (рис.1.6) спирається на архітектуру на основі служб (SBA). Елементи архітектури визначаються з точки зору мережних функцій (NF). Через інтерфейси загальної структури конкретна NF

пропонує свої послуги всім іншим авторизованим NF та/або всім, хто має дозвіл на використання послуги. Такий підхід пропонує модульність і можливість повторного використання [12].

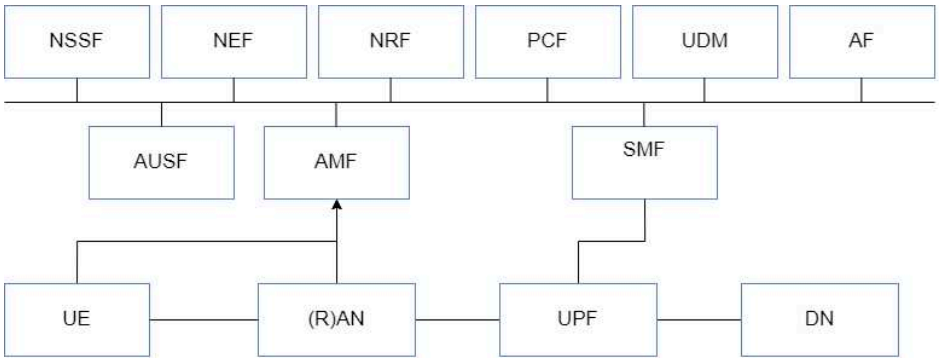

Рисунок 1.6 – Архітектура 5G Core

5G core network можна представити об’єктом AMF/UPF: функцією площини користувача (UPF), яка обробляє дані користувача, і функцією управління доступом та мобільністю (AMF) [12]. Основна функція керування доступом і мобільністю 5G Access and Mobility Management Function (AMF) отримує всю інформацію від обладнання користувача, пов’язану з підключенням і сеансом, і відповідає за вирішення задач керування з’єднанням і мобільністю [13].

Функція 5G User Plane Function (UPF) – фундаментальний компонент архітектури базової мобільної інфраструктури, який представляє еволюцію площини даних. За стратегією Control and User Plane Separation(CUPS) відбувається розділення функцій керування пакетним шлюзом (PGW) і площини користувача, що дозволяє децентралізувати компонент пересилання даних (PGW-U). Завдяки цьому, обробка пакетів і агрегація трафіку відбувається ближче до межі мережі, збільшуючи ефективність пропускної здатності та зменшуючи мережу.

Функція сервера автентифікації (AUSF – Authentication Server Function) необхідна для виконання функцій автентифікації користувача, забезпечення

безпеки, управління мобільністю, керування сеансами та управління абонентськими даними [14].

Функція мережного сховища (NRF – Network Repository Function) зберігає інформацію про функції мережі.

NEF (Network Exposure Function) відкриває можливості та ресурси мережі стороннім програмам.

PCF (Policy Control Function) – функція контролю політики.

UDR (Unified Data Repository) – функція зберігання структурованих даних.

UPF (User Place Function) відповідає за маршрутизацію та пересилання пакетів, перевірку пакетів і обробку QoS для даних користувача.

NSSF (Network Slice Selection Function) відповідає за вибір відповідного екземпляра сегмента мережі на основі UE (обладнання користувача) і вимог до послуг.

AF (Application Function) взаємодіє з основною мережею, головним чином, для цілей політики та стягнення плати. Він представляє зовнішні програми, які повинні спілкуватися з основними компонентами 5G [15].

Перехід від 4G до 5G призводить до змін в мережній архітектурі (рис. 1.7). Для мереж 5G визначено два варіанти розгортання – NSA (неавтономна архітектура) і SA (автономна архітектура). Основна відмінність NSA від SA полягає в тому, що NSA використовує вже існуючу мережу, тоді як SA – це нова архітектура мережі, яка дозволяє працювати без взаємодії з існуючим ядром 4G[16].

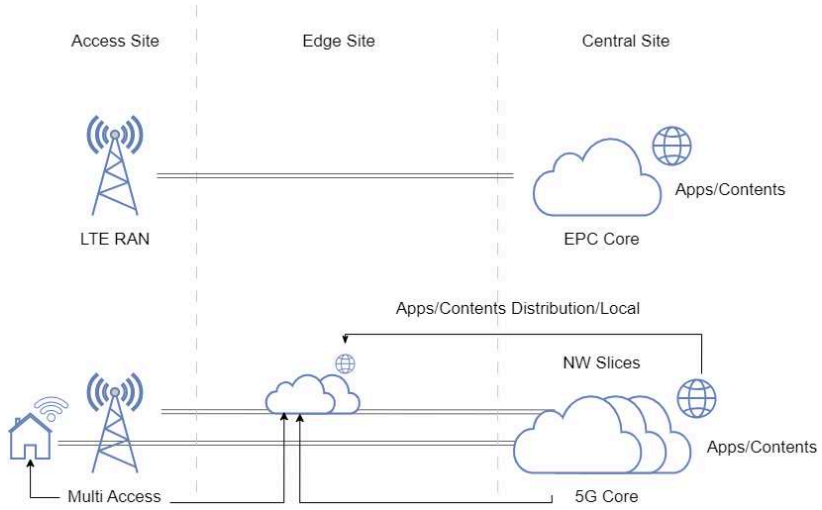

Рисунок 1.7 – Порівняння архітектур 4G LTE та 5G

В таблиці 1.1 наведено порівняння технологій 4G та 5G[16].

Таблиця 1.1 – Порівняння технологій 4G та 5G

№	Характеристика	4G	5G
1	2	3	4
1	Модель каналу	3GPP TR 36.814 ITU M.2135	3GPP TR 38.901 ITU M.2101
2	Архітектура мережі	децентралізована	віртуалізація хмарна децентралізована
3	Максимальна швидкість завантаження (download)	1 Гбіт/с	2.5 Gbps
4	Максимальна швидкість завантаження (upload)	500 Mbps	1.25Gbps
5	UL пікова швидкість передачі	500 Mbps	10 Gbps
6	DL пікова швидкість передачі	1 Gbps	20 Gbps
7	UL максимальна спектральна ефективність	6.75 b/s/Hz	15 b/s/Hz

Продовження таблиці 1.1

1	2	3	4
8	DL максимальна спектральна ефективність	15 b/s/Hz	30 b/s/Hz
9	Щільність підключення	105 disp./km^2	2106 disp./km^2
10	Мобільність	350 km/h	500 km/h
11	Пропускна здатність	0.1 M b/s/m^2	10 M b/s/m^2
12	Затримка	10–100ms	1–10 ms
13	Мережа доступу	RAN	C-RAN
14	Модуляція	QAM, QPSK	Amplitude Phase-Shift Keying technique.

На рисунку 1.8 показано різницю між основними показниками у процентному відношенні між мережами 4G та 5G. В мережах 5G пікова швидкість збільшилась на 95%, швидкість передачі даних користувача на 90%, ефективність використання спектру збільшилась у 3 рази в порівнянні з мережами 4G.

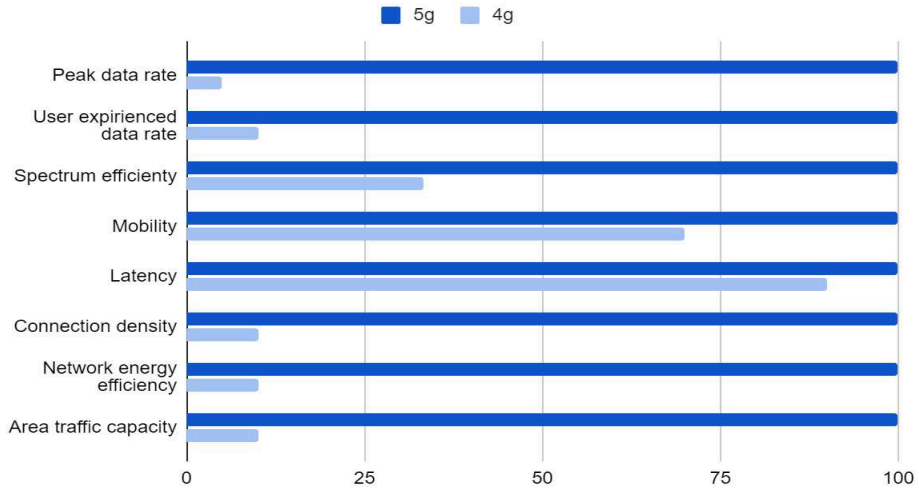

Рисунок 1.8 – Порівняння характеристик 4G LTE та 5G

Можливості мереж 5G досягаються за рахунок використання таких технологій, як massive MIMO, NFV, Edge computing, network slicing.

Технологія MIMO (Multiple–input/multiple–output) полягає в оснащенні базових станцій великою кількістю антен, що дозволяє передавати та отримувати більше одного сигналу даних одночасно через той самий радіоканал [17]. За рахунок того, що сигнал спрямований на кінцевого користувача, покращується покриття на межі стільника. Також за допомогою просторового мультиплексування з MU-MIMO системи бездротового зв'язку можуть одночасно комунікувати з різним обладнанням користувача, використовуючи однакові частотно-часові ресурси. Це дозволяє підвищити спектральну ефективность та пропускну здатність стільника [17,18].

Концепція NFV (віртуалізація мережевих функцій) зосереджена на відокремленні логічних функцій від фізичної реалізації. Метою NFV є віртуалізація набору мережних функцій шляхом реалізації їх у пакетах програмного забезпечення, які можуть гнучко створювати ті самі послуги, що й оригінальні. Робота NFV на віртуальних машинах дозволяє зменшити кількість пристроїв та витрати. Використання концепції NFV дозволяє пришвидшити та спростити масштабування мережної архітектури [19,20].

Граничні обчислення (Edge computing) — це структура розподілених обчислень, які змінюють спосіб обробки та зберігання даних, переміщуючи деякі основні функції мережі ближче до кінцевого користувача на межі мережі, а не покладаючись на центральне розташування. Така наближеність до джерела даних дозволяє покращити час відповіді та забезпечує кращу пропускну здатність [21].

На відміну від мереж попередніх поколінь мережі 5G використовують Network Slicing в якості однієї з основних технологій (рис. 1.9).

Network slice – це логічна мережа, яка надає визначені мережні можливості та характеристики мережі. Набір обчислювальних ресурсів, сховища та мережні ресурси утворюють розгорнутий сегмент мережі [22].

Кожен слайс мережі може мати свою власну логічну топологію, власні правила безпеки та характеристики продуктивності. Різні слайси можуть бути

призначені для різних послуг, забезпечувати різний пріоритет доступу до ємності та доставки, ізолювати трафік для певних користувачів або класів пристроїв. Такий підхід дозволяє максимально використовувати мережеві ресурси і забезпечувати гнучкість обслуговування.

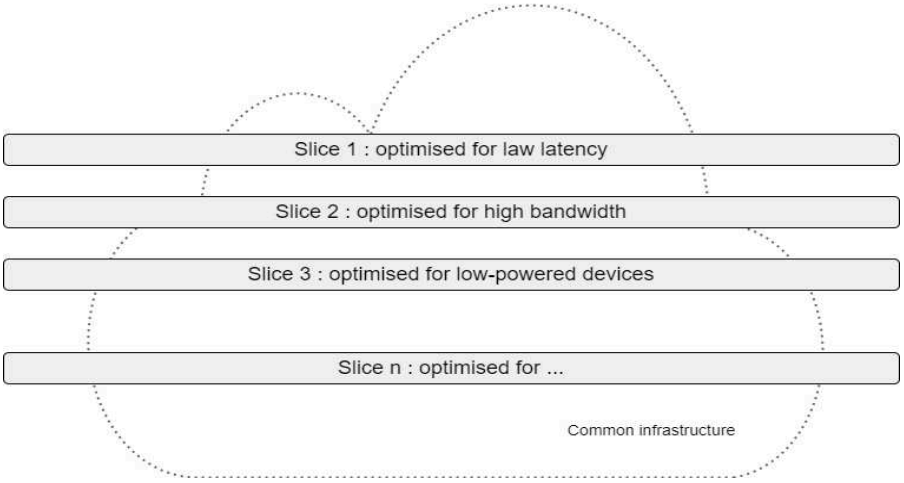

Рисунок 1.9 – Network slising

1.2 Сценарії використання сучасних мобільних мереж

Сучасні мобільні мережі поширюються в багатьох сферах життя. З розвитком технологій використовуються мережі розумних будинків, розумних міст, віддаленого користування банківськими послугами, оплати в інтернет-магазинах, застосування IoT в медицині, промисловості та інших сферах.

Датчики інтернету речей служать для профілактичного обслуговування, моніторингу продуктивності, дистанційного керування робототехнікою на заводах та в промисловості. Мережі охорони здоров’я охоплюють численні медичні машини, датчики пацієнтів, програми охорони здоров’я та пристрої моніторингу. В транспортній сфері автономні транспортні засоби повинні мати можливість обробляти інформацію та відповідним чином налаштовуватися за якомога менший час.

Також збільшується використання хмарних сервісів, що потребує наявності та необхідної якості каналу інтернет-зв’язку. Існують ризики технічних збоїв та небезпека порушення конфіденційності даних.

В незалежності від сфери використання пристрої мають залишатися безпечними, але доступними. Дані користувачів мають залишатися надійно захищеними, але доступними для конкретного корисувача або привілейованих осіб.

1.3 Забезпечення захисту даних в мережах

Мережі LTE та 5G підтримують надання послуг, для яких безпека є особливо важливою, наприклад, управління транспортними засобами, медициною тощо. Важливою задачею є захист мереж від крадіжки конфіденційних даних, атак на пристрої мережі. Розвиток мереж може призводити до розширення кількості та масштабів потенційних вразливостей [23].

Відповідно до [24] загрози можна поділити на:

- Загрози конфіденційності – загрози несанкціонованого ознайомлення з інформацією.
- Загрози цілісності – загрози несанкціонованої модифікації інформації.
- Загрози доступності – загрози, що можуть перешкодити використанню системи або інформації [24].

Вразливими до атак можуть бути різні об’єкти та сегменти мереж LTE та 5G: UE, RAN, базова мережа, додатки та служби, розміщені оператором або сторонніми розробниками (рис. 1.10) [25].

В таблиці 1.2 наведено основні вразливості LTE і 5G мереж [26]. Оцінки від 0 до 5 відповідають ступеню загрози, де 1 – найменша, 5 – найбільша.

Таблиця 1.2 – Вразливості LTE і 5G мереж

Загроза	LTE	5G
Traffic Hijack	3	2
Jamming	3	2
Interworking and roaming threats	3	2
Sniffing Base station configuration	3	3
Downgrade	3	3
Device tracking	3	3
VoLTE (Spamming, Spoofing, Phishing) / VoNR (security setting is the same as VoLTE)	3	3
Attacks on SMS	3	3
DoS	3	4
Rogue Base Station	3	5

В мережах 5G вирішено проблему перехоплення International Mobile Subscriber Identity (IMSI) шляхом впровадження Subscriber Permanent Identifier (SUPI). Також полегшено протидію атакам на DNS, покращено захист від перехоплення трафіку та глушіння сигналу. Але з новими можливостями ядра 5G додались і нові вразливості: Network Functions Virtualization, Network slicing та Software-Defined Networking vulnerabilities. Також залишилась вразливість з використанням одного ключа шифрування для двох послідовних з'єднань. Невирішеними залишились проблеми, пов'язані з ризиками реалізації атак, спрямованих на сервіси SMS та VoNR. 5G передбачає підключення до мережі великої кількості девайсів (MIoT), що провокує проведення масованих Dos атак на інтернет ресурси та мережу 5G. Методом протидії є аналіз аномального трафіку й розірванні зв'язку[26].

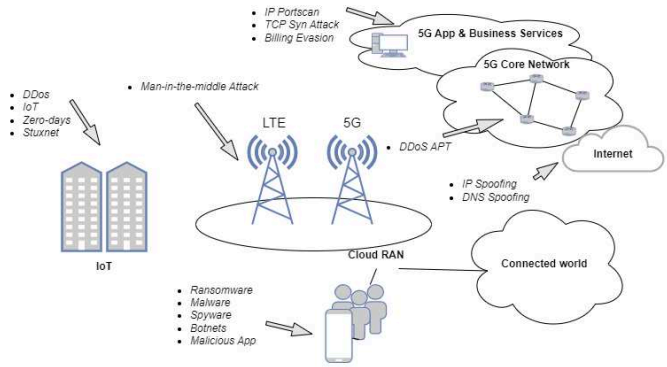

Рисунок 1.10 – Загрози в мережах 4G LTE та 5G

Через незахищений канал в повітряному інтерфейсі існує ймовірність атаки. Протоколи автентифікації призначені для забезпечення безпеки зв'язку в незахищених каналах. У [27] представлено атаку на протокол автентифікації 5G, спричинену незахищеним каналом, та запропоновано протокол автентифікації з розширеною безпекою для мережі 5G для захисту від описаної атаки у двох незахищених каналах (між UE та SN, а також між SN та HN).

Таким чином, важливою проблемою є забезпечення захищеного зв'язку, стійкого до загроз конфіденційності та достовірності інформації, що передається. Загрози конфіденційності пов'язані з можливістю читання інформації, надісланої в мережі неавторизованими особами. Загрози автентичності та цілісності переданих даних пов'язані з можливістю модифікації даних неавторизованими особами. Окрім автентичності інформації, важлива також автентичність відправника – впевненість щодо особи людини, яка отримує доступ до певних даних. Одним із методів захисту зв'язку є протоколи автентифікації, які використовуються, коли дві сторони встановлюють безпечний зв'язок в мережі [28].

Автентифікація користувача є ключовим компонентом безпеки для логічного контролю доступу до будь-яких цифрових даних служби в Інтернеті. Багато додатків потребують віддаленої автентифікації [29].

У [30] автори класифікують атаки на автентифікацію користувачів за наступними категоріями:

- Атаки з використанням грубої сили: зловмисник намагається видати себе за користувача, перевіряючи різні випадкові значення підтвердження особи (наприклад, пароль).
- Атаки спостереження: будь-яке спостереження може допомогти зловмиснику вгадати доказ особи.
- Атаки через видавання себе за іншу особу: зловмисник намагається згенерувати підтвердження особи.
- Атаки по бічному каналу: витік деякої інформації із систем автентифікації може бути використаний для створення підробленого підтвердження особи.

Зі збільшенням кількості сервісів росте кількість даних для автентифікації, які повинен пам’ятати користувач (паролі), або кількість карток, електронних ключей, які людина повинна мати для отримання доступу. Це створює певні незручності, які можуть бути вирішені за допомогою використання біометричної автентифікації.

Біометрична автентифікація, в свою чергу, створює нові проблеми для конфіденційності та безпеки. Хоча ця технологія може замінити потребу у створенні довгих та складних паролів, під час її використання також виникає небезпека викрадення особистих даних. На відміну від методів автентифікації на основні знань (паролів, криптографічних ключів), які відомі тільки користувачу, біометричні дані не є таємницею. Такі біометричні дані, як голос, обличчя, підпис, відбитки пальців, можуть бути записані, та потенційно використані без згоди користувача. Також, при компрометації даних, на відміну від паролів, крипто-ключей, PIN-кодів, карток, які можна змінити, біометричні дані постійно пов’язані з користувачем та не можуть бути відкликані [31]. В традиційних системах автентифікації рекомендованим є вживання різних паролів для різних систем, проте методи автентифікації на основі біометрії

покладаються на ті самі біометричні дані, що також підвищує ризик компрометації даних.

Біометричні дані є унікальними для кожної людини, їх неможливо змінити, на відміну від паролю, тому їх використання потребує забезпечення необхідного рівня захисту.

Схема біометричної автентифікації складається з двох етапів: перший передбачає реєстрацію користувача в біометричній системі на основі еталонних біометричних даних, а другий – порівняння нових отриманих біометричних даних з попередньо збереженим еталоном (верифікація).

Більшість атак на системи автентифікації спрямовані на те, щоб видати себе за певного користувача і отримати доступ до даних. Атаки повторення здійснюються шляхом повторного надсилання попередньо використаного вірного біометричного зразка до системи. Презентаційні атаки полягають у представленні біометричному датчику підробленого біометричного зразка. Наприклад, зображення обличчя користувача для імітації, макіяжу, масок [32].

Схеми автентифікації користувачів ретельно вивчалися протягом останніх двох десятиліть, наприклад, у [32,33] з різними припущеннями безпеки, різними криптографічними алгоритмами (від симетричної криптографії до еліптичних кривих).

На рисунку 1.11 наведено узагальнену схему біометричної автентифікації. На початку за допомогою біометричного сенсору мають бути отримані біометричні дані користувача, сформовано біометричний шаблон. Далі необхідні для автентифікації дані передаються мережею. На приймальній стороні вони порівнюються з попередньо зареєстрованим зразком, та робиться рішення про надання доступу.

Рисунок 1.11 – Узагальнена система віддаленої біометричної автентифікації

Під час віддаленої автентифікації можливими є різні загрози безпеці даних (рис. 1.12). Біометрична система на етапі реєстрації записує зразок біометричної характеристики користувача за допомогою датчика – наприклад, сканується райдужна оболонка ока, знімається відбиток пальця або зображення обличчя. З отриманої біометричної характеристики вилучається необхідна модальність, обчислюється вектор біометричних ознак. Система зберігає вектор у базі даних поряд з іншими ідентифікаторами, такими як ім’я або ідентифікаційний номер. Під час фази автентифікації користувач надає інший біометричний зразок, який порівнюється з шаблоном на сервері чи пристрої. При відповідності нового зразка збереженому шаблону за заданим порогом автентифікація проходить успішно.

На рівні роботи користувача з біометричним сенсором системи передачі даних можлива фальсифікація даних, наприклад, шляхом використання попередніх даних користувача. При атаці типу «маскарад» зловмисник видає себе за користувача, який має доступ до даних. Також, можливим є отримання зловмисником несанкціонованого доступу до біометричного шаблону під час автентифікації або його підміна. На етапі порівняння шаблонів для вібмови або надання доступу також можливе втручання, в результаті якого може бути отриманий несанкціонований доступ [34].

Окрім вище зазначених атак, слід відмітити, що під час передачі даних каналом зв’язку є загроза того, що дані будуть перехоплені[34].

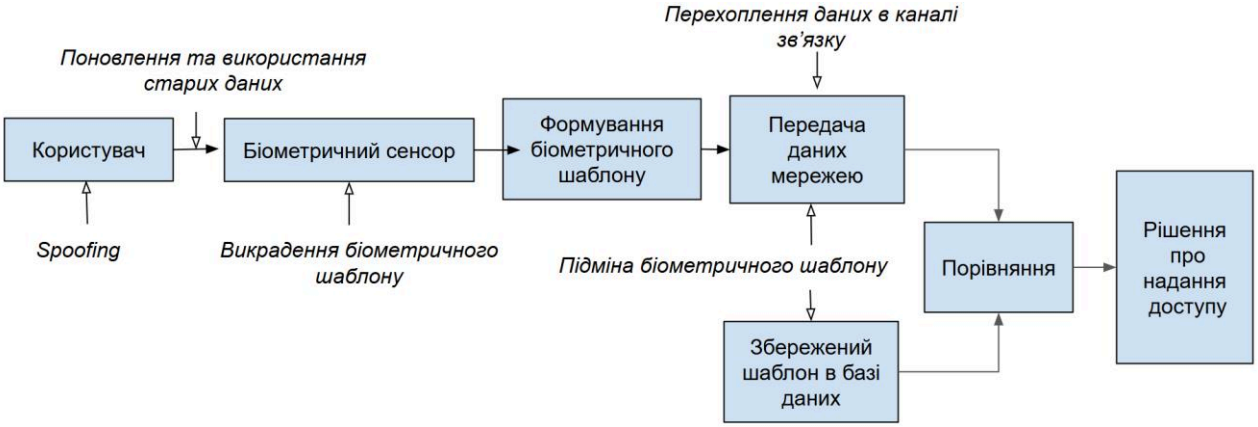

Рисунок 1.12 – Можливі атаки в системі автентифікації

Під час спуфінгових атак використовується певний тип неправдивого представлення інформації. При різних методах біометричної автентифікації використовуються різні характеристики, відповідно, зловмисники намагаються штучно їх відтворити. Наприклад, при автентифікації за відбитком пальця можливим є використання штучих відбитків, зроблених безпосередньо з відбитку або з поверхні. При розпізнаванні за геометрією обличчя може бути використана 3D-маска. При автентифікації за райдужною оболонкою ока – цифрове зображення або відео райдужної оболонки користувача, штучні контактні лінзи [35].

При використанні для автентифікації динамічних методів, наприклад, підпису особи, можливою є імітація цієї дії користувача [34].

Перелічені вище загрози виникають на етапі роботи користувача з біометричними датчиками, тому для захисту від таких загроз необхідним є попередження від розпізнавання з використанням підроблених біометричних зразків. Для боротьби з цим використовують дослідження природнього руху та скорочення райдужної оболонки ока, перевірку моделей відбиття світла або аналіз унікальної текстури поверхні райдужної оболонки. Для підтвердження належності відбитка користувачу – вимірювання температури, вологості та електричних властивостей шкіри пальця. При розпізнаванні за геометрією

обличчя – аналіз рухів обличчя, таких як моргання, або перевірку інформації про глибину 3D [34, 35].

Існують біометричні алгоритми, які спеціально розроблені для виявлення атак спуфінгу. Їх робота полягає в здатності відрізнити справжні біометричні ознаки від підроблених. Це досягається шляхом аналізу різних характеристик і шаблонів. Наприклад, під час розпізнавання відбитків пальців алгоритми можуть досліджувати структури, дрібні точки або загальну послідовність зображення відбитка пальця. Подібним чином у розпізнаванні обличчя алгоритми можуть зосереджуватися на конкретних точках обличчя, формах текстури або інформації про глибину. Аналізуючи ці унікальні характеристики, алгоритми спрямовані на виявлення будь-яких невідповідностей або порушень, які можуть свідчити про спробу атаки. Для реалізації таких алгоритмів використовуються методи машинного навчання, комп’ютерного зору та розпізнавання образів [35].

Іншим типом атаки може бути відтворення даних, які були раніше введені / отримані від користувача [34].

Після отримання біометричним сенсором даних формується біометричний шаблон, який містить дані, отримані з біометричного зразка та використовується в системі автентифікації для порівняння даних та надання рішення про дозвіл або відмову дозволу [34].

Переданий мережею біометричний шаблон також може бути перехвачений в каналі зв’язку. Таким чином атаки можливі на різних етапах роботи системи віддаленої біометричної автентифікації та важливим є урахування цього при створенні системи.

1.4 Висновки до розділу 1

Проведено аналіз розвитку сучасних мобільних мереж 4G LTE та 5G, розглянуто їх архітектуру та відмінності, проведено порівняння основних

характеристик. Розглянуто використання нових технологій, таких як massive MIMO, NFV, Edge computing, network slicing.

Проаналізовано основні сценарії використання сучасних мобільних мереж, таких, як мережі розумних будинків, віддалене користування банківськими послугами, оплати в інтернет магазниах, використання IoT в різних сферах. Доведено актуальність задачі підвищення захисту конфеденційних даних користувачів та протидії несанкціонованому доступу до даних.

Проведено дослідження стану безпеки сучасних мобільних мереж, визначено основні типи атак та загроз в мобільних мережах. Проаналізовано можливість їх перекриття застосуванням методів віддаленої автентифікації. Обгрунтовано необхідність застосування віддаленої автентрифікації для сценаріїв використання мереж 4G LTE та 5G. За підсумками порівняння методів віддаленої автентифікації для проведення досліджень було обґрунтовано застосування методів біометричної автентифікації.

Список використаних джерел у даному розділі наведено у повному списку використаних джерел під номерами 1-34.

2 ДОСЛІДЖЕННЯ МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Для забезпечення захисту інформації та управління доступом до ресурсів можуть бути використані біометричні методи, які дозволяють однозначно визначити суб'єкт доступу та його повноваження по відношенню до конкретного ресурсу. В багатьох системах для надання доступу використовуються електронні ключі, паролі, тощо. При компрометації їх можна замінтити. Біометричні ознаки людини є складними для підробки, немає можливості передати ці дані іншій особі, їх важко підробити. Для отримання біометричних зразків використовуються датчики. Дані відсилаються процесору. На цьому етапі відбувається вилучення всіх відмінних рис біометричного зразка. Далі біометричний зразок записується в базу даних та зберігається в якості шаблону, для можливості порявняння при автентифікації. Сучасні системи біологічного розпізнавання є якісними та надійними засобами автентифікації особи [36].

Метою цього розділу є дослідження найбільш поширених методів біометричної автентифікації, визначення основних критеріїв оптимальності біометричних систем автентифікації, виконання багатокритеріального аналізу біометричних показників.

2.1 Методи біометричної автентифікації

Існуючі алгоритми та методи біометричного розпізнавання можна поділити на дві основні групи: статичні та динамічні (рис. 2.1) [37, 38, 39, 40].

Статичні методи біометричної автентифікації ґрунтуються на унікальних невід'ємних фізіологічних характеристиках людини, властивих від народження. Прикладами таких методів є розпізнавання за відбитком пальця (дактилоскопія), розпізнавання за райдужною оболонкою ока, сітківкою ока,

геометрією обличчя, геометрією руки. Динамічні методи біометричної автентифікації ґрунтуються на поведінковій характеристиці людини в процесі відтворення певної дії. Прикладами таких методів є розпізнавання голосу, динаміка підпису. Використання сукупності цих методів дозволяє створювати мультимодальні біометричні системи [40, 41].

