

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технології безпеки 4G мереж з метою забезпечення безпеки передачі даних»

Студента 2 курсу, 8м групи,
спеціальності 125
«Кібербезпека та захист
інформації»
освітньої програми «Безпека
системелектронних
комунікацій в економіці»
Науковий керівник
доктор технічних наук,
професор кафедри інженерії
програмного забезпечення та
кібербезпеки

підпис студента

підпис керівника

Константінова Єгора
Вікторовича

Лахно Валерій
Анатолійович

Гарант освітньої програми
кандидат технічних наук,
професор кафедри інженерії
програмного забезпечення та
кібербезпеки

підпис гаранта

Хохлачова Юлія
Євгеніївна

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення та кібербезпеки

Освітній ступінь магістр

Освітня програма 125«Кібербезпека та захист інформації»

Затверджую

Зав. кафедри інженерії програмного
забезпечення та кібербезпеки

Криворучко О. В.

«13» грудня 2023 р.

Завдання

на кваліфікаційну роботу студентів

Константінову Єгору Вікторовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи «Технології безпеки 4G мереж з метою
забезпечення безпеки передачі даних»

Затверджена наказом ректора від «27» листопада 2023 р. № 4149

2. Строк здачі студентом закінченої роботи 15 листопада 2024

3. Цільова установка та вихідні дані до роботи

Мета роботи полягає в розробці нових підходів до забезпечення безпеки
передачі даних у 4G мережах, які підвищують стійкість до сучасних загроз.

Об'єкт дослідження 4G мережі як комплексна технологічна система передачі
даних .

Предмет дослідження методи забезпечення інформаційної безпеки у 4G
мережах, зокрема вдосконалення процесу автентифікації користувачів.

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст кваліфікаційної роботи (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1 ОГЛЯД ТЕХНОЛОГІЙ ТА СТАНДАРТІВ БЕЗПЕКИ 4G МЕРЕЖ

1.1. Загальна характеристика 4G мереж

1.2. Аналіз стандартів безпеки в 4G мережах

1.3. Огляд існуючих загроз та вразливостей

1.4. Висновки до розділу 1

РОЗДІЛ 2 ОБҐРУНТУВАННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В 4G МЕРЕЖАХ

2.1. Аналіз існуючих методів захисту

2.2. Порівняльна оцінка методів захисту

2.3. Вибір та обґрунтування методів для розробки системи безпеки

2.4. Висновки до розділу 2

РОЗДІЛ 3 РОЗРОБКА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В 4G МЕРЕЖАХ

3.1. Загальна архітектура системи забезпечення інформаційної безпеки в мережах четвертого покоління

3.2. Алгоритм захисту

3.3. Інтеграція штучного інтелекту з криптографічними протоколами

3.4. Висновок до розділу 3

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

6. Календарний план виконання роботи

№ пор.	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1.	<i>Вибір теми кваліфікаційної роботи</i>	07.11.2023	07.11.2023
2.	<i>Розробка та затвердження завдання на роботу магістра (стац/заоч)</i>	13.12.2023	13.12.2023
3.	<i>Вступ та перелік літературних джерел</i>	22.02.2024	22.02.2024
4.	<i>Розробка технічного завдання</i>	14.03.2024	14.03.2024
5.	<i>Розділ 1. Огляд технологій та стандартів безпеки 4G мереж</i>	10.04.2024	10.04.2024
6.	<i>Розділ 2. Обґрунтування методів забезпечення безпеки в 4G мережах</i>	23.05.2024	23.05.2024
7.	<i>Розділ 3. Розробка системи забезпечення безпеки передачі даних в 4G мережах</i>	05.09.2024	05.09.2024
8.	<i>Розробка програми та методики тестування</i>	27.09.2024	27.09.2024
9.	<i>Написання наукової статті</i>	16.04.2024	16.04.2024
10.	<i>Керівництво користувача</i>	11.10.2024	11.10.2024
11.	<i>Висновки та пропозиції</i>	16.10.2024	16.10.2024
12.	<i>Здача кваліфікаційної роботи на кафедрі (перша перевірка)</i>	18.10.2024	18.10.2024
13.	<i>Підготовка реферату та презентації доповіді</i>	28.10.2024	28.10.2024
14.	<i>Попередній захист кваліфікаційної роботи</i>	29.10.2024 – 31.10.2024	29.10.2024 – 31.10.2024
15.	<i>Здача зброшурованої кваліфікаційної роботи</i>	15.11.2024	15.11.2024
16.	<i>Зовнішнє рецензування кваліфікаційної роботи</i>	28.10.2024	28.10.2024
17.	<i>Підготовка до публічного захисту кваліфікаційної роботи</i>	02.12.2024– 03.12.2024	02.12.2024– 03.12.2024

7. Дата видачі завдання «16» листопада 2023 р.

8. Науковий керівник кваліфікаційної роботи _____

Лахно В.А.

(прізвище, ініціали, підпис)

9. Гарант освітньої програми _____ Хохлачова Ю.Є.

(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент _____ Константинов Є.В.

(прізвище, ініціали, підпис)

АНОТАЦІЯ

Ця робота присвячена створенню удосконаленої системи для забезпечення безпеки передачі даних у мобільних мережах четвертого покоління (4G) через використання біометричної автентифікації. Головною метою дослідження стало розроблення рішення, яке б комбінувало високий рівень захисту від актуальних кіберзагроз, таких як атаки типу «людина посередині» та перехоплення трафіку, із зручністю користування для абонентів.

Розроблена система використовує біометричні дані, такі як відбитки пальців чи технології розпізнавання обличчя, для верифікації особистості користувачів. В її основі лежить інтеграція криптографічних алгоритмів AES разом із токенизацією, що гарантує конфіденційність і цілісність переданої інформації. За рахунок впровадження штучного інтелекту у систему, вона реалізує багаторівневий захист, використовуючи зашифровані шаблони замість зберігання реальних біометричних даних, а також вживає токени, що значно зменшує ймовірність компрометації.

У дипломній роботі ретельно описані процеси аналізу загроз, обґрунтування вибраних методів захисту, розробка алгоритмів автентифікації та тестування запропонованого рішення. Для верифікації ефективності було проведено моделювання роботи системи, яке показало її стійкість до атак і відповідність вимогам безпеки сучасних мобільних комунікацій.

Це рішення надає можливість операторам мобільного зв'язку втілити нові підходи до забезпечення безпеки, в той же час покращуючи досвід користувачів і знижуючи ризики несанкціонованого доступу. Робота є прикладом інтеграції біометричних технологій та штучного інтелекту в телекомунікаційну галузь і має потенціал для використання в інших сферах, таких як електронна комерція або Інтернет речей (IoT).

Ключові слова: 4G, безпека, біометрична автентифікація, криптографія, AES, токенизація, атака «людина посередині», штучний інтелект.

ABSTRACT

This research is dedicated to developing an advanced system for securing data transmission in fourth-generation (4G) mobile networks through the application of biometric authentication. The primary objective of this study was to create a solution that combines a high level of protection against contemporary cyber threats, such as man-in-the-middle attacks and traffic interception, with user convenience.

The developed system employs biometric data, such as fingerprints or facial recognition, for user verification. It integrates AES cryptographic algorithms and tokenization to ensure data confidentiality and integrity. By incorporating artificial intelligence, the system implements multi-level protection using encrypted templates instead of storing actual biometric data and utilizing tokens, significantly reducing the risk of compromise.

The thesis provides a detailed description of threat analysis processes, justification of selected protection methods, development of authentication algorithms, and testing of the proposed solution. To verify its effectiveness, a system simulation was conducted, demonstrating its resilience to attacks and compliance with modern mobile communication security requirements.

This solution enables mobile operators to implement new approaches to security, improving user experience and reducing the risk of unauthorized access. The work exemplifies the integration of biometric technologies and artificial intelligence into the telecommunications industry and has the potential for application in other areas such as e-commerce and the Internet of Things (IoT).

Keywords: 4G, security, biometric authentication, cryptography, AES, tokenization, man-in-the-middle attack, artificial intelligence.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

4G – Fourth Generation (Мобільні мережі четвертого покоління).

LTE – Long Term Evolution (технологія передачі даних у 4G мережах).

AES – Advanced Encryption Standard (алгоритм симетричного шифрування).

AKA – Authentication and Key Agreement (протокол автентифікації).

IMSI – International Mobile Subscriber Identity (міжнародний ідентифікатор абонента мобільного зв'язку).

GUTI – Globally Unique Temporary UE Identity (глобально унікальний тимчасовий ідентифікатор пристрою).

MITM – Man-in-the-Middle (атака типу «людина посередині»).

DoS – Denial of Service (відмова в обслуговуванні).

DPI – Deep Packet Inspection (глибокий аналіз пакетів).

SIEM – Security Information and Event Management (система управління інцидентами безпеки).

IoT – Internet of Things (Інтернет речей).

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1 ОГЛЯД ТЕХНОЛОГІЙ ТА СТАНДАРТІВ БЕЗПЕКИ 4G МЕРЕЖ	8
1.1 Загальна характеристика 4G мереж	8
1.2 Аналіз стандартів безпеки в 4G мережах	10
1.3 Огляд існуючих загроз та вразливостей.....	14
1.4 Висновок до розділу 1	18
РОЗДІЛ 2 ОБҐРУНТУВАННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В 4G МЕРЕЖАХ	20
2.1 Аналіз існуючих методів захисту	20
2.2. Порівняльна оцінка методів	23
2.3 Вибір та обґрунтування методів для розробки системи безпеки.....	27
2.4 Висновки до розділу 2.....	30
РОЗДІЛ 3 РОЗРОБКА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В 4G МЕРЕЖАХ	32
3.1 Загальна архітектура системи забезпечення інформаційної безпеки в мережах четвертого покоління	32
3.2 Алгоритм захисту	36
3.3 Інтеграція штучного інтелекту з криптографічними протоколами	38
3.4 Висновок до розділу 4.....	40
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	42
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	44

ВСТУП

Мобільні мережі четвертого покоління (4G) є однією з ключових технологій сучасного світу, яка забезпечує високошвидкісну передачу даних, стабільний доступ до інтернет-сервісів, а також інтеграцію з інфраструктурою Інтернету речей (IoT). Стандарти 4G, зокрема LTE (Long Term Evolution) і LTE-Advanced, сприяли широкому впровадженню цифрових послуг, таких як мобільне телебачення, відеоконференції, фінансові транзакції, електронне урядування тощо.

