**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
Кафедра інформаційної безпеки

«До захисту допущено»
Завідувач кафедри

_____Дмитро ЛАНДЕ
(підпис)

“___” _____2023 р.

# Дипломна робота

**на здобуття ступеня бакалавра**

**зі спеціальності 125 «Кібербезпека»**

**на тему:**

**Структура мобільних мереж, їх вразливості та методи протидії**

Виконав (-ла): студент (-ка) __4__ курсу, групи ___ФБ-з91_____
(шифр групи)

_____Торопчін Євгеній Олександрович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник __к.т.н, доцент Гальчинській Леонід Юрійович_ _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2023 року

**Національний технічний університет України**
**«Київський політехнічний інститут імені Ігоря Сікорського»**
**Навчально-науковий фізико-технічний інститут**
**Кафедра інформаційної безпеки**

Рівень вищої освіти – перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма Системи, технології та математичні методи кібербезпеки

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____202_ р.

**ЗАВДАННЯ**
**на дипломну роботу студенту**

Торопчіну Євгенію Олександровичу

1. Тема роботи

Структура мобільних мереж, їх вразливості та методи протидії
_____
_____
_____

керівник роботи
Доц., к.т.н., доцент Гальчинській Леонід Юрійович_____,
затверджені наказом по університету від «_31_»_____05_____2023 року № 2105-с

2. Термін подання студентом роботи
____13.06.2023____

3. Вихідні дані до роботи:
навчальний та робочий плани_____
_____
_____

4. Зміст роботи:

- Проведення аналізу структури мобільної мережі
- Стан захищеності та відомі атаки на мобільну мережу
- Розробка методів протидій одній із вразливостей

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

6. Консультанти розділів роботи*

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |

7. Дата видачі завдання
___10.05.2023___

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів виконання дипломної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| | Отримання завдання | 10.05.2023 | |
| | Вивчення літератури | 11.05.2023 – 20.05.2023 | |
| | Написання плану | 21.05.2023 – 22.05.2023 | |
| | Написання першого розділу | 23.05.2023 – 30.05.2023 | |
| | Написання другого розділу | 31.05.2023 – 05.06.2023 | |
| | Проходження практики та аналіз вразливостей | 06.06.2023 – 09.06.2023 | |
| | Написання третього розділу диплому | 10.06.2023 – 12.06.2023 | |
| | Оформлення дипломної роботи | 13.06.2023 | |
| | Предзахист дипломної роботи | 14.06.2023 | |
| | Захист дипломної роботи | 19.06.2023 | |

Студент _____ _____
(підпис) (ініціали, прізвище)

Керівник роботи _____ Леонід Гальчинський
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено керівника дипломної роботи

# РЕФЕРАТ

Обсяг роботи 44 сторінки, 7 ілюстрацій, 1 блок схема та 14 джерел літератури.

Метою роботи є створення методу протидій однієї з існуючих вразливостей в мобільній мережі.

Об’єкт дослідження - мобільні мережі.

Предмет дослідження – небезпечне з’єднання та процедура автентифікації між пристроєм та базовою станцією.

Під час розробки методу захисту були використані такі методи дослідження:

Аналіз – для виявлення вразливостей, їх структурування та поставлення конкретних цілей протидії.

Моделювання – для розробки моделі поведінки системі та зменшення вірогідності використання вразливостей в протоколі з’єднання.

Результатом роботи є модель алгоритму методу додаткової перевірки безпечності передачі сигналу в GSM та UMTS протоколах зв'язку.

# Abstract

The volume of work is 44 pages, 7 illustrations, 1 block diagram and 14 sources of literature.

The purpose of the work is to create a method of counteracting one of the existing vulnerabilities in the mobile network.The object of research is mobile networks.

The subject of research is a secure connection and authentication procedure between a device and a base station.

During the development of the protection method, the following research methods were used:

• Analysis – to identify vulnerabilities, structure them and set specific countermeasures.

• Modeling – to develop a model of system behavior and reduce the likelihood of exploiting vulnerabilities in the connection protocol.

The result of the work is a model of the algorithm of the method of additional verification of signal transmission safety in GSM and UMTS communication protocols.

# Зміст

**Вступ** ..... 7
**1 Структура архітектури технологій мобільних мереж** ..... 7
**1.1 Архітектура 2G** ..... 9
**1.2 Шифрування даних у 2G** ..... 11
**1.3 Архітектура 3G** ..... 12
**1.4 Шифрування даних у 3G** ..... 13
**1.5 Архітектура 4G(Long Term Evolution)** ..... 14
**1.6 Шифрування даних у 4G** ..... 15
**1.7 Автентифікація користувачів** ..... 17
**2 Загрози використання мобільних мереж** ..... 18
**2.1 IMSI-перехоплювач** ..... 18
**2.2 Перехоплення зв'язку** ..... 21
**2.3 Підробка автентифікації** ..... 21
**2.4 Робота з шифруванням** ..... 22
**2.5 Зниження рівня обслуговування** ..... 23
**2.6 Методи підключення LTE CSS** ..... 24
**2.8 Атаки на зниження версії протоколу за допомогою базових станцій** ..... 27
**2.9 Атака SS7** ..... 28
**3 Пропозиції по підсиленню протидії кіберзагрозам для мобільних мереж** ..... 30
**3.1 Перевірка затримки з'єднання** ..... 31
**3.2 Перевірка бачення мережі** ..... 34
**3.3 Перевірка наявності переадресації трафіку** ..... 35
**Висновки** ..... 37
**ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ** ..... 38
**Додатки:** ..... 39

# Вступ

На сьогоднішній день у нашій країні кожна людина користується послугами того чи іншого оператора мобільного зв’язку. Його використовуюсь як дорослі, так і діти та люди похилого віку, адже всі хочуть як бути на зв’язку із друзями і сім’єю так і мати з’єднання з інтернетом майже у любій точці України. Сьогодні в Україні існують 3 значимих операторів мобільного зв’язку, це Київстар, Vodafone Україна та Lifecell. Але мало хто з абонентів дійсно розбирався як саме працює мобільний зв’язок, як по ньому передається трафік та які можуть виникати загрози порушення конфіденційності під час користування мобільними мережами.

То ж перш за все слід розібратись в тому як саме працює мобільний зв’язок в Україні. На сьогоднішній день в Україні існують технології GSM(2G), UMTS(3G) та LTE(4G), котрі у кожного оператора поєднані у власну систему зв’язку, а з початком вторгнення у нашу країну оператори об’єднали зусилля і відкрили можливість підключення до мережі іншого мобільного оператора у випадку коли немає зв’язку із власним мобільним оператором.

# 1 Структура архітектури технологій мобільних мереж

Мережа мобільного оператора побудована з використанням комбінації інфраструктури та технологій для надання послуг бездротового зв’язку своїм абонентам. Зазвичай мережа складається з наступних компонентів:

- Базові станції: це бездротові пристрої, такі як вежі стільникового зв’язку або малі стільники, стратегічно розташовані для забезпечення

покриття в певних областях. Вони передають і приймають сигнали на та з мобільних пристроїв (телефонів, планшетів тощо) у межах їх дії.