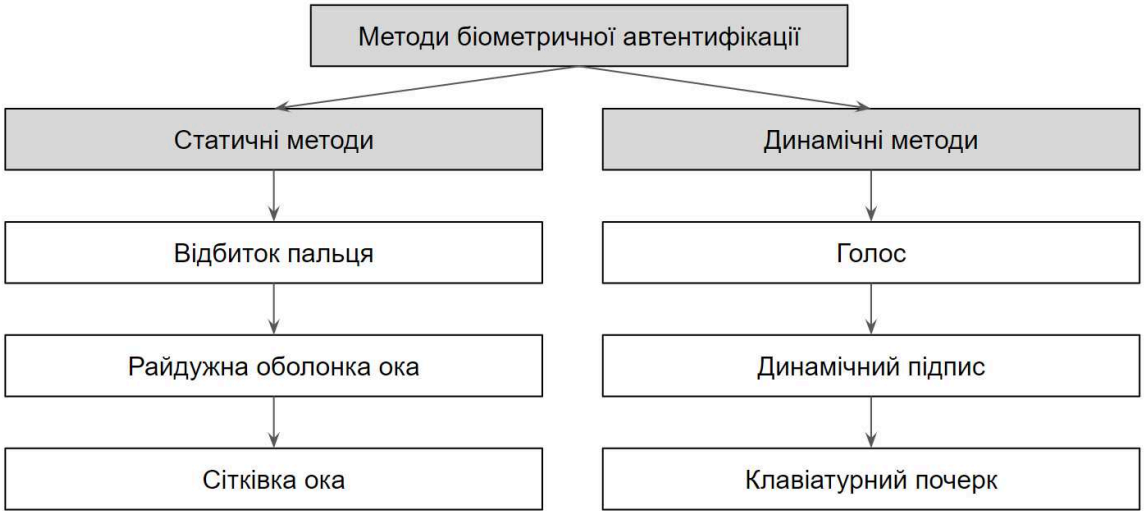

Рисунок 2.1 – Методи біометричної автентифікації

Розпізнавання за відбитками пальців – один із найвідоміших біометричних методів. Сканування відбитків пальців для автентифікації та авторизації, наприклад, в мобільних телефонах, мають високу точність. Перевагами цього методу є низький рівень помилок, швидке проходження автентифікації. До недоліків можна віднести те, що не всі пристрої мають датчик для сканування відбитка пальця, тому не зі всіх пристроїв можлива авторизація цим методом. Також залишається небезпека, пов’язана з витоком шаблону. Відбитки пальців залишаються відносно незмінними протягом багатьох років, і шаблон може бути використаний для авторизації для декількох послуг. Отримання зловмисником такого шаблону може призвести до того, що він отримає доступ до декількох служб користувача. Існують методи захисту

шаблонів, але вони все ще досліджуються [31]. Також в залежності від датчика, який використовується, може змінитись точність при автентифікації [37].

Автентифікація за райдужною оболонкою ока людини використовує її унікальний малюнок. Це забезпечує вищий рівень захищеності та стійкість до підробки, ніж розпізнавання за відбитками пальців. В роботі [42] проведено дослідження використання райдужної оболонки ока для біометричної автентифікації на смартфоні. Перевагою автентифікації за райдужною оболонкою ока є те, що рівень помилок при належному освітленні є низьким. Також цей метод є стійким до спуфінг-атак. До недоліків можна віднести те, що цей метод не має широкого використання на мобільних пристроях. Сканування ока вимагає від користувача залишатися нерухомим, і через несприятливі умови освітлення та обмежену стабілізацію мобільного пристрою можливі помилкові відхилення при авторизації. Оскільки більшість недоліків залежить від апаратного забезпечення, з розвитком обладнання, популяризацією smart glasses використання цього метода буде зростати.

Метод автентифікації за геометрією обличчя в загальному вигляді складається з таких кроків, як отримання зображення обличчя, виділення ознак (перетворення пікселів зображення обличчя на векторне представлення), розпізнавання та пошук відповідностей в базі даних. Технологія розпізнавання обличчя дозволяє проводити автентифікацію на відстані, може працювати з універсальним пристроєм, таким як смартфон або планшет, без потреби спеціальних пристроїв. В той же час технологія розпізнавання обличчя має певні труднощі при практичному застосуванні, включаючи розбіжності в зображеннях обличчя ідентичної людини (заплющення очей, зміна виразу обличчя), зміни обличчя внаслідок старіння, схожість облич (близнюки або сестри), а також аксесуари, що приховують частину обличчя (окуляри або маска). Цей метод є залежним від освітлення, навколишніх умов, які можуть погіршити якість зображення. В той же час існує високий ризик і потенційна небезпека витоку шаблону – фотографії широко поширені в мережі Інтернет.

Як і в інших методах біометричної автентифікації, витік шаблону може призвести до несанкціонованого доступу до декількох сервісів, в яких використовується даний метод автентифікації [41, 42].

Автентифікація за допомогою геометрії руки використовує порівняння таких параметрів руки, як довжина, товщина та форма пальців, ширина і товщина тильної сторони кисті руки, відстані між суглобами, тощо. Отримання шаблону є простим для користувача, на якість шаблону не впливає температура або вологість. Але пристрої для сканування кисті руки потребують певного місця, і такий метод не використовується в мобільних пристроях.

Серед існуючих методів необхідно обрати оптимальний для використання в системі віддаленої автентифікації. Основними параметрами, що характеризують методи є

C_resistance – стійкість до підробок та атак;

C_cost – вартість;

C_simplisity – простота використання для користувача

C_FAR – FAR;

C_FRR – FRR.

C_acceptance – визнання користувачами.

C_recognitionTime – час розпізнавання.

Відповідно до наведених вище критеріїв результуюча функція, яка ставить на меті максимізацію ефективності системи автентифікації, набуває вигляду:

$$ResultAuthFunc = \{\Big[\max\Big(\big([C_{resistance} \to max]\&[C_{simplicity} \to max]\&[C_{acceptance} \to max)\big)\Big] \mid ([C_{FRR} \to min]\&[C_{FAR} \to min]\&[C_{cost} \to min]\&\big[C_{recognitionTime} \to min\big]\Big)]\} \quad (2.1)$$

При максимізації стійкості до підробок та атак, простоти використання та визнання користувачами необхідно забезпечити мінімальний коефіцієнт помилкових прийомів та мінімальну частоту помилкових відмов, а також мінімізувати час розпізнавання та вартість системи.

Для обрання оптимального за сукупністю критеріїв методу необхідно проаналізувати існуючі методи за запропонованим переліком критеріїв та визначити переважний метод біометричної автентифікації.

В роботі для порівняння методів біометричної автентифікації було обрано метод аналізу ієрархій Сааті [43, 44]. Цей метод дозволяє вирішувати багатокритеріальні задачі прийняття рішень, що задовільняють необхідним критеріям.

2.2 Застосування методу аналізу ієрархій для визначення оптимального за сукупністю критеріїв методу біометричної автентифікації

На першому етапі для вирішення задачі вибору оптимального методу необхідно провести структурування проблеми у вигляді ієрархії. Елементам, що розглядаються, присвоюються оцінки за шкалою важливості елементів (табл. 2.1).

Таблиця 2.1 – Шкала важливості

Відносна важливість	Визначення
1	Однакова важливість елементів
3	Незначна перевага одного з елементів
5	Значна перевага одного з елементів
7	Суттєва перевага одного з елементів
9	Сильна перевага одного з елементів
2, 4, 6, 8	Проміжні значення

Після встановлення рівнів ієрархії формується матриця попарних порівнянь, яка вказує на зв'язок між елементами різних рівней, між елементами та критеріями порівняння. Для цього розглядаються елементи $C_i, \ldots, C_j$ другого рівня ієрархії, їх вплив на вибір кращого методу для вирішення конкретної задачі та формується матриця попарних порівнянь.

$$A = \begin{pmatrix} 1 & a_{12} & \ldots & a_{1j} \\ a_{21} & 1 & \ldots & a_{2j} \\ \ldots & \ldots & \ldots & .. \\ a_{i1} & a_{i2} & \ldots & 1 \end{pmatrix}, \tag{2.2}$$

де $a_{ij} = \frac{w_i}{w_j}$ - число, що відповідає значимості елемента C_i по відношенню до C_j.

Також розраховується власний вектор V_i та вектор пріоритетів P_i за формулами [44]:

$$V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}}, j = \overline{1,n}, \tag{2.3}$$

де n – число показників якості.

Вектор пріоритетів показників якості розраховується, як нормовані значення:

$$P_j = \frac{V_j}{S}, j = \overline{1,n}, \tag{2.4}$$

де

$$S = \sum_{j=1}^{n} V_j. \tag{2.5}$$

Після цього обчислюються значення глобального вектора пріоритетів.

$$C_i = \sum_{j=1}^{n} P_j Q_{ij}\ , i = \overline{1,N}, \tag{2.6}$$

де N – число систем, що порівнюються.

При аналізі методів біометричної автентифікації було сформовано наступну ієрархію. На першому рівні розташовано ціль вибору, на другому – критерії, за якими порівнюються методи, а на третьому – можливі методи біометричної автентифікації, між якими здійснюється вибір (рис. 2.2).

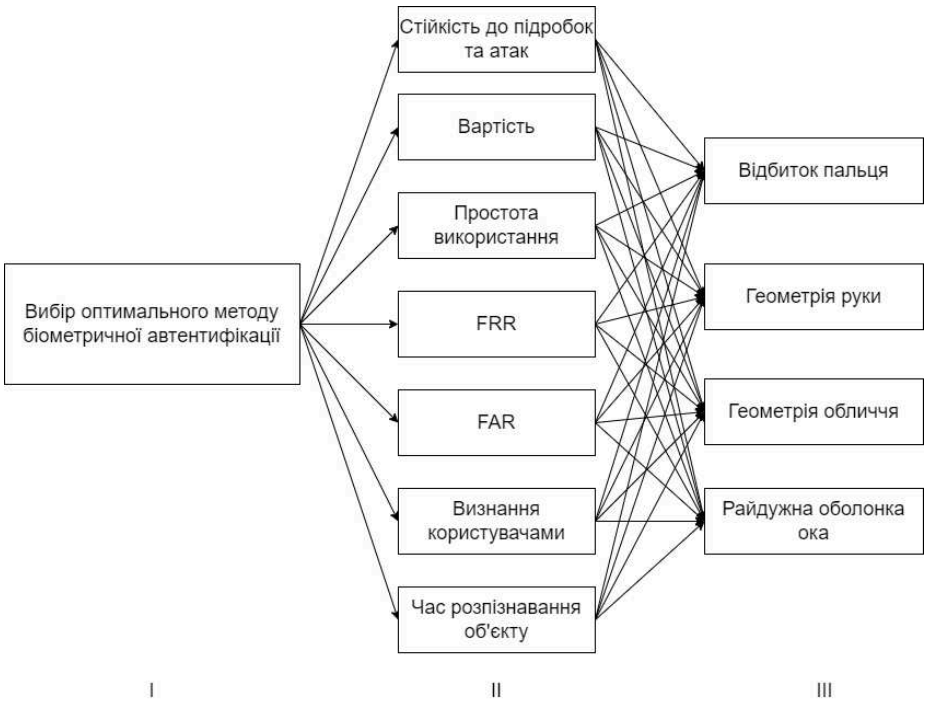

Рисунок 2.2 – Ієрархія для вибору оптимального методу біометричної автентифікації

Для порівняння найбільш розповсюджених методів статичної біометричної автентифікації були проаналізовані наступні показники біометричних систем[45]:

- визнання користувачами (зручність користування; згода на обробку отриманих даних; витрачений час, який потрібен людині для взаємодії з пристроєм);
- стійкість до підробок та атак;
- вартість;
- простота використання;

- FRR (частота відмов в обслуговуванні);
- FAR (частота помилкових спрацьовувань);
- час розпізнавання;
- розмір біометричного шаблону;
- стабільність роботи методу при хворобах та старінні.

Наступним кроком сформовано матрицю попарних порівнянь для критеріїв, за якими оцінюються методи. При її заповненні використано дані досліджень [46], які наведено в таблиці 2.2, де M – середній рівень, L – низький, H – високий. Виконано порівняння важливості обраних критеріїв для системи, що розглядається.

Таблиця 2.2 – Порівняльний аналіз показників біометричної автентифікації

Параметри	Відбиток пальця	Геометрія руки	Геометрія обличчя	Райдужна оболонка ока
Визнання користувачами	M	M	H	M
Стійкість до підробок	M	M	H	M
Вартість	L	H	L	M
Простота використання	H	H	H	M
FAR	2%	2%	1%	0,94%
FRR	2%	2%	1%	0,99%
Стабільність роботи при старінні/ хворобах	H	M	L	H

Для аналізу існуючих методів біометричної автентифікації було присвоєно оцінки за шкалою важливості елементів (табл. 2.1). Було проведено оцінку біометричних методів за шкалою, наведеною в таблиці 2.1. Результат зведено до таблиці 2.3 [37].

Таблиця 2.3 – Аналіз методів біометричної автентифікації за обраними критеріями

Біометричний метод	Визнання користувачами	Стійкість до підробок та атак	Вартість	Простота використання	FRR	FAR	Час розпізнавання	Розмір шаблону	Стабільність роботи при
Відбиток пальця	5	5	7	8	5	5	6	5	9
Геометрія руки	5	6	4	8	5	5	8	9	4
Геометрія обличчя	9	3	7	9	1	6	8	5	3
Райдужна оболонка	4	6	5	6	7	7	7	7	8

На наступному етапі за методом Сааті [42] є розрахунок матриць попарних порівнянь за формулою (2.2). Також, за формулами (2.3) та (2.4) було розраховано власні вектори та вектори пріоритетів. Це дозволило визначити кращий метод за розглянутими критеріями, враховуючи їх важливість для даної системи. Результати проведеного багатокритеріального аналізу наведено на рисунку 2.3.

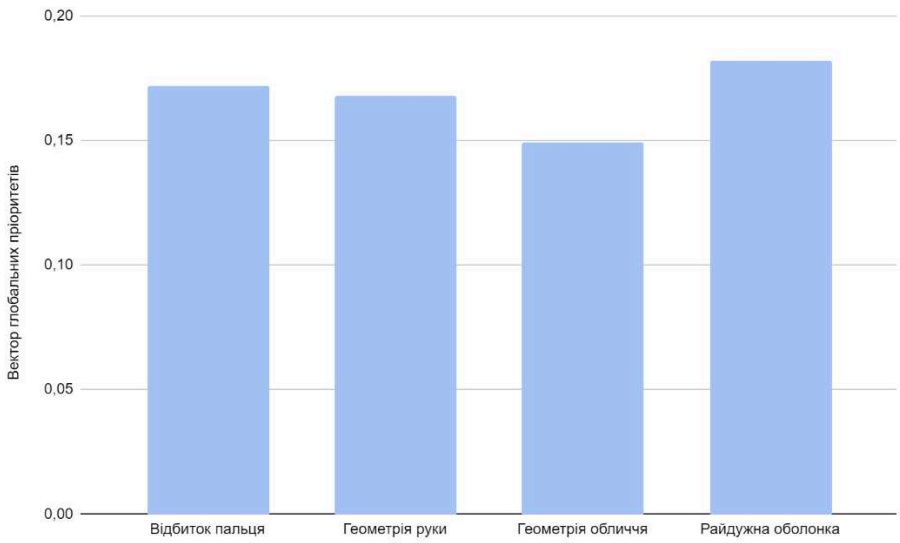

Рисунок 2.3 – Порівняння методів біометричної автентифікації

Оскільки різні характеристики методів мають різну вагу і по-різному сприймаються користувачами, були введені вагові коефіцієнти критеріїв, визначено оптимальний метод автентифікації з урахуванням цих ваг.

Результати аналізу показали, що найбільш високий коефіцієнт пріоритету має біометрична технологія розпізнавання за райдужною оболонкою ока. Близьким за значенням виявився метод розпізнавання особистості за відбитком пальцю.

Для подальшого дослідження було обрано метод біометричної автентифікації за райдужною оболонкою ока.

2.3 Дослідження ефективності методу біометричної автентифікації за райдужною оболонкою ока

Системи автентифікації за райдужною оболонкою ока є одними з найбільш стійких. При даному виді автентифікації розпізнавання відбувається за унікальним для кожної людини рисунком райдужної оболонки ока. Цей рисунок є унікальним для кожної людини, відрізняється навіть у близнюків і залишається незмінним протягом усього життя. Розпізнавання за райдужною оболонкою має наступні переваги. Цей метод автентифікації є швидким та має найвищу точність у порівнянні до інших методів [47]. Оскільки райдужна оболонка лівого та правого ока відрізняється, розпізнавання можна виконувати окремо для кожного ока. Також перевагою є те, що автентифікація можлива, коли людина в головному уборі, масці, окулярах або рукавицях. Завдяки використанню інфрачервоної камери розпізнавання доступне навіть вночі або в темряві. Також така автентифікація є безконтактною.

Підчас автентифікації за райдужною оболонкою ока отримане сенсором зображення проходить наступні етапи. Спочатку відбувається обробка зображення – виділення райдужної оболонки ока, нормалізація зображення, виділення області для генерації коду. Після цього застосовуються фільтри та

генерується двійковий код. Наступним етапом дані заносяться в базу даних і далі використовуються для порівняння даних, отриманих від сенсора та існуючих (рис. 2.4) [36].

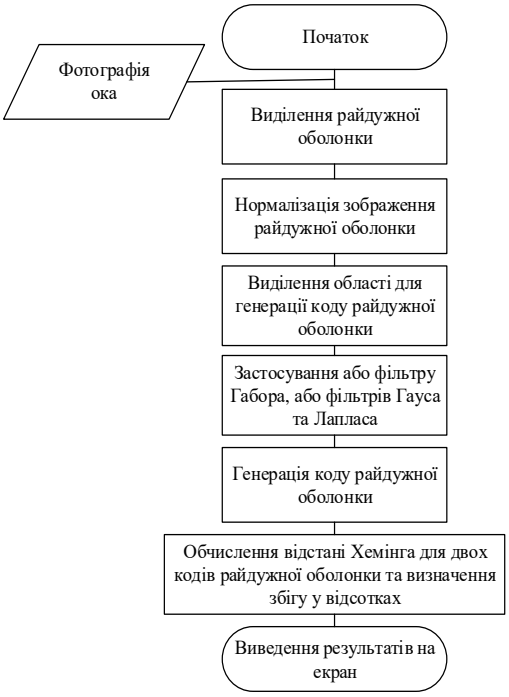

Рисунок 2.4 – Алгоритм розпізнавання за райдужною оболонкою ока

В роботі проведено моделювання алгоритму розпізнавання за райдужною оболонкою ока. При проведенні досліджень було використано зображення ока з бази даних CASIA-Iris-Interval [48]. Якщо зображення кольорові, то на початку необхідно перевести їх в градації сірого. На прикладі зображень (рис. 2.5) продемонстровано роботу програмної моделі процесу обробки райдужної оболонки ока [36].

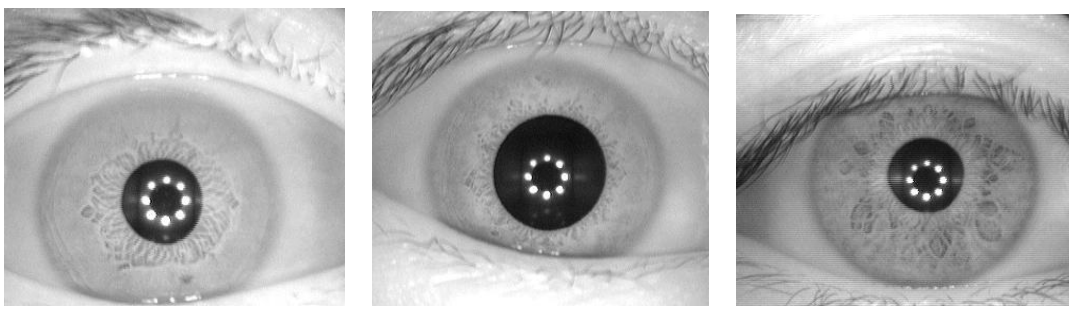

Рисунок 2.5 – Приклади зображень ока для автентифікації

На початку процесу розпізнавання за райдужною оболонкою відбувається знаходження області райдужної оболонки. Цю область можливо апроксимувати двома колами: перше виділяє межу між райдужною оболонкою та склерою, друге – межу між райдужною оболонкою та зіницею [49].

У 1986 році Джон Ф. Кенні розробив детектор краю Canny Edge [50], також відомий як оптимальний детектор. Детектор краю Canny задовільняє трьом критеріям виявлення краю[51]:

- забезпечує низький рівень помилок – виявляє лише існуючі краї;
- мінімізує різницю між реальними пікселями краю та виявленими пікселями;
- виявлений край позначається лише один раз.

Алгоритм виявлення краю за цим алгоритмом описано нижче.

Спочатку відбувається видалення шуму. Зменшення шуму, зглажування незначних деталей зображення є можливим при застосуванні фільтра Гауса [52] та передбачає згортання ядра, описаного функцією Гауса, з пікселями зображення. Функція, яка використовується для створення ядра, є двовимірною функцією Гауса (2.7):

$$f(x,y) = Ae^{-\frac{(x-x_0)^2}{2\sigma x^2}+\frac{(x-y_0)^2}{2\sigma x^2}}, \quad (2.7)$$

де A – амплітуда;

(x_o, y_o) – центр;

σx, σy – стандартні відхилення в напрямках x та y.

Під час обробки зображень розподіл Гауса потрібно апроксимувати ядром згортки. Значення з цього розподілу використовуються для побудови матриці згортки, а потім застосовуються до вихідного зображення, де початкове значення пікселя отримує найбільшу вагу, а сусідні пікселі отримують менші ваги, оскільки їх відстань до вихідного пікселя збільшується [53]. На

рисунку 2.6 наведено приклад зображення після застосування розмиття за Гаусом.

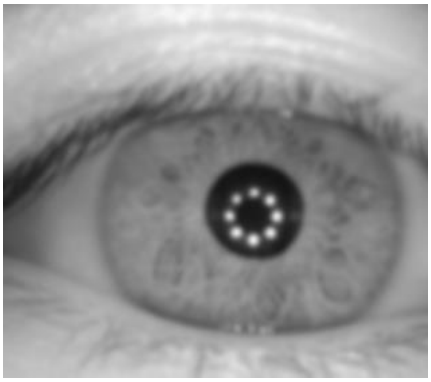

Рисунок 2.6 – Зображення після застосування фільтра Гауса

Наступний крок – виділення райдужної оболонки на зображенні. Виявлення країв є важливим етапом в цифровій обробці та сегментації зображень. Край є елементарною ознакою зображення, містить інформацію, яка відіграє важливу роль для отримання характеристик зображення та розпізнавання об’єктів. Виявлення краю зображення дозволяє зменшити обсяг даних і відсіює небажану інформацію, зберігаючи важливі властивості [37].

Далі за формулами (2.8) та (2.9) знаходиться градієнт зображення, який обчислюється за допомогою масок згортки 3x3 вздовж напрямків x і y [51]:

$$G_x \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix}, \tag{2.8}$$

$$G_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix}. \tag{2.9}$$

Сила градієнта та напрямок країв розраховуються за формулами (2.10) та (2.11) [51]. Після цього видаляються пікселі, які не вважаються частиною краю.

Залишаються лише тонкі лінії, що містять пікселі, які вважаються частиною краю.

$$G = \sqrt{G_x^2 + G_y^2}\ , \tag{2.10}$$

$$\theta = \arctan\left(\frac{G_y}{G_x}\right), \tag{2.11}$$

де G_x та G_y – градієнти вздовж напрямків x і y.

Останній крок – гістерезис. Якщо значення градієнта пікселя перевищує верхнє порогове значення, то піксель вважається крайовим пікселем. Якщо значення градієнта пікселя менше, ніж нижнє порогове значення, то піксель відхиляється. Якщо значення градієнта пікселя знаходиться між нижнім і верхнім пороговими значеннями, тоді піксель буде прийнято, лише якщо він приєднаний до пікселя, який перевищує верхній поріг [51]. Застосування детектора Canny зображене на рисунку 2.7.

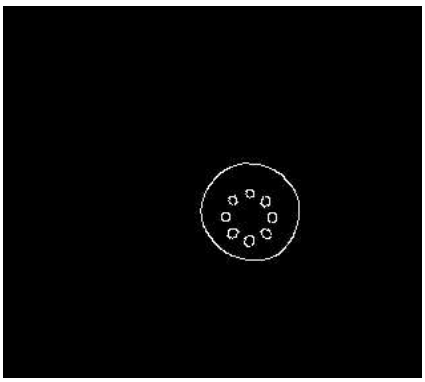

Рисунок 2.7 – Зображення після застосування детектора Canny

Наступним етапом є детектування зіниці. Перетворення Хафа – це стандартний алгоритм комп’ютерного зору, який можна використовувати для визначення параметрів простих геометричних фігур, таких як лінії та кола, присутніх на зображенні. Кругове перетворення Хафа може бути використано для отримання радіусу та координат центру області зіниці та райдужної

оболонки [34, 47]. За формулами (2.12) та (2.13) відбувається знаходження координат *x* та *y* полярної системи координат [37]:

$$x = r * (x_0 + Rcos(\alpha)), \tag{2.12}$$

$$y = r * (y_0 + Rsin(\alpha)), \tag{2.13}$$

де x_0 та y_0 – координати центру зображення райдужної оболонки;

R – радіус райдужної оболонки;

$r = \sum_{j=0}^{n} \frac{j}{n}$;

n – висота нормалізованого зображення;

j – значення координати ординати у пікселях нормалізованого зображення;

α – кутова координата, що розраховується за формулою $\sum_{i=0}^{\theta} \alpha = \frac{2\pi i}{\theta}$;

θ – ширина нормалізованого зображення;

i – значення координати абсциси у пікселях нормалізованого зображення.

Радіус та координати центру кола зіниці, які знайдено з використанням перетворення Хафа наведено на скріншоті (рис. 2.8).

```
x = 137.0; y = 177.0; r = 42
center = {137.0, 177.0}
radius = 42
```

Рисунок 2.8 – Радіуси центру кола після перетворення Хафа

Зовнішній контур райдужної оболонки було виділено з урахуванням діаметру оболонки 10-13 мм [37]. Виділено зовнішні та внутрішні межі райдужної оболонки ока на зображенні (рис. 2.9).

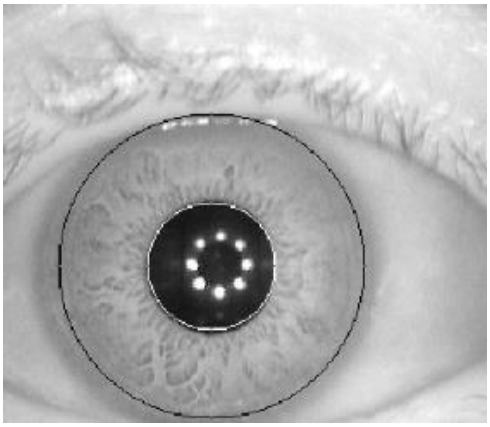

Рисунок 2.9 – Виділення контуру райдужної оболонки

Далі необхідно вилучити з зображення лише необхідну частину. Результат наведено на рисунку 2.10.

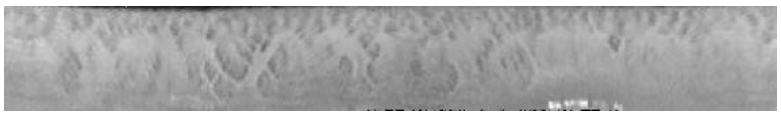

Рисунок 2.10 – Отриманий контур у полярних координатах

Далі з зображення видаляється інформація, яка не потрібна для процесу ідентифікації. Наприклад, це можуть бути фото повік. На рисунку 2.11 наведено зображення, яке приведене до необхідного вигляду.

Рисунок 2.11 – Контуру райдужної оболонки перед вилученням даних

Після отримання необхідної частини зображення відбувається застосування фільтру. В даній роботі розглянуто застосування фільтру Габора або комбінації фільтру Гауса та оператора Лапласа [37].

Одним із методів вилучення особливостей із зображення є фільтри Габора. Процес керується принципом невизначеності Габора, який стверджує,

що добуток роздільної здатності частоти на час має бути більшим за константу [54]. Ідея фільтрів Габора заснована на визначенні певних базисних функцій, що складаються з гаусових і синусоїдальних функцій. Цей фільтр застосовується для вилучення фазової інформації з обраної області. Фазова складова не залежить від контрасту зображення і освітлення [55].

Дійсні частини ядер фільтра Габора будуються за формулами (2.14–2.16) [34]:

$$g(x, y;\ \lambda, \theta, \psi, \sigma, \gamma) = e^{\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right)} \cos\left(2\pi \frac{x'}{\lambda}\right) + \psi, \tag{2.14}$$

$$x' = x\cos(\theta) + y\sin(\theta), \tag{2.15}$$

$$y' = x\sin(\theta) + y\cos(\theta), \tag{2.16}$$

де λ – довжина хвилі множника-косинуса;

θ – орієнтація нормалі паралельних смуг функції Габора в градусах;

ψ – зміщення за фазою в градусах;

γ – коефіцієнт стиснення, що характеризує елептичність функції Габора;

x – рядок у матриці ядра;

y – стовпець у матриці ядра.

На рисунку 2.12 наведено зображання після застосування фільтру Габора.

Рисунок 2.12 – Застосування фільтру Габора

Іншим варіантом є використання комбінації фільтру Гауса та оператора Лапласа. У цьому випадку фільтрація виконується згортанням кожної точки

вхідного масиву з гаусовим ядром та їх подальшого складання для створення вихідного масиву. Для виділення шуму використовується фільтр Гауса за формулою (2.6). Фільтр Лапласа базується на операторі Лапласа, особливість якого полягає в тому, що в області границі інтенсивності пікселів мають високу різницю. Лапласіан є двовимірною ізотропною мірою другої просторової похідної зображення [56]. Лапласіан зображення виділяє області швидкої зміни інтенсивності та часто використовується для виявлення країв. Лапласіан *L(x,y)* зображення зі значеннями інтенсивності пікселів *I(x,y)* задається наступною формулою (2.17):

$$L(x, y) = \frac{\delta^2 I}{\delta x^2} + \frac{\delta^2 I}{\delta y^2}, \tag{2.17}$$

де *x* – рядок у матриці ядра;

y – стовпець у матриці ядра.

Використання цього методу дозволяє зменшити рівень хибного прийняття або відхилення, зменшує залежність алгоритму від розташування зіниці та райдужної оболонки, зменшує час обробки та складність обчислення, порівняно з іншими методами [37]. Це є важливим, оскільки в практичних застосуваннях обробка зображення райдужної оболонки повинна бути точною і швидкою.

Використання цього фільтру показано на рисунку 2.13.

Рисунок 2.13 – Застосування комбінації фільтрів Гауса та оператора Лапласа

Наступним етапом виконується створення біометричного шаблону. Біометричний шаблон – це компактне представлення біометричної ознаки, що містить інформацію, яка необхідна для розпізнавання особи. Зображення райдужної оболонки зазвичай представляється у вигляді двійкового рядка

фіксованої довжини (IrisCode), який отримується шляхом бінаризації характеристик фільтрів, застосованих до даного зображення [57]. В залежності від того, який колір представляє піксель зображення після застосування фільтру, використовуються «0» – для чорного та «1» – для білого. Таким чином, підсумкова довжина коду райдужної оболонки залежить від кількості точок, тобто кількості пікселів зображення.