Однак стрімкий розвиток цих мереж супроводжується зростанням ризиків у сфері інформаційної безпеки. Кіберзагрози, такі як атаки типу «людина посередині» (Man-in-the-Middle), перехоплення трафіку, підробка ідентифікаційних даних та атаки на цілісність сигналізації, залишаються серйозною проблемою для операторів і користувачів мобільних мереж. Це обумовлює необхідність розробки і впровадження нових методів захисту, які відповідатимуть вимогам сучасних кіберзагроз та забезпечать високий рівень конфіденційності, цілісності і доступності інформації.

Актуальність теми зумовлена зростанням кількості кіберзагроз, спрямованих на порушення конфіденційності, цілісності та доступності даних, що передаються в 4G мережах. Питання захисту інформації набуває ще більшої уваги у зв'язку з інтеграцією цих мереж в інфраструктуру Інтернету речей (IoT), електронного урядування, електронної комерції тощо.

Об'єкт дослідження 4G мережі як комплексна технологічна система передачі даних.

Предмет дослідження – методи забезпечення інформаційної безпеки у 4G мережах, зокрема вдосконалення процесу автентифікації користувачів.

Мета дослідження розробка і обґрунтування нових підходів до забезпечення безпеки передачі даних у 4G мережах, які підвищують стійкість до сучасних загроз.

Для досягнення мети були поставлені такі завдання:

1. Провести аналіз сучасних технологій безпеки у 4G мережах.

2. Дослідити вразливості, що становлять загрозу для передачі даних.
3. Оцінити існуючі методи захисту за критеріями ефективності та відповідності сучасним вимогам.
4. Запропонувати вдосконалений метод автентифікації користувачів із використанням біометричних даних.
5. Розробити алгоритм захисту даних для 4G мереж та оцінити його ефективність.

Наукова новизна дослідження полягає у розробці вдосконаленого методу автентифікації користувачів у 4G мережах із використанням біометричних даних, що забезпечує високий рівень захисту від несанкціонованого доступу та підвищує стійкість до сучасних кіберзагроз.

Методи дослідження включають:

- Теоретичний аналіз літературних джерел і стандартів.
- Математичне моделювання для оцінки ефективності запропонованих методів.
- Комп'ютерне моделювання для перевірки працездатності розроблених рішень.

Результати дослідження можуть бути використані операторами мобільного зв'язку для підвищення рівня безпеки мереж 4G, а також при розробці стандартів для мереж наступних поколінь.

РОЗЛІЛ 1

ОГЛЯД ТЕХНОЛОГІЙ ТА СТАНДАРТІВ БЕЗПЕКИ 4G МЕРЕЖ

1.1 Загальна характеристика 4G мереж

Мобільні мережі четвертого покоління (4G) - це найсучасніші технології стільникового зв'язку, які забезпечують високошвидкісну передачу даних та доступ до різноманітних мультимедійних сервісів. 4G мережі базуються на стандартах 3GPP LTE (Long Term Evolution) та LTE-Advanced. Основними характеристиками 4G мереж є висока швидкість передачі даних, а саме до 1 Гбіт/с в режимі низхідного каналу від базової станції до користувача та 500 Мбіт/с у режимі висхідного каналу за стандартом LTE-Advanced. Це забезпечує можливість передавати великі обсяги мультимедійної інформації в режимі реального часу. Низька затримка, а саме менше 5 мс, що є критично важливою для забезпечення високої якості голосового зв'язку та мультимедійних послуг. Ефективне використання частотного спектра та збільшення ємності мережі за рахунок використання нових технологій доступу, таких як OFDMA та SC-FDMA. Підтримка мобільності на високих швидкостях руху до 350 км/год. Покращена архітектура мережі - спрощена конвергентна архітектура з розподіленими функціями для забезпечення гнучкості та масштабованості. Широкий спектр послуг, голосовий зв'язок, високошвидкісний доступ в Інтернет, потокове мультимедіа, мобільне ТБ тощо. Сумісність з попередніми поколіннями мобільних мереж 2G та 3G для забезпечення плавного переходу. Широкий спектр послуг: високошвидкісний доступ в Інтернет, голосовий зв'язок VoLTE (Voice over Long Term Evolution), відеодзвінки, потокове мультимедіа, мобільне ТБ тощо. [10]

Невід'ємною частиною в роботі мереж є архітектура. У 4G мережі архітектура складається з декількох ключових елементів (Рис. 1.1).

1. EPC (Evolved Packet Core) - вузлове оболонкове ядро пакетної мережі, що забезпечує базові функції комутації та маршрутизації IP-трафіку, підтримку мобільності, сесій та облік.
2. eNodeB це базова станція, яка відповідає за радіодоступ,

кодування/декодування даних, модуляцію/демодуляцію сигналів.

3. UE (User Equipment) - кінцеве абонентське обладнання (смартфон, модем, роутер).

4. Шлюзи (S-GW, P-GW) - забезпечують інтерфейс до зовнішніх мереж передачі даних та Інтернету.

5. MME (Mobility Management Entity) - вузол, що здійснює процеси управління мобільністю, автентифікацію, встановлення захищених тунелів та розподіл ресурсів. [10]

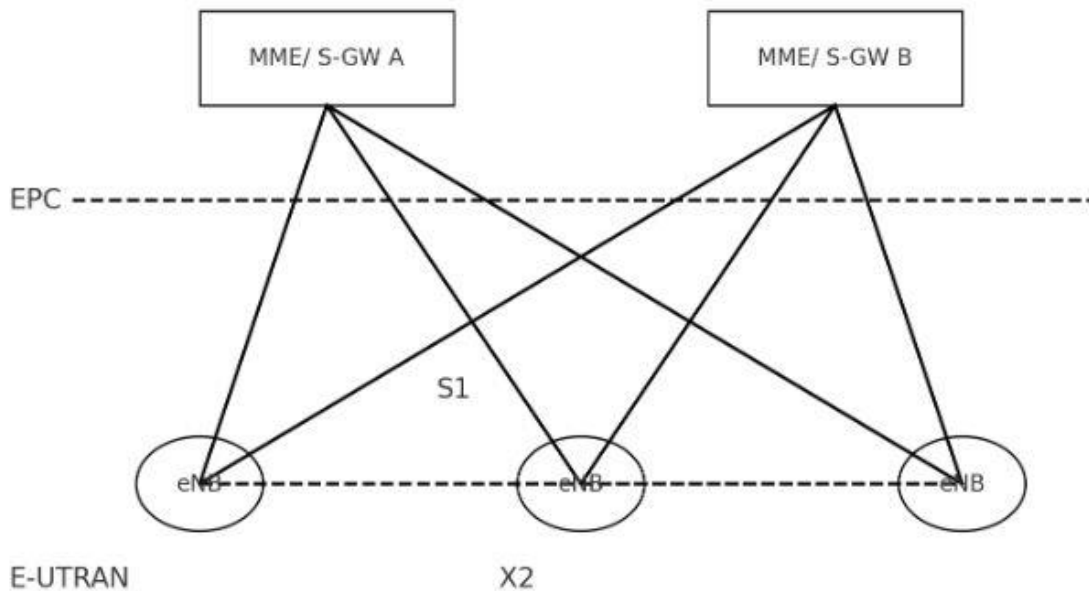


Рис 1.1 Спрощена архітектура мережі LTE

Джерело: розроблено автором

Проведений порівняльний аналіз технологій мобільного зв'язку демонструє суттєві переваги стандарту 4G над попереднім поколінням 3G. Практичні вимірювання засвідчують десятикратне збільшення швидкості передачі даних, що сягає показників 300 Мбіт/с при завантаженні та 75 Мбіт/с при висхідному з'єднанні. Такі параметри створюють належні умови для безперебійного функціонування ресурсоемних сервісів, зокрема потокової трансляції відеоконтенту високої чіткості та систем відео зв'язку.

Істотного покращення зазнав показник латентності мережі, який у технології 4G становить близько 20 мс, порівняно з діапазоном 50-150 мс у мережах третього покоління. Дане вдосконалення має принципове значення для функціонування систем доповненої реальності та забезпечення належної якості мережевих ігрових сервісів. [7]

У контексті подальшого технологічного розвитку слід відзначити, що архітектура мереж 4G послужила основою для розробки та впровадження технології п'ятого покоління. Незважаючи на появу 5G, мережі четвертого покоління зберігають домінуючі позиції у глобальному масштабі завдяки оптимальному співвідношенню надійності, пропускної здатності та універсальності застосування. Водночас актуальним завданням залишається адаптація інфраструктури 4G до зростаючих потреб Інтернету речей, що вимагає підвищення рівня масштабованості та кібербезпеки мережі. [7]

1.2 Аналіз стандартів безпеки в 4G мережах

Забезпечення безпеки в мережах 4G регламентується низкою стандартів, розроблених організацією 3GPP (3rd Generation Partnership Project). Центральним документом є специфікація 3GPP TS 33.401, яка визначає архітектуру безпеки для систем LTE (Long Term Evolution), а також детально описує механізми захисту, що застосовуються.[10]

Ключовими принципами безпеки в LTE є взаємна автентифікація користувача і мережі за допомогою протоколу Authentication and Key Agreement (АКА) та ключа KASME. У мобільних мережах стандарту LTE однією з найважливіших складових безпеки є автентифікація – це перевірка справжності користувача та самої мережі. Цей процес має на меті запобігти несанкціонованому доступу до мережі, а також захистити від атак типу «людина посередині» (Man-in-the-Middle). Процес автентифікації базується на протоколі АКА (Authentication and Key Agreement), який реалізовує взаємне підтвердження особи як з боку абонента, так і з боку мережі. У рамках цього процесу, після підключення до мережі, мобільний пристрій (UE) та мережевий елемент наприклад, елемент HSS — Home Subscriber Server обмінюються

серією перевірок і формують унікальний симетричний ключ, KASME, який використовується для подальшої криптографії. Завдяки KASME мережа і мобільний пристрій можуть генерувати додаткові ключі для шифрування трафіку, автентифікації повідомлень та перевірки цілісності даних. Такий підхід захищає від потенційних загроз, оскільки навіть якщо зловмисник спробує втрутитись у зв'язок, йому буде вкрай складно отримати доступ до справжніх ключів чи даних. [5]

Шифрування даних користувача за допомогою алгоритмів SNOW 3G, AES та ZUC. Шифрування є важливим інструментом для забезпечення конфіденційності в мобільних мережах LTE. Інакше кажучи, навіть якщо зловмисник перехопить дані, він не зможе їх прочитати без відповідного ключа. Для цього в LTE використовуються три основні криптографічні алгоритми:

1. SNOW 3G — це швидкий симетричний поточний шифр, який ефективно захищає дані в процесі передачі. Цей алгоритм вже активно використовувався в попередніх поколіннях мобільних мереж.
2. AES (Advanced Encryption Standard) — це стандарт шифрування, що застосовується для захисту найрізноманітніших даних. У LTE він застосовується для шифрування сигналів з високим рівнем безпеки.
3. ZUC — ще один поточний шифр, який використовується в LTE для захисту даних користувачів і забезпечення їх конфіденційності.