- Мобільний комутаційний центр (MSC): центральний комутаційний вузол мережі, який виконує маршрутизацію викликів, комутацію та інші основні функції. Він з'єднує мобільну мережу з телефонною мережею загального користування (PSTN) або іншими мережами.
- Home Location Register (HLR) і Visitor Location Register (VLR): ці бази даних зберігають інформацію про абонента та дані про місцезнаходження. HLR містить дані про постійних абонентів, тоді як VLR містить тимчасові дані для відвідувачів, які перебувають у мережі.
- База даних ідентифікації мобільного обладнання (IMEI): Ця база даних зберігає унікальні ідентифікаційні номери мобільних пристроїв, зареєстрованих у мережі.
- Центр автентифікації (AuC): він виконує автентифікацію та шифрування даних абонента для безпечного зв'язку.
- Шлюзовий вузол підтримки GPRS (GGSN) і обслуговуючий вузол підтримки GPRS (SGSN): ці вузли є частиною мережевої інфраструктури для надання послуг з комутацією пакетів даних, таких як доступ до Інтернету та обмін мультимедійними повідомленнями.
- Система підтримки операцій (OSS): це система керування, яка надає інструменти для моніторингу мережі, конфігурації, керування продуктивністю та усунення аварій та помилок конфігурації.
- Платіжна система: ця система обробляє рахунки абонентів і керує фінансовими аспектами мережі.

Ці компоненти працюють разом, щоб встановити та підтримувати з'єднання голосу та даних для мобільних абонентів. Архітектура мережі та використовувані технології можуть відрізнятися залежно від покоління

мережі (2G, 3G, 4G) і конкретних стратегій розгортання мобільного оператора.

Для детальнішого аналізу будемо брати структуру побудови системи зв’язку оператора Lifecell.

## 1.1 Архітектура 2G

У технології 2G (другого покоління) телефонне з’єднання з базовою станцією оператора встановлюється за допомогою ряду кроків. Ось спрощений огляд процесу:

- Реєстрація: коли ви вмикаєте свій мобільний телефон 2G, він шукає доступні мережі та реєструється в мережі оператора. Телефон надсилає сигнал на найближчу базову станцію, вказуючи на свою присутність і готовність до підключення.
- Пейджинг: базова станція підтверджує реєстрацію телефону та призначає йому тимчасовий ідентифікатор. Цей ідентифікатор використовується для визначення місцезнаходження телефону під час отримання вхідного дзвінка чи повідомлення.
- Розподіл каналів: базова станція призначає виділений частотний канал телефону для зв’язку. Цей канал дозволяє телефону передавати та приймати голосові сигнали або сигнали даних.
- Автентифікація та шифрування: телефон і мережа виконують процес автентифікації, щоб перевірити особу один одного. Це гарантує, що лише авторизовані пристрої зможуть отримати доступ до мережі. Шифрування також застосовується для захисту зв’язку між телефоном і мережею.
- Передача голосу/даних: після завершення автентифікації та шифрування телефон може передавати голос або сигнали даних через

призначений канал. Ці сигнали кодуються та модулюються в радіохвилі та передаються між телефоном і базовою станцією.

- Передача обслуговування через базову станцію: коли телефон переміщується в зоні покриття мережі, мережа може ініціювати процес передачі обслуговування для передачі виклику або сеансу даних на сусідню базову станцію. Це забезпечує безперервне підключення під час переміщення між різними зонами покриття.

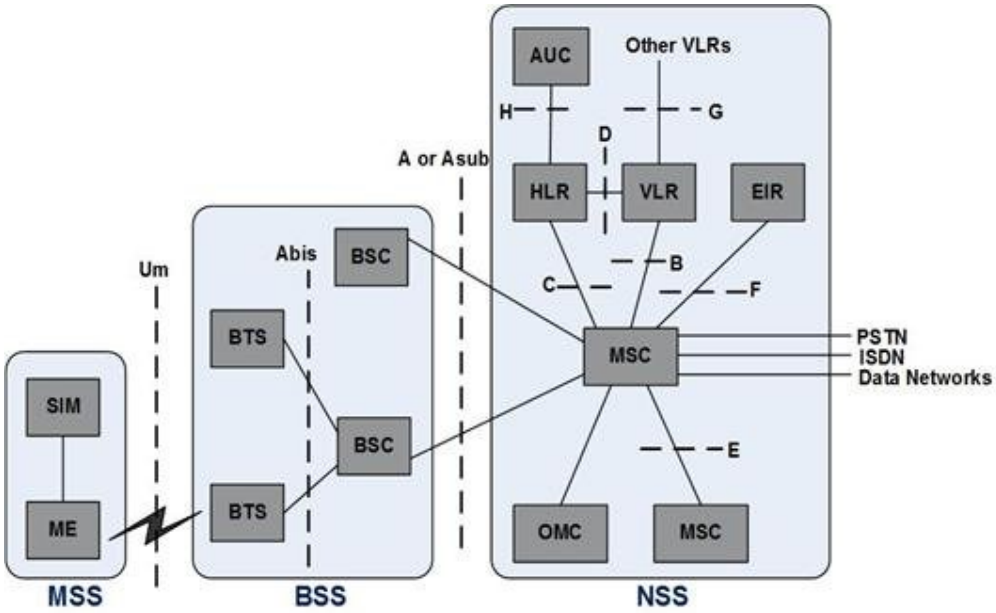



Рисунок 1.1 Архітектура 2G

Архітектуру 2G технології поділена на 3 сектори. Найменший сектор MSS – Mobile Stations System де:

- SIM – Subscriber Identification Module (сім карта)
- ME – Mobile Entity або по іншому Mobile Station – мобільний телефон, або банкомат, система оплати paypass та інше.

Визначимо інформацію що ідентифікую SIM карти та мобільні станції:

IMSI – International Mobile Subscriber Identifier

MSIN – Mobile Subscriber Identification Number

IMEI – International Mobile Equipment Identifier

Другий сектор BSS – Base Stations System, займається з’єднанням абонентів та передачею інформації, в ньому присутні:

- BTS – Base Transceiver Station
- BSC – Base Station Controller

Найбільший сектор NSS, також його називають Switching Sub System, що займається комутацією зв’язку, регістрацією та аутентифікацією абонента, хендовером, визначенням місця знаходження, з’єднанням з іншими мережами, та контролюванням роботи всіма вищезазначеними елементами. В системі SSS присутні такі елементи як:

- MSC – Mobile Switching Center
- HLR/VRL – Home/Visit Location Register
- AUC – Authentification Center
- EIR – Equipment Identity Register
- OMC – Operations and Maintenance Center
- NMC – Network Management Center

## 1.2 Шифрування даних у 2G

В технології 2G (другого покоління), дані передаються у вигляді цифрових сигналів, які кодуються і модулюються на радіохвилі для передачі між мобільним пристроєм і базовою станцією оператора.