Перед внесенням даних користувача до бази даних виконується перевірка на наявність його даних. При внесенні даних про нового користувача їм присвоюється ідентифікатор.

Під час процесу розпізнавання користувача на вхід системи поступає зображення ока, виконується його обробка (виділення контуру райдужної оболонки, нормалізація та виділення необхідної ділянки), накладання фільтру та проведення генерації коду райдужної оболонки ока. Після цього виконується перебір усіх наявних кодів та їхнє порівняння з щойно отриманим за допомогою відстані Хемінга. Відстань Хемінга дорівнює числу позицій, в якій відповідні елементи двох послідовностей однакової довжини різні, і обчислюється за формулою 2.18:

$$d_{ij} = \sum_{k=1}^{p} \left| x_{ik} - x_{jk} \right|, \tag{2.18}$$

де d_{ij} – відстань Хемінга для послідовностей i та j;

p – довжина послідовностей;

k – номер елементу;

x – елемент.

Якщо в базі даних знайдено шаблон, який відповідає щойно згенерованому коду, пошук припиняється, та користувачу надається допуск до необхідних даних.

2.4 Результати дослідження

Для аналізу ефективності роботи та стійкості до завад алгоритмів з використанням фільтра Габора та фільтра Гауса і оператора Лапласа на тестові зображення було накладено шум Перліна. Результати виявлення порогу шуму наведено на рисунку 2.14.

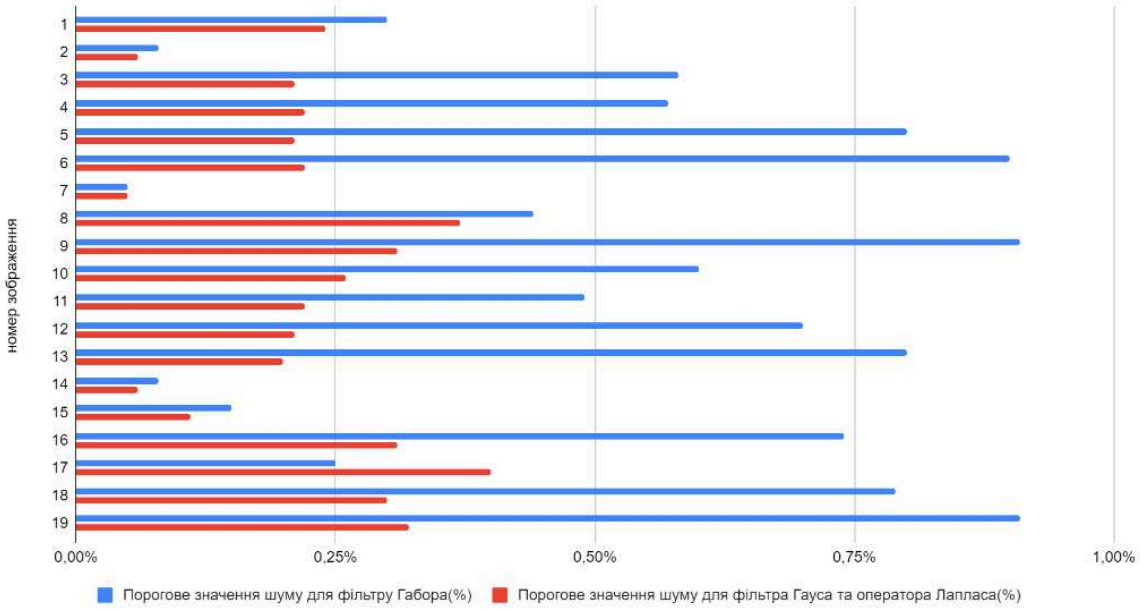

Рисунок 2.14 – Значення порогу шуму для досліджуваних фільтрів

Значення SNR, які було отримано за формулою (2.19) дозволяють провести аналіз рівня завад, який був внесений пороговим значенням шуму для кожного зображення.

$$SNR = \sum_{x,y}(C_{x,y})^2 / \sum_{x,y}(C_{x,y} - S_{x,y})^2, \quad (2.19)$$

де $C_{x,y}$ – значення пікселя оригінального зображення;

$S_{x,y}$ – значення пікселя зображення після накладення шуму;

x – номер рядка;

y – номер стовпця.

Отримані за формулою (2.20) значення середньоквадратичного відхилення MSE (Mean Square Error) дозволяють кількісно оцінити величину спотворення оригінальних зображень:

$$MSE = \frac{1}{XY}\sum_{x,y}(C_{x,y} - S_{x,y})^2, \quad (2.20)$$

де $C_{x,y}$– значення пікселя оригінального зображення;

$S_{x,y}$– значення пікселя зображення, на яке був накладений шум X – кількість рядків пікселів;

Y – кількість стовпців пікселів;

x – номер рядка;

y – номер стовпця.

Результати отриманих значень SNR та MSE при використанні різних фільтрів зведені в таблицю 2.4 [37].

Таблиця 2.4 – Результати значень SNR та MSE

	Фільтр Габора			Фільтр Гауса та оператор Лапласа		
№	Поріг шуму	SNR	MSE	Поріг шуму	SNR	MSE
1	2	3	4	5	6	7
1	0,30%	903,554	0,7534	0,24%	1002,56	0,6223
2	0,08%	5693,88	0,1019	0,06%	5693,88	0,1019
3	0,58%	701,555	1,0883	0,21%	1279,66	0,5201

Продовження таблиці 2.4

1	2	3	4	5	6	7
4	0,57%	637,09	1,1933	0,22%	1364,99	0,5825
5	0,80%	493,31	1,5636	0,21%	1373,18	0,517
6	0,90%	315,263	1,9502	0,22%	1243,95	0,5637
7	0,05%	4484,2	0,149	0,05%	4484,2	0,149
8	0,44%	1719,13	0,6809	0,37%	2085,07	0,5691
9	0,91%	348,905	1,9371	0,31%	910,96	0,7212
10	0,60%	450,362	1,4835	0,26%	1347,67	0,5123
11	0,49%	539,07	1,1144	0,22%	1282,39	0,5058
12	0,70%	453,353	1,4313	0,21%	883,443	0,6069
13	0,80%	390,077	1,8531	0,20%	1455,69	0,5592
14	0,08%	3173,49	0,2199	0,06%	3173,43	0,2198
15	0,15%	5538,27	0,1334	0,11%	5538,27	0,1334
16	0,74%	426,166	1,6139	0,31%	1019,82	0,7377
17	0,25%	346,255	1,8381	0,40%	1293,74	0,6528
18	0,79%	364,068	1,8408	0,30%	1205,53	0,6798
19	0,91%	349,177	1,999	0,32%	1012,94	0,6989

Отримані вищі значення SNR характеризують меншу кількість шуму на зображеннях. Це говорить про те, що фільтр Габра та комбінація фільтру Гауса та оператора Лапласа є стійкими до накладання шуму. Як видно з таблиці 2.4, значення SNR при використанні фільтрів Гауса та оператора Лапласа є більшими від SNR при використанні фільтру Габору, а порогові значення шуму навпаки є меншими. Аналізуючи отримані значення, можна зробити висновок,

що використання комбінації фільтрів Гауса та оператора Лапласа забезпечує більшу стійкість до шумів.

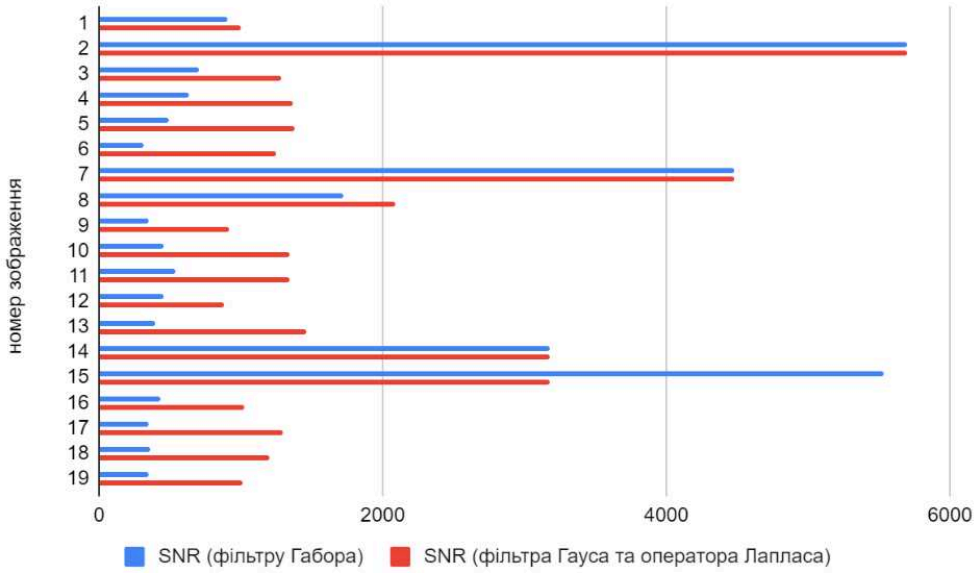

Рисунок 2.15 – Значення SNR для досліджуваних фільтрів

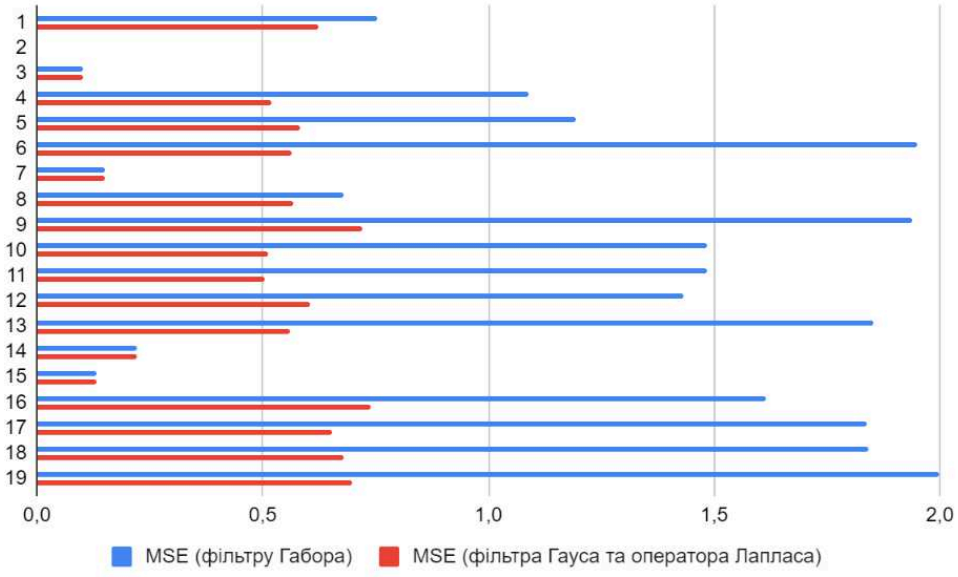

Рисунок 2.16 – Значення MSE для досліджуваних фільтрів

Значення SNR при використанні фільтра Гауса та оператора Лапласа в середньому в 2,3 рази більше, ніж при використанні фільтра Габора. При вищих

значеннях SNR отримано менші значення MSE, які, в свою чергу, в середньому в 2,1 рази є меншими у разі використання фільтра Гауса та оператора Лапласа.

Якість зображення може призвести до помилкового позитивного рішення про надання доступу або до помилкової відмови в доступі. Для оцінки ймовірності виникнення помилок розраховано FAR (False Acceptance Rate) та FRR (False Rejection Rate). Враховуючи максимальне значення MSE при зашумлених зображеннях та використанні фільтру Габора, було визначено, що майже 90% протестованих зображень мають ймовірність FAR близьку до нуля. Значення FRR досліджуваних зображень дорівнює 0,295 при використанні фільтру Габора та 0,047 при використанні комбінації фільтру Гауса та оператора Лапласа. Показники ймовірності виникнення помилок свідчать про те, що використання в алгоритмі автентифікації за райдужною оболонкою ока фільтрів Гауса та оператора Лапласа забезпечує кращу якість [37].

На рисунку 2.17 наведено схему біометричної автентифікації з врахуванням отриманих результатів.

Рисунок 2.17 – Схема з урахуванням результатів (обраний фільтр)

При наявності переваг, описаних вище, перед традиційними системами автентифікації у систем біометричної автентифікації є певні недоліки.

Можливі наступні помилкові спрацьовування: системи біометричної автентифікації іноді можуть неправильно ідентифікувати осіб, наприклад, сканер відбитків пальців може не розпізнати відбиток пальця людини, якщо він брудний або заплямований. Можуть виникнути проблеми з освітленням та

якістю зображення при роботі з камерою, що призведе до незручностей для користувачів.

Якщо системи біометричної автентифікації зберігають інформацію про людей, наприклад, їхні відбитки пальців або риси обличчя, то існує ймовірність крадіжки цих даних та використання для несанкціонованого доступу.

У відповідності до цього виникає проблема захисту цих даних як у пристроях, в базах даних, так і під час передачі мережею. Розглянемо основні методи захисту біометричних шаблонів.

2.5 Огляд методів захисту біометричних шаблонів

Біометричні шаблони мають бути унікалними та не пов’язаними, для того, щоб при компрометації даних була можливість відізвати та створити новий шаблон. Також перетворені шаблони повинні бути сформовані таким чином, щоб не було можливості відновити початковий біометричний зразок .

В [31, 58] запропоновано різні схеми захисту біометричних шаблонів.

Схеми захисту біометричних шаблонів зазвичай класифікуються, як біометричні криптосистеми (також називаються допоміжними схемами на основі даних) і біометрія з можливістю скасування (cansalable biometrics, також відома як трансформація функцій).

На рисунку 2.18 наведено основні методи захисту біометричних шаблонів [31]. Надійність роботи таких систем залежить від того, чи добре захищено ключ чи пароль. При використанні методів на основі однобічних перетворень зазвичай обчислювально важко відновити оригінальний шаблон по трансформованому навіть при наявності ключа [37, 61].

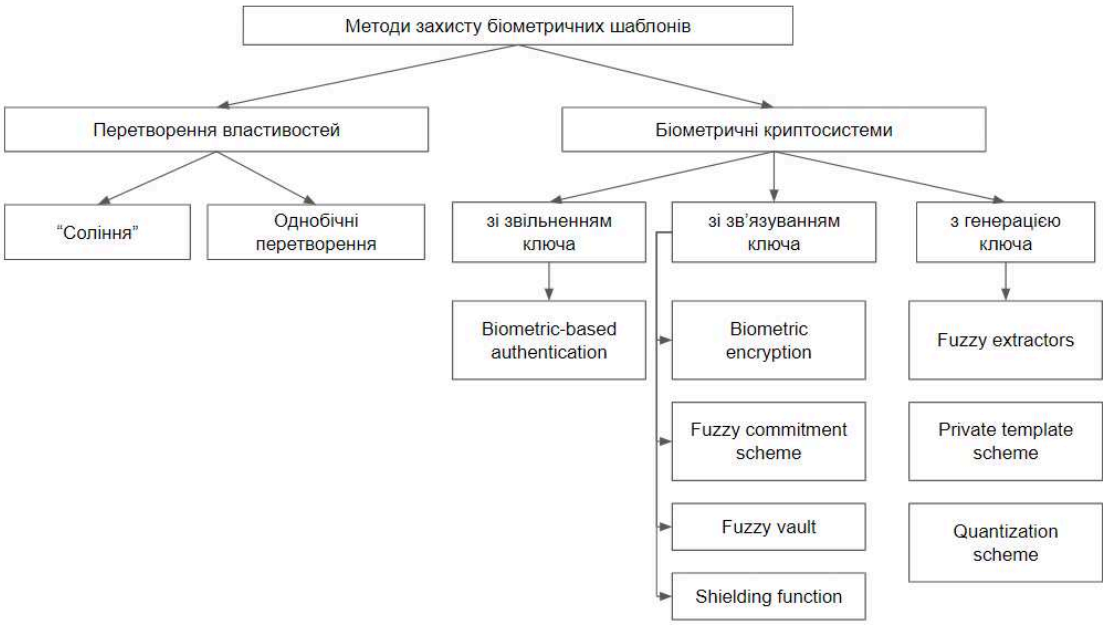

Рисунок 2.18 – Методи захисту біометричних шаблонів

У підходах трансформації ознак до біометричного шаблону застосовується необоротна або одностороння функція. Трансформований шаблон зберігається в базі даних як псевдонімний ідентифікатор, параметри перетворення зберігаються як допоміжні дані. Під час автентифікації використання допоміжних даних робить можливим застосування тієї ж функції перетворення до біометричного шаблону та порівняння трансформованого шаблону зі збереженим в базі даних (рис. 2.19) [57]. Такі методи ділять на методи «соління» та методи з використанням однобічних перетвореннь в залежності від типу функції, що використовується [34, 59].

Соління або біохеш — це підхід захисту шаблону, у 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 поданий під час автентифікації. Ця потреба в додатковій інформації у вигляді ключа збільшує ентропію біометричного шаблону і, отже, ускладнює для противника вгадування шаблону [34].

Методи захисту біометричних шаблонів, які засновані на використанні «соління» передбачають модифікацію отриманих біометричних ознак за допомогою функції, яка залежить від ключа або пароля користувача. Використання нечітких контейнерів на основі застосування методів «соління» є ефективним методом побудови множини представлень біометричних даних біометричного зразку. Ефективність цього методу досягається збільшенням ентропії біометричних даних при накладенні на біометричні зразки псевдовипадкових послідовностей. Також використання ключа призводить до збільшення відстані Хемінга між біометричними зразками. До недоліків можна віднести те, що при компрометації ключа, шаблон не буде безпечним. Також методи повинні забезпечувати високий рівень якості розпізнавання навіть під час змін в біометричних даних користувача [37].

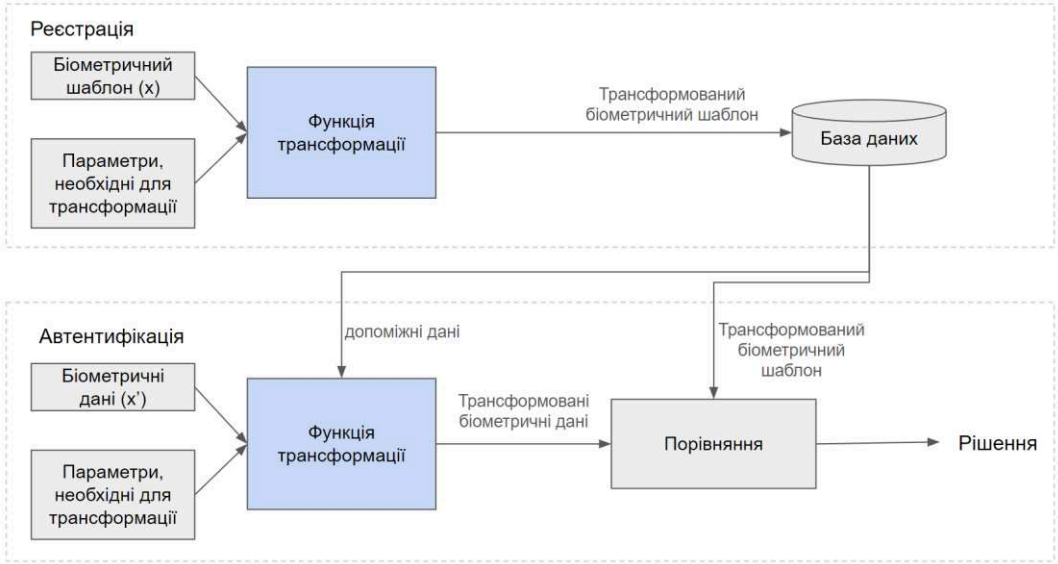

Рисунок 2.19 – Узагальнена схема методів перетворення властивостей

Методи, засновані на однобічних перетвореннях, передбачають шифрування біометричного шаблону за допомогою однобічної функції. Параметри цієї функції формуються за допомогою спеціального ключа, який повинен бути доступним під час процесу автентифікації користувача.

Головною особливістю такого підходу є складність відновлення початкових біометричних даних [37].

Параметри функції визначаються ключем, який повинен бути доступним під час автентифікації. Основними характеристиками такого підходу є те, що при наявності трансформованого біометричного шаблону обчислювально важким є відновлення оригінальних біометричних даних і при компрометації ключа забезпечується вищий рівень безпеки. Недоліком цього методу є те, що 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, що ускладнює проектування такої функції [34, 37, 59].

Біометричні криптосистеми на нечітких екстракторах та на нечітких контейнерах будуються з використанням завадостійкого кодування [34, 60, 57]. На першому етапі біометричні дані в певному сенсі «об'єднуються» з кодовими словами або синдромними послідовностями. Для нечітких екстракторів додатково утворюються відкриті допоміжні дані, які допомагають при вилученні секретного параметра на нечітких заданих біометричних даних (рис. 2.20). На етапі автентифікації застосовується завадостійке декодування, що усуває можливу невизначеність, яка може бути викликана 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)[34].

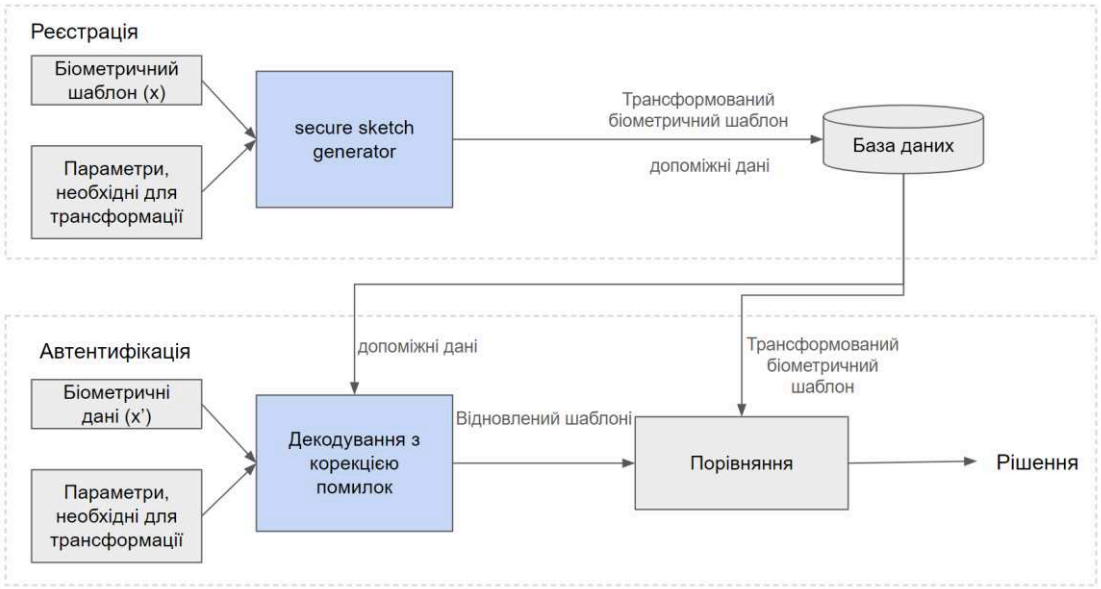

Рисунок 2.20 – Узагальнена схема методів біометричних криптосистем

Біометричні криптосистеми можна розділити на системи зі звільненням ключа (key release cryptosystems), системи зі зв’язуванням ключа (key binding cryptosystems) та системи з генерацією ключа (key generation cryptosystems) [62].

2.6 Дослідження методів захисту біометричних шаблонів

Під час досліджень було сформовано біометричні шаблони зі зразків зображень, але зберігання коду райдужної оболонки в базі даних та використання в такому вигляді є небезпечними. Для дослідження захисту біометричного коду було використано методи, на основі зворотніх та незворотніх перетворень. Реалізовано методи подібні до BIN-SALT, BIN-COMBO, алгоритми яких описано в роботі [63], а також метод Min-Hashing. Метод BIN-COMBO використовує лише інформацію з самої біометрії, BIN-SALT використовує додаткову зовнішню випадкову інформацію для спотворення [66].

Для розгорнутих зображень райдужної оболонки в градаціях сірого зазвичай два зображення поєднуються в пікселі за допомогою додавання або множення.

При використанні методу BIN-SALT [63] шаблон райдужної оболонки (iriscode) представлений матрицею $m \times n$ $X \in \{0, 1\}$, де m – номер рядка, n – номер стовпця. X може бути згенерований фільтрацією Габора до розгорнутої області райдужної оболонки та двійковим квантуванням. Потім бінарний алгоритм «соління» математично описується для одного класу,

$$Y = K \oplus X, \tag{2.21}$$

де K – матриця випадкового ключа розміром $m \times n$ для бінарної «солі» з бінарним елементом;

Y – $m \times n$ перетворений біометричний шаблон;

$\oplus$ – операція XOR.

Випадковий ключ K зазвичай отримується двійковим квантуванням випадкових значень із гауссового розподілу $N(0,1)$ для кожного елемента. Цей метод виконує умови захисту інформації для систем біометрії з можливістю скасування. Нормалізована відстань Хеммінга (NHD) зазвичай використовується для порівняння двійкових шаблонів, точність і оборотність можна підтвердити обчисленням каскадної операції XOR. При компрометації випадкового ключа K вихідний біометричний шаблон X можна повністю відновити з Y і K.

В реалізованій програмі «соління» коду райдужної оболонки було реалізовано метод BIN-SALT. За допомогою генератору випадкових чисел до коду райдужної оболонки ока було згенеровано бінарний ключ, довжина якого дорівнювала довжині коду райдужної оболонки. Бінарний ключ був згенерований лише один раз і є спільним для всіх біометричних шаблонів. Програма передбачає генерацію нового ключа у разі викрадення біохешу

одного з користувачів. В якості ключа також може використовуватися модифікований пароль користувача (наприклад, при двохфакторній автентифікації). Недоліком усіх варіацій методів біометричного «соління» є те, що у разі отримання бінарного ключа або секретного вектору зловмисник зможе відновити код райдужної оболонки користувача [66].

Другий метод – метод на основі незворотнього перетворення BIN-COMBO. За допомогою генератора випадкових чисел було створено послідовність, кількість елементів в якій дорівнювала кількості рядків в оригінальному коді райдужної оболонки. Кожне значення згенерованої послідовності визначає кількість елементів, на які слід обернути елементи рядка. Після цього за допомогою генератора випадкових чисел було обрано просте число. Усі рядки, порядкові номери яких ділилися на це число, були з'єднані з наступними за ними рядками за допомогою операції XOR. Недоліком даного методу є те, що у зв'язку із скороченням коду райдужної оболонки після модифікацій ефективність системи розпізнавання погіршилася [66].

Третій метод – Min-Hashing [64]. У процесі роботи алгоритму Min-Hashing записується індекс першої зустрічі біту, який дорівнює 1, для ряду двійкових векторів, рядки яких були перемішані. Нехай A і B – два індексні вектори, породжені з двійкового вектора, h – хеш-функція, яка рахує хеші для елементів цих множин. Далі слід визначити функцію h_{min} (S), яка обчислює функцію h для всіх членів будь-якої безлічі S і повертає найменше її значення. Після цього необхідно обчислити h_{min} (A) і h_{min} (B). Порівняння значень h_{min} (A) і h_{min} (B) не дасть бажаного результату, оскільки ймовірність того, що вони будуть стовідсотково рівні, дуже низька. Вирішити цю проблему можна за допомогою коефіцієнту подібності Жаккара, який вимірює подібність між множинами.

Він визначається як розмір перетину, поділений на величину з'єднання двох множин, і наведений у наступній формулі:

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A|+|B|-|A \cap B|}, \quad (2.22)$$

де A – перша множина;

B – друга множина.

За описаним алгоритмом Min-Hashing була зроблена програмна реалізація третього зазначеного методу захисту біометричних шаблонів. Для знаходження коефіцієнту подібності Жаккара було запрограмовано наступну формулу, яка відображає формулу 5.1:

$$\mathrm{J}(a,b) = \frac{c}{a+b-c}, \quad (2.23)$$

де a – кількість елементів у першому біохеші;

b – кількість елементів у другому біохеші;

c – кількість елементів, яка знаходиться в обох біохешах.

Коефіцієнт подібності Жаккара також може використовуватися для порівняння біохешей, які були згенеровані за допомогою перших двох методів.

Варто зазначити, що коефіцієнт Жаккара не є єдиною мірою знайдення подібності хешованих кодів райдужної оболонки ока. Знайти міру подібності можна також за допомогою відстані Хемінга [66]. Вона представляє собою кількість бітових позицій, в яких два біта різні, і розраховується за наступною формулою:

$$\mathrm{d_{ij}} = \sum_{\mathrm{k=1}}^{\mathrm{p}} \left| \mathrm{x_{ik}} - \mathrm{x_{jk}} \right|, \quad (2.24)$$

де d_{ij} – відстань Хемінга для послідовностей i та j;

p – довжина послідовностей;

k – номер елементу;

x – елемент.

Наступним кроком є знаходження відсотоку подібності двох біохешей, оскільки кількість елементів є достатньо великою і може змінюватися при зміні розміру частини райдужної оболонки ока, яка використовується для аналізу.

Після результатів порівняння біохешей одним із зазначених методів програма аналізує, чи є достатнім результат подібності, щоб допустити користувача далі. Даний поріг для обох методів був визначений за допомогою експериментальних досліджень. У наступному розділі порівнюються усі зазначені методи біометричного захисту шаблону у використанні із різними методами знаходження подібності, а також визначається ймовірність кожного до помилок у відхиленні доступу зареєстрованому користувачу чи його наданні зловмиснику [66].

2.7 Аналіз ефективності методів захисту біометричного шаблону

Описані у попередньому розділі методи захисту біометричного шаблону райдужної оболонки ока були протестовані на 100 зображеннях з бази CASIA-Iris-Interval. Для оцінки ефективності роботи програмної реалізації на основі описаних вище алгоритмів були проведені дослідження. Оцінено вплив методів захисту біометричних шаблонів на ефективність розпізнавання.

Спочатку було порівняно методи на основі перетворення властивостей. Для незахищеного коду райдужної оболонки та описаних вище методів захисту біометричного шаблону BIN-COMBO та BIN-SALT проведено аналіз отриманих значень відстаней Хемінга, порівняння з яким визначає прийняття рішення про надання доступу користувачу. Для прикладу наведемо відстані Хемінга у відсотках для десяти незахищених кодів райдужної оболонки (табл. 2.5) [66].