Всі ці алгоритми використовують 128-бітні ключі, що є достатньо надійним для забезпечення конфіденційності даних навіть в умовах швидкого розвитку обчислювальних технологій.

Забезпечення цілісності даних і повідомлень за допомогою MAC (Message Authentication Code). Для того щоб забезпечити цілісність даних, окрім того, що дані повинні бути зашифровані, важливо також, щоб вони залишались цілими — тобто, щоб їх ніхто не міг змінити в процесі передачі. Для цього в LTE використовуються механізми автентифікації повідомлень (MAC), які базуються на тій самій криптографії, що і для шифрування SNOW

3G або AES. Ці коди автентифікації додаються до кожного пакета даних, для того щоб при отриманні інформації обидві сторони могли перевірити, чи не було повідомлення змінено під час передачі. Це особливо важливо для мережевих операцій, де кожне повідомлення може мати критичне значення для стабільної роботи системи. [8]

Ідентифікація абонента в мережах стільникового зв'язку завжди має бути захищеною. Для цього в LTE застосовується технологія тимчасових ідентифікаторів. Кожен користувач має постійний номер, це унікальний номер IMSI (International Mobile Subscriber Identity), який ідентифікує його в мережі. Однак, щоб забезпечити цей ідентифікатор від потенційного викриття та зловживань, замість нього під час роботи в мережі використовуються тимчасові ідентифікатори GUTI (Globally Unique Temporary UE Identity). GUTI змінюється кожного разу, коли пристрій підключається до мережі, тому навіть якщо зломисник зможе перехопити його, він не отримає доступу до реальної інформації про користувача.

Захист сигналізації між мережевими вузлами за допомогою 3GPP TS 33.210. Безпека на рівні сигналізації є ще одним важливим аспектом в мережах LTE. Сигнальні повідомлення використовуються для керування з'єднаннями, налаштуванням зв'язку між пристроями та вузлами мережі. Ці повідомлення часто містять критичну інформацію, яка може бути використана зломисниками для атаки. Стандарт 3GPP TS 33.210 визначає вимоги до захисту сигналізації між мережевими елементами, використовуючи різноманітні методи криптографії для забезпечення конфіденційності та цілісності цієї інформації. [8]

Незважаючи на комплексний підхід до забезпечення безпеки, в стандартах LTE наявні певні недоліки та потенційні вразливості, а саме:

1. Довжина ключів 128 біт для алгоритмів шифрування на сьогоднішній день вважається достатньою для забезпечення захисту від більшості атак. Однак, із постійним зростанням обчислювальних потужностей та вдосконаленням методів криптоаналізу, таких як атаки квантових

комп'ютерів, ця довжина може стати вразливою. Тому майбутні системи повинні враховувати можливість переходу до довших ключів, наприклад 256 біт, щоб забезпечити надійний захист на тривалий термін.

2. Вразливість реалізацій шифрування до атак типу відновлення ключа може бути спричинена недостатньо надійною генерацією векторів ініціалізації (IV). У випадку використання скомпрометованих або передбачуваних IV, зловмисники можуть отримати доступ до ключів шифрування, використовуючи відкритий чи шифрований текст. Це підкреслює важливість удосконалення алгоритмів генерації випадкових чисел, щоб забезпечити безпеку навіть за умов інтенсивного навантаження на мережу.

3. Недоліки в реалізації механізмів захисту від повторного використання векторів ініціалізації (IV) можуть призвести до атак відтворення трафіку. Такі атаки дозволяють зловмисникам маніпулювати трафіком, відтворюючи або змінюючи передані дані. Для вирішення цієї проблеми необхідно забезпечити унікальність кожного IV у рамках сеансу зв'язку та використовувати методи, які виключають можливість повторного використання однакових значень.

4. Складність управління ключами шифрування є серйозним викликом для мереж 4G. Кожен користувачський пристрій (UE) потребує окремого ключа, а їх загальна кількість в масштабах мережі може сягати мільярдів. Це створює ризик компрометації через людські помилки, недостатньо захищені канали передачі ключів або збої в системах керування ключами. Необхідне впровадження автоматизованих систем керування ключами, які можуть зменшити ризики, забезпечуючи централізований контроль і постійний моніторинг.

5. Відсутність ефективних механізмів взаємної автентифікації особливо відчутна в системах Інтернету речей (IoT), де різні пристрої та мережі мають взаємодіяти між собою. Ця прогалина створює ризики, оскільки зловмисники можуть отримати доступ до мережі, видаючи себе за легітимні пристрої. Для усунення цієї проблеми необхідно впровадити універсальні стандарти автентифікації, які забезпечують високу швидкість і точність перевірки

пристроїв.

б. Потенційні недоліки в процедурах сигналізації становлять ще одну важливу загрозу. Зокрема, атаки на сигнальні канали, такі як атаки «відмова в обслуговуванні» (DoS), можуть паралізувати функціонування мережі, створюючи перевантаження. Для зниження цих ризиків рекомендується впровадження механізмів захисту, які зможуть виявляти та блокувати підозрілий трафік на ранніх етапах, а також збільшення стійкості процедур сигналізації до навмисних втручань. [9]

Саме через більшість з цих недоліків розробниками стандартів LTE постійно проводиться робота із забезпечення максимального рівня безпеки з урахуванням новітніх досліджень у сфері криптографії та захисту інформації, аналізу атак та виявлених інцидентів в існуючих мережах LTE. Це необхідно для підвищення стійкості 4G систем до найсучасніших кіберзагроз та забезпечення надійного захисту конфіденційності, цілісності та доступності передаваної інформації.

1.3 Огляд існуючих загроз та вразливостей

Незважаючи на рівень та технологічний розвиток 4G мереж, забезпечення безпеки передачі даних є критично важливим завданням, оскільки ці мережі використовуються для передачі конфіденційної інформації, такої як персональні дані користувачів, фінансові транзакції та корпоративні комунікації. Мережі 4G мають вбудовані механізми безпеки, проте все ж таки залишаються вразливими до різноманітних загроз та атак, які можуть поставити під загрозу конфіденційність, цілісність та доступність даних.

Сучасні телекомунікаційні мережі, зокрема мережі четвертого покоління (4G), забезпечують користувачам широкий спектр послуг, проте вони також є привабливою мішенню для кіберзлочинців. Однією з найбільш поширених загроз для безпеки таких мереж є атаки на аутентифікацію. Цей тип атак передбачає комплекс заходів, спрямованих на порушення процесу ідентифікації та перевірки прав доступу користувачів або пристроїв до мережевих ресурсів. [6]

Зловмисники можуть використовувати різноманітні методи для компрометації процесу аутентифікації, такі як підбір паролів (brute-force attacks), а саме системний перебір можливих комбінацій паролів для доступу до облікових записів. Словникові атаки (dictionary attacks), використання словників поширених паролів для підбору паролів.

Перехоплення трафіку є однією з найбільш поширених технік, що використовується кіберзлочинцями для отримання несанкціонованого доступу до конфіденційної інформації. Зловмисники можуть перехоплювати мережевий трафік за допомогою різноманітних методів, таких як прослуховування мережі (sniffing), атаки «людина посередині» (man-in-the-middle attacks та IP спוףінг, що характеризує собою підробку IP-адреси для обману мережевих пристроїв.

Конфіденційність даних є одним з основних принципів інформаційної безпеки. Атаки на конфіденційність спрямовані на несанкціонований доступ до конфіденційної інформації, такої як персональні дані, фінансові дані, комерційна таємниця тощо. Крім перехоплення трафіку, зловмисники можуть використовувати такі методи як соціальна інженерія. Цей метод являє собою маніпуляцію людьми для отримання конфіденційної інформації. Також зловмисники використовують вразливості програмного забезпечення, а саме експлуатацію відомих вразливостей для отримання доступу до систем і даних.

Забезпечення цілісності даних гарантує, що інформація не буде змінена або пошкоджена під час передачі або зберігання. Однак, атаки на цілісність даних можуть призвести до серйозних наслідків, основними та відомими з яких є фінансові втрати, репутаційні ризики та порушення нормативно-правових актів.[6]

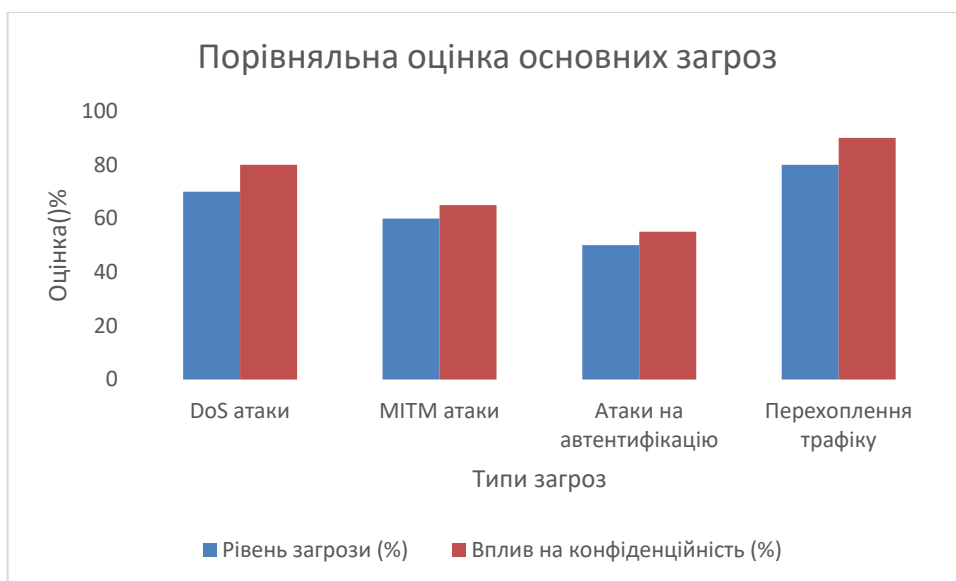
Атаки DoS (Denial of Service) та DDoS (Distributed Denial of Service) спрямовані на перевантаження мережевих ресурсів або окремих серверів, що призводить до відмови в обслуговуванні. Цей тип атак може бути використаний для дестабілізації роботи мережі, виведення з ладу веб-сайтів або інших критично важливих сервісів.