Щодо шифрування, в 2G мережах використовується алгоритм шифрування з назвою A5. Цей алгоритм шифрує голосові та дані пакети, які передаються по мережі, для забезпечення конфіденційності. Проте варто відзначити, що шифрування в 2G є менш сильним порівняно з подальшими поколіннями мобільних технологій, і його безпеку можна компрометувати за

допомогою спеціального обладнання і атак з використанням розширених обчислювальних можливостей.

У зв'язку з цим, новіші покоління мобільних технологій, такі як 3G, 4G і 5G, використовують більш потужні алгоритми шифрування для забезпечення вищого рівня безпеки при передачі даних через мобільні мережі.

## 1.3 Архітектура 3G

Структура 3G виглядає простіше, оскільки велика кількість елементів із технології 2G була об’єднана у єдині елементи, Такі як RNC, MGW та MSC.

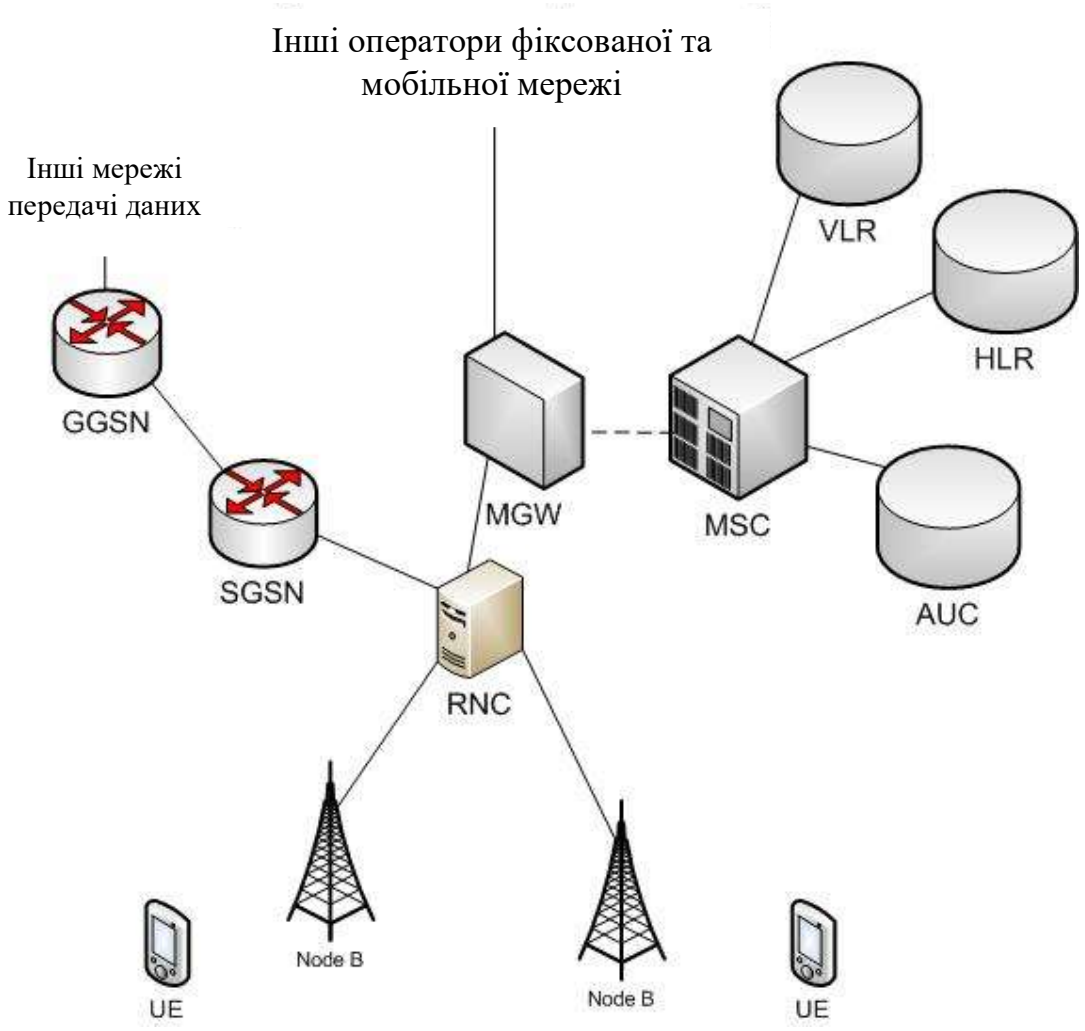


Рисунок 1.2 Архітектура 3G

Абревіатура мобільних телефонів та інших пристроїв була змінена на UE – User Equipment, а BTS змінилась на Node-B.

RNC – Radio Network Controller, окрім передачі інформації також він став займатись Хендовером, до того ж раніше взаємодія RNC була зав'язана тільки на MSC, тепер же RNC може напряму взаємодіє с іншими RNC для виконання хендоверу що значно зменшує навантаження на MSC.

MGW – Media Gateway це апаратура що взяла на себе комутацію та маршрутизацію голосових даних, що також раніше виконував MSC.

MSC-S – Mobile Switching Center – Server все ще керує всіма реєстрами та комутатором.

Група SGSN - GGSN займається комутацією пакетних даних до зовнішньої мережі

## 1.4 Шифрування даних у 3G

В технології 3G (третього покоління) передача даних відбувається за допомогою пакетної комутації (Packet Switching). Дані розбиваються на пакети і передаються по мережі окремо, а не у вигляді безперервного потоку, як у технології 2G. Це дозволяє оптимізувати використання ресурсів мережі та підвищити швидкість передачі даних.

Щодо шифрування, в 3G мережах також використовується алгоритм шифрування з назвою KASUMI. Цей алгоритм забезпечує шифрування голосових даних і пакетів даних, що передаються по мережі 3G, для забезпечення конфіденційності та безпеки передачі. Алгоритм KASUMI є більш потужним і безпечним порівняно з алгоритмом A5, який використовується в 2G мережах.