Таблиця 2.5 – Відстань Хемінга між незахищеними кодами райдужної оболонки.

Номер зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
img1	100%	72%	79%	59%	67%	70%	75%	75%	70%	69%
img2	72%	100%	71%	58%	65%	68%	71%	69%	65%	65%
img3	79%	71%	100%	60%	70%	70%	75%	74%	71%	71%
img4	59%	58%	60%	100%	57%	57%	59%	60%	58%	57%
img5	67%	65%	70%	57%	100%	63%	66%	66%	62%	62%
img6	70%	68%	70%	57%	63%	100%	69%	69%	65%	64%
img7	75%	71%	75%	59%	66%	69%	100%	71%	68%	68%
img8	75%	69%	74%	60%	66%	69%	71%	100%	68%	67%
img9	70%	65%	71%	58%	62%	65%	68%	68%	100%	64%
img10	69%	65%	71%	57%	62%	64%	68%	67%	64%	100%

Згідно з таблицею 2.5 значення відстані Хемінга для даних зразків різних користувачів знаходяться між 57% та 79% Враховуючи це, порогове значення відстані Хемінга для незахищеного шаблону райдужної оболонки ока обрано рівним 80% (рис. 2.21).

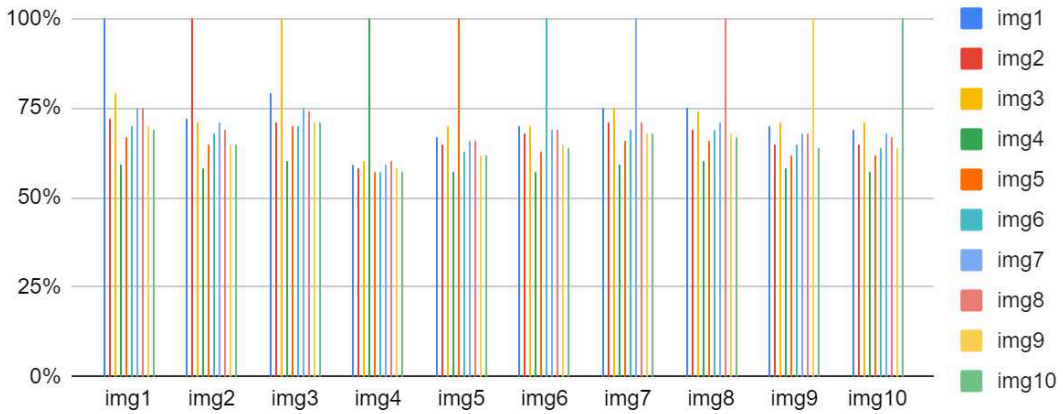

Рисунок 2.21 – Значення відстані Хемінга між незахищеними кодами райдужної оболонки

Аналогічним чином було встановлено порогові значення відстані Хемінга при використанні методу «соління» BIN-SALT та методу перетворення ознак

BIN-COMBO. Результати порівняння біометричних шаблонів зображень райдужних оболонок, які були захищені за допомогою методу біометричного «соління», наведені у таблиці 2.6.

Таблиця 2.6 – Відстань Хемінга між захищеними кодами райдужних оболонок ока за допомогою біометричного «соління»

Номер зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
img1	100%	73%	77%	60%	67%	71%	75%	75%	71%	70%
img2	73%	100%	71%	58%	65%	68%	72%	69%	66%	66%
img3	77%	71%	100%	60%	70%	71%	75%	75%	71%	71%
img4	60%	58%	60%	100%	58%	58%	59%	60%	59%	58%
img5	67%	65%	70%	58%	100%	63%	67%	66%	63%	63%
img6	71%	68%	71%	58%	63%	100%	70%	70%	66%	64%
img7	75%	72%	75%	59%	67%	70%	100%	72%	69%	68%
img8	75%	69%	75%	60%	66%	70%	72%	100%	68%	68%
img9	71%	66%	71%	59%	63%	66%	69%	68%	100%	64%
img10	70%	66%	71%	58%	63%	64%	68%	68%	64%	100%

Виходячи з даних таблиці 2.6 можна виділити найменшу та найбільшу відстані Хемінга. Після використання методу BIN-SALT для захисту біометричного шаблона найменше значення відстані Хемінга збільшилося на 1%, а найбільше значення зменшилось на 2%. Таким чином, порогове значення відстані Хемінга у разі використання методу біометричного «соління» становить 78% (рис. 2.22) [66].

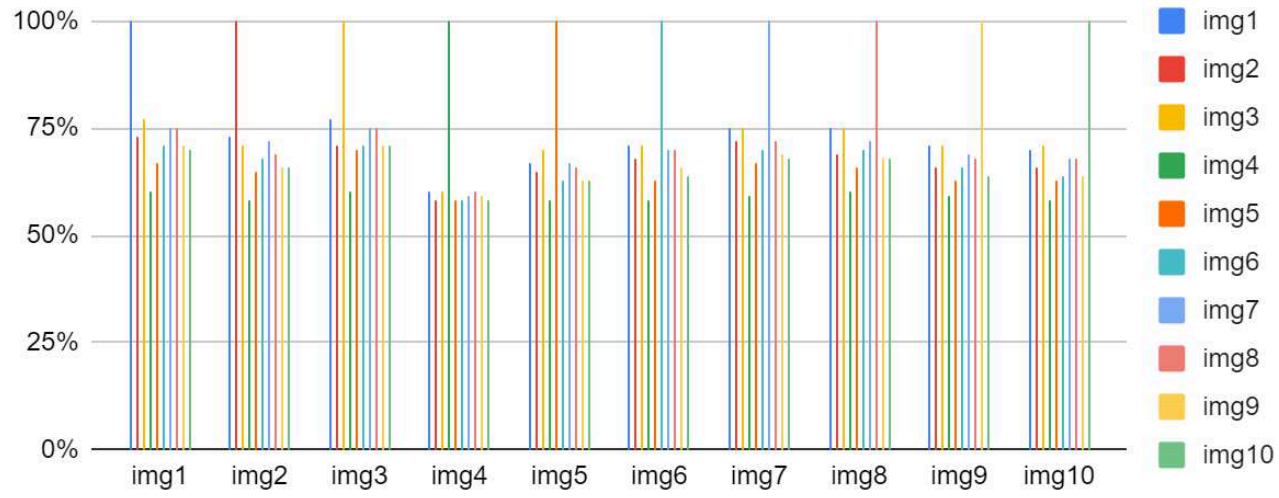

Рисунок 2.22 – Відстань Хемінга між захищеними кодами райдужних оболонок ока за допомогою біометричного «соління»

Результати порівнянь кодів райдужних оболонок після застосування до них незворотної трансформації із використанням методу BIN-COMBO за допомогою відстані Хемінга наведені у таблиці 2.7.

Таблиця 2.7 – Значення відстані Хемінга у відсотках між захищеними кодами райдужок за допомогою методу BIN-COMBO.

Номер зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
img1	100%	71%	76%	60%	67%	70%	73%	73%	70%	69%
img2	71%	100%	70%	58%	65%	68%	70%	68%	65%	76%
img3	76%	70%	100%	60%	70%	70%	74%	73%	70%	70%
img4	60%	58%	60%	100%	58%	58%	60%	59%	59%	58%
img5	67%	65%	70%	58%	100%	63%	66%	65%	62%	62%
img6	70%	68%	70%	58%	63%	100%	69%	68%	65%	64%
img7	73%	70%	74%	60%	66%	69%	100%	70%	68%	67%
img8	73%	68%	73%	59%	65%	68%	70%	100%	67%	66%
img9	70%	65%	70%	59%	62%	65%	68%	67%	100%	64%
img10	69%	65%	70%	58%	62%	64%	67%	66%	64%	100%

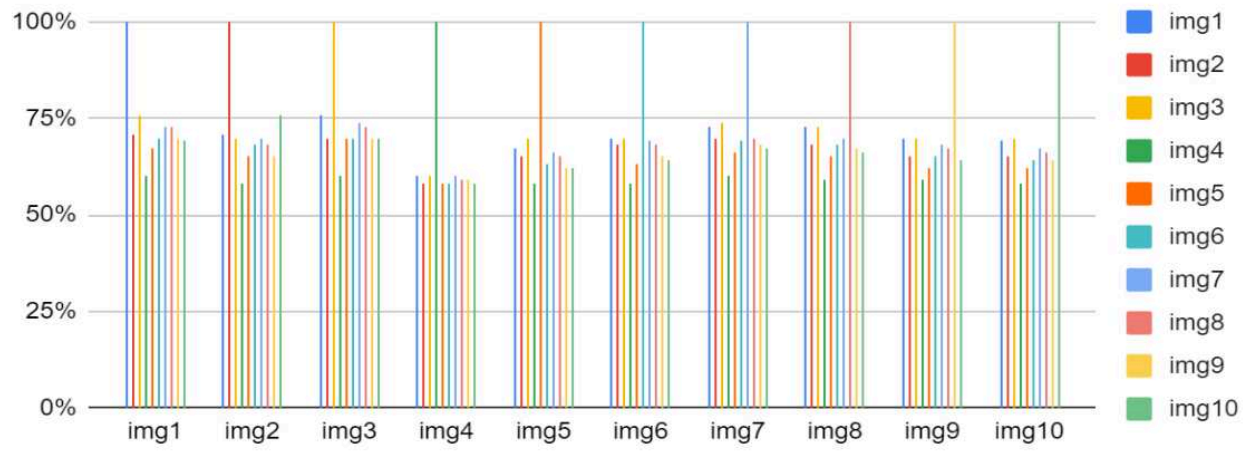

Рисунок 2.23 – Значення відстані Хемінга між захищеними кодами райдужних оболонок ока за допомогою методу BIN-COMBO

Проаналізувавши дані в таблиці 2.7, можна виділити найменшу та найбільшу різниці у відстані Хемінга шаблонів райдужних оболонок ока, що досліджувались. Найменше значення для захищеного коду райдужки за допомогою методу BIN-COMBO становить 58%, а найбільше – 76%, що на 4% нижче, ніж при використанні незахищених шаблонів та на 2% менше, ніж при використанні методу BIN-SALT. Пороговим значенням було обрано 77% [66].

Таким чином, метод перетврення ознак BIN-COMBO виявився кращим з двох змодельованих методів захисту біометричного шаблону.

Наступним кроком цей метод було порівняно з методом Min-Hashing. Для порівняння було обрано коефіцієнт Жаккара (2.22), оскільки хеш-функції не можна порівнювати між собою за допомогою відстані Хемінга. Результати порівнянь кодів райдужних оболонок після застосування Min-Hashing для десяти зображень наведені у таблиці 2.8 [66].

Виходячи з даних таблиці 2.8 найменше значення коефіцієнту Жаккара становить 0,03. Найбільше значення становить 0,136. У зв’язку з цим порогове значення коефіцієнту Жаккара для цього методу було обране 0,14 (рис. 2.24).

Таблиця 2.8 – Значення коефіцієнту подібності Жаккара після застосування Min-Hashing

Номер зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
img1	1	0,095	0,136	0,050	0,094	0,096	0,121	0,119	0,079	0,091
img2	0,095	1	0,112	0,051	0,088	0,083	0,100	0,107	0,076	0,091
img3	0,136	0,112	1	0,051	0,118	0,110	0,133	0,121	0,093	0,120
img4	0,050	0,051	0,051	1	0,039	0,042	0,053	0,051	0,030	0,052
img5	0,094	0,088	0,118	0,039	1	0,084	0,087	0,102	0,064	0,091
img6	0,096	0,083	0,110	0,042	0,084	1	0,088	0,095	0,073	0,087
img7	0,121	0,100	0,133	0,053	0,087	0,088	1	0,107	0,082	0,094
img8	0,119	0,107	0,121	0,051	0,102	0,095	0,107	1	0,085	0,101
img9	0,079	0,076	0,093	0,030	0,064	0,073	0,082	0,085	1	0,074
img10	0,091	0,091	0,120	0,052	0,091	0,087	0,094	0,101	0,074	1

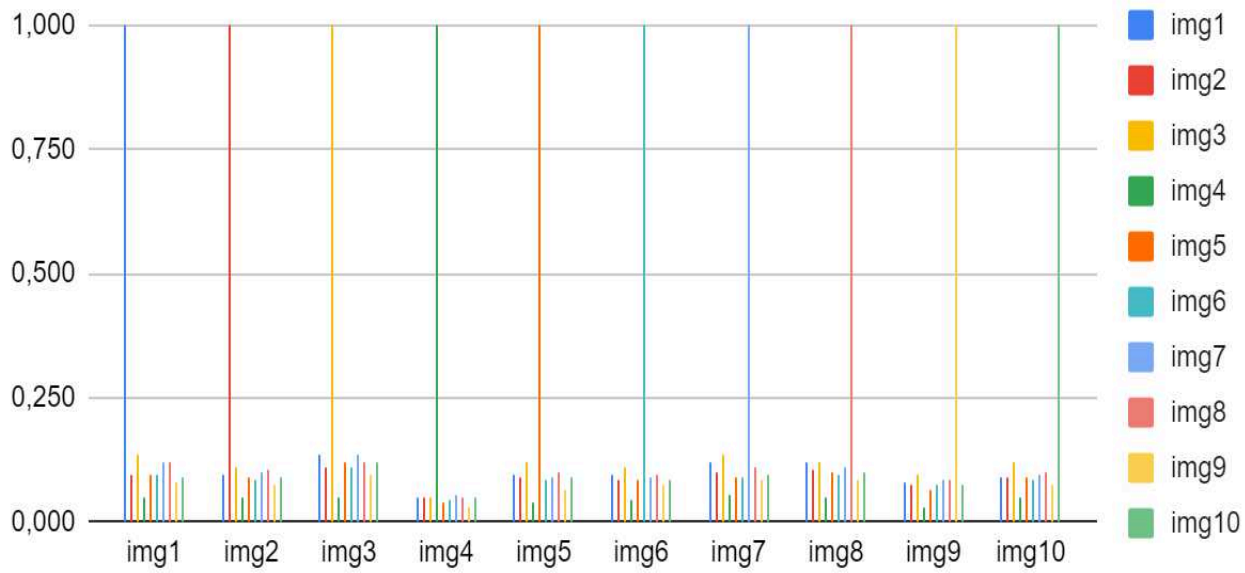

Рисунок 2.24 – Значення коефіцієнту подібності Жаккара після застосування методу Min-Hashing

Порівняння значення коефіцієнту Жаккара між захищеними кодами райдужок за допомогою методу BIN-COMBO наведено в таблиці 2.9 [66].

Таблиця 2.9 – Значення коефіцієнту подібності Жаккара після застосування методу BIN-COMBO

Номер зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
img1	1	0,082	0,118	0,031	0,082	0,080	0,103	0,096	0,064	0,080
img2	0,082	1	0,091	0,038	0,068	0,067	0,076	0,077	0,053	0,077
img3	0,118	0,091	1	0,035	0,098	0,090	0,103	0,100	0,071	0,088
img4	0,031	0,038	0,035	1	0,025	0,028	0,036	0,028	0,024	0,033
img5	0,082	0,068	0,098	0,025	1	0,068	0,067	0,085	0,049	0,080
img6	0,080	0,067	0,090	0,028	0,068	1	0,075	0,080	0,053	0,070
img7	0,103	0,076	0,103	0,036	0,067	0,075	1	0,069	0,058	0,068
img8	0,096	0,077	0,100	0,028	0,085	0,080	0,069	1	0,059	0,078
img9	0,064	0,053	0,071	0,024	0,049	0,053	0,058	0,059	1	0,058
img10	0,080	0,077	0,088	0,033	0,080	0,070	0,068	0,078	0,058	1

Значення коефіцієнту Жаккара для методу BIN-COMBO знаходяться в діапазоні між 0,024 та 0,118, що робить цей метод кращим серед трьох розглянутих методів (рис. 2.25).

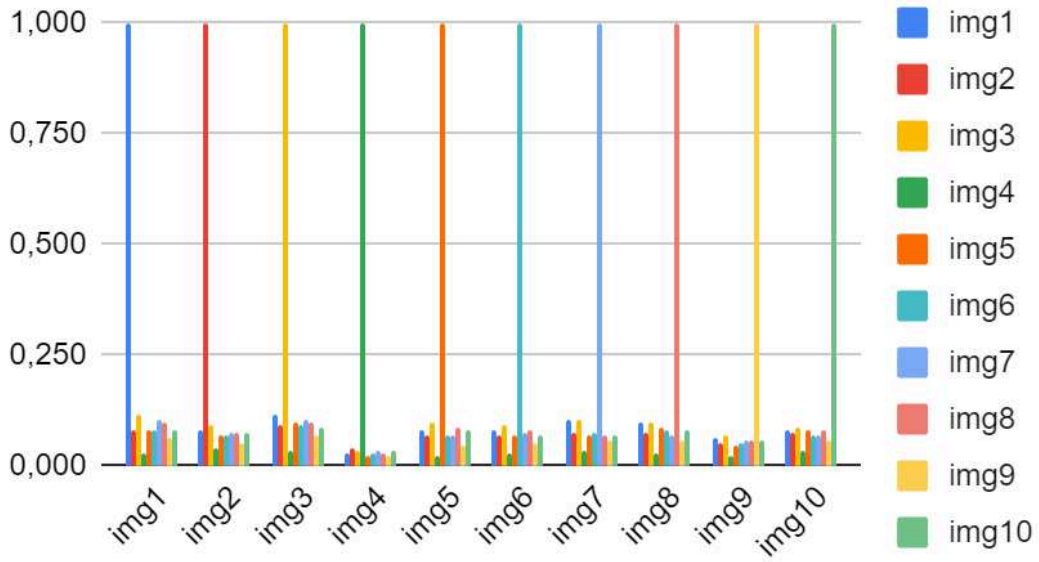

Рисунок 2.25 – Значення коефіцієнту подібності Жаккара після застосування методу BIN-COMBO

Для дослідження ефективності та стійкості описаних вище методів захисту біометричних шаблонів у поєднанні з однаковими методами обробки фотографії до зображень було застосовано шум Перліна.

В основі цього шуму лежить функція, що має псевдовипадковий вигляд, але всі її візуальні деталі мають однаковий розмір. Ця властивість дозволяє контролювати накладання шуму. Для накладання шуму Перліна на зображення райдужної оболонки ока було розроблено програму на мові програмування Java. Дана програма передбачає накладання шуму на зображення за наданим відсотком. Приклад зображення після накладання шуму Перліна наведений на рисунку 2.26 [66].

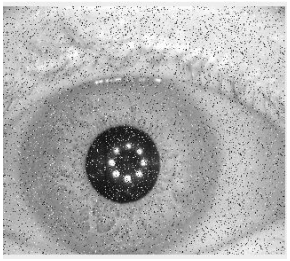

Рисунок 2.26 – Зображення ока після накладання шуму

На зображення, що досліджуються, було накладено шум Перліна у різних відсотках. Було визначено відсоток шуму для оригінальних та захищених кодів райдужної оболонки. Результати досліджень порогового значення шуму для зазначених вище варіантів наведені у таблиці 2.10 [66].

Таблиця 2.10 – Порогові відсотки шуму для кожного з досліджуваних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки.

Номер зображення	Пороговий відсоток шуму при незахищеному коді райдужки	Пороговий відсоток шуму при використанні BIN-SALT	Пороговий відсоток шуму при використанні BIN-COMBO	Пороговий відсоток шуму при використанні Min-Hashing
01	1.5	2.8	2.15	0.97
02	1.05	1.1	1.10	3.7

Продовження таблиці 2.10

03	0.21	0.85	0.80	0.21
04	0.51	0.52	0.51	0.51
05	0.18	0.16	0.18	0.15
06	0.57	0.55	0.57	0.49
07	0.15	0.17	0.18	0.15
08	0.62	0.62	0.64	0.61
09	0.19	0.19	0.19	0.17
10	0.52	0.52	0.52	0.52

Візуально простежити відмінність та подібність між відсотками шуму для різних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки можна на гістограмі, зображеній на рисунку 2.27.

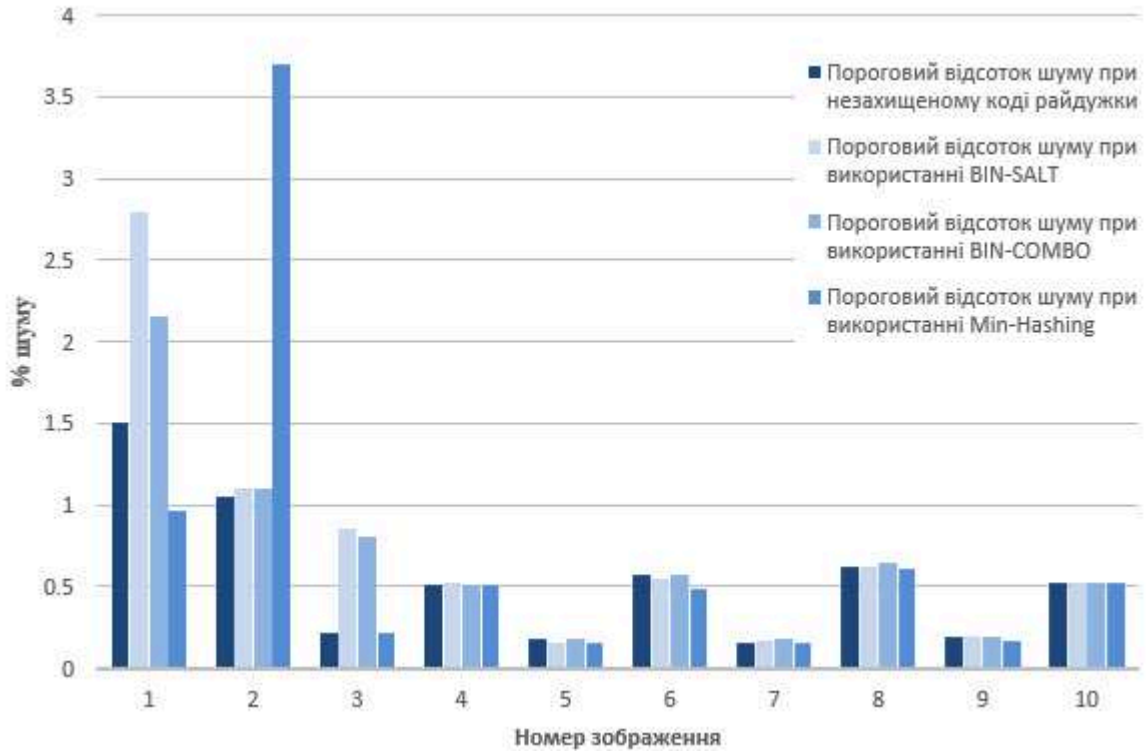

Рисунок 2.27 – Гістограма значень порогів шуму для різних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки ока

Виходячи з результатів, наведених на рисунку 2.27, можна зробити висновок, що поріг шуму при незахищеному коді райдужної оболонки є

найнижчим серед усіх інших майже для всіх фотографій, в той час, як показники при використанні Min-Hashing є відносно нестабільними.

Для того, щоб проаналізувати рівень завад, що був внесений пороговим значенням шуму, було обчислено значення SNR (signal to noise ratio) (2.15) для кожного зображення при використанні різних методів захисту біометричного шаблону та при відсутності їх використання. Також SNR використовується для визначення характеристики якості зображення. Для аналізу величини спотворень оригінального зображення було розраховане MSE за формулою (2.18). Отримані показники зведено до таблиці 2.11 [66].

Таблиця 2.11 – Значення SNR та MSE.

№ зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
	Незахищений код райдужної оболонки									
Шум (%)	1,5	1,05	0,21	0,51	0,18	0,57	0,15	0,62	0,19	0,52
SNR	415,7	544,5	3039,0	1719,0	5146,8	1408,0	4859,4	1193,7	5462,3	1880,4
MSE	100,5	52,5	9,4	15,6	15,6	23,9	7,5	38,5	4,9	14,1
	BIN-SALT									
Шум (%)	2,8	1,1	0,85	0,52	0,16	0,55	0,17	0,62	0,19	0,52
SNR	225,66	544,47	663,47	1694,67	5146,77	1531,09	4859,42	1193,72	5462,32	1880,42
MSE	145,103	52,5139	43,0102	15,851	4,8185	21,9568	7,4757	38,5234	4,9289	14,1279
	BIN-COMBO									
Шум (%)	2,15	1,1	0,8	0,51	0,18	0,57	0,18	0,64	0,19	0,52
SNR	296,49	544,46	747,67	1435,2	5146,77	1407,97	4859,42	1115,17	5462,32	1880,42
MSE	140,8807	52,5139	38,1663	18,7167	4,8185	23,8768	7,4757	41,2367	4,9289	14,128
	Min-Hashing									
Шум (%)	0,97	3,7	0,21	0,51	0,15	0,49	0,15	0,61	0,17	0,52
SNR	605,91	152,58	3038,98	1718,95	5146,77	1778,62	4859,42	1193,72	5462,32	1880,42
MSE	68,9377	147,3877	9,3899	15,6271	4,8185	18,9011	7,4757	38,5234	4,9289	14,1279

Виходячи з результатів показників SNR, наведених у таблиці 2.11, меншому відсотку шуму відповідають більші показники SNR, що характеризують низьку кількість завад на зашумлених зображеннях. Таким

чином, можна зробити висновок, що усі описані алгоритми є стійкими, оскільки вони мало чутливі до накладання шуму. Для порівняння значень SNR та виділення найбільш стійкого до завад методу показники співвідношення SNR для різних методів було побудовано гістограму, яка наведена на рисунку 2.28.

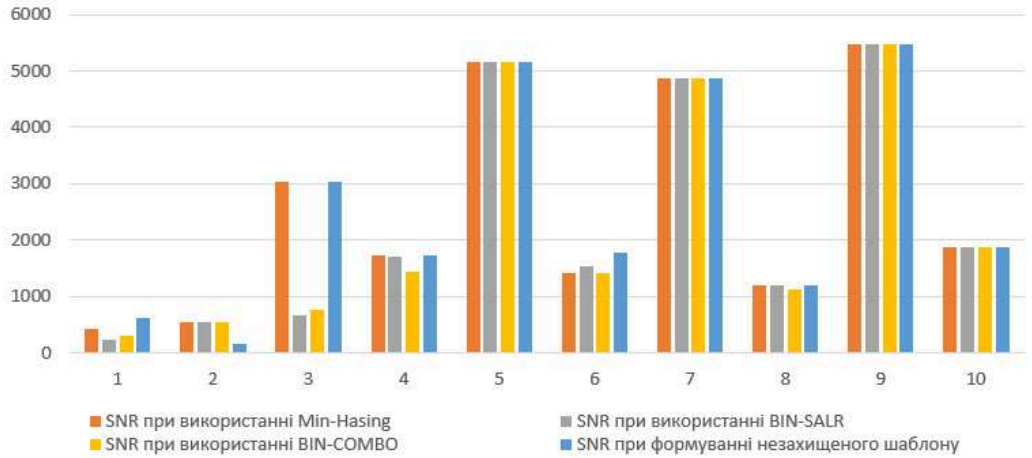

Рисунок 2.28 – Значення SNR між оригінальними та зашумленими зображеннями

Виходячи з даних, наведених на рисунку 2.28, можна зробити висновок, що найбільш чутливими до завад виявилися алгоритм розпізнавання по райдужній оболонці ока із використанням Min-Hashing та алгоритм без використання будь-яких методів захисту біометричного шаблону. Натомість найменш чутливим до завад є алгоритм із використанням BIN-COMBO для захисту коду райдужної оболонки. Такі показники зумовлені тим, що під час генерації біохешу за цим методом, деяка кількість важливої інформації втрачається під час операції XOR, яка застосована для двох рядків.

Оскільки найближчі показники SNR до показників SNR незахищеного шаблону має алгоритм із використанням Min-Hashing, можна зробити висновок, що даний метод захисту біометричного шаблону менше за інші спотворює важливу інформацію і є найбільш точним у порівнянні з BIN-SALT та BIN-COMBO [66].

Результати розрахунків MSE між оригінальними зображеннями наведені у таблиці 2.12.

Таблиця 2.12 – Показники MSE між оригінальними зображеннями

Номер зображення	img1	img2	img3	img4	img5	img6	img7	img8	img9	img10
img1	0	3427.6	3619.3	5434.2	3845.7	3490.4	2556.8	2278.1	3785.8	4061.5
img2	3427.6	0	1643.9	3556.4	1683.4	3930.7	3710.1	4760.2	2108.2	2207.0
img3	3619.3	1643.9	0	2670.7	2019.6	2737.3	3031.9	4671.8	1827.7	2130.2
img4	5434.2	3556.4	2670.7	0	2609.1	2884.2	4037.5	5289.7	2218.7	2147.6
img5	3845.7	1683.4	2019.6	2609.1	0	2952.8	3144.6	4585.4	1228.8	1431.2
img6	3490.4	3930.7	2737.3	2884.2	2952.8	0	1573.0	2975.2	2576.6	2940.8
img7	2556.8	3710.1	3031.9	4037.5	3144.6	1573.0	0	2768.1	3314.9	3617.1
img8	2278.1	4760.2	4671.8	5289.7	4585.4	2975.2	2768.1	0	4350.5	4081.6
img9	3785.8	2108.2	1827.7	2218.7	1228.8	2576.6	3314.9	4350.5	0	1650.3
img10	4061.5	2207.0	2130.2	2147.6	1431.2	2940.8	3617.1	4081.6	1650.3	0

Із даних, наведених у таблиці 2.12, можна визначити, що найменше значення MSE становить 1431, найбільше – 5434,2.

Оцінити ймовірність виникнення помилок при розпізнаванні для кожного алгоритму можна за допомогою наступних показників.

1) Коефіцієнт помилкового спрацьовування (False Acceptance Rate, FAR). Даний показник представляє собою процентний поріг, який визначає ймовірність того, що одна людина може бути прийнята за іншу.

2) Коефіцієнт помилкової відмови в доступі (False Rejection Rate, FRR). Даний показник представляє собою ймовірність того, що зареєстрована людина може бути не розпізнана системою.

Із зменшенням кількості помилкових пропусків кількість помилкових відхилень буде зростати і навпаки. Точка, в якій перетинаються лінії, також має назву – рівний показник помилок (Equal Error Rate, EER). У цій точці відсоток помилкових пропусків та помилкових відхилень однаковий [25]. Ідеальний

графік кореляції коефіцієнту помилкового пропуску та коефіцієнту помилкової відмови в доступі наведений на рисунку 2.29.