Мережі 4G, як і будь-які інші технології, мають свої вразливості. Зловмисники можуть використовувати ці вразливості для отримання несанкціонованого доступу до мережевого обладнання, а також для організації інших типів атак, таких як перехоплення трафіку, модифікація даних та відмова в обслуговуванні.

До небезпечних та рідких атак відноситься напад на ядерну частину мережі (Core Network). Необхідно підкреслити, що напад на ядерну частину мережі являє собою серйозну небезпеку для телекомунікаційної інфраструктури, яка може вивести з ладу безпеку та функціонування мережі. Оскільки ядро мережі займається обробкою та маршрутизацією основного потоку даних, а також відповідальне за підтвердження та надання доступу користувачам, напади на цю складову можуть викликати значні перебої в безпеці та втрату конфіденційних даних. Останні наукові дослідження в царині кібербезпеки виявили новий тип атак, націлених на ядрі мережі. Візьмемо до уваги приклад атаки на ядерну частину мережі. Вранці 12 грудня 2023 року зловмисники здійснили напад на «серце» найкрупнішого мобільного оператора в Україні – «Київстар», яке відповідає за обробку трафіку між абонентами та сервісами. З метою обмеження масштабів збитків, компанія була змушена тимчасово вимкнути зв'язок. Бази даних клієнтів не реагували на запити мережі щодо профілів користувачів і надання послуг. В результаті споживачі по всій країні залишилися без мобільного зв'язку та домашнього інтернету. Цей напад серйозно вплинув на взаємодію між людьми, на функціонування численних сервісів, а також на безпеку громадян, оскільки на деякий час прекратило надходження сповіщень про повітряні тривоги. Офіційний веб-сайт компанії та мобільний додаток також вийшли з ладу. Ця кібератака стала, безумовно, наймасштабнішою в Україні з моменту початку повномасштабних військових дій. [3]

Для візуального розуміння серйозності сучасних загроз була створена діаграма. На діаграмі проаналізовано та наведено порівняльну оцінку рівня серйозності основних загроз у 4G мережах та їх впливу на конфіденційність

даних.



Діаграма 1. Порівняльна оцінка рівня серйозності основних загроз

Джерело: розроблено автором

На представленій діаграмі (Діаграма 1.) можна спостерігати порівняльний аналіз рівня основних загроз, характерних для 4G мереж, а також їхній вплив на конфіденційність особистих даних. Найбільш руйнівний вплив мають перехоплення трафіку, що становлять 90% загального впливу, і DoS атаки, що оцінюються в 80%. Водночас, атаки типу MITM та загрози, пов'язані з автентифікацією, проявляють дещо менш значний вплив

Нормативні та юридичні ризики є ключовим чинником забезпечення безпеки 4G мереж. Ці ризики можуть виникати, коли оператори мереж порушують та не виконують вимоги та правила, закладені в законодавстві та нормативно-правових актах, які в свою чергу керують питанням захисту даних, конфіденційності та безпеки. Такі ризики можуть призвести не тільки до фінансових втрат компанії, а й до підриву репутації та довіри з боку користувачів.

Впровадження комплексу заходів безпеки, а саме вдосконалені методи автентифікації, шифрування, а також системи виявлення та реагування на

атаки в реальному часі є основним способом для протидії цим загрозам. Регулярне оновлення систем та навчання персоналу також є критично важливими для підтримання належного рівня безпеки в мережах 4G.

1.4 Висновок до розділу 1

Проведений аналіз технологій і стандартів безпеки 4G мереж дозволяє зробити важливі висновки щодо поточного стану безпеки в цих системах та їх потенційних вразливостей. Мобільні мережі четвертого покоління є одним із найбільш масштабних технологічних досягнень сучасності, що забезпечують високошвидкісну передачу даних, стабільність з'єднання та можливість інтеграції різноманітних цифрових сервісів. Однак, їх розширена функціональність створює нові виклики у сфері захисту даних.

Дослідження стандартів безпеки в 4G мережах показало, що базова архітектура включає такі важливі компоненти, як протокол аутентифікації EPS-AKA, шифрування трафіку та захист сигналізації. Ці заходи значно підвищують рівень безпеки користувачів, але мають свої обмеження в умовах сучасного кіберпростору. Зокрема, стандартні механізми не завжди здатні ефективно протидіяти складним атакам, які використовують новітні технології, такі як машинне навчання або автоматизований аналіз трафіку.

Крім того, огляд існуючих загроз і вразливостей підтвердив, що атаки на процеси аутентифікації, передачу даних та управління мережею залишаються основними проблемами безпеки 4G. Такі атаки, як перехоплення даних, атаки «людина посередині» або несанкціонований доступ, становлять значну загрозу як для конфіденційності, так і для стабільності роботи мережі. Особливу увагу слід приділити атакам, спрямованим на процес хендовера, оскільки вони можуть порушити мобільність користувачів під час переходу між базовими станціями.

Загалом, проведений аналіз підтвердив необхідність удосконалення існуючих стандартів та методів захисту, а також розробки нових підходів, спрямованих на забезпечення більш високого рівня безпеки в 4G мережах. Ці результати формують міцну основу для подальших досліджень та розробок,

що будуть розглянуті у наступних розділах роботи.

РОЗДІЛ 2

ОБҐРУНТУВАННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В 4G МЕРЕЖАХ

2.1 Аналіз існуючих методів захисту

У сучасних умовах функціонування 4G мереж безпека передачі даних є ключовим фактором, який забезпечує надійність і конфіденційність інформації, що циркулює у мобільних мережах. У цьому розділі буде проаналізовано існуючі методи захисту, зокрема ті, що використовуються для шифрування, аутентифікації, а також механізми виявлення та запобігання атакам.

Загальні підходи до захисту даних у 4G мережах базуються на стандартах, визначених організацією 3GPP (3rd Generation Partnership Project). Шифрування даних відіграє ключову роль у забезпеченні безпеки в мережах 4G мереж, де його основна мета полягає в збереженні та захисті інформації від несанкціонованого доступу. Використання криптографічних алгоритмів, таких як Advanced Encryption Standard (AES), відомого як Rijndael, гарантує безпеку комунікаційних каналів. AES, який знаходить своє застосування у різних сферах інформаційної безпеки, забезпечує конфіденційність інформації та ефективно захищає дані під час передачі по радіоканалу [2]

Додатковий рівень безпеки забезпечується за допомогою алгоритму шифрування .A5/3 (KASUMI), який застосовується у стандарті LTE. Цей алгоритм забезпечує захист даних, переданих між мобільними пристроями, і спільно з AES формує міцну систему захисту інформації у мережах 4G. Комбінація цих криптографічних алгоритмів у 4G мережах створює надійний бар'єр для захисту конфіденційності та цілісності даних, що передаються через мобільні мережі, і відіграє критичну роль у забезпеченні ефективної безпеки в мережах 4G.

Ще одним важливим аспектом безпеки є аутентифікація та авторизація користувачів у 4G мережах, що є головними процедурами у забезпеченні безпеки мереж. У системі 4G використовуються протоколи аутентифікації,

такі як EAP-SIM (Extensible Authentication Protocol – Subscriber Identity Module) та EPS-AKA (Evolved Packet System Authentication and Key Agreement). Ці протоколи забезпечують безпеку під час обміну інформацією між користувачем або пристроєм та мережею. (Рис 1.2)

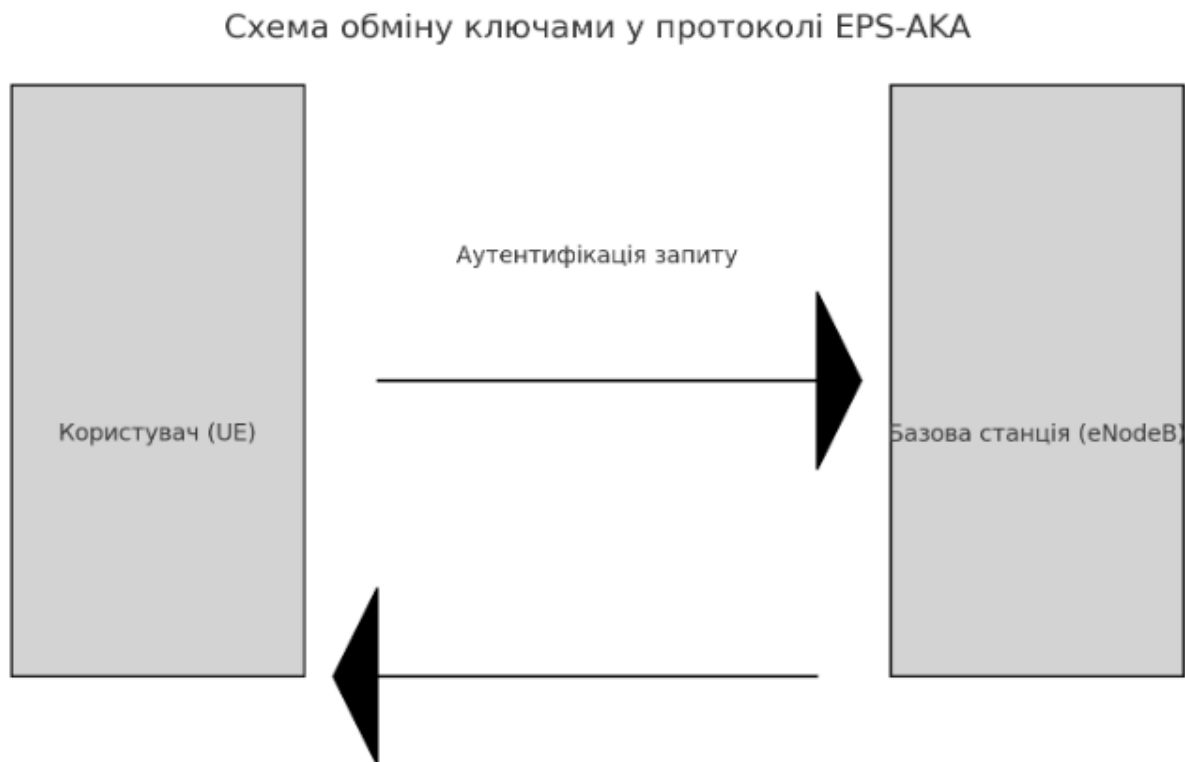


Рис.1.2 Схема обміну ключами у протоколі EPS-AKA

Джерело: розроблено автором

Процес аутентифікації включає в себе перевірку ідентифікаційних даних, таких як ім'я користувача та пароль, які в свою чергу надаються користувачем або пристроєм, а перевіряються мережею. При успішній перевірці даних, користувачу або пристрою надається доступ до мережі. Авторизація визначає рівень доступу який має користувач або пристрій після проходження аутентифікації. Цей процес базується на встановлених політиках безпеки мережі, які визначаються, які ресурси мають доступ до конкретних користувачів або пристроїв. До прикладу, різні користувачі можуть мати

різний рівень доступу до ресурсів мережі залежно від ролі або привілеїв.