## 1.5 Архітектура 4G(Long Term Evolution)

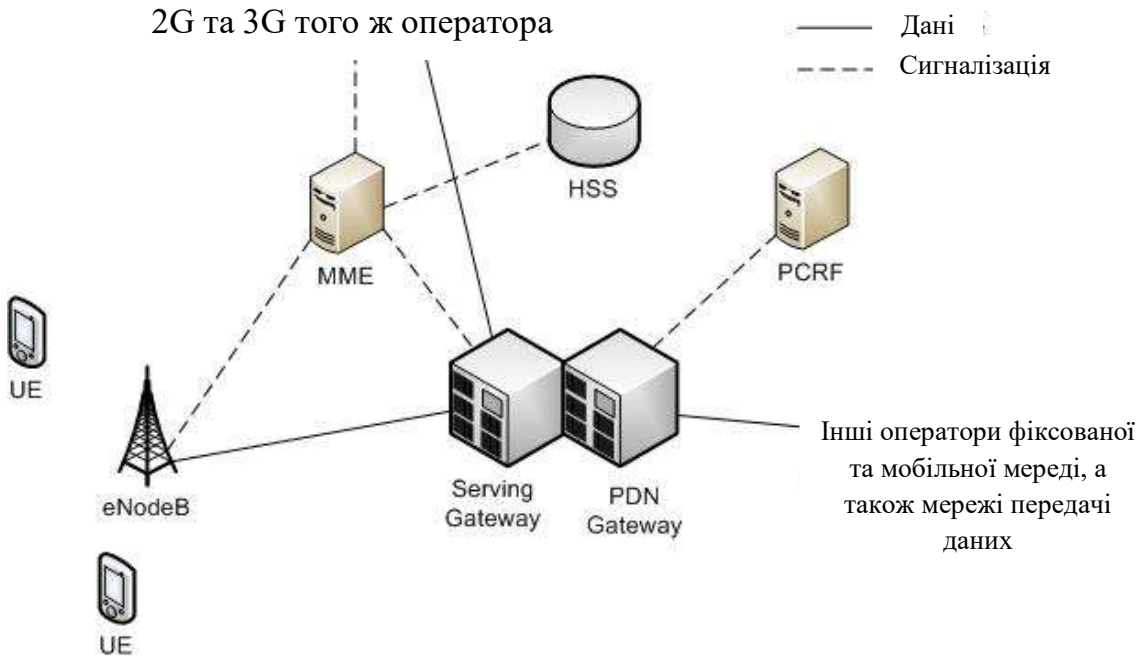



Рисунок 1.3 Архітектура 4G

Зі схеми мережі LTE, представленої вище, вже видно, що структура мережі сильно відрізняється від мереж стандартів 2G та 3G. Істотних змін зазнала і підсистема базових станцій, і підсистема комутації. Було змінено технологію передачі даних між обладнанням користувача та базовою станцією. Також зазнали зміни та протоколи передачі даних між мережевими елементами. Вся інформація (голос, дані) передається у вигляді пакетів. Таким чином, вже немає поділу на частини, що обробляють або тільки голосову інформацію, або тільки пакетні дані.

Можна виділити такі основні елементи мережі стандарту LTE:

- Serving SAE Gateway або Serving Gateway (SGW) – обслуговуючий шлюз мережі LTE. Призначений для обробки і маршрутизації пакетних даних базових станцій, що надходять з/в підсистему. По суті, замінює MSC, MGW та SGSN мережі UMTS. SGW має пряме з'єднання з мережами другого і

третього поколінь того ж оператора, що спрощує передачу з'єднання з них з причин погіршення зони покриття, перевантажень і тому подібне.

- Public Data Network (PDN) SAE Gateway або PDN Gateway (PGW) – шлюз до/від мереж інших операторів. Якщо інформація (голос, дані) передаються з/в мережі даного оператора, вони маршрутизуються саме через PGW.
- Mobility Management Entity (MME) – вузол керування мобільністю. Призначений для керування мобільністю абонентів мережі LTE.
- Home Subscriber Server (HSS) – сервер абонентських даних. HSS є об'єднання VLR, HLR, AUC виконаних в одному пристрої.
- Policy and Charging Rules Function (PCRF) – вузол виставлення рахунків абонентам за послуги зв'язку.

## 1.6 Шифрування даних у 4G

В технології 4G (четвертого покоління) передача даних відбувається за допомогою пакетної комутації (Packet Switching), так само як і в технології 3G. Проте, 4G забезпечує значно вищі швидкості передачі даних порівняно з 3G.

Щодо шифрування, в 4G мережах також використовується потужний алгоритм шифрування з назвою AES (Advanced Encryption Standard). AES є одним з найбільш безпечних алгоритмів шифрування, який використовується у світових стандартах безпеки і забезпечує конфіденційність передачі даних через мережу.

Шифрування в технології 4G використовується для захисту конфіденційності та цілісності переданих даних, що включають голосову інформацію, текстові повідомлення, веб-сторінки, файлові передачі та інші види даних. За допомогою шифрування AES, дані стають незрозумілими для

сторонніх осіб, що забезпечує їхню безпеку під час передачі через мережу 4G.

## Загальна архітектура мобільної мережі

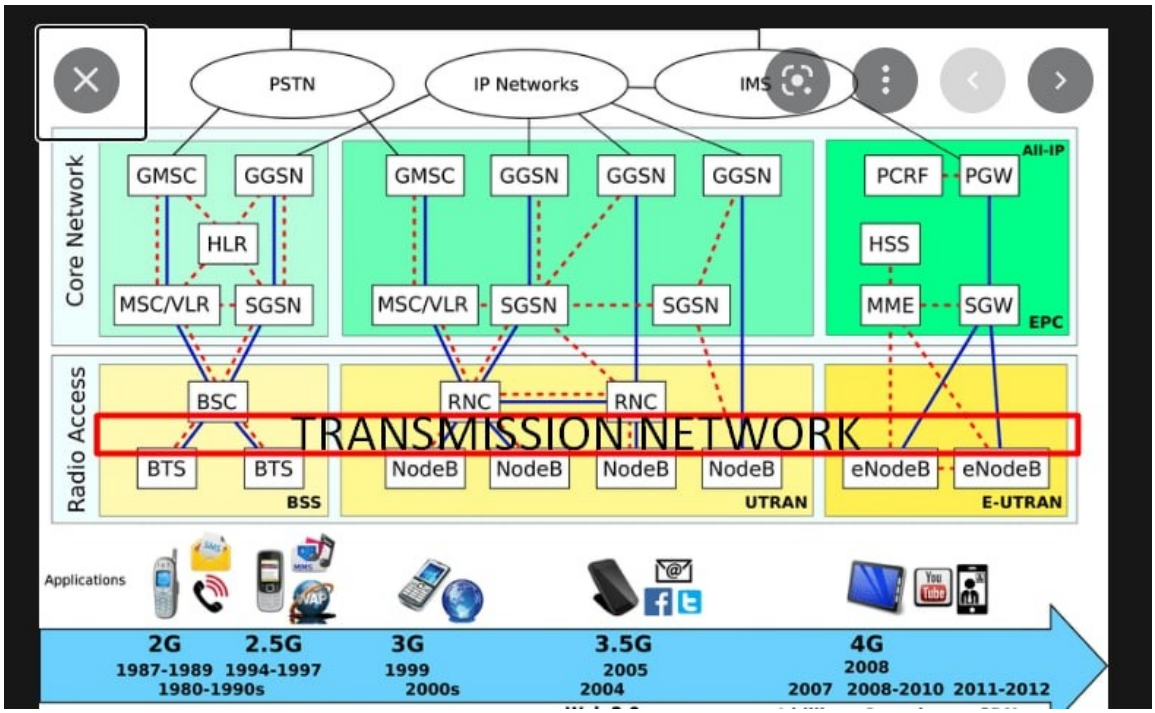



Рисунок 1.4 Загальна архітектура мобільної мережі

На сьогоднішній день архітектура об’єднаних технлогій зв’язку можна зобразити таким чином, оскільки кожна з технологій все ще використовується мобільними операторами.

## 1.7 Автентифікація користувачів

У процесі виробництва SIM-карт виробник заносить до ROM кожної карти випадкове число, зване “Ki” (Key for identification). Це число буде секретним ключем для цієї SIM-картки. Коли SIM-картки доставляються мобільному оператору, з ними передаються дані про Ki кожної нової SIM-картки. Ці дані (як пар (IMSI, Ki)) заносять у “центр аутентифікації” мобільної мережі (AuC) у 2G технології, в інших технологіях AuC об’єднується з деякими іншими елементами для створення більш комплексних структур.