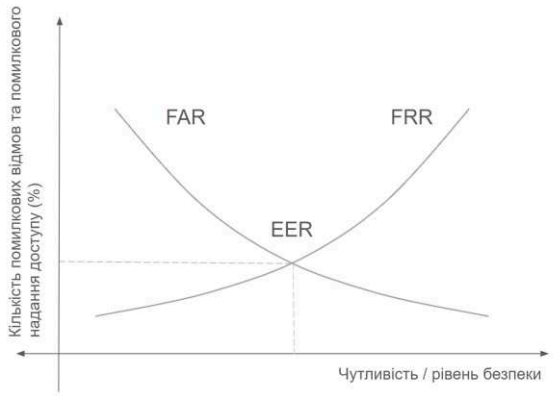

Рисунок 2.29 – Графік кореляції показників FAR та FRR

Зазвичай зниження FAR до найнижчого можливого рівня призведе до різкого збільшення показника FRR. Значення FAR та FRR можуть бути налаштовані в програмному забезпеченні системи безпеки шляхом коригування відповідних критеріїв. У досліджуваній програмі це можна зробити за допомогою коригування порогу допуску, який був вище визначений експериментальним шляхом для кожного із методів захисту біометричного шаблону та для незахищеного коду.

Для підрахунку коефіцієнту помилкового пропуску були обрані найбільші значення MSE та знайдено кількість показників MSE між оригінальними зображеннями. Після цього кількість таких значень було поділено на кількість усіх можливих пар різних зображень, окрім пари з однаковими зображеннями. У результаті були отримані значення FAR для всіх варіантів алгоритмів.

Для підрахунку коефіцієнту помилкової відмови в доступі кожне значення MSE для зашумлених зображень для кожного варіанту алгоритму було помножене на коефіцієнт, а саме збільшено у стократному розмірі. Після цього була знайдена кількість показників відмінності для кожного конкретного

зображення між усіма іншими, які менше значення MSE для конкретного зображення між відповідним йому зашумленим зображенням. У результаті таких розрахунків були отримані значення FRR для всіх варіантів алгоритмів. Підраховані за зазначеними вище алгоритмами показники FAR та FRR наведені у таблиці 2.13 [66].

Таблиця 2.13 – Значення показників FAR та FRR для досліджуваних методів

Характеристика алгоритму	FRR	FAR
Незахищений біометричний шаблон	0.26	0.15
Використання BIN-SALT для створення біохешу	0.33	0.46
Використання BIN-COMBO для створення біохешу	0.34	0.42
Використання Min-Hashing для створення біохешу	0.24	0.46

Отже, виходячи з показників FAR та FRR, наведених у таблиці 2.19, можна зробити висновок, що нижчу ймовірність помилок має алгоритм розпізнавання по райдужній оболонці ока, в якому не застосований жодний із методів захисту біометричного шаблону. Серед алгоритмів із захистом біометричного шаблону найбільш кращі показники має алгоритм із використанням BIN-COMBO для створення біохешу. Кращий показник FRR серед розглянутих алгоритмів має алгоритм із використанням Min-Hashing. Виходячи з цього можна зробити висновок, що система із використанням Min-Hashing буде достатньо зручною для користувача. Показники FAR серед алгоритмів із використанням методів біометричного шаблону мають незначні відмінності, а для Min-Hashing та BIN-COMBO є рівними. В той же час показник FRR є значно кращим для алгоритму із використанням Min-Hashing для створення біохешу [66].

Ефективність роботи алгоритмів також може бути оцінена за критерієм швидкості роботи методу захисту біометричного шаблону. Цей параметр є важливим, оскільки довгий час обробки при великій кількості зображень у базі

даних може спричинити незручність у використанні. Крім того, цей показник може допомогти визначити обчислювальні потужності для сервера, на якому будуть зберігатися захищені біометричні шаблони та буде відбуватись автентифікація користувачів. Час роботи програми був підрахований для вищерозглянутих методів.

Кожний з алгоритмів був протестований у сукупності з етапами виділення райдужної оболонки ока, нормалізації зображення, виділення найбільш інформативного фрагменту, накладання фільтру та генерації коду райдужної оболонки. Результати швидкості роботи програми на основі алгоритму розпізнавання за райдужною оболонкою ока в залежності від кількості біохешей або кодів користувачів у базі наведені у таблиці 2.14 [66].

Таблиця 2.14 – Час роботи програми в залежності від кількості шаблонів у базі

Кількість шаблонів у базі	Час роботи програми (мс)			
	Незахищені шаблони	BIN-SALT	BIN-COMBO	Min-Hashing
1	2	3	4	5
1	6462	7133	7207	7168
2	6473	7190	7102	8457
3	6546	7431	7234	9798
4	6559	7400	7294	12228
5	6598	8131	8114	15490
6	6617	8143	8302	17076
7	6687	8207	8549	20469
8	6697	8302	9160	24973
9	6764	8521	10078	29416
10	6929	8881	10440	33586

Виходячи з даних, наведених у таблиці 2.20, можна зробити висновок, що збільшення кількості біометричних шаблонів впливає на час обробки шаблонів. При використанні методу BIN-SALT час зростає в 1,2 рази, BIN-COMBO – в 1,4

рази, Min-Hashing – в 4,8 рази порівняно з обробкою незахищених шаблонів. У зв'язку з цим велика кількість зображень при малих потужностях облікових машин може змусити користувача чекати, що може впливати на зручність користування пристроєм [64].

На рисунку 2.30 наведено графіки часу обробки шаблонів в залежності від кількості зображень при використання різних алгоритмів захисту.

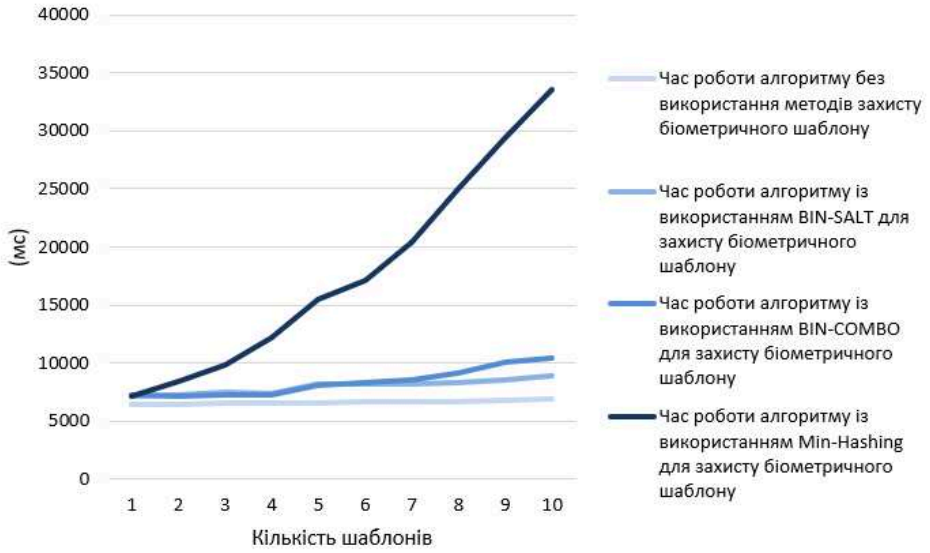

Рисунок 2.30 – Графік залежності часу роботи програми при використанні різних алгоритмів від кількості шаблонів у базі

Таким чином, було проведено дослідження якості роботи системи автентифікації за райдужною оболонкою ока без використання методів захисту біометричного шаблону та при використанні різних алгоритмів захисту. Дослідження показали, що найменша ймовірність помилкових відхилень доступу для зареєстрованих користувачів та помилкового надання доступу отримані при використанні алгоритму без використання методів захисту біометричного шаблону, який не є безпечним. Інші алгоритми, в яких використовується захист біометричного шаблону, мають близькі показники коефіцієнту ймовірності надання доступу зловмиснику. Найменші значення

показника коефіцієнту ймовірності відмови у доступі зареєстрованому користувачу має алгоритм із використанням Min-Hashing, але він має найгірші показники з часу. Також, згідно з аналізом SNR, алгоритм із використанням Min-Hashing є найбільш чутливим до завад, оскільки має найбільші значення у співвідношенні «сигнал/шум».

Отже, незважаючи на довший час обробки, алгоритм з використанням Min-Hashing для захисту біометричного шаблону райдужної оболонки ока людини є найбільш ефективним, оскільки є найбільш зручним для користувачів у зв'язку з найнижчим показником коефіцієнту помилкової відмови зареєстрованому користувачу та найбільш стійким до завад у порівнянні з іншими методами захисту біометричного шаблону райдужної оболонки ока, які були досліджені у даній роботі.

2.8 Висновки до розділу 2

Проаналізовано основні методи біометричної автентифікації. Методом багатокритеріальної оптимізації визначено метод, оптимальний за критеріями визнання користувачами, стійкості до підробок та атак, вартості, простоти використання, частоти відмов в обслуговуванні та частота помилкових спрацьовувань. Провдено оцінку біометричних методів автентифікації після ранжування за шкалою важливості та розраховано вектори пріоритетів. Поведений аналіз за вищеперерахованими критеріями показав, що найвищий вектор глобальних пріоритетів за методом аналізу ієрархій виявився для методу автентифікації за райдужною оболонкою ока, що на 0,01 вище ніж у методу автентифікації за відбитком пальця та на 0,033 вище ніж у методу автентифікації за геометрією руки.

Для дослідження цього методу була побудована експериментальна модель за допомогою мови програмування Java.

Ця модель дозволила визначити найкращий за критеріями FAR та FRR набір фільтрів. Запропоновано методи захисту біометричного шаблону. Найкращий результат показав метод з використанням фільтрів Гауса та оператора Лапласа.

Визначено переважний за критеріями завадозахищеності та ймовірності помилки метод біометричної автентифікації (моб. мережі), відмінністю якого є врахування стійкості до завад в каналах зв’язку. Це дало змогу підвищити завадостійкість та ефективність систем віддаленої автентифікації в телекомунікаційних мережах. Найбільш стійким до завад виявився метод BIN-COMBO.

Список використаних джерел у даному розділі наведено у повному списку використаних джерел під номерами 34-64.

3 ДОСЛІДЖЕННЯ МЕТОДІВ ПРИХОВУВАННЯ ШАБЛОНУ

Для систем автентифікації актуальним є питання безпеки біометричних даних, що передаються по мережі, так як існує ймовірність їх перехоплення. Для вирішення цієї проблеми доцільно використовувати сукупність методів: формування біохеша для захисту даних від компрометації та мережної стеганографії для підвищення стійкості та прихованості процесу віддаленої автентифікації.

3.1 Застосування стеганографічних систем для підвищення захищеності біометричного шаблону

Стеганографічна система – це сукупність методів і засобів, завдяки яким формується прихований канал передачі інформації [66]. Інформація, яка має бути передана приховано, може бути вбудована у стегоконтейнер. Стегоконтейнером може бути зображення, аудіо-, відеофайли або та інша інформація, що має надмірність. При незначній модифікації таких контейнерів факт передачі вбудованих даних складно виявити. Основною метою стеганографії є забезпечення передавання даних відкритим каналом зв’язку від відправника до одержувача даних таким чином, щоб повідомлення було передано непоміченим та незміненим.

На рисунку 3.1 наведено узагальнену схему стеганографічної системи.

Системи, в яких мають бути забезпечені високі характеристики безпеки, під час вбудовування можуть використовувати ключ безпеки та шифрування даних. В загальному вигляді вбудовану систему можна визначити як:

$$C' = Em(C, En(S, k_1), k_2), \tag{3.1}$$

де S – дані, що вбудовуються;

C – стегоконтейнер;

C' – секретні дані.

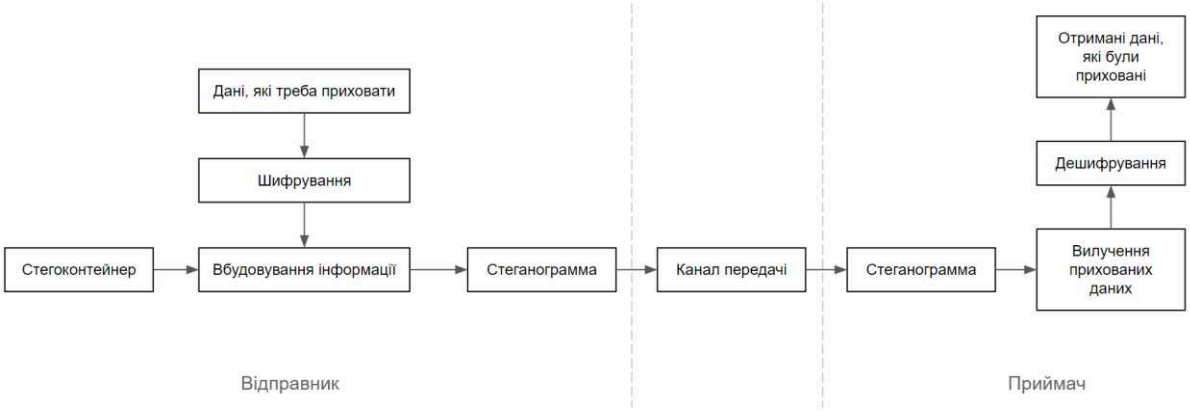

Рисунок 3.1 – Узагальнена схема стеганографічної системи

Для шифрування *En()* використовуються секретні ключі *(k1 і k2)*. Після шифрування інформація вбудовується в стегоконтейнер *Em()*. Стеганограма C' надсилається одержувачу каналом зв'язку, а на стороні одержувача відбувається вилучення стеганограми та дешифрування:

$$Sr' = D(Ex(\mathrm{C}^*, k_2), k_3), \tag{3.2}$$

де Sr – вихідні дані, що були вбудовані;

Ex() – функція вилучення даних;

D – функція дешифрування;

C^* – отриманий стегоконтейнер після передачі каналом зв'язку.

Контейнер може бути спотворений під впливом завад або атак в каналі зв'язку. Тому важливим є застосування методів підвищення завадостійкості для збереження можливості вилучення даних при отриманні стегоконтейнеру.

Існує багато робіт, які присвячені дослідженню використання стеганографії в різних сферах. Використання в якості контейнерів зображень,

відео та аудіо застосовується з метою захисту авторського права, як і цифрові водяні знаки [67]. В такому випадку приховані дані надають інформацію про власника або автора захищеного контенту. В роботі [73] пропонується захист даних під час автентифікації користувачів в IoT за допомогою протоколу еліптичної криптографії Галуа. Зашифровані конфіденційні дані вбудовуються у зображення низької складності.

Мережна стеганографія забезпечує процес прихованої передачі даних шляхом використання прихованого каналу, який використовує для передачі смугу пропускання інших дозволених каналів зв'язку та мережні протоколи моделі OSI в якості стегоконтейнерів. При незначній модифікації заголовків пакетів, полів корисного навантаження або порядку передачі пакетів інформація може бути передана приховано, не впливаючи значно на роботу мережі [67].

3.2 Аналіз існуючих методів мережної стеганографії

Модель взаємозв'язку відкритих систем (OSI) – це концептуальна модель, створена Міжнародною організацією зі стандартизації (International Organization for Standardization), яка описує комунікацію систем зв'язку за допомогою стандартних протоколів. Ця модель складається з 7 рівнів: Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data link layer, Physical layer. В залежності від функцій та протоколів кожного з рівнів можливою є реалізація різних методів мережної стеганографії [67].

Application layer забезпечує доступ додатків до мережних сервісів. На цьому рівні можливо реалізувати методи вбудовування даних в зображення, відео (методи приховування в просторовій області, в частотній області та методи розширення спектру), аудіо (кодування найменш значущих біт, метод фазового кодування, метод розширення спектру), використовуючи методи спотворення найменш значущих біт [70-72]. Також на цьому рівні можливим є

вбудовування в HTTP-заголовки. В [74] запропоновано метод HTTP Entity Tag tunnelling. В [75] запропоновано використовувати приховані канали для виявлення атак типу «людина посередині». В [76] запропоновано метод, що імітує додаток браузера для надсилання запитів HTTP, динамічно розподіляє запити HTTP до різних браузерів, вбудовує приховану інформацію за допомогою математичної комбінації та динамічно налаштовує об'єкти доступу, часовий інтервал пакетів даних і довжину пакетів даних, таким чином, покращуючи приховування каналу. В [78] наведено огляд існуючих прихованих каналів, які можуть бути створені за допомогою HTTP/1.x, та їх робота з HTTP/2.

Рисунок 3.2 – Функції протоколів OSI, що використовуються для мережної стеганографії

Presentation layer відповідає за переклад, шифрування та стиснення даних.

Session layer дозволяє користувачам встановлювати активні сеанси зв'язку. Зокрема, відповідає за встановлення, підтримку, синхронізацію та завершення сеансів між програмами. На цьому рівні можливим є використання протоколу SIP для прихованої передачі даних [79, 80].

Transport layer отримує дані від прикладного рівня. Виконується їх сегментація, додаються номери портів джерела та призначення в заголовок сегмента, потім повідомлення передається на мережний рівень. Методи стеганографії, що працюють на цьому рівні, використовують ретрансмісію втрачених пакетів, а також заголовки для створення прихованого каналу зв'язку.

Основною функцією Network layer є передача мережних пакетів від джерела до одержувача. Пакет інкапсулюється у фрейм та доставляється на рівень каналу даних. На стороні отримувача відбувається зворотній процес. Data link layer забезпечує безпомилкову передачу інформації, відповідає за кодування, декодування та організацію вихідних і вхідних даних. Фізичний рівень відповідає за передачу потоків вихідних даних через фізичне середовище. На цих рівнях працюють такі методи, як доповнення символів OFDM для WLAN, доповнення кадрів Ethernet та інші [67].

Згідно з наведеною в [81] класифікацією існуючих методів мережної стеганографії, методи діляться на методи модифікації пакетів (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 [82], SCTP (Stream Control Transmission Protocol) протоколів [83] і методи, які модифікують корисне навантаження пакета, наприклад, Transcoding Steganography [84].

В заголовках IP пакетів є поля, що мають надмірність або не використовуються під час передачі даних. Такі поля можуть бути використані для передачі стеганограми.

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 вносить стеганограму [84].

Такі методи, як LACK, HICCUPS, RSTEG є гибридними.

LACK (Lost Audio Packets Steganography) – це метод мережної стеганографії при використанні якого змінюються часові залежності та відбувається модифікація RTP-пакетів. Завдяки тому, що пакети, час життя яких було вичерпано відкидаються і не використовуються для відновлення даних, можливим є приховування інформації. З голосового потоку на стороні передавача обирається пакет та його корисне навантаження замінюється стеганограмою. Перед передачею цей пакет затримується. При умові, що одержувач знає про передачу прихованої інформації, він отримає цей пакет та вилучить стеганограму. В іншому випадку пакет буде відкинуто. При передачі великого об’єму інформації значно зросте затримка, що може призвести до виявлення факту передачі прихованих даних[85, 88].

Метод мережної стеганографії HICCUPS (Hidden Communication System for Corrupted Networks) використовує чутливість бездротових мереж до спотворення даних. 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 кадрах [86, 88].

Метод RSTEG (Retransmission Steganography) ґрунтується на повторному пересиланні пакетів. Коли отримувач знає про передачу прихованих даних, він не визнає пакет успішно прийнятим для того, щоб навмисно викликати повторну передачу, що буде містити вбудоване повідомлення замість корисного навантаження [84,88].

Методи мережної стеганографії, які використовують протокол HTTP, базуються на тому, що цей протокол використовується для передачі запитів на сервер і відповідей кінцевому одержувачу в роботі веб-додатків. Існують методи, в яких дані вбудовуються в HTTP-заголовки [87].

3.3 Визначення оптимального методу мережної стеганографії методом аналізу ієрархій

Для порівняння вище розглянутих методів та обрання з них кращих для використання у системі «Розумний будинок» та для віддаленої автентифікації користувачів використано метод аналізу ієрархій [41, 88].

Для обрання оптимальних методів для виконання цих задач проаналізуємо найбільш розповсюджені показники стеганографічних систем: пропускну здатність, стеганографічну вартість, складність реалізації, а також складність виявлення прихованої інформації[88].

Стеганографічна пропускна здатність – це кількість секретних даних, які можливо відправити за одиницю часу при використанні певного методу та носія.

Складність виявлення – це неможливість виявляти стеганограму в межах певного носія. Найбільш популярний спосіб для виявлення стеганограми – аналіз статистичних характеристик перехоплених даних і порівняння їх з типовими характеристиками цього носія.

Стеганографічна вартість характеризує ступінь погіршення якості носія, викликаної процедурою вбудовування стеганограми.

На рисунку 3.3 наведено ієрархію для вибору оптимального методу мережної стеганографії. 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 нижнього рівня на загальну мету [85,88].

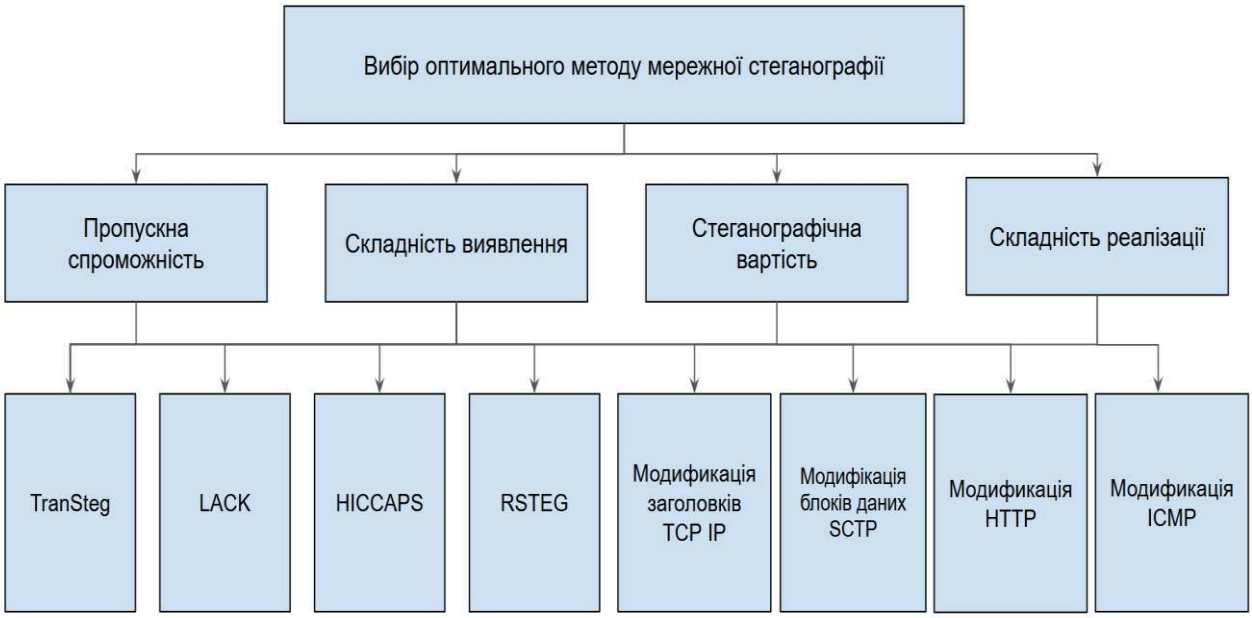

Рисунок 3.3 – Декомпозиція задачі вибору оптимального стеганографічного методу за допомогою ієрархічної моделі

Використовуючи існуючі характеристики методів [81-86], а також порівняння методів мережної стеганографії [67] за алгоритмом, описаним в розділі 2, сформовано матриці попарних порівнянь між елементами відносно кожного елемента більш високого рівня, які виступають критеріями для порівняння. Спочатку проведено попарне порівняння важливості показників, що характеризують стеганографічні системи та є важливими для вирішення поставленої задачі. Результати цих розрахунків з використанням формул (2.1 - 2.5) наведені в таблицях 3.1 та 3.2 [88].

Таблиця 3.1 – Попарне порівняння впливу показників ефективності методів мережної стеганографії для системи «Розумний будинок»

	Пропускна здатність	Складність виявлення	Стеганографічна вартість	Складність реалізації	Власний вектор V_i	Вектор пріоритетів P_i
Пропускна здатність	1	1/4	1/2	1/3	0,45	0,10
Складність виявлення	4	1	1/2	1/2	1,00	0,22
Стегано-графічна вартість	2	2	1	1/2	1,19	0,26
Складність реалізації	3	2	2	1	1,86	0,41

Таблиця 3.2 – Попарне порівняння впливу показників ефективності методів мережної стеганографії для систем віддаленої автентифікації

	Пропускна здатність	Складність виявлення	Стеганографічна вартість	Складність реалізації	Власний вектор V_i	Вектор пріоритетів P_i
Пропускна здатність	1	1/4	1/3	1/2	0,45	0,10
Складність виявлення	4	1	1/2	1/3	0,90	0,20
Стегано-графічна вартість	3	2	1	1/3	1,19	0,26
Складність реалізації	2	3	3	1	2,06	0,45

На рисунку 3.4 представлено діаграму пріоритетів пропускної здатності, складності виявлення, стеганографічної вартості та складності реалізації для систем «Розумний будинок» та систем віддаленої автентифікації.

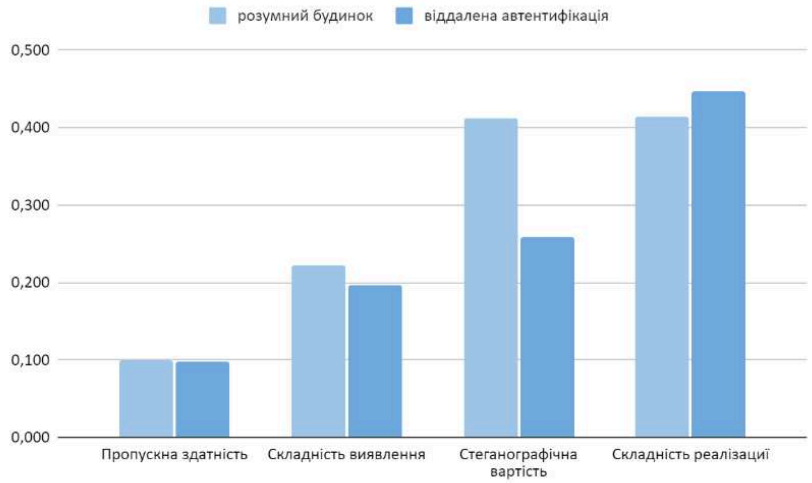

Рисунок 3.4 – Вектори пріоритетів критеріїв оцінки стеганографічних методів для систем, що розглядаються

Далі виконано попарні порівняння обраних методів мережної стеганографії по відношенню до показників якості. Результати наведено у таблицях 3.3-3.6 та на рисунках 3.5-3.8 [88]:

Таблиця 3.3 – Матриця попарних порівнянь методів мережної стеганографії по відношенню до пропускної здатності

	TranSteg	LACK	HICCUPS	RSTEG	Модифікація заголовків TCP/IP	Модифікація блоків даних SCTP	HTTP	ICMP	Власний вектор	Вектор пріоритетів
TranSteg	1	2	3	5	5	6	6	5	3,58	0,32
LACK	1/2	1	2	3	5	6	6	5	2,68	0,24
HICCUPS	1/3	1/2	1	2	2	6	6	2	1,62	0,14
RSTEG	1/5	1/3	1/2	1	1	3	3	1	0,86	0,08
Модифікація заголовків TCP/IP	1/5	1/5	1/2	1	1	3	3	1	0,81	0,07
Модифікація блоків даних SCTP	1/6	1/6	1/6	1/3	1/3	1	1/2	1/3	0,31	0,03
HTTP	1/6	1/6	1/6	1/3	1/3	2	1	1/3	0,37	0,03
ICMP	1/5	1/5	1/2	1	1	3	3	1	0,81	0,07

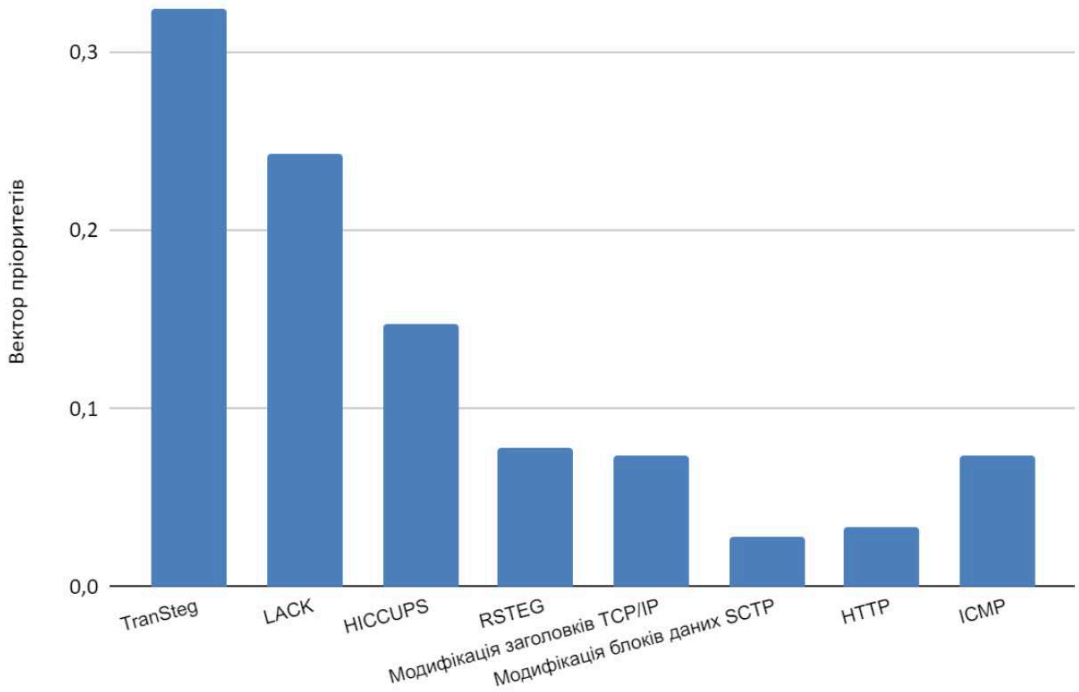

Рисунок 3.5 – Вектори пріоритетів пропускної здатності для стеганографічних методів

Таблиця 3.4 – Матриця попарних порівнянь методів мережної стеганографії по відношенню до складності виявлення