Щоб ефективно ілюструвати процес вибору методів захисту у 4G мережах, необхідно не лише вказати основні ризики та загрози, але й забезпечити послідовне розуміння етапів ухвалення рішень у разі виявлення небезпеки. Одним із таких інструментів є схеми. Це допоможе відобразити логіку процесу у вигляді взаємопов'язаних елементів, що полегшує сприйняття матеріалу. У нашому випадку схема допоможе показати послідовність кроків, які оператор мережі або система повинні виконати для аналізу потенційної загрози, вибору відповідного методу захисту та його подальшої реалізації. Запропонована схема має структуру, що базується на аналізі типу загрози та ухваленні рішень на основі результатів цього аналізу. Основні кроки включають визначення типу атаки, вибір методу ідентифікації загрози наприклад, сигнатурний аналіз або аналіз поведінки, ухвалення рішення щодо необхідності блокування доступу або запуску додаткових заходів безпеки, а також впровадження гібридного підходу за потреби. Такий підхід дозволяє не лише оптимізувати процес реагування на загрози, але й підвищує загальну ефективність системи захисту (Рис.1.3).

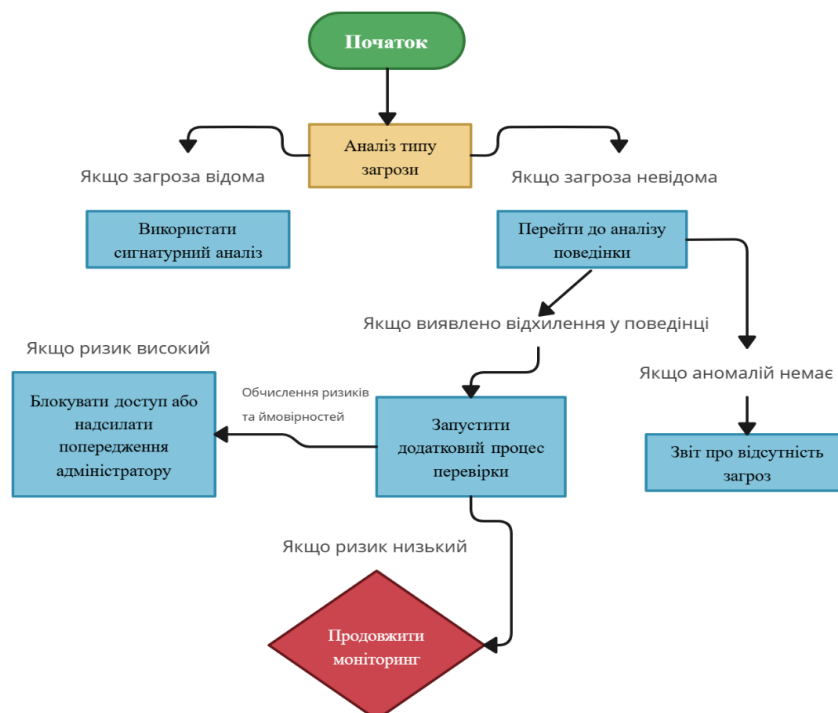


Рис. 1.3 Схеми процесу вибору методів захисту

Джерело: розроблено автором

Схеми також демонструє важливість використання сучасних технологій, таких як машинне навчання, яке дозволяє проводити глибокий аналіз поведінкових аномалій у трафіку. Це особливо актуально для сучасних мереж, де кількість невідомих загроз постійно зростає.

2.2. Порівняльна оцінка методів

У сучасному житті умови розвитку мобільних технологій та передачі даних у 4G мережах є одним з основних та важливих факторів, що визначає ефективність функціонування мережі. Оскільки 4G мережі забезпечують швидку передачу великої кількості даних, що включають конфіденційну інформацію, алгоритми шифрування, такі як AES Snow 3G, стали головними інструментами для захисту даних на різних етапах їх передачі.

У контексті забезпечення безпеки мереж, особливо важливим пунктом є вибір криптографічного алгоритму для шифрування даних, саме від ефективності його роботи залежить рівень захисту даних користувачів. При порівнянні цих двох алгоритмів, можна оцінити не лише їх криптографічну стійкість, а також їх відповідність вимогам сучасних технологій, зокрема енергоефективність, обчислювальна складність та вплив на швидкість передачі даних.

Рівень захищеності обох алгоритмів є високим, проте AES має низку переваг. Алгоритм AES широко використовується у глобальних стандартах шифрування, а саме в банківських системах, для захисту даних у системах електронних платежів та VPN, що забезпечує його надійність і підтверджену ефективність. AES пропонує варіанти довжини ключа в 128, 192 і 256 біт, що забезпечує високу стійкість до різноманітних атак, включаючи методи підбору ключа та атаки через зловмисне вторгнення. Завдяки своєму статусу глобального стандарту, AES постійно перевіряється та вдосконалюється, що робить його більш стійким до нових типів кіберзагроз.

На відміну від AES, Snow 3G був розроблений спеціально для мобільних мереж, з урахуванням обмежених ресурсів мобільних пристроїв. Саме це надає йому низку переваг у мобільних середовищах. Він використовує 128-бітні ключі і забезпечує достатній рівень безпеки для мобільних мереж, проте, через обмежену сферу застосування, його криптографічна стійкість була досліджена менше. Це створює певні обмеження для використання Snow 3G поза межами мобільних технологій, зокрема у таких сферах, як корпоративна безпека чи захист електронних платіжних систем.

Таким чином, з точки зору криптографічного аналізу, AES переважає Snow 3G, оскільки є більш вивченим і перевіреном, використовуваним у багатьох галузях і підтвердженим багаторічними дослідженнями. AES забезпечує високий рівень захисту, не тільки завдяки довжині ключів, але й завдяки його адаптивності до нових загроз у галузі кібербезпеки. [8]

З іншого боку, Snow 3G може бути доцільним вибором для специфічних випадків, таких як мобільні мережі, де вимоги до обчислювальних потужностей та енергоефективності вищі, ніж вимоги до глобальної криптографічної стійкості. Однак його використання поза цією сферою, через недостатню криптографічну перевірку, обмежує його застосування в інших індустріях.

Обчислювальна складність є важливим фактором при виборі методів безпеки, оскільки вона впливає на швидкість передачі даних та енергоспоживання пристроїв. Алгоритми шифрування, такі як AES та Snow 3G, вимагають значних обчислювальних ресурсів для виконання криптографічних операцій. Однак, сучасні апаратні реалізації цих алгоритмів дозволяють значно прискорити процес шифрування та зменшити енергоспоживання. [4]

Проаналізувавши ці два алгоритми можна дійти висновку, що AES має перевагу не лише через ширший спектр застосування, але й завдяки своєму статусу глобального стандарту, який постійно перевіряється та вдосконалюється. Саме цей алгоритм залишається найбільш оптимальним

вибором для забезпечення максимальної стійкості та захисту інформації.

Автентифікація користувачів за протоколом АКА також забезпечує високий рівень захищеності, використовуючи взаємну автентифікацію між мобільним пристроєм та мережею. Завдяки використанню симетричних алгоритмів (Milenage, TUAK) та секретних ключів, збережених на SIM-карті, протокол АКА ефективно запобігає несанкціонованому доступу до мережі та захищає від атак, таких як клонування SIM-карт або перехоплення ключів. [8]

VPN-технології (Virtual Private Network), зокрема протоколи IPsec (Internet Protocol Security) і SSL/TLS (Secure Sockets Layer / Transport Layer Security), забезпечують додатковий рівень захисту конфіденційності даних під час їх передачі через публічні мережі, такі як Інтернет. Ці технології використовують надійні криптографічні алгоритми, зокрема AES (Advanced Encryption Standard) і 3DES (Triple Data Encryption Standard), для шифрування даних, що дозволяє гарантувати високу стійкість до несанкціонованого доступу.

Протоколи автентифікації, такі як IKE (Internet Key Exchange) для IPsec і SSL/TLS для захисту веб-з'єднань, відповідають за перевірку особистості учасників з'єднання, що дозволяє забезпечити їхню достовірність. Вони гарантують, що дані надходять лише від авторизованих джерел і отримуються тільки призначеними отримувачами.

Проте важливо зазначити, що ефективність VPN-системи значною мірою залежить від правильності її налаштування. Окрім використання надійних алгоритмів, необхідне належне управління криптографічними ключами і сертифікатами, що забезпечує безперервність захисту навіть при зміні параметрів з'єднання або оновленні програмного забезпечення. Крім того, ефективність протоколів VPN безпосередньо залежить від стійкості самих криптографічних алгоритмів до сучасних методів зламу.

Автентифікація за допомогою протоколу АКА (Authentication and Key Agreement) та механізми контролю цілісності, зокрема UIA2 (User Identity Authentication 2), є важливими елементами захисту в мобільних мережах. Вони

забезпечують надійний контроль доступу та перевірку достовірності даних, що передаються, однак ці механізми додають певне обчислювальне навантаження на систему.

Важливо відзначити, що це навантаження є відносно невеликим, порівняно з навантаженням, яке створюється під час шифрування даних. Оскільки ці механізми зазвичай використовують симетричні алгоритми шифрування, такі як Milenage, TUAК (Telecommunications User Authentication Key) та СМАС (Cipher-based Message Authentication Code), вони здатні виконувати операції автентифікації та перевірки цілісності даних швидко та ефективно. [9]

Ці алгоритми дозволяють забезпечити високу продуктивність і швидкість передачі даних, що важливо для підтримки з'єднань в реальному часі, не впливаючи на їх ефективність. Завдяки застосуванню симетричних алгоритмів, які працюють з меншими обчислювальними ресурсами в порівнянні з асиметричними, досягається оптимальне співвідношення між безпекою і швидкістю передачі.

Енергоефективність є важливим фактором для мобільних пристроїв, які працюють від акумулятора. Методи безпеки, які вимагають значних обчислювальних ресурсів (наприклад, шифрування даних), можуть швидко виснажувати батарею пристрою. Тому важливо використовувати енергоефективні реалізації криптографічних алгоритмів та оптимізувати їх використання для збереження заряду акумулятора.

Проаналізувавши переваги та недоліки кожного методу за різними критеріями, можна зробити висновок, що найбільш ефективними та збалансованими є комбінації методів, які забезпечують високий рівень захищеності при прийнятній обчислювальній складності та енергоефективності. Наприклад, використання алгоритму АЕС для шифрування даних, протоколу АКА для автентифікації користувачів.