Коли мобільний телефон намагається зареєструватися в мережі, його IMSI передається AuC, який передає назад випадкове число (RAND). Далі SIM-карта і AuC паралельно виконують те саме обчислення: (SRES, Kc) = A3/A8(RAND, Ki), де “A3/A8” - назва стандартних алгоритмів обчислення SRES (Signed RESponse) і Kc (Key for ciphering) відповідно.

Телефон передає обчислене SIM-карткою значення SRES назад до AuC, який порівнює його зі своїм SRES. Якщо результати збіглися, то SIM-картка – справжня.

Обчислене значення Kc зберігається в AuC/HLR/VLR та енергонезалежній пам'яті SIM-картки до наступної реєстрації картки в мережі та використовується для шифрування голосового трафіку, що йде радіоінтерфейсом.

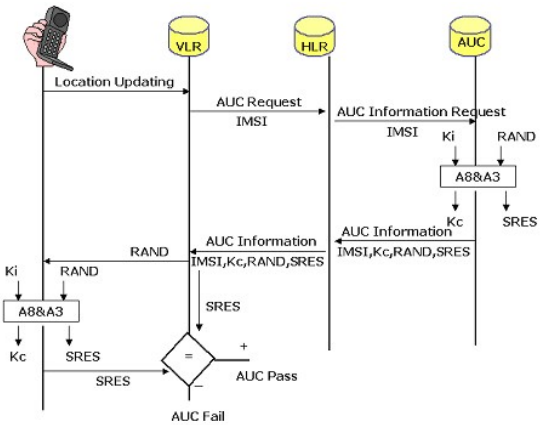



Рис 1.5 Модель автентифікації користувачів

# 2 Загрози використання мобільних мереж

## 2.1 IMSI-перехоплювач

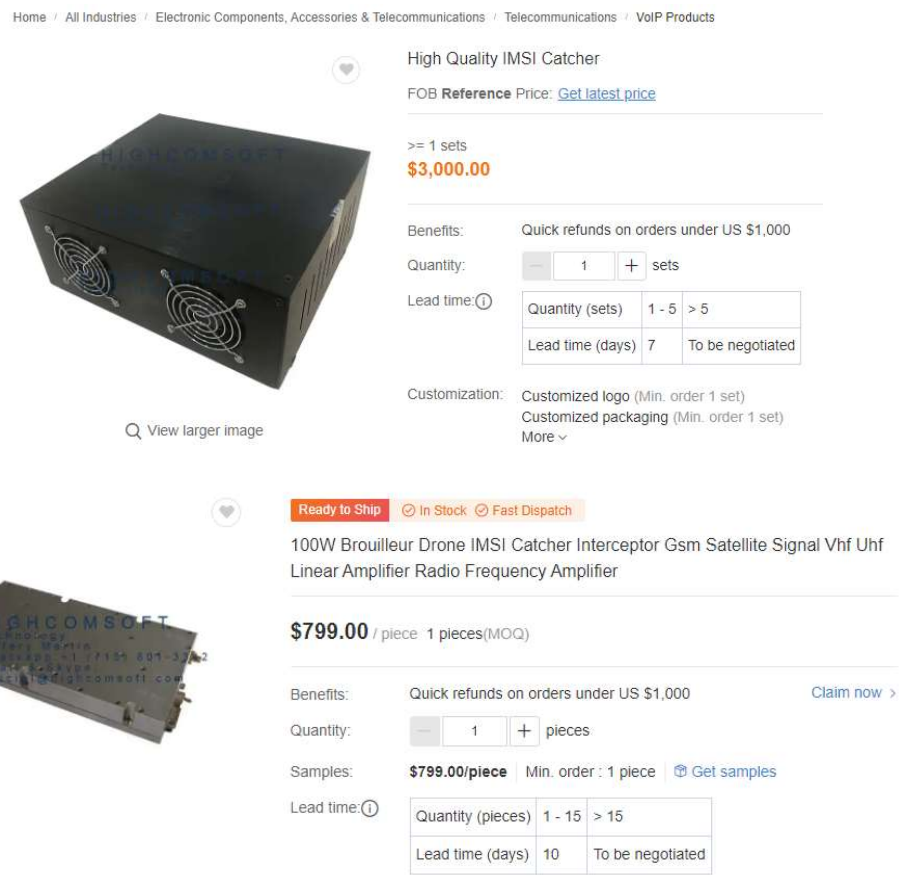



Рисунок 2.1, 2.2 Доступні IMSI перехоплювачі

Із аналізу архітектури різних технологій можна зробити висновок що, хоч і спрощується архітектура, але не робить зловмисне втручання простішим з кожною технологією через сильніший метод кодування даних. Але вразливості все одно залишаються через роботу старіших технологій. То ж пропоную розглянути деякі з вразливостей мобільних мереж.

Міжнародний перехоплювач ідентифікації абонента мобільного зв’язку, або IMSI-перехоплювач, — це пристрій для підслуховування телефонних розмов, який використовується для перехоплення мобільного трафіку та відстеження даних про місцезнаходження користувачів мобільних телефонів. По суті, «підроблена» мобільна вишка, яка діє між цільовим

мобільним телефоном і справжніми вежами постачальника послуг, вважається атакою «людина посередині» (MITM). Стандарт бездротового зв'язку 3G пропонує деяке зниження ризику завдяки взаємній автентифікації, яка вимагається як від телефону, так і від мережі. Однак складні атаки можуть знизити рівень 3G і LTE до мережевих служб, що не є LTE, для яких не потрібна взаємна автентифікація.

Перехоплювачі IMSI використовуються в ряді країн правоохоронними та розвідувальними органами, але їх використання викликає значні занепокоєння щодо громадянської свободи та конфіденційності та суворо регулюється в деяких країнах, наприклад, у німецькому Strafprozessordnung (StPO / Кримінально-процесуальний кодекс). Деякі країни навпаки не мають зашифрованого трафіку телефонних даних (або дуже слабке шифрування), тому IMSI-catcher стає непотрібним.

Класичні «ловці IMSI» просто записують найближчі IMSI, а потім не взаємодіють зі своїми цільовими телефонами значною мірою, крім цього. Вони буквально «ловлять» (тобто записують) IMSI, видаючи себе за справжні базові станції, а потім випускають цільові телефони (Педжет, 2010).

У мережах GSM телефони намагатимуться підключитися до будь-якої базової станції, яка транслює сигнал із найвищою потужністю.

Зображення телефону, який підключається до CSS замість вежі стільникового зв'язку, оскільки CSS має більший сигнал.

Коли телефон визначив базову станцію як таку, що має найсильніший сигнал, він може почати узгодження з'єднання з нею. Базова станція спочатку просить телефон надіслати їй свої можливості шифрування. Якщо базова станція є CSS, а не вежею стільникового зв'язку, вона може проігнорувати відповідь або налаштувати її без шифрування.