	TranSteg	LACK	HICCUPS	RSTEG	Модифікація заголовків TCP/IP	Модифікація блоків даних SCTP	HTTP	ICMP	Власний вектор	Вектор пріоритетів
TranSteg	1	2	1/2	3	4	4	4	3	2,21	0,23
LACK	1/2	1	1/3	2	3	3	3	2	1,44	0,15
HICCUPS	2	3	1	3	4	4	4	3	2,77	0,28
RSTEG	1/3	1/2	1/3	1	2	2	2	1	0,90	0,09
Модифікація заголовків TCP IP	1/4	1/3	1/4	1/2	1	1	1	1/2	0,52	0,05
Модифікація блоків даних SCTP	1/4	1/3	1/4	1/2	1	1	1	1/2	0,52	0,05
HTTP	1/4	1/3	1/4	1/2	1	1	1	1/2	0,52	0,05
ICMP	1/3	1/2	1/3	1	2	2	2	1	0,90	0,09

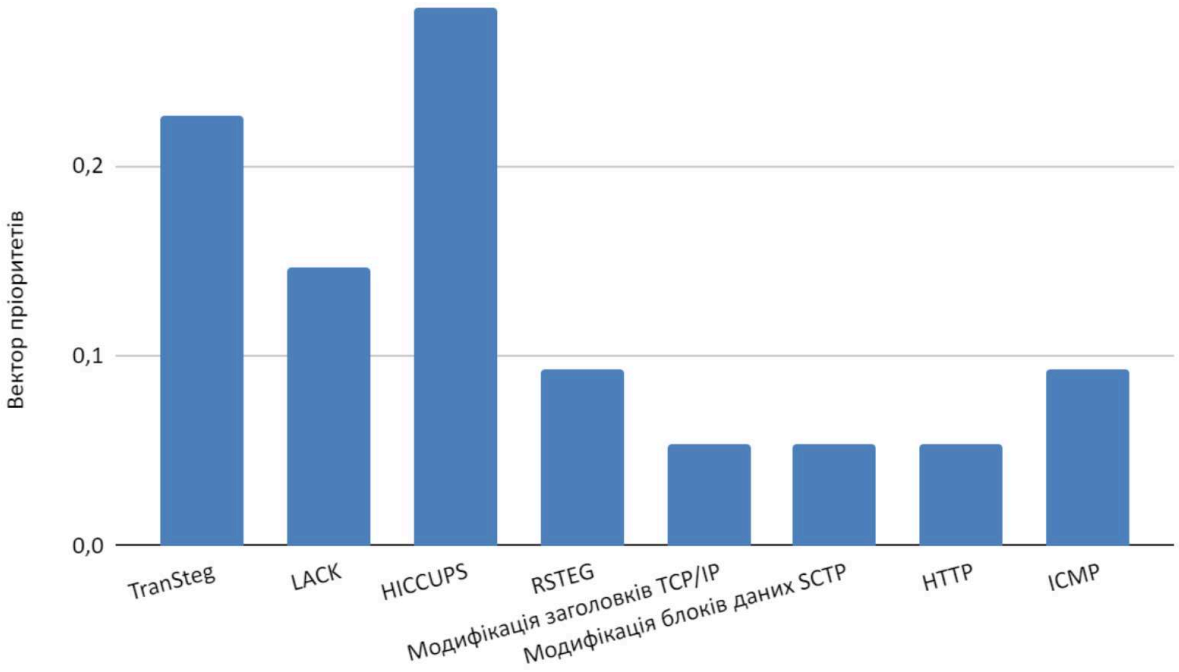

Рисунок 3.6 – Вектори пріоритетів складності виявлення для стеганографічних методів

Таблиця 3.5 – Матриця попарних порівнянь методів мережної стеганографії по відношенню до стеганографічної вартості

	TranSteg	LACK	HICCUPS	RSTEG	Модифікація заголовків TCP/IP	Модифікація блоків даних SCTP	HTTP	ICMP	Власний вектор	Вектор пріоритетів
TranSteg	1	1/2	1/3	1/3	1	2	2	1	0,83	0,12
LACK	2	1	2	1/2	1	2	2	1	1,30	0,18
HICCUPS	3	1/2	1	1	6	3	4	4	2,14	0,29
RSTEG	3	2	1	1	1/6	1/4	1/5	1/5	0,56	0,07
Модифікація заголовків TCP IP	1	1	1/6	1/6	1	3	2	2	0,87	0,12
Модифікація блоків даних SCTP	1/2	1/2	1/3	1/4	1/3	1	2	2	0,64	0,09
HTTP	1/2	1/2	1/4	1/5	1/2	1/2	1	1	0,49	0,06
ICMP	1	1	1/4	1/5	1/2	1/2	1	1	0,58	0,08

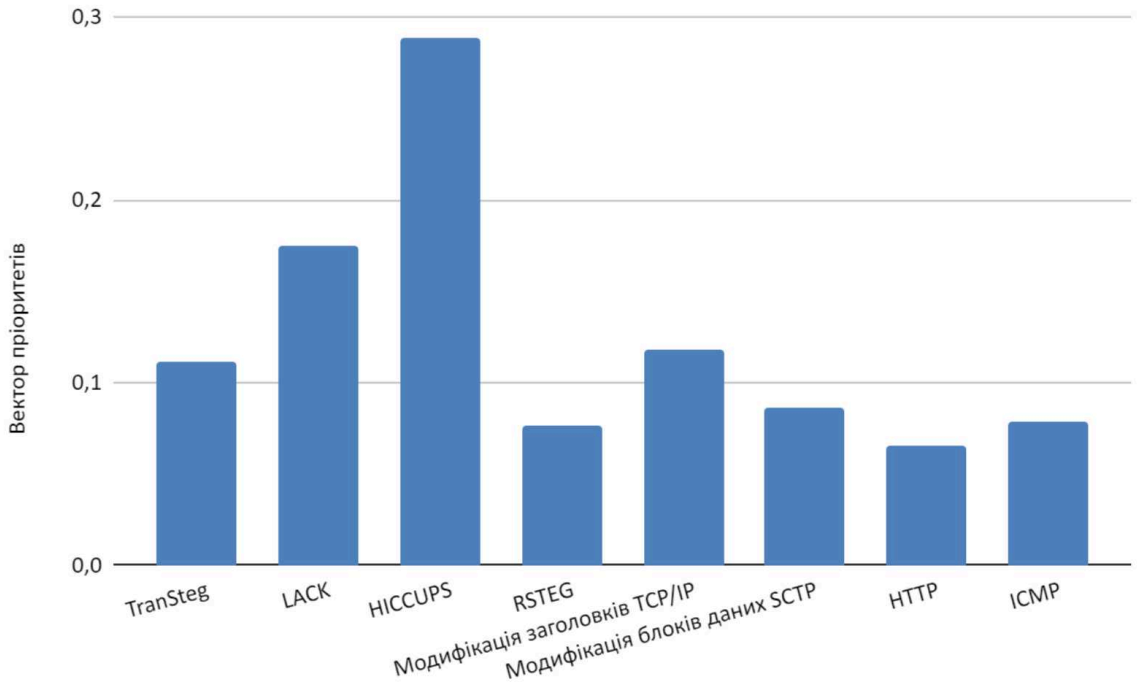

Рисунок 3.7 – Вектори пріоритетів стеганографічної вартості

Таблиця 3.6 – Матриця попарних порівнянь методів мережної стеганографії по відношенню до складності реалізації

	TranSteg	LACK	HICCUPS	RSTEG	Модифікація заголовків TCP/IP	Модифікація блоків даних SCTP	HTTP	ICMP	Власний вектор	Вектор пріоритетів
TranSteg	1	3	3	4	1/2	2	1/2	1/2	1,32	0,13
LACK	1/3	1	1	2	1/6	1/4	1/5	1/5	0,43	0,04
HICCUPS	1/3	1	1	2	1/5	1/3	1/4	1/4	0,48	0,05
RSTEG	1/4	1/2	1/2	1	1/6	1/4	1/5	1/5	0,32	0,03
Модифікація заголовків TCP IP	2	6	5	6	1	3	2	2	2,85	0,27
Модифікація блоків даних SCTP	1/2	4	3	4	1/3	1	1/2	1/2	1,09	0,11
HTTP	2	5	4	5	1/2	2	1	1	1,94	0,18
ICMP	2	5	4	5	1/2	2	1	1	1,94	0,19

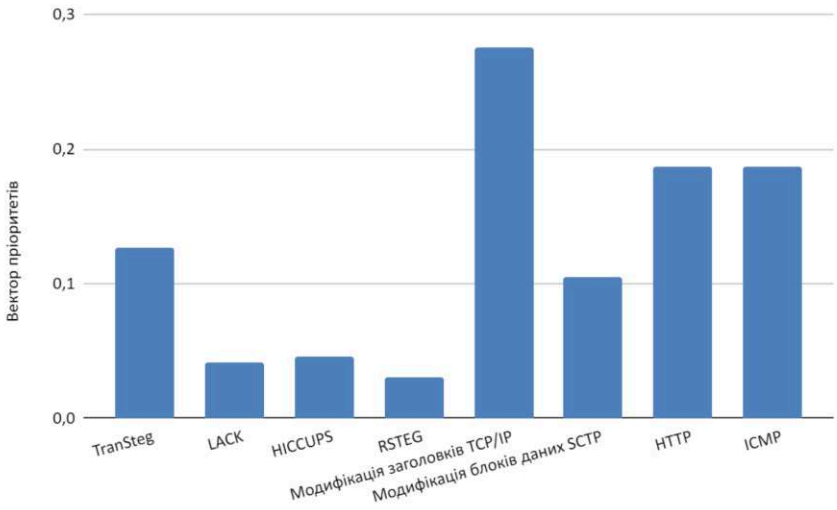

Рисунок 3.8 – Вектори пріоритетів складності виявлення для стеганографічних методів

В таблицях 3.7 - 3.8 наведено отримані оцінки вектора пріоритетів показників якості мережної стеганографії і векторів пріоритетів по відношенню до методів мережної стеганографії, що розглядаються, а також результати обчислення значень глобального вектора пріоритетів.

$$C_i = \sum_{j=1}^{n} P_j Q_{ij} \ , \ i = \overline{1, N}, \tag{3.7}$$

де N – число систем, що порівнюються.

Таблиця 3.7 – Результати обчислення значень компонентів глобального вектора пріоритетів для системи розумний будинок

Методи	Вектори пріоритетів методів за критеріями:				Головний вектор пріоритету
	Пропускна здатність	Складність виявлення	Стеганографічна вартість	Складність реалізації	
1	2	3	4	5	6
TranSteg	0,32	0,23	0,12	0,13	0,16

Продовження таблиці 3.7

1	2	3	4	5	6
LACK	0,24	0,15	0,18	0,04	0,12
HICCUPS	0,14	0,28	0,29	0,05	0,17
RSTEG	0,08	0,09	0,07	0,03	0,06
Модифікація заголовків TCP IP	0,07	0,05	0,12	0,27	0,16
Модифікація блоків даних SCTP	0,03	0,05	0,09	0,11	0,08
HTTP	0,03	0,05	0,06	0,18	0,11
ICMP	0,07	0,09	0,08	0,19	0,13

Таблиця 3.8 – Результати обчислення значень компонентів глобального вектора пріоритетів для віддаленої автентифікаціїї

Методи	Вектори пріоритетів методів за критеріями:				Головний вектор пріоритету
	Пропускна здатність	Складність виявлення	Стеганографічна вартість	Складність реалізації	
TranSteg	0,32	0,23	0,12	0,13	0,16
LACK	0,24	0,15	0,18	0,04	0,12
HICCUPS	0,14	0,28	0,29	0,05	0,16
RSTEG	0,08	0,09	0,07	0,03	0,06
Модифікація заголовків TCP IP	0,07	0,05	0,12	0,27	0,17
Модифікація блоків данных SCTP	0,03	0,05	0,09	0,11	0,08
HTTP	0,03	0,05	0,06	0,18	0,11
ICMP	0,07	0,09	0,08	0,19	0,13

В таблиці 3.9 зведено глобальні вектори пріоритетів для системи розумний будинок та для віддаленої автентифікації.

Таблиця 3.9 – Результати обчислення глобальних векторів пріоритетів для системи «Розумний будинок» та для віддаленої автентифікації.

№	Методи	«Розумний будинок»	Віддалена автентифікація	Підтвердження справжності диктора
1	TranSteg	0,164	0,16	0,16
2	LACK	0,12	0,12	0,12
3	HICCUPS	0,17	0,16	0,16
4	RSTEG	0,06	0,06	0,06
5	Модифікація заголовків TCP/IP	0,16	0,17	0,16
6	Модифікація блоків данных SCTP	0,08	0,08	0,08
7	HTTP	0,11	0,11	0,11
8	ICMP	0,13	0,13	0,12

На рисунку 3.9 наведено результати багатокритеріального аналізу методом аналізу ієрархій.

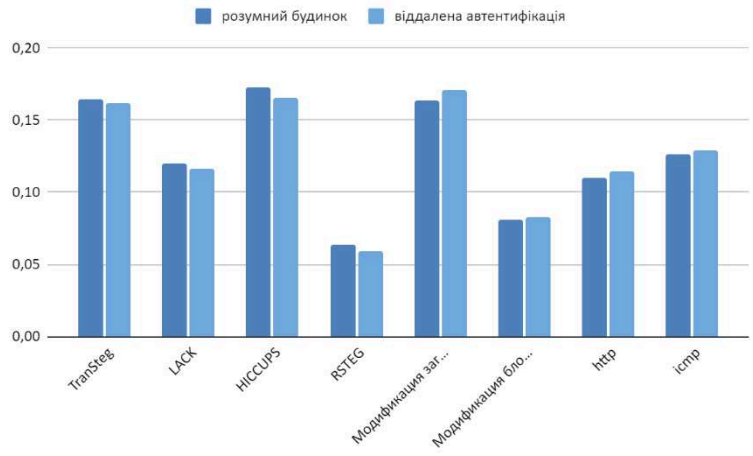

Рисунок 3.9 – Вибір оптимального методу

Аналіз показав, що в результаті багатокритеріального аналізу кращим за сукупністю критеріїв для обраних сценаріїв виявився стеганографічний метод HICCUPS, також високі пріоритети у методу TranSteg та методу модифікації заголовків TCP/IP. Ці методи можуть бути використані для захисту даних при автентифікації у розглядаємих системах. Враховуючи складність реалізації методів для подальшого дослідження, було обрано методи модифікації заголовків протоколів TCP/IP, HTTP, ICMP [88].

3.4 Застосування обраного методу мережної стеганографії для підвищення захищеності віддаленої автентифікації

Біометрична система розпізнавання встановлює відповідність конкретних поведінкових або фізіологічних характеристик користувача деякому заздалегідь заданому шаблону. Фізичний або поведінковий зразок знімається системою під час занесення в список (на основі унікальних біометричних даних створюється шаблон), а також під час процесів ідентифікації та перевірки. При автентифікації шаблон, що зберігається в базі, порівнюється з новим зразком та приймається рішення про надання даному користувачу доступу до певної інформації [34].

Передача біометричного шаблону у відкритому вигляді є небезпечною, тому що зловмисник може перехопити його та використати для несанкціанованого доступу до інформації. При збереженні шаблону використовується шифрування.

Для підвищення надійності передачі біометричної інформації при автентифікації запропоновано передавати біохеш методами мережної стеганографії. Це дозволить приховати сам факт передачі даних та значно ускладнить їх перехоплення. Біохеш складається з 128 або 256 байт, які можливо передавати, використовуючи існуючі методи стеганографії з

урахуванням потреб конкретної системи, засобами яких вона реалізована, та в залежності від протоколів, що використовуються [91].

На рисунку 3.10 представлено запропоновану узагальнену модель прихованої передачі для підвищення захищеності систем віддаленої автентифікації користувачів [34].

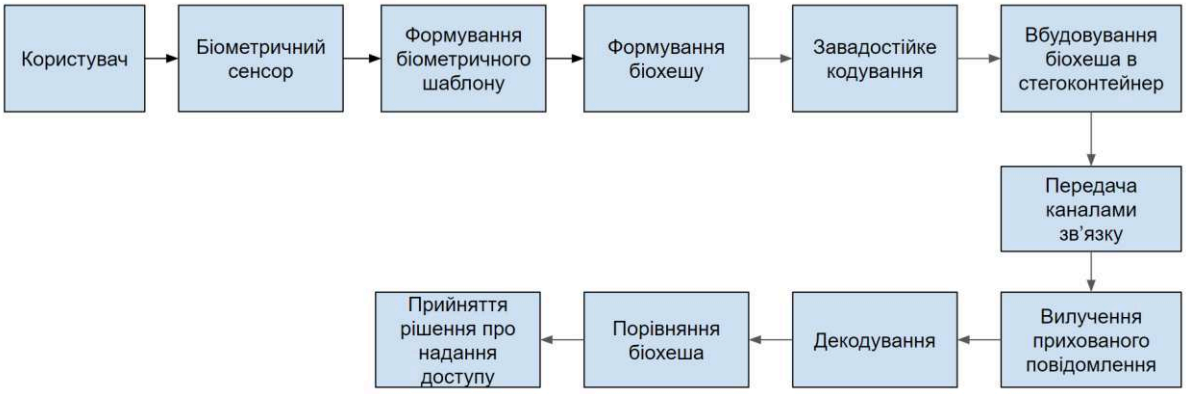

Рисунок 3.10 – Узагальнена модель біометричної автентифікації з використанням мережної стеганографії.

Для дослідження роботи моделі було обрано три методи, які використовують мережні фрагменти даних (Protocol Data Units, PDUs) протоколів TCP, HTTP та ICMP [66, 89].

3.4.1 Метод приховування даних у HTTP-заголовках

Для прихованої передачі даних можуть бути використані різні характеристики HTTP-повідомлень. При приховуванні даних може бути змінено структуру, зміст та порядок заголовків[89-91]. В даному методі дані приховуються за допомогою додавання пробілів в середину заголовків. Для дослідження методу було використано програму, яка моделює клієнт-серверну систему. Перед передачею дані, які мають бути передані, у двійковому форматі вбудовуються в заголовки запитів HTTP у вигляді додаткових пробілів. При передачі “0” кодується додаванням одного пробілу, “1” – двох. Для збільшення прихованості дані не вбудовуються після двокрапки. За допомогою цього

методу можливим є приховування 36 бітів даних в одному заголовку. На рисунку 3.11 наведено HTTP-заголовок, отриманий за допомогою програми Wireshark при прихованій передачі даних. Кольором виділено вбудовані дані (код літери S) [66].

```
GET /test/test.php?id=1 HTTP/1.1\r\n
dnt: 1\r\n
accept-language: bg-BG,bg;q=0.8,en;q=0.6,de;q=0.7\r\n
x-requested-with: XMLHttpRequest\r\n
connection: keep-alive\r\n
cache-control: must-revalidate,public, max-age=0  \r\n
upgrade-insecure-requests: 1  \r\n
referer: http://www.mysite.com/ \r\n
accept-charset: utf-8, iso-8859-1;q=0.5,  *;q=0.1 \r\n
host: 127.0.0.1  \r\n
accept-encoding: gzip, deflate,  sdch  \r\n
user-agent: Mozilla/5.0 (Windows NT 10.0;  Win64;  x64) AppleWebKit/537.36  (KHTML,  like  Gecko) Chrome/58.0.3029.110  Safari/537.36 \r\n
accept: text/html,  application/xhtml+xml, application/xml;q=0.9,  image/webp,  */*;q=0.8  \r\n
\r\n
```

Рисунок 3.11 – Вбудована стеганограма в HTTP-заголовок

3.4.2 Метод приховування даних в TCP-заголовках

Протокол транспортного рівня TCP забезпечує надійну доставку даних від відправника до одержувача. На рисунку 3.12 наведено структуру TCP-пакета. Вбудовування прихованих даних можливе в такі поля, як Window Size, TCP Option, ACK number [66, 89].

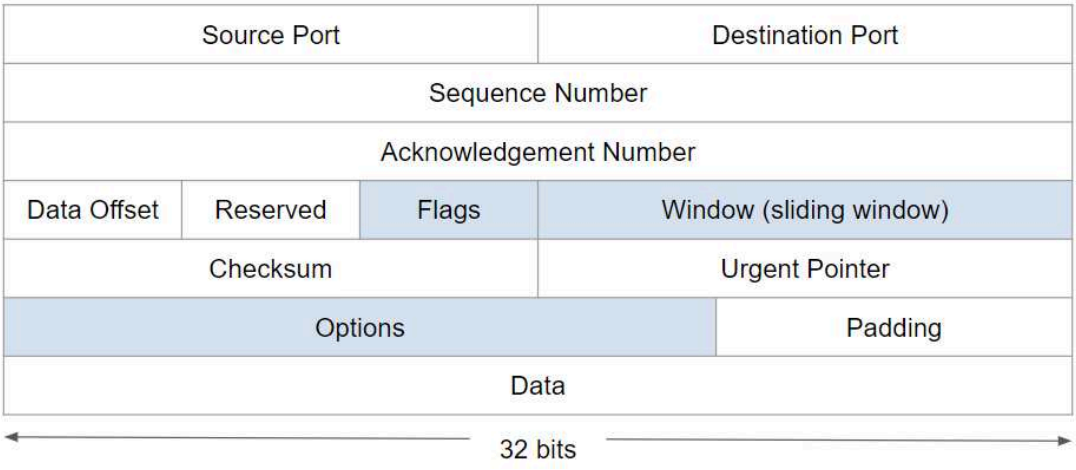

Рисунок 3.12 – Структура TCP-заголовка

Було проведено дослідження реалізації приховування даних у полі Window Size. Це поле призначено для зазначення кількості даних, які можуть

бути надіслані до отримання підтвердження. Розмір цього поля складає 2 байти, відповідно, в один сегмент можливим є вбудовування максимально 2 байт даних. Для надійності було проведено вбудовування одного байту прихованих даних.

Обробка даних перед вбудовуванням відбувається за наступним алгоритмом [89]:

1 байт повідомлення записується в десятковій системі числення (n).

$M = n * 150$.

Якщо $M < 10000$, $M = M * 6$.

Отримане число M записується в поле Window Size.

Один байт в десятковій системі числення може приймати значення від 0 до 255, відповідно до цього обрано множники 150 та 6. Результат множення числа, яке представляє байт повідомлення на 150 не перевищує максимальне значення поля Window Size (16 байт => 65535). Числа 150 та 6 виступають у якості секретних ключей, які необхідні для вилучення повідомлення на приймальній стороні. На стороні приймача програма виконує зворотні перетворення для отриманих значеннь з поля Window Size. Для керування полями TCP, було використано Python Framework Scapy. Приклад роботи програми наведено на рисунках 3.13 (a-b)[66].

```
########## [Steganography] ##########
Write the path of the file for Steganography:'steg.txt'
Do you want send the packet with Steganography:'y'
```

а) Передача стеганограми

```
########## [Recovering Message] ##########
Enter the path of the packets to analyze: 'packets.txt'
Write the output file name: 'result.txt'
Writing into the file...
Closing files...
```

б) Отримання переданих даних

Рисунок 3.13 – Приклад роботи програми

Цей метод дозволяє передавати в прихованому вигляді різні типи даних.

3.4.3 Метод приховування даних в ICMP-заголовках

Наступний протокол, який можна модифікувати – ICMP. Пакет ICMP має поле, яке вказує тип повідомлення. Якщо повідомлення має тип помилки, воно містить тип і код.

ICMP – повідоблення починається з трьох полів: восьмибітного цілого числа, що позначає тип повідомлення «Type», восьмибітного поля «Code» та шістнадцятибітного поля «Checksum» (рис. 3.14).

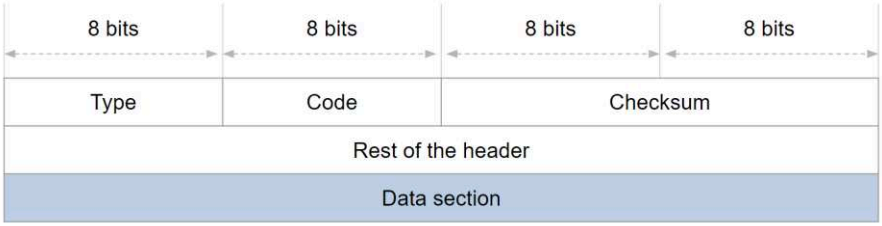

Рисунок 3.14 – Формат пакету ICMP

Якщо обрати поле «Type» в якості «Echo request», то п’ятий та шостий байт будуть з поля «Identifier», а сьомий і восьмий – з «Sequence number». В даному випадку дані можна приховувати саме в цих двох полях. В результаті за допомогою даного методу можна приховувати до чотирьох байтів даних в кожний ICMP пакет.

Для дослідження методу приховування даних в ICMP-заголовках було використано програму, яка виконує стиснення та шифрування даних за допомогою AES (Advanced Encryption Standard) 265 CBC (Cipher Block Chaining). В першому режимі роботи ця програма дає можливість приховати 60 байтів інформації в одному стегоконтейнері в полях «Identifier» (2 байти), «Sequence number» (2 байти) та поле даних (розмір залежить від розміру пакета). Другий режим має меншу пропускну здатність, тому що вбудовування відбувається в два поля: «Identifier» та «Sequence number» [66].

Оскільки зазначені методи мають використовуватися для віддаленої автентифікації, велике значення при оцінюванні їх ефективності має стійкість до завад та шумів у відкритих каналах зв’язку.

3.5 Аналіз показників методів стеганографії, що досліджуються

Враховуючи те, що метою застосування є прихована передача інформації, стеганограма має бути стійкою до виявлення. Вбудовування інформації призводить до надлишкової інформації, повторних передач пакетів, які можуть впливати на кількість трафіка, що може вказувати на наявність стеганограми.

Методи, що використовувались в роботі для прихованої передачі біометричних даних при автентифікації, були досліджені за такими показниками як коефіцієнт корисної дії та швидкодія (табл. 3.10).

Таблиця 3.10 – Порівняння методів стеганографії

	HTTP		TCP		ICMP («Secure»)		ICMP («Fast»)	
ККД	36 / 4944		8 / 160		32 / 512		480 / 512	
Розмір стеганограми	24 байти	1 Мбайт	24 байти	1 Мбайт	24 байти	1 Мбайт	24 байти	1 Мбайт
Швидкодія, сек	0,0032	302,97	2,4153	>1 год.	0,0067	0,1430	0,0006	0,0126

Для перехоплення трафіку було використано Wireshark — програму, яка дозволяє аналізувати мережні протоколи. Було проведено дослідження методів з використанням протоколів HTTP, TCP, ICMP [66].

Аналіз стійкості до виявлення стеганограми при використанні методу з вбудовуванням в поля протоколу HTTP показав, що при передачі невеликої кількості вбудованих даних (24 байти) статистичні характеристики трафіку майже не змінюються, при збільшенні кількості вбудованих даних зростає кількість пакетів HTTP та TCP. Передача HTTP заголовка вимагає нового з’єднання (початку сеансу TCP). На рисунку 3.15 представлено зміну кількості пакетів в залежності від розміру вбудованої стеганограми [66].

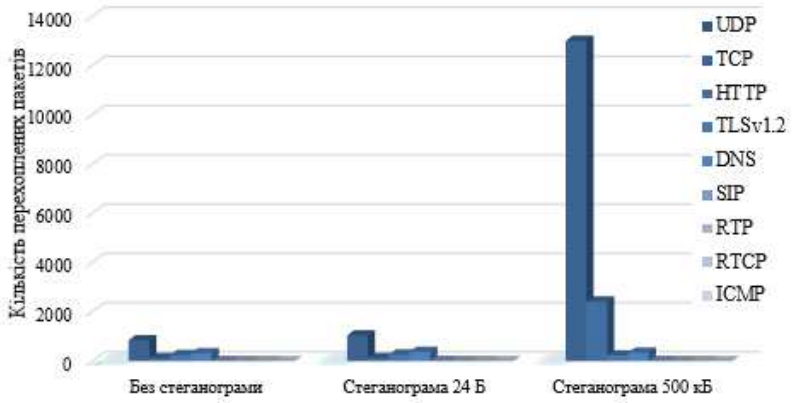

Рисунок 3.15 – Дослідження статистичних характеристик трафіку при використанні методу HTTP стеганографії

Дослідження методу з використанням TCP показало незначне зростання трафіку TCP при передачі 24 байт даних. При передачі 500 кбайт даних кількість пакетів TCP зростає майже на 50%, що підвищує ймовірність виявлення факту передачі стеганограми (рис. 3.16) [66].

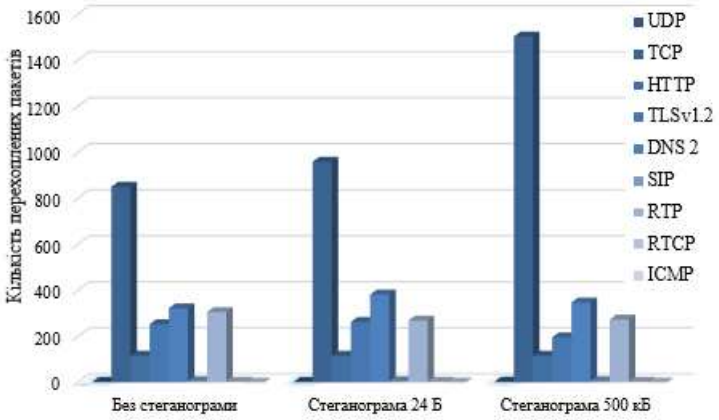

Рисунок 3.16 – Дослідження статистичних характеристик трафіку при використанні методу TCP стеганографії

Дослідження методу ICMP стеганографії було проведено для двох реалізованих алгоритмів вбудовування: швидкого та безпечного. Кількість пакетів різного типу в залежності від кількості вбудованих даних стеганограми представлено на рисунках 3.17 та 3.18.

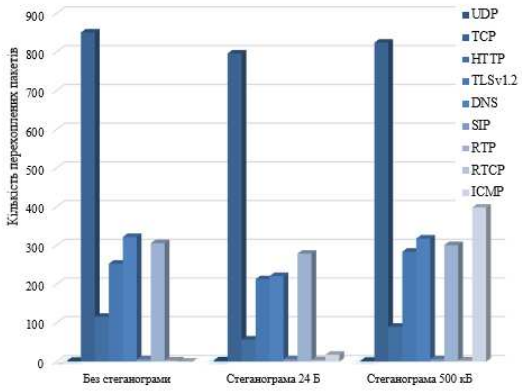

Рисунок 3.17 – Дослідження статистичних характеристик трафіку при використанні методу ICMP стеганографії, метод «Secure»

При передачі даних розміром 500 кБ для методу «Secure» кількість ICMP пакетів значно зростає. При використанні методу«Fast» кількість нових ICMP пакетів є значно меншою, завдяки цьому використання даного методу зменшує ймовірність виявлення стеганограми [66].