Однак, вибір конкретних методів та їх комбінацій залежить від специфічних вимог та умов конкретної мережі, а також від доступних ресурсів

та бюджету оператора зв'язку. Тому важливо ретельно проаналізувати всі фактори та адаптувати методи безпеки до потреб конкретної 4G мережі.

2.3 Вибір та обґрунтування методів для розробки системи безпеки

Розвиток та впровадження вдосконалених методів безпеки в 4G мережах є важливою складовою, оскільки для забезпечення надійного захисту даних під час їх передачі слід враховувати багато факторів. Застосування передових технологій та системних рішень у поєднанні з постійним моніторингом і аналізом можливих загроз дозволить забезпечити безпеку та надійність в 4G мережа у майбутньому. Оскільки аутентифікація та авторизація допомагає забезпечити ефективний контроль доступу та зменшити ризик несанкціонованого доступу до мережевих ресурсів, що є критичним для забезпечення безпеки в мережах. (Рис. 1.4)



Рис. 1.4 Принцип проведення аутентифікації та авторизації

Джерело: згенеровано на основі [2]

Фільтрація трафіку відіграє ключову роль у забезпеченні безпеки та ефективного управління мережевими ресурсами. Процес дозволяє виявляти та блокувати небажаний трафік, який в свою чергу може бути потенційно шкідливим та може становити загрозу для безпеки мережі та даних користувачів. Одним з методів фільтрації є фільтрація за IP-адресою, що

дозволяє блокувати трафік з певних IP-адрес. Цей метод дозволяє уникати трафіку, який може містити шкідливе програмне забезпечення або спам, зменшуючи загрози для мережі та її користувачів.

Ще одним методом є фільтрація за портом, яка спрямована на обмеження трафіку на певних мережевих портах. Кожен порт використовується для конкретного типу комунікацій або протоколу, і блокування трафіку на певних портах може запобігти надходженню спаму чи атак, які використовують певні протоколи. Deep Packet Inspection (DPI) – це високотехнологічний метод, що використовується для аналізу вмісту пакетів даних з метою виявлення шкідливого трафіку DPI дозволяє системі перевіряти кожен пакет даних, що проходить через мережу, на предмет наявності вірусів, загроз безпеки та інших аномалій. Цей метод надає великий рівень захисту та дозволяє операторам мережі вчасно виявляти та реагувати на потенційні загрози безпеки [2].

Виявлення та реагування на інциденти в мережах 4G вважається критичним аспектом забезпечення безпеки, оскільки дозволяє операторам мережі швидко реагувати на потенційні загрози та вчасно приймати заходи для їх запобігання. Для цього часто використовується система управління подіями та інцидентами безпеки, відома як Security Incident and Event Management (SIEM).

SIEM виконує важливі функції, такі як збір даних безпеки з різних джерел у мережі, мережеве обладнання, програмне забезпечення та інші системи. Ці дані аналізуються для виявлення ненормальної чи підозрілої активності, яка може вказувати на потенційні загрози безпеці. SIEM використовує різноманітні алгоритми для ідентифікації аномальних патернів та видачі сповіщень операторам про потенційні загрози. Після виявлення інциденту SIEM може автоматично або за допомогою інтервенції оператора запускати відповідні процедури реагування, включаючи блокування підозрілих джерел, відправку сповіщень про інциденти до відповідних осіб та реєстрацію подій для подальшого аналізу. Завдяки SIEM оператори мережі

можуть підтримувати високий рівень безпеки в 4G мережах, вчасно виявляти та реагувати на потенційні загрози, що допомагає запобігти можливим атакам та забезпечити надійну та безпечну роботу мережі для користувачів [2].

Регулярне оновлення програмного забезпечення мережевих елементів та мобільних пристроїв дозволяє усувати виявлені вразливості та підтримувати актуальний рівень безпеки. Для цього необхідно впровадити процеси управління оновленнями, тестування та розгортання нових версій програмного забезпечення.

Навчання персоналу з питань кібербезпеки є критично важливим для підтримки високого рівня захищеності мережі. Співробітники повинні бути обізнані про актуальні загрози, політики безпеки та кращі практики. Регулярні тренінги та навчальні програми допоможуть підвищити обізнаність персоналу та зменшити ризики, пов'язані з людським фактором.

Вибір та обґрунтування методів безпеки для розробки системи 4G мереж є важливим кроком у створенні надійного та ефективного захисту інформації. Запропонована комбінація методів, що включає шифрування даних за допомогою AES, автентифікацію користувачів за протоколом АКА. Ці методи були обрані на основі їх криптографічної стійкості, ефективності, сумісності зі стандартами та можливості практичної реалізації. Результати досліджень, тестувань та моделювання підтверджують їх ефективність у протидії різним типам загроз та забезпеченні конфіденційності, цілісності та доступності інформації в 4G мережах.

Крім того, врахування додаткових аспектів, таких як управління ключами, регулярне оновлення програмного забезпечення, моніторинг подій безпеки та навчання персоналу, дозволяє підтримувати високий рівень захищеності мережі в довгостроковій перспективі та адаптуватися до нових викликів та загроз.

Обґрунтований вибір методів безпеки закладає міцний фундамент для подальшої розробки та впровадження системи безпеки 4G мереж. Він враховує як технічні, так і організаційні аспекти забезпечення безпеки, що є запорукою

успішної реалізації та функціонування системи в реальних умовах.

2.4 Висновки до розділу 2

Досліджено та розглянуто методи забезпечення безпеки в 4G мережах з метою захисту від атак на передачу даних. Також проаналізовано актуальні проблеми та оцінено сучасні засоби захисту, такі як шифрування, аутентифікація, авторизація, фільтрація трафіку, а також виявлення та реагування на інциденти.

У цьому розділі було проведено аналіз існуючих методів забезпечення безпеки в 4G мережах, зокрема шифрування даних, автентифікації користувачів, контролю цілісності, захисту сигналізації та використання VPN-технологій. Було здійснено порівняльну оцінку цих методів за критеріями криптографічної стійкості, обчислювальної складності, впливу на швидкість передачі даних та сумісності зі стандартами.

На основі проведеного аналізу та порівняння було обґрунтовано вибір методів для розробки системи безпеки 4G мереж, а саме використання алгоритму AES для шифрування даних, протоколу АКА з SIM-картами для автентифікації користувачів.

Було визначено ключові вимоги до системи безпеки, які включають забезпечення конфіденційності та цілісності даних, надійну автентифікацію користувачів, захист сигналізації, ефективне управління ключами, масштабованість та продуктивність, сумісність зі стандартами, керованість та моніторинг, відмовостійкість та надійність, а також відповідність регуляторним вимогам.

Результати проведеного дослідження та сформульовані вимоги лягли в основу подальшої розробки системи безпеки 4G мереж. Запропоновані методи та підходи дозволять забезпечити високий рівень захисту даних та протидіяти різноманітним загрозам в умовах зростаючих обсягів інформації та кількості підключених пристроїв в мережах четвертого покоління. Розроблена система безпеки матиме практичну цінність для операторів мобільного зв'язку та користувачів, які прагнуть захистити свої дані та забезпечити

конфіденційність комунікацій в епоху повсюдного використання мобільних технологій.

РОЗДІЛ 3

РОЗРОБКА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В 4G МЕРЕЖАХ

3.1 Загальна архітектура системи забезпечення інформаційної безпеки в мережах четвертого покоління

Проаналізувавши існуючі методи безпеки в 4G мережах, виявлено потребу у вдосконаленні методу аутентифікації користувачів для забезпечення високого рівня захисту даних під час їх передачі. У сучасних мобільних мережах безпека передачі даних відіграє ключову роль, оскільки забезпечення конфіденційності та цілісності інформації користувачів є одним із головних завдань. Аутентифікація користувачів має вирішальне значення для контролю доступу до мережі. З цієї причини виникає необхідність у вдосконаленні методів аутентифікації, які б забезпечили надійний захист від несанкціонованого доступу та зберегли контроль над ресурсами мережі. [4]

Новий метод, запропонований на основі вже існуючих методів аутентифікації, має на меті підвищення рівня безпеки в 4G мережах шляхом вдосконалення процесу перевірки ідентичності користувачів та їх авторизації. Зокрема, новий метод може базуватися на використанні біометричних даних користувачів, таких як відбитки пальців або сканування обличчя, для аутентифікації. Це дозволить збільшити безпеку, оскільки біометричні дані є унікальними для кожного користувача та їх важко підробити [2] (Рис. 1.4)

Біометричні дані зберігаються у спеціалізованих зашифрованих базах даних. Сервер операторів 4G мереж використовується технологія токенізації, яка перетворює унікальні біометричні параметри на криптографічні токени. Ця технологія дозволяє мінімізувати ризик розкриття даних користувачів навіть у випадку компрометації бази. Попередньо дані проходять через кілька етапів обробки:

1. Попереднє шифрування, коли біометрична інформація передається на сервер у зашифрованому вигляді з використанням протоколів AES для забезпечення конфіденційності.

2. Перетворення в шаблони, замість збереження самих біометричних даних система генерує математичні шаблони, які неможливо відновити до первинної форми.
3. Серверна автентифікація, коли шаблон порівнюється з раніше збереженими даними, і виключно лише у разі повного збігу користувач отримає доступ до мережі [1]