Після цього базова станція надсилає запит ідентифікації, на який телефон відповідає своїм IMSI. Телефон робить це тому, що IMSI зберігається на вашій SIM-картці, виданій вашим оператором мобільного

зв’язку, а телефонна мережа має ідентифікувати, що ви насправді є клієнтом-платником, пов’язаним із оператором мобільного зв’язку. Отримавши ваш IMSI, CSS повертає ваш телефон до реальної мережі та переходить до спроби захопити IMSI іншого телефону. Це все, що потрібно, щоб отримати IMSI з телефону поблизу!

CSS надсилає запит ідентифікації, щоб отримати IMSI цільового мобільного телефону. Після цього він продовжує повторювати ту саму дію з іншими телефонами.

Якщо правоохоронні органи використовують такий CSS у певній географічній зоні, після того, як вони отримають відповідні IMSI, вони зможуть використовувати юридичний процес, щоб отримати більше даних про всіх користувачів, які були присутні.

На карті показані вежі стільникового зв’язку з сірими колами, що розходяться від них. CSS (яка тут зображена як вантажівка з сигналом) випромінює червоне коло, яке перекриває інші кола веж стільникового зв’язку.

Звідси можна розпочати багато складніших атак, але так працює найпростіший вид ловців IMSI: вони просто збирають IMSI під час процедури підключення, потім переривають процедуру підключення та переходять до наступної цілі.

У пізніших протоколах (наприклад, 4G/LTE) телефони дещо розумніші, не підключаючись до будь-якої випадкової базової станції з високою потужністю сигналу, тому зловмиснику потрібні більш складні методи, щоб переконати телефон підключитися до їх CSS.

## 2.2 Перехоплення зв’язку

Наскільки нам відомо, перехоплення зв’язку між мобільним телефоном і законною вежею стільникового зв’язку можливе лише в GSM (на відміну від пізніших протоколів 3G або 4G). На це є дві причини:

Спілкування через GSM не завжди вимагає шифрування.

Навіть коли шифрування ввімкнено, кілька криптографічних алгоритмів, які використовуються в GSM, можуть бути зламані (і в режимі реального часу).

Уявіть, що CSS намагається розпочати активну атаку, де він перехоплює зв’язок телефону. Щоб це зробити, CSS має бути в змозі розташуватися між телефоном і вежею, що зазвичай називають атакою «машина посередині» (MitM).

Існує два основні кроки для заповнення MitM:

Підробка автентифікації: CSS має переконати мережу, що це дійсно цільовий мобільний телефон.

Дійте з будь-яким шифруванням, яке намагається встановити мережа (тобто вимкніть його або спробуйте зламати).

## 2.3 Підробка автентифікації

CSS уже отримав IMSI телефону за допомогою запиту ідентифікації:

CSS звертається до законної стільникової вежі із запитом на оновлення місцезнаходження. Цей тип запиту використовується для оновлення стільникової мережі про місцезнаходження телефону (зокрема, його LAC), що телефон має періодично робити, щоб мережа могла швидко направляти виклики та повідомлення до нього.

У відповідь на запит на оновлення розташування стільникова мережа просить CSS ідентифікувати себе за допомогою запиту ідентифікації. CSS відповідає, використовуючи вкрадений IMSI.

У цей момент вежа відповідає криптографічним викликом, для вирішення якого потрібен секретний ключ Ki (збережений на SIM-карті). Оскільки CSS не має доступу до Ki, він передає його на телефон для вирішення. Телефон вирішує виклик, передає його CSS, який потім передає його назад у мережу.

Після цього мережа приймає з'єднання між нею та CSS як автентифіковане.

Нагадую що це стосується лише 2G.

## 2.4 Робота з шифруванням

Існує кілька алгоритмів шифрування, які використовуються в GSM, і на високому рівні вони мають такі назви, як: A5/1, A5/2 тощо ... з A5/0, який використовується для вказівки, що шифрування не використовується.

Якщо мережа намагається вказати, що вона хоче спілкуватися за допомогою шифрування, CSS може просто відповісти, сказавши, що він не має можливостей шифрування та за замовчуванням A5/0. Зараз CSS завершив атаку MitM і може читати текстові повідомлення, що надсилаються між телефоном і реальною мережею.

Крім того, якщо мережа вирішить використовувати для зв'язку алгоритм A5/1, цей тип шифрування може бути зламано в реальному часі. Крім того, алгоритм A5/2 настільки слабкий, що його використання було заборонено з 2006 року. Хоча відомі атаки на A5/3, немає відомих атак у реальному часі.

Чому користувачі не сповіщені про те, що шифрування вимкнено? Згідно зі специфікаціями GSM, користувачі стільникових телефонів повинні

отримувати сповіщення, коли шифрування вимкнено, і на деяких ринках це було раніше. Однак це викликало багато плутанини, оскільки:

Люди подорожували б зі своїми телефонами в місця, де вежі стільникового зв’язку налаштовані дуже по-іншому (наприклад, у деяких країнах шифрування стільникових мереж заборонено), і це призводило до того, що спливаючі вікна «Попередження: шифрування вимкнено» часто з’являлися.

Вишки стільникового зв’язку всюди були неправильно налаштовані, через що це спливаюче вікно також часто з’являлося.

Ці проблеми призвели до того, що багато споживачів і дзвінків у службу підтримки операторів мобільного зв’язку збентежені, що призвело до того, що попередження зрештою було вимкнено.

## 2.5 Зниження рівня обслуговування

Незважаючи на те, що, наскільки нам відомо, перехоплення зв’язку можливе лише в GSM, можна знизити рівень з’єднання цільового стільникового телефону з 3G або 4G на GSM. Це пов’язано з тим, що загалом базова станція може вибирати будь-які параметри конфігурації, які вона хоче, включаючи можливість запитувати перехід до версії протоколу. Крім того, хтось може заглушити діапазони 3G або 4G, закачуючи в них велику кількість білого шуму, що робить надто шумним для встановлення з’єднання, і телефони знижуватимуться в пошуках придатного сигналу.

## 2.6 Методи підключення LTE CSS

Також важливо розуміти, як CSS може обійти захисні заходи в LTE та інших сучасних протоколах, які покликані запобігти підключенню телефонів до будь-якої базової станції з достатньо високою потужністю.

У GSM телефони завжди шукають вежу з вищою потужністю сигналу для підключення. Однак у LTE, якщо потужність сигналу перевищує певний достатній поріг, телефон не шукатиме інші вежі для підключення, щоб заощадити енергію.

Крім того, телефони LTE відстежують список «найближчих сусідів», який передається з вежі, до якої вони підключені. Якщо з будь-якої причини вони втратять з'єднання з вежею, до якої вони під'єднані (або можливість під'єднатись до неї), вони спробують під'єднатись до тих, які були оголошені у списку найближчих сусідів, перш ніж виконувати повне сканування доступні діапазони LTE для інших відповідних веж стільникового зв'язку.