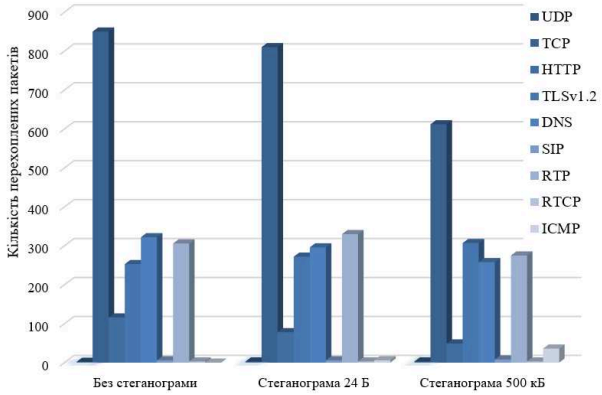

Рисунок 3.18 – Дослідження статистичних характеристик трафіку при використанні методу ICMP стеганографії, метод «Fast»

Проаналізувавши отримані результати можна зробити висновок, що метод мережної стеганографії з використанням протоколу HTTP не дозволяє приховано передавати велику кількість даних та є чутливим до завад. Також при використанні цього методу значно збільшуться трафік.

Метод стеганографії з використанням TCP має більшу стійкість до завад, але невисоку швидкодію. Використання в якості контейнерів ICMP пакетів дозволяє ефективніше приховувати дані, цей метод має кращу завадостійкість. Кількість трафіку не змінюється значно, що говорить про кращу прихованість даних. Також цей метод працює швидше. Метод «Secure» забезпечує оптимальну пропускну здатність та складність реалізації, стеганограма при використанні цього метода займає менше 7% від розміру пакета [66].

3.6 Висновки до розділу 3

В розділі запропоновано рішення для підвищення безпеки біометричних даних, що передаються мережею.

Розглянуто застосування стеганогрфічних систем з використанням різних типів даних для прихованої передачі даних.

Для досліджень обрано методи мережної стеганографії, які забезпечують процес прихованої передачі даних шляхом використання прихованого каналу, який використовує смугу пропускання інших дозволених каналів зв’язку. Проведено багатокритеріальний аналіз описаних методів методом аналізу ієрархій. За сукупністю таких критеріїв, як стеганографічна пропускна здатність, складність виявлення, стеганографічна вартість, було обрано методи модифікації заголовків протоколів TCP/IP, HTTP, ICMP для подальшого дослідження в сценаріях використання в системах «розумний будинок» та віддаленої автентифікації.

Для підвищення надійності передачі біометричної інформації при автентифікації запропоновано передавати біохеш методами мережної стеганографії. Представлено запропоновану узагальнену модель прихованої передачі для підвищення захищеності систем віддаленої автентифікації користувачів. Змодельовано роботу методів, які використовують мережні фрагменти даних PDUs протоколів TCP, HTTP та ICMP. Ці методи буди

порівняні за такими показниками, як коефіцієнт корисної дії та швидкодія. Проведені дослідження показали, що вбудовування в ICMP пакет дозволяє використати від 6,25% до 93,75% від розміру пакету, вбудовування за допомогою метода TCP – 5%, метод вбудовування в HTTP дозволяє використати лише 0,75% від загального розміру пакету [66].

Проаналізовано вплив передачі пакетів, що містять вбудовані дані, на статистичні характеристики трафіку. Визначено, що метод HTTP стеганографії має низьку пропускну здатність. При його застосуванні TCP та HTTP трафік різко збільшується. Метод вбудовування у заголовок TCP також призводить до збільшення кількості пакетів при збільшенні кількості даних, що передаються та має низьку швидкодію. Кращим з методів виявився метод вбудовування в ICMP-пакети.

Список використаних джерел у даному розділі наведено у повному списку використаних джерел під номерами 66-91.

4 МЕТОДИ ВДОСКОНАЛЕННЯ ЗАВАДОСТІЙКОСТІ ТА СТІЙКОСТІ ДО АТАК ПІД ЧАС ПЕРЕДАЧІ ДАНИХ КОРИСТУВАЧА

Для віддаленої автентифікації часто використовуються мобільні пристрої, підключені до мереж мобільних операторів зв'язку. Тому доцільним є дослідження передачі даних в мобільних мережах з урахуванням факторів, які можуть впливати на якість передачі [94].

Розповсюдженою на сьогоднішній день є технологія LTE. Враховуючи це, в роботі розглянуто математичну модель фізичного рівня мережі LTE. Під час досліджень важливим є врахування впливу параметрів каналу зв'язку та мобільного пристрою на якість роботи системи віддаленої автентифікації.

4.1 Модель каналу зв'язку з завадами

Під час віддаленої автентифікації передача даних відбувається мережею фізичного рівня LTE. Кінцевим етапом має бути верифікація користувача шляхом порівняння біохешів – попередньо зареєстрованого в базі даних, та переданого мережею.

Як описано в розділі 1, до основних технологій LTE відносяться OFDM, багатоантенні системи MIMO, Turbo Channel Coding та Link Adaptation.

Для дослідження передачі стеганограми при віддаленій біометричній автентифікації було змодельовано фізичний рівень мережі LTE у середовищі MATLAB [93]. На цьому рівні відбувається обробка бітів даних, що передані з інших рівнів до фізичного рівня.

Основними компонентами моделі є передавач, канал передачі даних та приймач. На стороні передавача сигнал обробляється в логічному (Downlink Shared Channel, DLSCH) та фізичному (Physical Downlink Shared Channel, PDSCH) каналах (рис. 4.1)[93].

Рисунок 4.1 – Узагальнена модель фізичного рівня мережі LTE

Обробка DLSCH складається з наступних етапів. Спочатку відбувається приєднання циклічного надлишкового коду (Cyclic Redundancy Check, CRC), дані сегментуються на підблоки, відбувається канальне кодування (турбокодування). Далі відбувається операція, під час якої обирається кількість вихідних біт відповідно до потрібної швидкості кодування – узгодження швидкості та перетворення кодових блоків на кодові слова (рис. 4.2) [93].

Рисунок 4.2 – Етапи обробки на рівні DLSCH

Обробка даних в PDSCH починається зі скремблювання кодових слів та модуляції. Модель підтримує наступні алгоритми модуляції: Quadrature Phase Shift Keying (QPSK), 16 Quadrature Amplitude Modulation (QAM), 64QAM [93].

Quadrature Phase Shift Keying (QPSK) використовує чотирирівневий фазовий стан для одночасної передачі 2 біт/символ шляхом вибору одного з чотирьох можливих фазових зсувів несучої, де кожне значення фази несучої

відповідає окремій парі бітів повідомлення. Це дозволяє передавати в два рази більше інформації з використанням тієї самої смуги пропускання порівняно з BPSK.

При використанні модуляції (QPSK) інформація, що передається, міститься у фазі синусоїдальної несучої. Фаза несучої приймає одне з чотирьох рівновіддалених значень, таких як π/4, 3π/4, 5π/4, 7π/4. Сигнал, що передається визначається як

$$s_i(t) = \begin{cases} \sqrt{\frac{2E}{T}} cos\left[2\pi f_c t + (2i-1)\frac{\pi}{4}\right], \ 0 \le t \le T, \\ 0 \end{cases} \quad (4.1)$$

де *i*= 1, 2, 3, 4;

E – енергія переданого сигналу на символ;

$T = 2T_b$ – тривалість символу, яка вдвічі перевищує тривалість біту.

Кожне з чотирьох рівновіддалених значень фази відповідає унікальній парі бітів (00,01,10,11). В розгорнутому вигляді в інтервалі $0 \le t \le T$ сигнал можна представити як

$$s_i(t) = \sqrt{\frac{2E}{T}} cos\left[(2i-1)\frac{\pi}{4}\right] \cos(2\pi f_c t) - \sqrt{\frac{2E}{T}} sin\left[(2i-1)\frac{\pi}{4}\right] \sin(2\pi f_c t), \quad (4.2)$$

де *i*= 1, 2, 3, 4.

Приймач QPSK складається з синфазного (In-phase Channel, I)-каналу та квадратурного (Quadrature Channel, Q)-каналу із загальним входом. Кожен канал складається з модулятора, фільтра низьких частот, семплера та пристрою прийняття рішень. В загальному вигляді QPSK передавач та приймач наведені на рисунках 4.3 – 4.4.

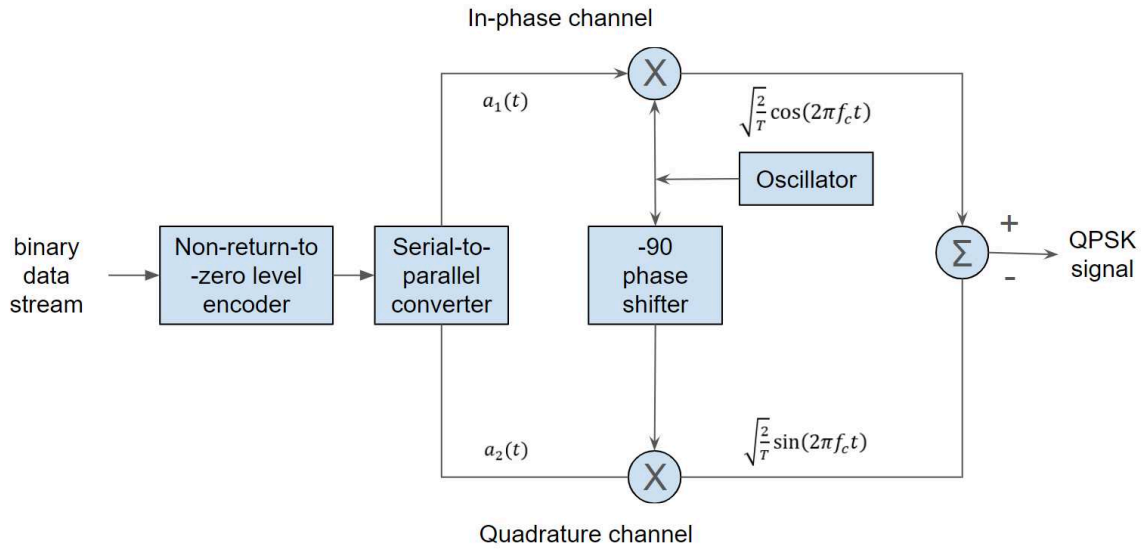

Рисунок 4.3 – QPSK передавач

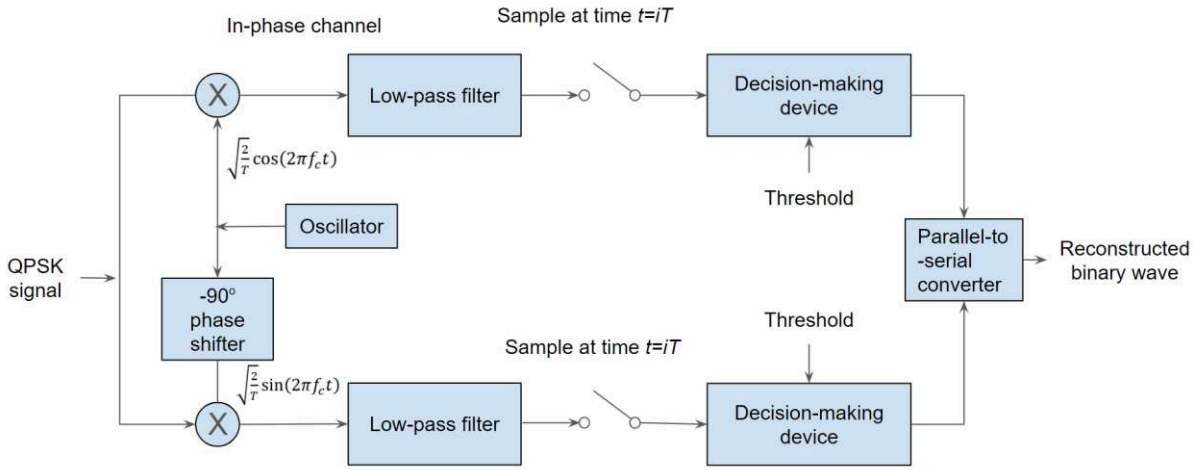

Рисунок 4.4 – QPSK приймач

Ймовірність бітової помилки може бути визначена як

$$P_{e(QPSK)} = Q\left[\sqrt{\frac{2E_b}{N_0}}\right], \tag{4.3}$$

E_b – енергія на біт;

N_0 – спектральна щільність потужності шуму.

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-(\frac{t^2}{2})} dt, \tag{4.4}$$

$$\int a^x dx = \frac{a^x}{lna} + C. \tag{4.5}$$

Quadrature Amplitude Modulation (QAM) передбачає одночасне надсилання двох різних сигналів на одній несучій частоті. Комбінація ASK і PSK дає методику модуляції вищого порядку, таку як QAM. Використовується в основному в цифрових телекомунікаційних системах і програмах доставки більш високої інформації, таких як системи кабельних модемів. Коли необхідна швидкість передачі даних перевищує 8PSK, доцільно перейти до QAM, оскільки можна досягти більшої відстані між сусідніми точками в площині I і Q шляхом рівномірного розподілу точок. Складність полягає в тому, що демодулятор повинен належним чином визначити як амплітуду, так і фазу, оскільки точки не мають однакової амплітуди. Існують різні форми QAM: 16QAM, 64QAM, 128QAM і 256QAM. QAM вищого порядку дає простір для більшої кількості точок у групі, відповідно, можливою є передача більшої кількості бітів на символ, що дозволяє передавати дані в меншій смузі пропускання. Якщо середня енергія сузір’я залишається постійною, символи повинні бути дуже близько один до одного, і це робить їх більш вразливими до шуму та інших спотворень, що призводить до більш високого рівня бітових помилок. Цей сигнал повинен передаватися з більшою потужністю, щоб символ розповсюджувався більше, таким чином, знижуючи енергетичну ефективність цього методу порівняно з іншими методами модуляції. QAM вищого порядку дозволяють передавати більше даних, що робить їх спектрально ефективнішими, однак вони менш надійні порівняно з QAM нижчого порядку.

Можна виразити загальну форму сигналів QAM математично:

,

$$S_i(t) = \sqrt{\frac{2E_{min}}{T_s}} a_1 \cos(2\pi f_c t) + \sqrt{\frac{2E_{min}}{T_s}} b_1 \sin(2\pi f_c t),$$
$$0 \le t \le T, i = 1, 2, 3, 4 \ldots M, \quad (4.6)$$

де E_{min} – енергія сигналу з найменшою амплітудою;

a_l і b_l є парою незалежних цілих чисел, обраних відповідно до розташування конкретної сигнальної точки.

Середня ймовірність помилки з адитивним білим гаусовським шумом (Additive white Gaussian noise, AWGN) для QAM можна представити у вигляді:

$$P_e \cong 4\left(1 - \frac{1}{\sqrt{M}}\right) Q\left(\sqrt{\frac{2E_{min}}{N_0}}\right). \quad (4.7)$$

На рисунку 4.5 наведено схему QAM модулятора.

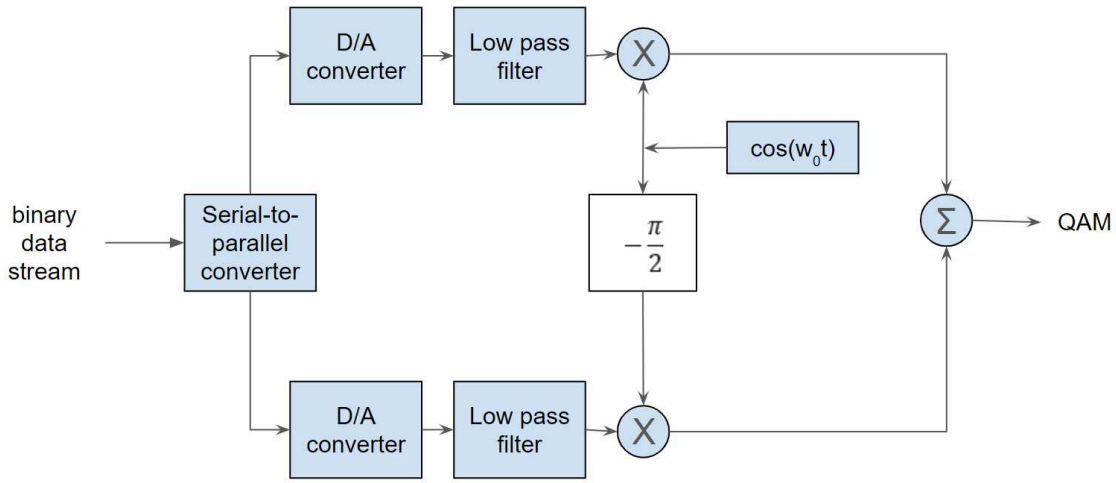

Рисунок 4.5 – Схема модуляції QAM

Для покращення продуктивності системи, стійкості до AWGN використовується кодування з виправленням помилок.

Після модуляції відбувається попереднє кодування та розподіл на потоки для передачі через кілька антен (MIMO). У низхідному каналі операції з декількома несучими засновані на схемі модуляції OFDM. Схема застосування

технологій MIMO та модуляції OFDM для каналу PDSCH показано на рисунку 4.6) [91].

Вибір методів значною мірою впливає на характеристики, продуктивність і загальні фізичні досягнення системи зв'язку. Цифрова модуляція й надалі залишатиметься актуальною для голосового зв'язку та передачі інформації в найкоротші терміни в межах доступної смуги пропускання за доступною ціною та з найменшою кількістю ймовірність помилки.

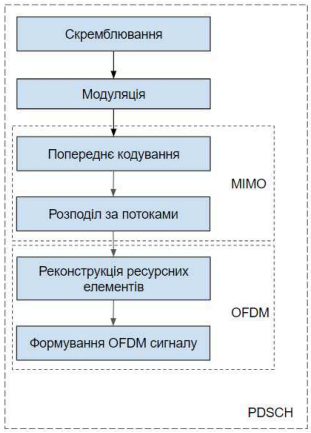

Рисунок 4.6 – Етапи обробки на рівні PDSCH

Імітаційна модель здійснює обробку даних, що надходять з підрівня MAC до фізичного рівня, та передбачає наявність завмирань та адитивного білого гаусового шуму (AWGN). Таким чином, моделювання каналу виконується шляхом комбінування багатопроменевого каналу MIMO із затуханням та каналу з AWGN. До параметрів каналів MIMO відносяться конфігурації антен, профілі багатопроменевої затримки/завмирання, максимальні доплерівські зсуви і рівні просторової кореляції в антенах на стороні передавача та приймача. Канал AWGN, як правило, характеризується значеннями SNR або дисперсії шуму. На приймальному боці до прийнятих символів виконуються операції, зворотні тим, що виконувались на стороні передавача. Після передачі даних через модель фізичного рівня LTE їх було порівняно з оригінальними [97].

У системах зв’язку якість передачі зазвичай кількісно визначається або частотою бітових помилок (Bit Error Rate, BER), або частотою помилок пакетів (Packet Error Rate, PER). Основною метою проектування цифрової системи зв’язку є досягнення найменшої ймовірності помилки та ефективне використання пропускної здатності каналу.

Співвідношення сигнал/шум (SNR) – це різниця між потужністю сигналу, який відтворює система, порівняно з силою або амплітудою її фонового шуму. Відповідно до теорії Шеннона, максимальна пропускна здатність каналу зі смугою пропускання W з потужністю сигналу S, на яку впливає білий шум середньої потужності N, визначається як

$$C = Wlog_2\left(1 + \frac{S}{N}\right). \tag{4.8}$$

4.2 Дослідження завадостійкості біометричних хешів до зовнішніх впливів під час передачі каналом зв’язку.

На рисунку 4.7 наведено схему обробки даних перед передачею мережею[77].

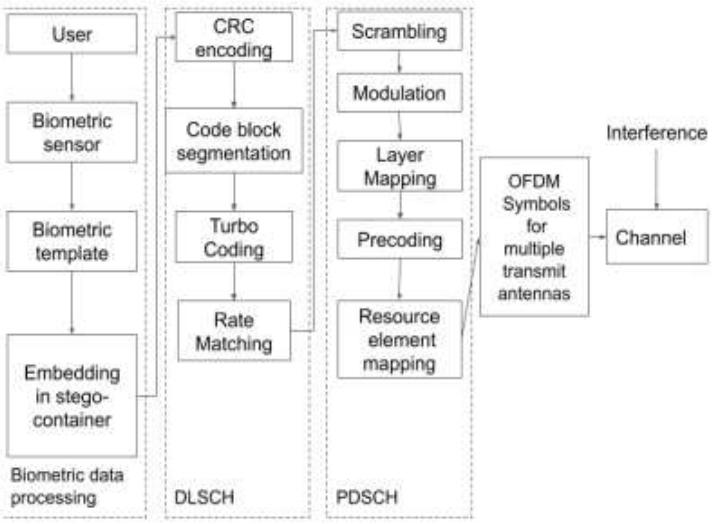

Рисунок 4.7 – Схема обробки даних перед передачею мережею

Після виконання хешування та виправлення помилок кодування дані вбудовуються в стегоконтейнер та передаються через модель мережі LTE. Модель мережі LTE включає передавач, бездротовий канал зв’язку та приймач.

Проведено дослідження впливу параметрів передавача на працездатність системи віддаленої біометричної автентифікації при наявності в каналі зв’язку завад та доплерівських зсувів. Для цього було проведено оцінку порогу спрацьовування системи при використанні 16QAM і MIMO 2x2 при швидкості коду 1/2 (табл. 4.1) [94].

Таблиця 4.1 – Поріг спрацьовування системи віддаленої автентифікації

Доплерівський зсув / SNR (дБ)	0	10	40	80
1	2	3	4	5
6,2	–	–	–	–
6,3	–	–	–	–
6,4	1	–	–	–
1	2	3	4	5
6,5	1	1	1	–
6,6	1	1	1	–
6,7	1	1	1	–
6,8	1	1	1	–
6,9	1	1	1	–
7	1	1	1	–
7,1	1	1	1	–
7,2	1	1	1	–
7,3	1	1	1	–
7,4	1	1	1	–
7,5	1	1	1	–
7,6	1	1	1	–

Продовження таблиці 4.1

7,7	1	1	1	–
7,8	1	1	1	1

Під час аналізу було оцінено поріг спрацьовування системи. В таблиці символом «–» позначено відмову системи прийняти біохеш через велику кількість помилок. Результати досліджень показали, що зростання максимального доплерівського зсуву при зниженні співвідношення сигнал/шум погіршує якість роботи системи. При відсутності доплерівського зсуву порогом спрацьовування системи є значення SNR = 6,4 дБ, при появі та зростанні MDS поріг спрацьовування збільшується до 7,8 дБ. Наявність у каналі доплерівського зсуву буде вимагати збільшення потужності передавача або підвищення завадостійкості та інших алгоритмів модуляції [97].

Наступним параметром, що був досліджений, є швидкість коду, що характеризує співвідношення кількості символів на вході завадостійкого кодера до кількості символів на виході. Зменшення швидкості коду знижує ефективну швидкість передачі даних, але дає можливість підвищити завадостійкість [94]. Результати наведено на рисунку 4.8. Дослідження проведено при швидкості коду 1/2 та 1/3 при модуляції 16QAM та при рівнях доплерівських зсувів 0 Гц та 80 Гц [97].

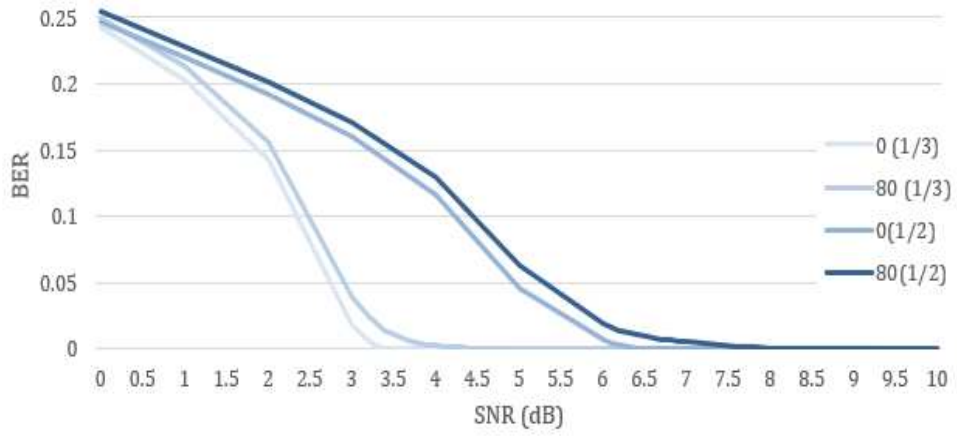

Рисунок 4.8 – Залежність SNR від BER

При відсутності доплерівських зсувів зменшення швидкості коду дозволяє покращити поріг спрацьовування системи (при швидкості коду 1/2 SNR=6,4 дБ, при швидкості коду 1/3 SNR=3,4 дБ). Також при такій швидкості коду наявність максимальних доплерівських зсувів незначно погіршує поріг спрацьовування (при MDS=0 Гц SNR=6,4 дБ, при MDS=80 Гц SNR=7,8 дБ). Таким чином, можна зробити висновок, що швідкість коду має більший вплив на якість спрацьовування системи. На стороні передавача можливо змінювати такий параметр, як алгоритм модуляції. В технології LTE можливим є використання таких алгоритмів модуляції, як QPSK, 16 QAM та 64 QAM. Channel Quality Indicator (CQI) може приймати значення від 1 (найгірша якість) до 15 (найкращі мережні умови) (табл. 4.2) [97].

Таблиця 4.2 – Залежність алгоритму модуляції від індикатору стану каналу

CQI	1	4	5	6	7	8	9	10	11
Алгоритм модуляції	QPSK	QPSK	QPSK	QPSK	16 QAM	16 QAM	16 QAM	64 QAM	64 QAM
Біт/символ	2	2	2	2	4	4	4	6	6

Було проведено дослідження залежності кількості бітових помилок від співвідношення сигнал/шум за умови використання алгоритмів модуляції 16QAM та 64QAM при швидкості коду 1/3 та різних рівнях доплерівських зсувів (0 та 80). Результати дослідження показали (рис. 4.9), що алгоритм QPSK навіть при найгірших параметрах каналу забезпечує значення BER на рівні $3.5 \cdot 10^{-6}$, в той час, як алгоритми 16QAM та 64QAM можуть забезпечити лише $1 \cdot 10^{-5}$ та $1.5 \cdot 10^{-3}$ відповідно для значень SNR, що відповідають порогу спрацьовування системи. Базуючись на отриманих результатах, можна зробити висновок, що в системі віддаленої автентифікації навіть при високих показниках співвідношення SNR не рекомендується використовувати 64QAM [97].

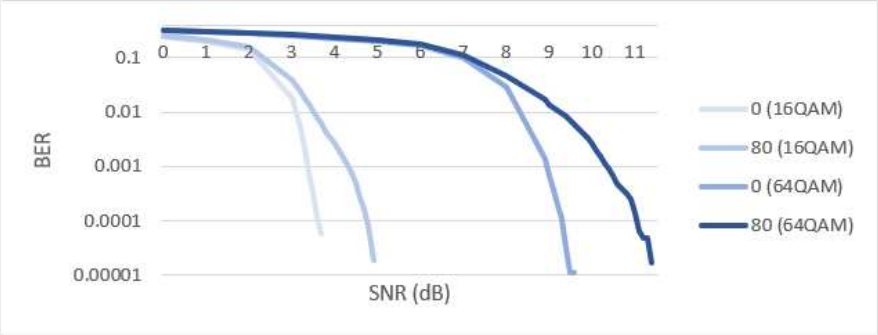

Рисунок 4.9 – Залежність SNR від BER при використанні різних алгоритмів модуляції

Також було проведено дослідження налаштувань багатоантенного прийому та передачі MIMO. В роботі був оцінений вплив застосування схем MIMO 1x1, 2x2 та 4x4 на завадостійкість (рис. 4.10). Проведено аналіз залежності кількості бітових помилок (BER) від співвідношення сигнал/шум (SNR) за умови використання багатоантенної техніки MIMO при швидкості коду 1/3 та модуляції 16QAM[97].

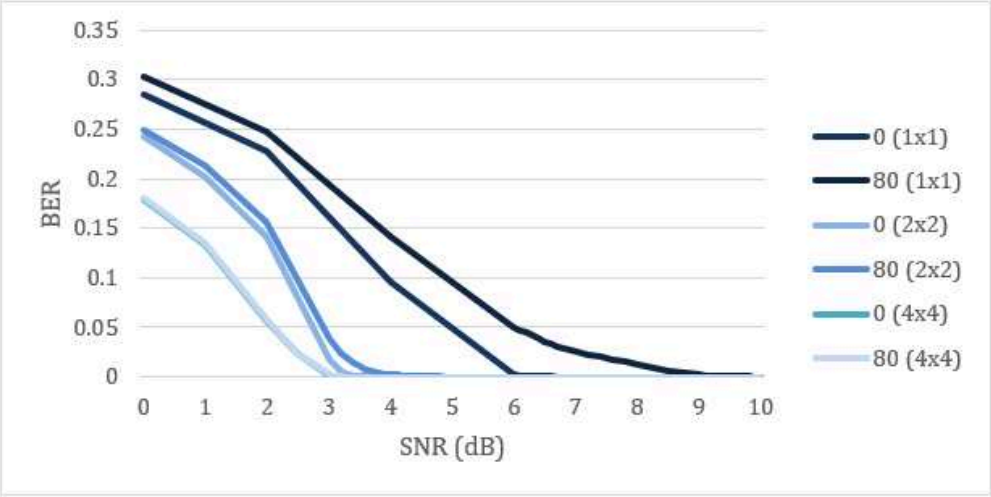

Рисунок 4.10 – Залежність SNR від BER при різних схемах MIMO

Застосування MIMO дозволяє майже вдвічі підвищити завадостійкість і, таким чином, покращити пороги розпізнавання автентифікаційних даних. В

результаті досліджень можна зробити висновок, що покращити якість роботи системи віддаленої біометричної автентифікації можна шляхом використання адаптивних налаштувань на стороні передавача та використання засобів підвищення завадостійкості. Аналіз результатів показав, що найкращє співвідношення між завадостійкістю та швидкістю при віддаленій біометричній автентифікації в мережі LTE забезпечує модуляція 16QAM. Квадратурну амплітудну модуляцію 64QAM не бажано використовувати під час проведення транзакцій. Висновки базуються на тому, що у разі відсутності впливу доплерівських зсувів поріг спрацьовування системи з використанням модуляції QPSK становить SNR = 0 дБ, з модуляцією 16QAM SNR = 3,4 дБ, а з 64QAM значення SNR = 9 дБ [97].