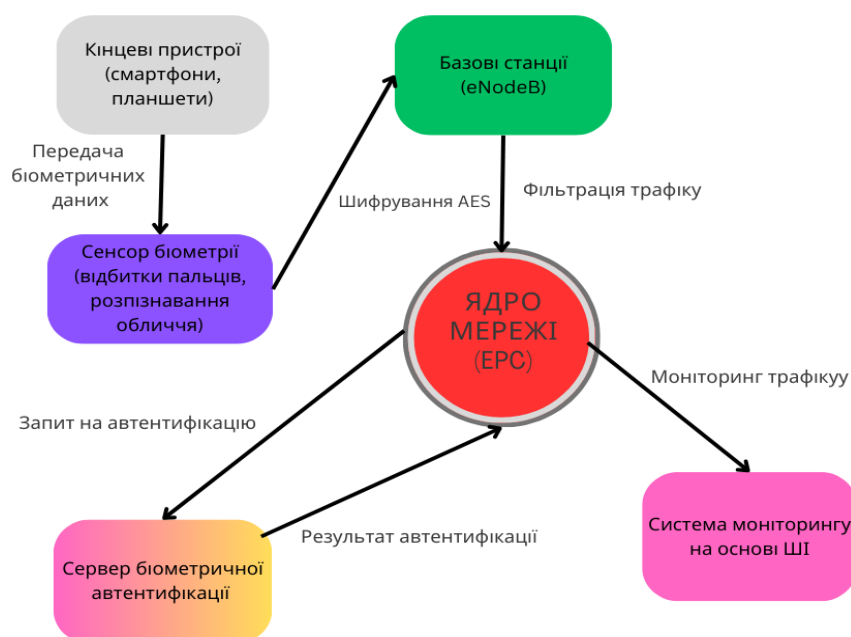


Рис. 1.5 Схема архітектури системи із використанням біометричної аутентифікації

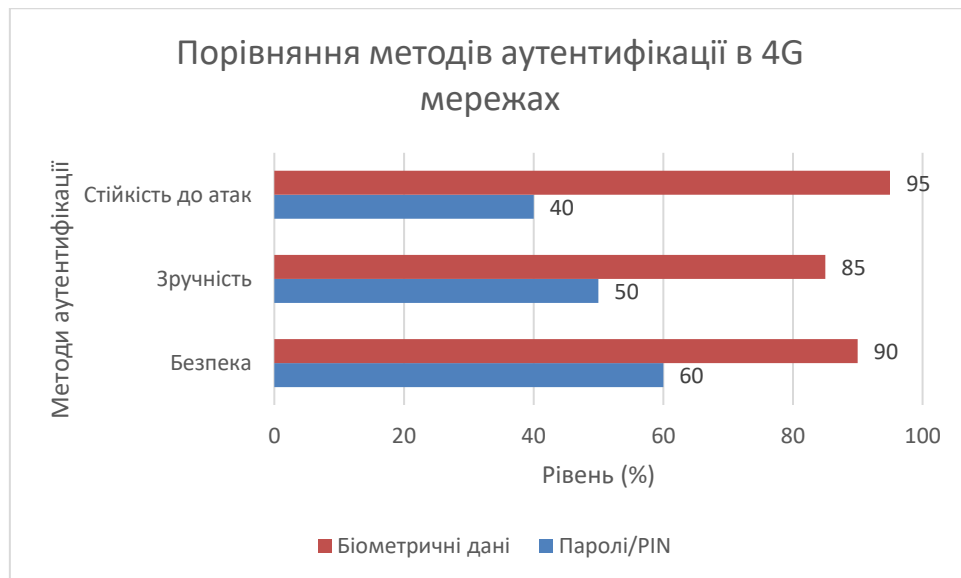
Джерело: розроблено автором

На рисунку 1.5 запропонована архітектура забезпечує багаторівневий захист даних. За рахунок того, що біометрична автентифікація інтегрується в процес перевірки ідентифікації на початковому етапі підключення, допомагає їй надійно ідентифікувати користувача ще до надання доступу до мережі. Головним елементом системи є сервер біометричних даних, який обробляє інформацію користувача в захищеному середовищі, що сприяє забезпеченню захисту, а також захищеному доступу до системи. [1]

Крім того, застосування нового методу може сприяти покращенню зручності користувачів, оскільки вони можуть бути аутентифіковані автоматично, без необхідності запам'ятовування складних паролів або ідентифікаторів. Таким чином, вдосконалення методів аутентифікації користувачів є важливим кроком у напрямку забезпечення ефективного захисту в 4G мережах. Новий метод, який базується на біометричних даних, може стати ефективним засобом захисту, забезпечуючи високий рівень безпеки та зручності для користувачів мобільних мереж [2].

Підвищення рівня безпеки методів аутентифікації в 4G мережах може бути досягнуто завдяки використанню біометричних даних. Зараз біометричні технології вже широко застосовуються для ідентифікації користувачів на смартфонах, планшетах та інших електронних пристроях. Наприклад, сканування відбитків пальців або розпізнавання обличчя вже давно є стандартними методами аутентифікації на багатьох сучасних пристроях. Крім того, біометричні дані застосовуються і для ідентифікації особи при вході в банківські додатки чи під час проведення електронних платежів. Використання біометричних даних в процесі аутентифікації не лише забезпечує високий рівень безпеки, але й робить процес більш зручним для користувачів. В порівнянні з традиційними методами, такими як введення паролів або PIN-кодів, використання біометричних даних є більш надійним і складнішим для підробки або вторгнення. Крім того, це дозволяє уникнути проблем, пов'язаних з забутими або втраченими паролями, що часто є джерелом потенційних загроз для безпеки.

Для порівняння ефективності традиційних і біометричних методів було проведено аналіз за трьома основними параметрами, а саме рівень безпеки, зручність використання та стійкість до атак. Результати аналізу представлені на діаграмі 2, яка демонструє переваги біометричних методів у контексті сучасних загроз.



Діаграма 2. Порівняння рівня безпеки, зручності та стійкості до атак методів аутентифікації

Джерело: розроблено автором

Як видно з діаграми 2, біометричні методи значно перевершують традиційні за всіма критеріями. Саме висока стійкість до атак та зручність використання роблять їх особливо ефективними для застосування в 4G мережах. Запровадження біометричної аутентифікації не лише підвищує рівень захисту, але й усуває проблеми, пов'язані із забутими або втраченими паролями користувачів.

Таким чином, використання біометричних даних у методах аутентифікації в 4G мережах дозволить підвищити безпеку передачі даних та зробить процес взаємодії користувача з мережею більш зручним і безпечним [2]. Це сприятиме створенню надійних механізмів захисту в умовах зростаючих загроз кібербезпеки.

Впровадження біометричної технології в 4G мережі є ключовим кроком у покращенні методів безпеки передачі даних. Оскільки біометричні дані, такі як відбитки пальців або розпізнавання обличчя, є унікальними та індивідуальними для кожної людини, вони стають важкими до підробки. Це робить біометричну аутентифікацію ефективним методом запобігання несанкціонованому доступу до мережі. Однією з основних переваг

використання біометричних даних у методах аутентифікації є їх висока надійність. Технологія відбитків пальців, наприклад, має високу точність та майже повністю виключає можливість підробки. Крім того, процес сканування обличчя може бути швидким та зручним для користувача, забезпечуючи високий рівень безпеки без необхідності запам'ятовування паролів чи інших ідентифікаторів. Алгоритм послідовних дій для використання покращеного методу аутентифікації в 4G мережі може включати кілька кроків [2]. Наприклад, користувач може використовувати свій смартфон або інший пристрій з біометричною аутентифікацією для входу в мережу. Після введення своїх біометричних даних система проводить автоматичну перевірку та порівняння збережених даних, після чого надає доступ до мережі у випадку підтвердження ідентифікації.

3.2 Алгоритм захисту

Алгоритм методу аутентифікації з використанням біометричних даних - це систематичний процес підтвердження ідентичності користувача на основі його унікальних біологічних параметрів. Спочатку користувач реєструється в системі, надаючи свої біометричні дані, такі як відбитки пальців або розпізнавання обличчя. Ці дані обробляються та зберігаються у безпечному місці. Під час спроби входу до системи, користувачу пропонується підтвердити свою ідентичність за допомогою біометричних даних. Система порівнює представлені дані зі збереженими у системі. Якщо біометричні дані співпадають зі збереженими, користувачу надається доступ до системи. Деякі системи можуть використовувати додаткові заходи безпеки, такі як двофакторна аутентифікація, де після успішної біометричної аутентифікації, користувачу може бути запропоновано ввести пароль або пін-код для підтвердження ідентичності. Такий підхід до аутентифікації забезпечує ефективний та надійний захист від несанкціонованого доступу до системи на основі унікальних біологічних параметрів користувача. Такий покращений метод аутентифікації не лише забезпечує високий рівень безпеки, але й робить процес входу в мережу більш зручним та ефективним для користувачів [2]. Це

відповідає сучасним вимогам до безпеки та дозволяє операторам мережі ефективно захищати дані користувачів від потенційних загроз (Рис.1.6)



Рис.1.6 Алгоритм методу аутентифікації з використанням біометричних даних

Джерело: розроблено автором

Процедура реєстрації у системі 4G мережі включає в себе надання біометричних даних, таких як відбитки пальців або розпізнавання обличчя. Ці дані зберігаються на серверах оператора мобільного зв'язку, що забезпечується відповідно до всіх вимог конфіденційності та захисту даних.

Під час спроби використання 4G мережі, користувач обирає опцію біометричної аутентифікації, після чого пристрій користувача звертається до серверів мобільного оператора для отримання доступу до біометричних даних.

Система здійснює порівняння представлених біометричних даних зі збереженими на сервері. Якщо біометричні дані співпадають, користувачу надається дозвіл на доступ до 4G мережі.

Для забезпечення додаткового рівня безпеки, користувачу надається можливість використання двофакторного захисту. Ця функція дозволяє активувати додатковий захист паролем або пін-кодом. Після успішної біометричної ідентифікації користувач повинен підтвердити себе за допомогою додаткового паролю або пін-коду, що додає додатковий рівень

безпеки до процесу аутентифікації.

3.3 Інтеграція штучного інтелекту з криптографічними протоколами

Запроновані вдосконалені методи безпеки в 4G мережах спрямовані на підвищення ефективності захисту даних шляхом використання передових технологій та алгоритмів. Вони охоплюють в собі використання штучного інтелекту (ШІ) для аналізу та виявлення аномального мережевого трафіку, що дозволяє оперативно виявляти потенційні загрози безпеці. ШІ здатний аналізувати великі обсяги даних і виявляти незвичайні, відхилені від звичайних патерни трафіку, що може свідчити про можливі атаки або вразливості мережі. Це дозволяє операторам мережі вчасно реагувати на потенційні загрози та вживати необхідні заходи для їх запобігання. Крім того, розробка нових підходів до криптографічного захисту даних і механізмів аутентифікації грає ключову роль у забезпеченні надійного рівня безпеки та конфіденційності в 4G мережах. Для більш чіткого розуміння технічного процесу представлено схему, яка демонструє ключові етапи обробки біометричних даних із використанням криптографічних протоколів та аналізу за допомогою ШІ (Рис. 1.7).