Отже, як зловмисник може змусити телефон, що використовує LTE, підключитися до їх CSS? Одним з методів може бути маскування під вежу в списку найближчого сусіда (наприклад, та сама частота, той самий ідентифікатор стільника тощо) і передача на вищій потужності, щоб телефон з часом перемкнувся.

Але є більш швидка техніка! Він ґрунтується на тому факті, що частотам LTE призначаються різні пріоритети (це називається «повторним вибором сектора на основі абсолютного пріоритету»), і якщо телефон бачить, що базова станція працює на частоті з вищим пріоритетом, ніж та, на якій він працює, він повинен переключитися на нього незалежно від потужності сигналу. Щоб виявити частоти з вищим пріоритетом, які використовуються в даній області, все, що потрібно, це витягти їх із незашифрованих конфігураційних повідомлень від базових станцій, які будь-хто може відстежувати (Shaik et al, 2017).

Основним аспектом бездротової технології є модель пейджингового зв'язку. Коли мережа має повідомлення, яке вона хоче спрямувати на телефон, вона надсилає «повідомлення пейджингового виклику RRC», яке отримує кожен телефон, який прослуховує частоту пейджингового зв’язку свого оператора в цій зоні (а це фактично кожен телефон), із запитом на цей конкретний телефон. щоб зв’язатися з базовою станцією для узгодження завершення з’єднання для отримання дзвінка або повідомлення. Таким чином, телефони постійно прослуховують повідомлення пейджингового виклику RRC, а також приймають і відкидають ті, що не адресовані їм.

RRC є скороченням від Radio Resource Control, який є протоколом, який використовується для зв’язку між мобільним телефоном і базовою станцією. Серед іншого, RRC піклується про встановлення з’єднання та сповіщення на пейджинг про те, що ви отримуєте повідомлення чи телефонний дзвінок.

Точний спосіб роботи пейджінгу залежить від кількох факторів, включаючи тип повідомлення, яке мережа намагається скерувати до вас. Наприклад, скажімо, мережа намагається скерувати телефонний дзвінок до вас. Телефонні дзвінки вважаються високопріоритетними (оскільки хтось з іншого боку чекає, поки ви підключитесь), тому мережа сповіщає кожну вежу стільникового зв’язку в останній зоні розташування вашого телефону, щоб надіслати повідомлення пейджингового виклику RRC, адресоване вашому телефону (як на відміну від лише останньої стільникової вежі, яку використовував телефон).

Пейджингові повідомлення RRC зазвичай адресуються до TMSI, але іноді також використовуються IMSI та IMEI. Відстежуючи ці незашифровані пейджингові канали, будь-хто може записати IMSI та TMSI, які, на думку мережі, знаходяться в певній зоні. Зловмисник може співвіднести TMSI або IMSI з конкретним цільовим телефоном, оскільки зараз збір TMSI, IMSI означає просто запис псевдонімів.

Крім того, телефони періодично передають незашифровані повідомлення про своє місцезнаходження та вимірювання якості стільникового зв’язку, які будь-хто з відповідним обладнанням може легко перехопити. Іноді ці повідомлення містять точне GPS-місцезнаходження телефону, але зазвичай інформації про силу сигналу сусідніх стільників достатньо, щоб обчислити місцезнаходження телефону.

Першим кроком базового тесту зони розташування є ініціювання приблизно 10-20 сповіщень на телефон цілі за допомогою телефонних дзвінків, а також моніторинг повідомлень пейджингового виклику RRC, які надсилаються. Щоб не попереджати користувача, зловмисник може майже відразу покласти трубку після початку дзвінка, щоб повідомлення пейджингового виклику потрапило на телефон, але користувач насправді не отримує сповіщення про вхідний дзвінок.

Оскільки на іншій лінії хтось очікує, щоб з’єднатися з вами, телефонні дзвінки вважаються більш пріоритетними, тому мережа сповіщає кожну вежу стільникового зв’язку в останній зоні розташування, у якій знаходився телефон, щоб надіслати повідомлення пейджингового виклику RRC (на відміну від лише останньої вежа стільникового зв’язку, яку використовував телефон). Тоді зловмисник може використати аналіз перехресть набору зі своїми своєчасними викликами, щоб визначити TMSI цілі з повідомлень RRC. Але слід зазначити що для використання цього методу у зловмисника має бути доступ до інформації базових станцій що є куди більш витратним методом.

Використовуючи ці методи, зловмисники можуть змусити навіть LTE-телефон підключитися до свого CSS, що розкриває IMSI телефону та дозволяє наступні атаки.

## 2.7 Відстеження місцезнаходження

Часто, коли обговорюється небезпека CSS, увага приділяється їхній здатності перехоплювати комунікацію. Однак на практиці наслідки відстеження місцезнаходження в реальному часі часто набагато серйозніші. Потенціал відстеження місцезнаходження вашим постачальником мобільного зв'язку неминучий, тому конкретна модель загрози, яка тут використовується, — це третя сторона (наприклад, правоохоронний орган), яка намагається отримати ваше місцезнаходження без співпраці з вашим постачальником мобільного зв'язку.

Загалом існує два типи відстеження місцезнаходження, на які здатні CSS:

- Перевірка присутності: перевірка, чи присутній телефон у географічній зоні чи її немає (де географічна зона зазвичай означає «зону розташування» раніше, тобто групу клітинок)
- Точне місцезнаходження: визначення точних або приблизних GPS-координат телефону за допомогою трилатерації або змусивши телефон повідомити зловмиснику свої точні GPS-координати

## 2.8 Атаки на зниження версії протоколу за допомогою базових станцій

Припустімо, що зловмисник налаштував свій CSS і обманом змусив ціль підключитися. Після початкової процедури підключення телефон надішле «Запит на оновлення зони відстеження» (скорочено «TAU»). Цей тип повідомлення використовується телефоном, щоб стільникова мережа оновлювала інформацію про останнє місцезнаходження телефону, щоб

мережа могла швидше направляти виклики до нього. Запити TAU зазвичай надсилаються телефонами щоразу, коли вони підключаються до нової базової станції.

CSS відповідає повідомленням «TAU Reject». У повідомленні про відмову є те, що називається «номерами причин EMM», що вказує, чому повідомлення було відхилено. У цьому випадку зловмисник встановлює значення 7 («Послуги LTE заборонені»).

Отримавши це значення EMM, телефон видаляє всю інформацію про попередню реальну мережу, до якої він був підключений, а потім переходить у стан, коли він вважає свою SIM-карту недійсною для LTE. Потім він шукає мережі 3G і GSM для підключення та більше не намагатиметься узгодити з'єднання LTE, доки не буде перезавантажено (Shaik et al, 2017).

## 2.9 Атака SS7

Недоліки застарілих протоколів із розвитком методів злому створюють ідеальні умови для посилення зловмисних дій у переповнених мобільних мережах. У 2022 році SonicWall зафіксувала зростання кількості зловмисних програм Інтернету речей (IoT) на 87%, і, як очікується, у 2023 році продовжить руйнувати мобільну безпеку з експоненціальною швидкістю.

Одна з найвідоміших вразливостей мобільної мережі, яка загрожує постачальникам мобільних послуг і користувачам за останні роки: лазівки SS7.