Застосування декількох антен також підвищує якість каналу зв'язку. Наприклад, для значення BER, що дорівнює 0,14, за умови використання антенної конфігурації – 1x1 (MDS = 80 Гц) SNR становить 4 дБ, а для MIMO 4x4 (MDS = 80 Гц) для того ж самого значення BER SNR дорівнює 1 дБ. Це вказує на перевагу використання технології MIMO 4x4 [97].

Пороги спрацьовування системи віддаленої біометричної автентифікації при MDS = 0 Гц: MIMO 1x1 SNR = 6,1 дБ; MIMO 2x2 SNR = 3,4 дБ; MIMO 4x4 SNR = 3,1 дБ [97].

Крім модуляції та антенної конфігурації, було визначено, що швидкість коду також впливає на значення BER. Поріг спрацьовування системи зменшився майже вдвічі від SNR = 6,4 дБ для швидкості коду 1/2 до SNR=3,4 дБ для 1/3 [97].

Отже, при використанні систем віддаленої біометричної автентифікації в мережах мобільного зв'язку, доцільним є використання параметрів передавача із застосуванням схем MIMO 2x2 і 4x4, кодів 1/3 та модуляції 16QAM. У цьому випадку можна досягти найкращих результатів зі спрацьовування системи. За умови найгірших мережних умов пріоритет треба віддавати застосуванню схеми MIMO 4x4, модуляції QPSK та використанню кодів 1/3 [97].

4.3 Висновки до розділу 4

В роботі вперше досліджено ефективність методів мережної автентифікації за умови використання канального кодування на тлі каналів зв’язку з завадами та оцінено методом математичного моделювання стійкість методів мережної автентифікації до виявлення, що складає наукову новизну вказаної роботи [97].

Результати роботи показали, що якість роботи системи віддаленої біометричної автентифікації може бути істотно покращена за допомогою застосування додаткових засобів завадостійкості та використання адаптивних налаштувань на стороні передавача. На основі отриманих результатів дослідження можна зробити висновок, що краще співвідношення між завадостійкістю та швидкістю при проведенні віддаленої біометричної автентифікації в мережі LTE забезпечує модуляція 16QAM. 64QAM не бажано використовувати під час проведення транзакцій, так як у разі відсутності впливу доплерівських зсувів поріг спрацьовування системи з використанням модуляції QPSK становить SNR = 0 дБ, з модуляцією 16QAM SNR = 3,4 дБ, а з 64QAM значення SNR дорівнює 9 дБ [97].

Список використаних джерел у даному розділі наведено у повному списку використаних джерел під номерами 92-97.

ВИСНОВКИ

Проведено аналіз розвитку сучасних мобільних мереж 4G LTE та 5G, розглянуто їх архітектуру та відмінності, проведено порівняння основних характеристик. Розглянуто використання нових технологій, таких як massive MIMO, NFV, Edge Computing, Network Slicing. Проаналізовано основні сценарії використання сучасних мобільних мереж, таких, як мережі розумних будинків, віддалене користування банківськими послугами, оплати в інтернет магазниах, використання IoT в різних сферах. Доведено актуальність задачі підвищення захисту конфеденційних даних користувачів та протидії несанкціонованому доступу до даних.

Проведено дослідження стану безпеки сучасних мобільних мереж, визначено основні типи атак та загроз в мобільних мережах. Проаналізовано можливість їх перекриття застосуванням методів віддаленої автентифікації. Обгрунтовано необхідність застосування віддаленої автентрифікації для сценаріїв використання мереж 4G LTE та 5G. За підсумками порівяння методів віддаленої автентифікації для проведення досліджень було обґрунтовано застосування методів біометричної автентифікації. Це дало змогу підвищити завадостійкість та ефективність систем віддаленої автентифікації в телекомунікаційних системах.

Методом багатокритеріальної оптимізації вперше визначено оптимальний за критеріями визнання користувачами, стійкість до підробок та атак, вартість, простота використання, частота відмов в обслуговуванні та частота помилкових спрацьовувань. Проведений аналіз за вищеперерахованими критеріями показав, що найвищий вектор глобальних пріоритетів за методом аналізу ієрархій виявився для методу автентифікації за райдужною оболонкою ока, що на 0,01 вище ніж в методу автентифікації за

відбитком пальця та на 0,033 вище ніж в методу автентифікації за геометрією руки.

Запропонований підхід дозволив визначити найкращий за критеріями FAR та FRR набір фільтрів. Запропоновано методи захисту біометричного шаблону. Найкращий результат показав метод з використанням фільтрів Гауса та оператора Лапласа.

Визначено переважний за критеріями завадозахищеності та ймовірності помилки метод біометричної автентифікації, відмінністю якого є врахування стійкості до завад в каналах зв'язку. Це дало змогу підвищити завадостійкість та ефективність систем віддаленої автентифікації в телекомунікаційних системах. Найбільш стійким до завад виявився метод BIN-COMBO.

Запропоновано передавати біохеш методами мережної стеганографії. Представлено запропоновану узагальнену модель прихованої передачі для підвищення захищеності систем віддаленої автентифікації користувачів. Змодельовано роботу трьох методів, які використовують мережні фрагменти даних PDUs протоколів TCP, HTTP та ICMP. Ці методи буди порівняні за такими показниками, як коефіцієнт корисної дії та швидкодія. Проведені дослідження показали, що вбудовування в ICMP пакет дозволяє використати від 6,25% до 93,75% від розміру пакету, вбудовування за допомогою метода TCP – 5%, метод вбудовування в HTTP дозволяє використати лише 0,75% від загального розміру пакету [66].

Проаналізовано вплив передачі пакетів, що містять вбудовані дані, на статистичні характеристики трафіку. Визначено, що метод HTTP стеганографії має низьку пропускну здатність. При його застосуванні TCP та HTTP трафік різко збільшується. Метод вбудовування в TCP також є помітним – призводить до збільшення кількості пакетів при збільшенні інформації, що передається, а також має низьку швидкодію. Кращим з методів виявився метод вбудовування в ICMP-пакети.

Вдосконалено метод передачі автентифікаційної інформації телекомунікаційними системами, відмінністю якого є послідовне застосування методів отримання біометричного шаблону, узгодження параметрів передачі з якістю каналу зв’язку, завадостійкого кодування та мережної стеганографії. Це дозволило підвищити захищеність передачі інформації та завадостійкість.

Вперше визначений переважний за критеріями швидкодії, прихованості та пропускної здатності метод мережної стеганографії. Це дало змогу покращити ефективність системи віддаленої автентифікації за рахунок застосування визначеного методу.

Вдосконалено метод віддаленої біометричної автентифікації, відмінністю якого є застосування мережної стеганографії та врахування дії завад в каналах зв’язку. Це дало можливість сформувати вимоги щодо підвищення загальної ефективності систем віддаленої автентифікації в телекомунікаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богенс К. Стандартизація та спектр для систем IMT [Електронний ресурс] / К. Богенс // Регіональний семінар МСЕ для стран Європи та СНГ \"Цифрове майбутнє на основі 4G/5G\". – 2018. – Режим доступу до ресурсу: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2014.05.18%20-%20Karlis%20Bogens.pdf.

2. Remmert H. What is 5G? Part 1 - Evolution and the Next Generation [Електронний ресурс] / Harald Remmert – Режим доступу до ресурсу: https://www.digi.com/blog/post/2019/what-is-5g-part-1-evolution-and-the-next-generatio.

3. Zarrinkoub H. Understanding LTE with MATLAB - From Mathematical modeling to simulation and prototyping / Houman Zarrinkoub. – [S. l.] : John Wiley & Sons, Inc., 2014.

4. Silva M. M. d. On the 5G and Beyond [Electronic resource] / Mário Marques da Silva, João Guerreiro // Applied Sciences. – 2020. – Vol. 10, no. 20. – P. 7091. – Mode of access: https://doi.org/10.3390/app10207091 (date of access: 15.06.2024). – Title from screen.

5. Handbook on International Mobile Telecommunications (IMT). – Switzerland : ITUPublications, 2022. – 114 p

6. Remmert H. What Is 5G Network Architecture? [Електронний ресурс] / Harald Remmert // Digi International Inc.. – 2021. – Режим доступу до ресурсу: https://www.digi.com/blog/post/5g-network-architecture.

7. 5G spectrum bands explained– low, mid and high band | Nokia [Electronic resource] // Nokia. – Mode of access: https://www.nokia.com/thought-leadership/articles/spectrum-bands-5g-world/ (date of access: 19.11.2024). – Title from screen.

8. 3GPP Specification series [Електронний ресурс] – Режим доступу до ресурсу: https://www.3gpp.org/dynareport?code=25-series.htm.

9. What is UE? [Електронний ресурс] – Режим доступу до ресурсу: https://inseego.com/ie/resources/5g-glossary/what-is-ue/.

10. 3GPP TS 23.101 version 8.0.0 Release 8 [Електронний ресурс] // European Telecommunications Standards Institute. – 2009. – Режим доступу до ресурсу: https://www.etsi.org/deliver/etsi_ts/123100_123199/123101/08.00.00_60/ts_123101v080000p.pdf.

11. NG-RAN Architecture [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.3gpp.org/news-events/3gpp-news/ng-ran-architecture.

12. 5G System Overview [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.3gpp.org/technologies/5g-system-overview.

13. Singh N. What is the 5G Access and Mobility Management Function (AMF)? [Електронний ресурс] / Nicole Singh. – 2023. – Режим доступу до ресурсу: https://techcommunity.microsoft.com/t5/azure-for-operators-blog/what-is-the-5g-access-and-mobility-management-function-amf/ba-p/3707685.

14. AUSF (Authentication Server Function) In 5G-NR [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://techlteworld.com/ausf-authentication-server-function-in-5g-nr/.

15. Kumar A. 4G/5G Core Network Architecture Comparison [Електронний ресурс] / Abhijeet Kumar. – 2023. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/4g5g-core-network-architecture-comparison-5g-learning-ktule.

16. 2G to 6G Telecom Journey [Електронний ресурс] // 5G 6G & O-RAN. – 2023. – Режим доступу до ресурсу: https://ec.linkedin.com/posts/5g-learning_2g-to-6g-telecom-journey-throughput-the-activity-7056416276381929472-Yll5.

17. Massive MIMO: survey and future research topics [Electronic resource] / Daniel C. Araújo [et al.] // IET Communications. – 2016. – Vol. 10, no. 15. – P. 1938–1946. – Mode of access: https://doi.org/10.1049/iet-com.2015.1091 (date of access: 15.06.2024). – Title from screen.

18. What Is Massive MIMO? [Електронний ресурс] – Режим доступу до ресурсу: https://www.mathworks.com/discovery/massive-mimo.html.

19. Network Functions Virtualisation (NFV) [Electronic resource] // ETSI. – Mode of access: https://www.etsi.org/technologies/nfv?highlight=YToxOntpOjA7czozOiJuZnYiO30= (date of access: 15.06.2024). – Title from screen.

20. Friend D. What exactly is NFV and how can it be used in 5G networking? [Electronic resource] / Derek Friend // LinkedIn. – Mode of access: https://www.linkedin.com/pulse/what-exactly-nfv-how-can-used-5g-networking-derek-friend (date of access: 15.06.2024). – Title from screen.

21. What Is Edge Computing? | IBM [Electronic resource] // IBM - United States. – Mode of access: https://www.ibm.com/topics/edge-computing (date of access: 15.06.2024). – Title from screen.

22. Stallings W. 5G wireless: a comprehensive introduction / William Stallings. – [S. l.] : Pearson Education, Limited, 2021

23. Securing 5G networks [Electronic resource] // Council on Foreign Relations. – Mode of access: https://www.cfr.org/report/securing-5g-networks (date of access: 15.06.2024). – Title from screen.

24. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] : НОРМ. ДОК. від 28.04.1999 р. № НД ТЗІ 2.5-004-99. – Режим доступу: https://tzi.com.ua/downloads/2.5-004-99.pdf. – Назва з екрана.

25. The evolution of security in 5G [Electronic resource]. – [S. l.] : 5G Americas Whitepaper, 2018. – 41 p. – Mode of access: https://www.5gamericas.org/wp-

content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf (date of access: 15.06.2024). – Title from screen.

26. Matsko O. Y. Security analysis of telecommunication networks of the 5G generation [Electronic resource] / O. Y. Matsko // Modern Information Security. – 2022. – Vol. 52, no. 4. – Mode of access: https://doi.org/10.31673/2409-7292.2022.040003 (date of access: 15.06.2024). – Title from screen.

27. A security enhanced 5G authentication scheme for insecure channel [Electronic resource] / Xinxin Hu [et al.] // IEICE transactions on information and systems. – 2020. – E103.D, no. 3. – P. 711–713. – Mode of access: https://doi.org/10.1587/transinf.2019edl8190 (date of access: 15.06.2024). – Title from screen.

28. Identyfikacja, uwierzytelnianie i autoryzacja [Electronic resource] // Computerworld. – Mode of access: https://www.computerworld.pl/news/Identyfikacja-uwierzytelnianie-i-autoryzacja,299422.html (date of access: 15.06.2024). – Title from screen.

29. Gernot T. Robust biometric scheme against replay attacks using one-time biometric templates [Electronic resource] / Tanguy Gernot, Christophe Rosenberger // Computers & Security. – 2024. – Vol. 137. – P. 103586. – Mode of access: https://doi.org/10.1016/j.cose.2023.103586 (date of access: 15.06.2024). – Title from screen.

30. User authentication on mobile devices: approaches, threats and trends [Electronic resource] / Chen Wang [et al.] // Computer networks. – 2020. – Vol. 170. – P. 107118. – Mode of access: https://doi.org/10.1016/j.comnet.2020.107118 (date of access: 15.06.2024). – Title from screen.

31. Patel V. M. Cancelable Biometrics: a review [Electronic resource] / Vishal M. Patel, Nalini K. Ratha, Rama Chellappa // IEEE signal processing magazine. – 2015. – Vol. 32, no. 5. – P. 54–65. – Mode of access: https://doi.org/10.1109/msp.2015.2434151 (date of access: 15.06.2024). – Title from screen.

32. Sundararajan A. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems [Electronic resource] / Aditya Sundararajan, Arif I. Sarwat, Alexander Pons // ACM computing surveys. – 2019. – Vol. 52, no. 2. – P. 1–36. – Mode of access: https://doi.org/10.1145/3309550 (date of access: 15.06.2024). – Title from screen.

33. Gait recognition as an authentication method for mobile devices / M.-S. Axente et al. Sensors. 2020. Vol. 20, no. 15. P. 4110. URL: https://doi.org/10.3390/s20154110 (date of access: 15.06.2024).

34. 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. URL: https://doi.org/10.20535/srit.2308-8893.2022.3.05 (date of access: 15.06.2024).

35. Bodepudi, A., & Reddy, M. (2020). Spoofing Attacks and Mitigation Strategies in Biometrics-as-a-Service Systems. Eigenpub Review of Science and Technology, 4(1), 1–14.

36. Чернікова В. Г. Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока [Електронний ресурс] / В. Г. Чернікова, А. А. Астраханцев, Г. Є. Ляшенко // Системи озброєння і військова техніка. – 2018. – № 1(53). – С. 195–202. – Режим доступу: https://doi.org/10.30748/soivt.2018.53.28 (дата звернення: 15.06.2024). – Назва з екрана.

37. Ляшенко Г. Є., Астраханцев А. А. Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2017. № 2(148). С. 111–114. URL: https://doi.org/10.30748/soi.2017.148.20 (дата звернення: 15.06.2024).

38. Jain A. K. 50 years of biometric research: accomplishments, challenges, and opportunities [Electronic resource] / Anil K. Jain, Karthik Nandakumar, Arun Ross // Pattern recognition letters. – 2016. – Vol. 79. – P. 80–105. – Mode of access:

https://doi.org/10.1016/j.patrec.2015.12.013 (date of access: 15.06.2024). – Title from screen.

39. Zuo J. Cancelable iris biometric / Jinyu Zuo, Nalini K. Ratha, Jonathan H. Connell // 19th International Conference on Pattern Recognition. – 2008.

40. Teixeira C. H. C. Min-Hash Fingerprints for Graph Kernels: A Trade-off among Accuracy, Efficiency, and Compression / Carlos H. C. Teixeira, Silva Arlei, Meira Jr Wagner // Journal of Information and Data Management. – 2012. – No. 3.

41. A survey of biometric approaches of authentication / N. Yusuf et al. International journal of advanced computer research. 2020. Vol. 10, no. 47. P. 96–104. URL: https://doi.org/10.19101/ijacr.2019.940152 (date of access: 15.06.2024).

42. Developing iris recognition system for smartphone security / L. A. Elrefaei et al. Multimedia tools and applications. 2017. Vol. 77, no. 12. P. 14579–14603. URL: https://doi.org/10.1007/s11042-017-5049-3 (date of access: 15.06.2024).

43. Saaty R. W. The analytic hierarchy process–what it is and how it is used. Mathematical modelling. 1987. Vol. 9, no. 3-5. P. 161–176. URL: https://doi.org/10.1016/0270-0255(87)90473-8 (date of access: 15.06.2024).

44. Saaty T. The analytic hierarchy process / T. Saaty. – New York : McGraw Hill, 1980. – 270 p.

45. Jain A. K. An introduction to biometric recognition [Electronic resource] / A. K. Jain, A. Ross, S. Prabhakar // IEEE transactions on circuits and systems for video technology. – 2004. – Vol. 14, no. 1. – P. 4–20. – Mode of access: https://doi.org/10.1109/tcsvt.2003.818349 (date of access: 15.06.2024). – Title from screen.

46. Biometric cryptosystems: issues and challenges [Electronic resource] / U. Uludag [et al.] // Proceedings of the IEEE. – 2004. – Vol. 92, no. 6. – P. 948–960. – Mode of access: https://doi.org/10.1109/jproc.2004.827372 (date of access: 15.06.2024). – Title from screen.

47. Iris recognition: biometric authentication | NEC [Electronic resource] // NEC. – Mode of access: https://www.nec.com/en/global/solutions/biometrics/iris/index.html (date of access: 15.06.2024). – Title from screen.

48. Center for biometrics and security research [Electronic resource]. – Mode of access: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp (date of access: 15.06.2024). – Title from screen.

49. Masek L. Recognition of human iris patterns for biometric identification / Masek Libor. – [S. l.], 2003. – 61 p.

50. Canny J. A computational approach to edge detection [Electronic resource] / John Canny // IEEE transactions on pattern analysis and machine intelligence. – 1986. – PAMI-8, no. 6. – P. 679–698. – Mode of access: https://doi.org/10.1109/tpami.1986.4767851 (date of access: 15.06.2024). – Title from screen.

51. Reddy P. K. Canny scale edge detection / Pradeep Kumar Reddy, C. Nagaraju, I. Rajasekhar Reddy // International journal of engineering trends and technology (IJETT). – 2015. – P. 1–4.

52. Ito K. Gaussian filters for nonlinear filtering problems [Electronic resource] / K. Ito, K. Xiong // IEEE transactions on automatic control. – 2000. – Vol. 45, no. 5. – P. 910–927. – Mode of access: https://doi.org/10.1109/9.855552 (date of access: 15.06.2024). – Title from screen.

53. Investigation on the effect of data quality and quantity of concrete cracks on the performance of deep learning-based image segmentation [Electronic resource] / Gang Xu [et al.] // Expert systems with applications. – 2023. – P. 121686. – Mode of access: https://doi.org/10.1016/j.eswa.2023.121686 (date of access: 15.06.2024). – Title from screen.

54. Biosignal processing and classification using computational learning and intelligence [Electronic resource]. – [S. l.] : Elsevier, 2022. – Mode of access:

https://doi.org/10.1016/c2019-0-00985-5 (date of access: 15.06.2024). – Title from screen.

55. Dunn D. Optimal Gabor Filters for Texture Segmentation / D. Dunn, W. Higgins // International Journal of Computer Vision. – 2009. – Vol. 6. – P. 947-964.

56. Spatial filters - Laplacian/Laplacian of Gaussian [Electronic resource] // Informatics Homepages Server. – Mode of access: https://homepages.inf.ed.ac.uk/rbf/HIPR2/log.htm (date of access: 15.06.2024). – Title from screen.

57. Nandakumar K. Biometric Template Protection: bridging the performance gap between theory and practice [Electronic resource] / Karthik Nandakumar, Anil K. Jain // IEEE signal processing magazine. – 2015. – Vol. 32, no. 5. – P. 88–100. – Mode of access: https://doi.org/10.1109/msp.2015.2427849 (date of access: 15.06.2024). – Title from screen.

58. Investigation of the Influence of Image Quality on the Work of Biometric Authentication Methods

59. PalmHashing: a novel approach for cancelable biometrics [Electronic resource] / Tee Connie [et al.] // Information processing letters. – 2005. – Vol. 93, no. 1. – P. 1–5. – Mode of access: https://doi.org/10.1016/j.ipl.2004.09.014 (date of access: 15.06.2024). – Title from screen.

60. Кузнецов А. Нечіткий екстрактор на перешкодостійких кодах для біометричної криптографії / А. Кузнецов, Р. Сергієнко, А. Уварова // Радіотехніка. – 2018. – № 195. – С. 224–234.

61. Poongodi P. A study on biometric template protection techniques [Electronic resource] / Poongodi P, Betty P // International journal of engineering trends and technology. – 2014. – Vol. 7, no. 4. – P. 202–204. – Mode of access: https://doi.org/10.14445/22315381/ijett-v7p244 (date of access: 15.06.2024). – Title from screen.

62. Луценко М.С. Порівняльний аналіз біометричних криптосистем / М.С. Луценко, О.О. Кузнецов, Д.І. Прокопович-Ткаченко, В.П. Звєрєв, А.О. Уварова // Прикладная радиоэлектроника. – 2018. – Том 17, № 3, 4 – с.182-191.

63. Zuo J. Cancelable iris biometric / Jinyu Zuo, Nalini K. Ratha, Jonathan H. Connell // 19th International Conference on Pattern Recognition. – 2008.

64. Teixeira C. H. C. Min-Hash Fingerprints for Graph Kernels: A Trade-off among Accuracy, Efficiency, and Compression / Carlos H. C. Teixeira, Silva Arlei, Meira Jr Wagner // Journal of Information and Data Management. – 2012. – No. 3.

65. Ляшенко Г. Є. Аналіз методів захисту біометричних шаблонів / Г. Є. Ляшенко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тез. доп. дванадцятої міжнародної науково-технічної конференції, 27–28 квітня 2022 р. – Т. 1. – Баку–Харків–Жиліна, 2022. – С. 77.

66. Liashenko, G., Astrakhantsev, A. (2021). Implementation Biometric Data Security in Remote Authentication Systems via Network Steganography. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-030-58359-0_14.(Scopus)

67. Lubacz J. Principles and overview of network steganography [Electronic resource] / Jozef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski // IEEE communications magazine. – 2014. – Vol. 52, no. 5. – P. 225–229. – Mode of access: https://doi.org/10.1109/mcom.2014.6815916 (date of access: 16.06.2024). – Title from screen.

68. Handel T. G. Hiding data in the OSI network model / Theodore G. Handel, Maxwell T. Sandford II // Lecture notes in computer science. – 2005. – No. 1174. – P. 23–38.

69. Zhao H. SIP steganalysis using chaos theory / Hong Zhao, Xueying Zhang // 2012 International conference on computing, measurement, control and sensor network. – 2012. – P. 95–100.

70. Сучасні стеганографічні методи захисту інформації [Електронний ресурс] / О. І. Стасюк [та ін.] // Ukrainian information security research journal. – 2011. – Т. 13, № 1 (50). – Режим доступу: https://doi.org/10.18372/2410-7840.13.1994 (дата звернення: 16.06.2024). – Назва з екрана.

71. Шостак Н. Порівняльний аналіз ефективності методів вбудовування цифрових водяних знаків в відеофайли / Н. Шостак, А. Астраханцев, С. Романько // Sciences of europe. – 2017. – № 15. – С. 92–95.

72. Ivanenko O. The concept of steganographic algorithm which has high performance of characteristics defined as significant / O. Ivanenko, A. Астраханцев // 2014 first international scientific-practical conference problems of infocommunications science and technology (PIC s&t`2014). – 2014. – P. 177–179.

73. M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73-80, Jan. 2020, doi:10.1109/TSMC.2019.2903785 https://ieeexplore.ieee.org/abstract/document/8675777

74. Horenbeeck M. V. Deception on the network: thinking diff Deception on the network: thinking differently about co ently about covert channels / Maarten Van Horenbeeck // 7th australian information warfare and security conference. – 2006.

75. Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks / Erik Brown [et al.]. – 2010.

76. Covert Channel Construction Method Based on HTTP Composite Protocols [Electronic resource] / Longxing Jin [et al.] // Journal of Electrical and

Computer Engineering. – 2022. – Vol. 2022. – P. 1–7. – Mode of access: https://doi.org/10.1155/2022/2257524 (date of access: 23.06.2024). – Title from screen.

77. Astrakhantsev A. Noise resistance of remote authentication via lte network / Andrii Astrakhantsev, Galyna Liashenko, Anna Shcherbak // Information and telecommunication sciences. – 2020. – No. 2. – P. 38–43. – Mode of access: https://doi.org/10.20535/2411-2976.22020.38-43.

78. Dimitrova B. Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2) [Electronic resource] / Biljana Dimitrova, Aleksandra Mileva // Journal of Computer and Communications. – 2017. – Vol. 05, no. 05. – P. 98–111. – Mode of access: https://doi.org/10.4236/jcc.2017.55008 (date of access: 23.06.2024). – Title from screen.

79. Mazurczyk, W., Szczypiorski, K. (2008). Covert Channels in SIP for VoIP Signalling. In: Jahankhani, H., Revett, K., Palmer-Brown, D. (eds) Global E-Security. ICGeS 2008. Communications in Computer and Information Science, vol 12. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-69403-8_9

80. H. Zhao and X. Zhang, "SIP Steganalysis Using Chaos Theory," 2012 International Conference on Computing, Measurement, Control and Sensor Network, Taiyuan, China, 2012, pp. 95-100, doi: 10.1109/CMCSN.2012.25.

81. 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

82. Cauich, E., Gómez Cárdenas, R., Watanabe, R. (2005). 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

83. Frączek W. Hiding information in a Stream Control Transmission Protocol [Electronic resource] / Wojciech Frączek, Wojciech Mazurczyk, Krzysztof

Szczypiorski // Computer Communications. – 2012. – Vol. 35, no. 2. – P. 159–169. – Mode of access: https://doi.org/10.1016/j.comcom.2011.08.009 (date of access: 23.06.2024). – Title from screen.

84. 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

85. Mazurczyk W. Lost audio packets steganography: the first practical evaluation [Electronic resource] / Wojciech Mazurczyk // Security and Communication Networks. – 2012. – Vol. 5, no. 12. – P. 1394–1403. – Mode of access: https://doi.org/10.1002/sec.502 (date of access: 23.06.2024). – Title from screen.

86. Szczypiorski, Krzysztof. “HICCUPS : Hidden Communication System for Corrupted Networks.” (2003).

87. Buchwald P. Network steganography method for user’s identity confirmation in web applications / Paweł Buchwald, Maciej Rostański, Krystian Mączka // Theoretical and Applied Informatics. – 2014. – No. 26. – P. 177–187.

88. G. Liashenko, A. Astrakhantsev and V. Chernikova, Network steganography application for remote biometrie user authentication, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 326-330, doi: 10.1109/DESSERT.2018.8409153.(Scopus)

89. Аналіз скритності та стійкості до шуму в каналах зв’язку методів мережної стеганографії / А. О. Щербак, А. А. Астраханцев, О.В. Щербак, Г.Є. Ляшенко // Проблеми телекомунікацій. – 2018. – No. 2(23). – P. 89–98. – Mode of access: https://doi.org/10.30837/pt.2018.2.07. (Фахове видання. Належить до категорії Б)

90. Blasco J., Hernandez-Castro J.C., de Fuentes J. M., Ramos B. A Framework for Avoiding Steganography Usage over HTTP // Networks and Computer Applications. – 2012. – Vol. 35, Issue 1. – P. 491-501. – DOI: 10.1016/j.jnca.2011.10.003.

91. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications. IEEE Series on Information and Communication Networks Security, 1st Edition, Wiley, 2016. – 256 p. – DOI: 10.1002/9781119081715.

92. Ляшенко Г. Моделювання методів мережної стеганографії для підвищення надійності віддаленої аутентифікації / Галина Ляшенко, Анна Щербак // Проблеми інформатизації. Тези доповідей шостої міжнародної науково-технічної конференції 14 – 16 листопада 2018 року. – 2018. – С. 16.

93. Zarrinkoub D. H. Understanding LTE with MATLAB® [Electronic resource] / Dr Houman Zarrinkoub. – Chichester, UK : John Wiley & Sons, Ltd, 2014. – Mode of access: https://doi.org/10.1002/9781118443446 (date of access: 23.06.2024). – Title from screen.

94. Ляшенко Г. Модель впливу завад на біометричні шаблони при передачі мобільними мережами / Галина Ляшенко // Проблеми інформатизації. Тези доповідей восьмої міжнародної науково-технічної конференції. – 2020. – Т. 2. – С. 65.

95. Ляшенко Г. Є. Аналіз можливих атак на систему біометричної автентифікації / Г. Є. Ляшенко // Проблеми інформатизації : тези доп. 7-ї міжнар. наук.-техн. конф., 13-15 листопада 2019 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2019. – С. 90.

96. Kowalik S. Symulacja cyfrowa modulacji 16-qam / Stanisław Sowalik // Wyższa Szkoła Biznesu w Dąbrowie Górniczej.

97. Дослідження завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами / А. О. Щербак, А. А. Астраханцев, О.В. Щербак, Г.Є. Ляшенко // Проблеми телекомунікацій.-2020. - Вып. №1(26). - С. 63-72. (Фахове видання. Належить до категорії Б)