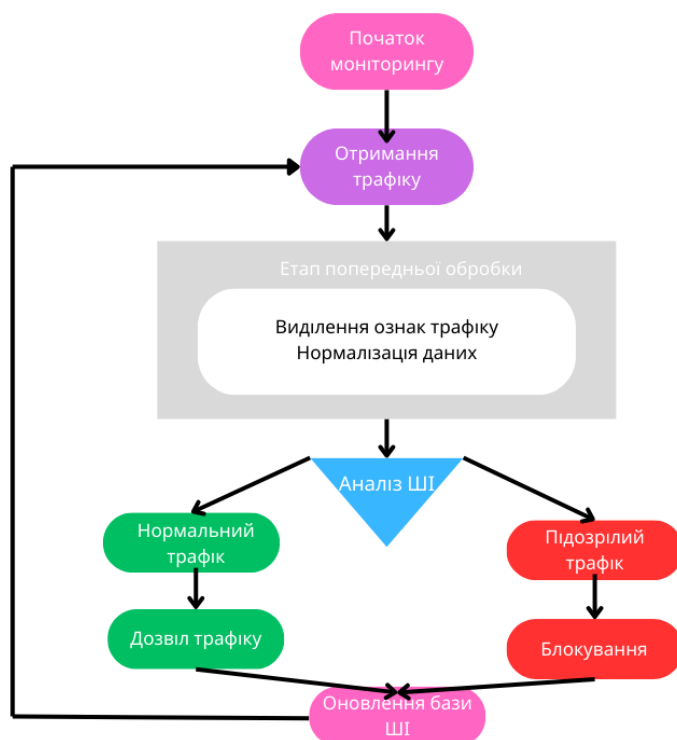


Рис. 1.7 Схеми технічного алгоритму обробки даних із залученням ШІ та криптографії

Джерело: розроблено автором

Схеми рисунку 1.5 демонструє комплексний процес моніторингу та аналізу мережевого трафіку з використанням технологій штучного інтелекту для забезпечення безпеки в 4G мережах. Процес складається з декількох основних етапів, кожен з яких виконує функцію, яка сприяє роботі загальній системі.

Процес починається з моніторингу, після чого система переходить до етапу отримання трафіку. На етапі попередньої обробки відбуваються два критичні процеси, а саме виділення характерних ознак трафіку та нормалізація даних, що забезпечує підготовку інформації для подальшого аналізу штучним інтелектом.

Наступним ключовим компонентом є аналіз ШІ, який представляє собою точку прийняття рішень, де система, базуючись на попередньо навчених моделях, класифікує трафік на два потоки: нормальний та підозрілий. Цей етап є важливим для забезпечення безпеки мережі, оскільки це вплине на подальший розвиток подій у системі.

У випадку визначення трафіку як нормального, система надає дозвіл на його проходження. Якщо трафік класифікується як підозрілий, система активує механізм блокування для запобігання потенційним загрозам у мережі.

Завершальним етапом є оновлення бази даних ШІ, який забезпечує постійне вдосконалення системи шляхом приєднання нових даних про характеристики трафіку. Цей процес реалізується через зворотній зв'язок, позначений на схемі стрілкою, що повертається до етапу отримання трафіку, забезпечуючи циклічність та безперервність процесу моніторингу.

Дана архітектура системи спроможна забезпечити комплексний підхід до безпеки мережі, поєднуючи переваги штучного інтелекту з традиційними методами захисту, що дозволить ефективно протидіяти сучасним

кіберзагрозам у телекомунікаційних мережах четвертого покоління.

Криптографічні протоколи використовуються для шифрування та захисту передачі даних між користувачами та мережею, забезпечуючи їх конфіденційність та цілісність. У контексті забезпечення безпеки в 4G мережах, розробка нових підходів до криптографічного захисту даних і механізмів аутентифікації відіграє критичну роль у забезпеченні надійного рівня безпеки та конфіденційності. Криптографічні протоколи використовуються для шифрування та захисту передачі даних між користувачами та мережею, забезпечуючи їх конфіденційність та цілісність і знаходячись в центрі системи безпеки мобільних комунікацій [2].

3.4 Висновок до розділу 4

В цьому розділі було розроблено та детально проаналізовано комплексну систему забезпечення безпеки для мереж четвертого покоління, яка поєднує в собі передові технології біометричної аутентифікації, криптографічного захисту та штучного інтелекту. Дослідження показало, що інтеграція біометричних методів ідентифікації з традиційними механізмами безпеки створює багаторівневу систему захисту, яка підвищує надійність та ефективність захисту даних користувачів.

Впровадження біометричної аутентифікації демонструє значні переваги порівняно з традиційними методами, що підтверджується проведенням порівняльним аналізом за критеріями безпеки, зручності використання та стійкості до атак. Важливо відзначити, що біометричні характеристики, будучи унікальними для кожного користувача, забезпечують вищий рівень захисту від несанкціонованого доступу порівняно з класичними методами захисту : паролі чи PIN-коди.

Розроблений алгоритм захисту, який базується на біометричній аутентифікації, передбачає багатоетапну верифікацію користувача з можливістю застосування додаткового рівня захисту у вигляді двофакторної аутентифікації. Така архітектура системи забезпечує надійний захист від потенційних загроз, зберігаючи зручність користування системою для

користувача.

Також було приділено увагу інтеграції технологій штучного інтелекту з криптографічними протоколами, що дозволило створити адаптивну систему моніторингу та аналізу мережевого трафіку. Запропонована система здатна ефективно виявляти та блокувати підозрілу активність, постійно вдосконалюючись завдяки механізму машинного навчання.

Використання сучасних криптографічних алгоритмів, таких як Advanced Encryption Standard (AES) та протоколів аутентифікації Extensible Authentication Protocol (EAP), у поєднанні з біометричними даними створює потужний захисний механізм. Цей підхід забезпечує не лише високий рівень безпеки, алей й відповідає сучасним вимогам щодо швидкодії та ефективності обробки даних у мережах четвертого покоління.

Запропонована система демонструє здатність до адаптації та масштабування, що є критично важливим для забезпечення довгострокової ефективності захисту в умовах динамічного розвитку технологій та появи нових викликів у безпеці. Таким чином, розроблена система забезпечення безпеки передачі даних у мережах четвертого покоління представляє собою комплексне рішення, що відповідає сучасним вимогам до захисту інформації та створює надійний фундамент для подальшого розвитку безпечних телекомунікаційних систем.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У ході виконання кваліфікаційної роботи було досліджено проблематику забезпечення безпеки передачі даних у мобільних мережах четвертого покоління (4G). На основі проведеного аналізу сучасних кіберзагроз, оцінки існуючих методів захисту та розробки нового підходу до автентифікації користувачів, вдалося досягти поставленої мети дослідження.

Проведений аналіз продемонстрував, що 4G мережі, попри високу функціональність та швидкість передачі даних, залишаються вразливими до атак, спрямованих на порушення конфіденційності, цілісності та доступності інформації. Серед найпоширеніших загроз виділяються атаки типу «людина посередині», перехоплення трафіку, маніпуляції з ідентифікаційними даними користувачів та атаки на сигналізацію.

Дослідження існуючих методів захисту показало, що базові механізми безпеки, такі як автентифікація за протоколом АКА, шифрування трафіку (AES, Snow 3G) та захист сигналізації, забезпечують лише мінімальний рівень безпеки в умовах сучасних загроз. Це обумовило необхідність удосконалення підходів до автентифікації та підвищення стійкості системи до атак.

У рамках роботи було запропоновано новий метод автентифікації користувачів із використанням біометричних даних, що інтегрує сучасні криптографічні алгоритми з унікальними параметрами кожного користувача. Такий підхід забезпечує високий рівень захисту, оскільки біометричні дані є складними для підробки та не потребують запам'ятовування паролів. Розроблений метод включає використання зашифрованих шаблонів біометричних даних, токенизації для мінімізації ризиків компрометації та багаторівневого захисту інформації.

Окрім цього, у роботі було створено алгоритм аналізу даних за допомогою штучного інтелекту (ШІ), який використовується для виявлення та реагування на потенційні загрози у 4G мережах. Алгоритм дозволяє проводити аналіз аномалій у трафіку, ідентифікувати підозрілі активності та автоматично ініціювати захисні заходи, що значно підвищує ефективність моніторингу та

знижує ризик впливу атак.

Розроблений метод автентифікації забезпечує надійну перевірку ідентифікації користувачів, захист даних під час передачі та зручність для кінцевих користувачів.

Пропозиції, які рекомендовано розглянути для того щоб у майбутньому забезпечити комфортну та безпечну систему для операторів мереж:

1. Інтегрувати розроблений метод біометричної автентифікації у системи операторів мобільного зв'язку з урахуванням потреб конкретних мереж.

2. Розширити використання алгоритмів ШІ для моніторингу безпеки мереж, адаптуючи їх до умов зростаючого трафіку та кількості пристроїв в Інтернеті речей (IoT).

3. Розробити рекомендації для регуляторів телекомунікацій щодо впровадження нових стандартів безпеки, які враховують використання біометричних даних та адаптивних систем аналізу загроз.

4. Проводити регулярне навчання персоналу операторів зв'язку з питань кібербезпеки та управління сучасними системами захисту.

5. Забезпечити подальше вдосконалення методів управління ключами шифрування для зменшення ризиків компрометації в умовах великих масштабів мереж.

Результати дослідження можуть бути використані для модернізації існуючих систем захисту 4G мереж, а також слугувати основою для розробки нових підходів до безпеки у мережах п'ятого покоління (5G).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біометричні системи: перспективи впровадження в інформаційну безпеку / Ред. Бабій О. І. – Київ: Техніка, 2021. – 255 с.
2. Вдосконалені методи безпеки в 4G мережах з метою забезпечення ефективного захисту від атак на передачу даних – [Електронний ресурс]. – Режим доступу: <http://perspectives.pp.ua/index.php/nts/issue/view/260>
3. Abomhara M., Kjøien G. M. Security and privacy in the Internet of Things: Current status and open issues / M. Abomhara, G. M. Kjøien. – *Computer Networks*. – 2020. – №57 (3). – С. 33–45.
4. AES Cryptographic Algorithms [Електронний ресурс]. – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>.
5. Cavoukian A. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy / Ann Cavoukian, Alex Stoianov. – [Електронний ресурс]. – Режим доступу: <https://www.ipc.on.ca/wp-content/uploads/Resources/biometrics.pdf>.
6. Cherdantseva Y., Hilton J. A Reference Model of Information Assurance & Security / Y. Cherdantseva, J. Hilton. – *International Journal of Computer Science & Information Security*. – 2019. – №9 (2). – С. 27–35.
7. ETSI TR 122 978. Universal Mobile Telecommunications System (UMTS); LTE; Feasibility study for Proximity Services (ProSe) (3GPP TR 22.803 version 12.2.0 Release 12). – [Електронний ресурс]. – Режим доступу: <https://www.etsi.org/>.
8. Singh S., Arora N. Biometric-based authentication systems in 4G networks: A systematic review / S. Singh, N. Arora. – *Journal of Information Security and Applications*. – 2022. – №65. – С. 103112.
9. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 7th Edition. – Pearson Education, 2017. – 848 с.
10. 3GPP TS 33.401. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; LTE; Security architecture. – [Електронний ресурс]. – Режим доступу: <https://www.3gpp.org/>.