Замість того, щоб націлюватися на конкретні пристрої, складні атаки здійснюються на цілі мережі. З точки зору постачальника послуг мобільного зв'язку, коли протокол SS7 вашої мережі успішно зламано, хакери отримують доступ до особистої інформації вашого абонента. Вони можуть отримувати доступ до текстових повідомлень, телефонних дзвінків,

відстежувати місцезнаходження пристрою та все без вашого відома чи відома абонента.

Протокол SS7 це набір протоколів сигналізації телефонії що відповідає за налаштування та завершення телефонних дзвінків через мережу цифрової сигналізації для забезпечення бездротового стільникового та дротового зв'язку. Він використовується для ініціювання більшості публічних телефонних дзвінків у світі через PSTN (телефонну мережу загального користування). Саме цей протокол можливо

Атака SS7 – це кібератака, котра використовують вразливі місця в протоколі SS7 для компрометації та перехоплення голосових і SMS-повідомлень у стільниковій мережі. Подібно до атаки Man In the Middle, атаки SS7 націлені на мобільний зв'язок, а не на передачу по Wi-Fi.

Атаки SS7 використовують можливості автентифікації протоколів зв'язку, які працюють на основі протоколу SS7, щоб прослуховувати голосові та текстові повідомлення. За словами експертів з телекомунікацій, все, що знадобиться кіберзлочинцю для успішного запуску атаки SS7, — це комп'ютер під керуванням Linux і SS7 SDK, які можна безкоштовно завантажити з Інтернету.

Після підключення до мережі SS7 хакер може націлюватися на абонентів у мережі, водночас обманюючи мережу, змушуючи її вважати, що пристрій хакера насправді є вузлом MSC/VLR.

**Що з цим може зробити хакер?**

Коли хакер успішно виконує фішингову атаку MitM, він отримує доступ до тих самих обсягів і типів інформації, які зазвичай зарезервовані для використання службами безпеки. Можливість підслуховувати дзвінки та текстові повідомлення, а також місцезнаходження пристроїв дає хакерам змогу отримувати цінну інформацію.

Також хакер має змогу включити безумовну переадресацію, що буде перенаправляти всі ваші дзвінки, смс та трафік.

Загальний запобіжний захід, яким користуються багато, є однією з цілей атак SS7. Двох факторна автентифікація (також відома як 2FA) через SMS з використанням SS7 за своєю суттю має недоліки, оскільки ці SMS-повідомлення незашифровані, і хакери знають, як їх перехопити. Маючи в руках код із SMS, кіберзлочинець потенційно може скинути ваш пароль до будь якого вашого облікового запису де використовується двох факторна автентифікація або навіть банківського рахунку.

# 3 Пропозиції по підсиленню протидії кіберзагрозам для мобільних мереж

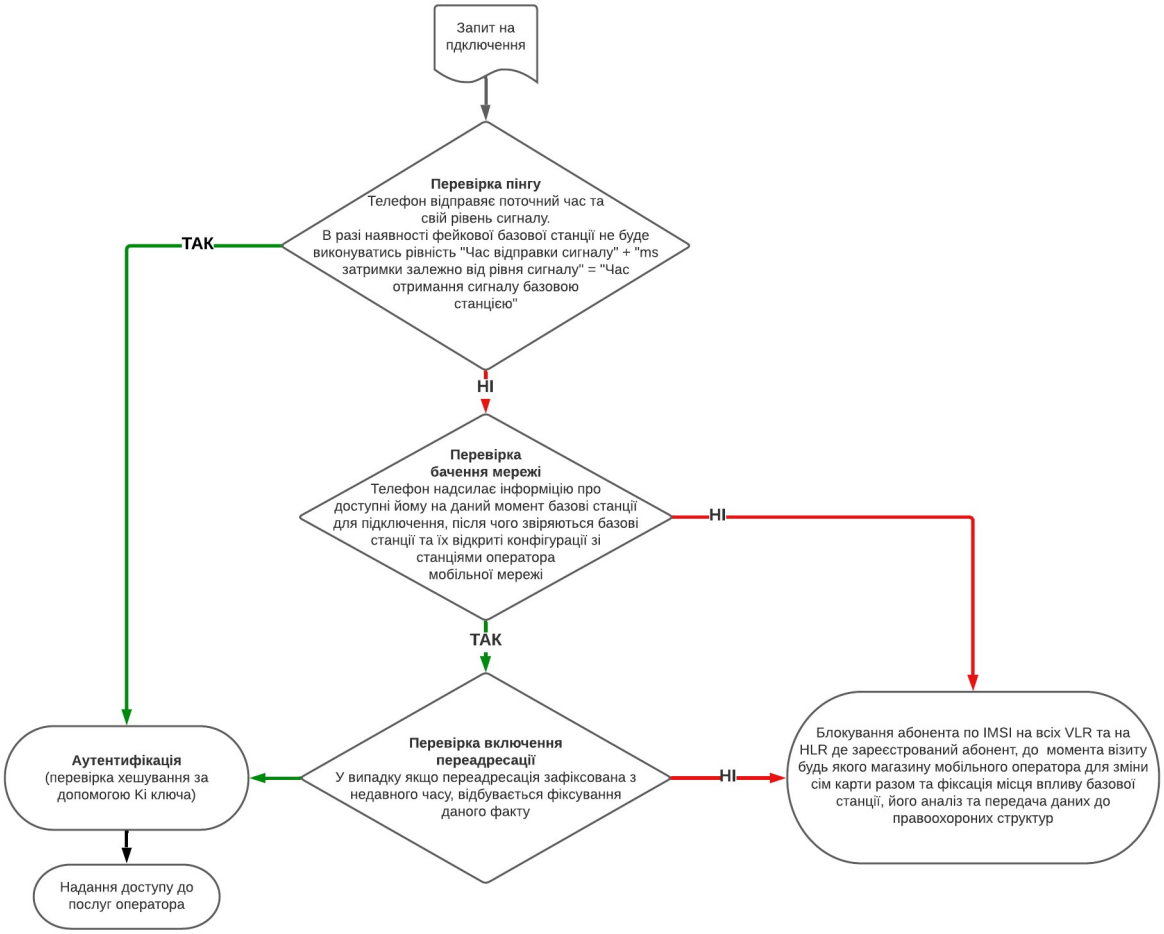
На даний момент, найефективнішим методом атаки на мережі мобільного оператора на даний момент є перехоплення IMSI користувача за допомогою фальшивої Базової станції, PUND та відповіді від MU, що в комбінації дає можливість дізнатись KI ключ. Саме ця комбінація - IMSI та KI ключ займають найважливіше місце у безпеці з’єднання між MU та базовою станцією.

Зловмисник, маючи на руках цю інформацію отримує доступ до ваших звінків, смс розсилок та отримує можливість атаки на службовий протокол SS7, що в свою чергу призведе до втрачі трафіку на деякий час.

Тож ми маємо зосередитись на протидії не наслідкам втрачі конфіденційної інформації, такої як IMSI та KI ключ, а протидії методу витягування цієї конфіденційної інформації. Для цього було розроблено алгоритм перевірки з’єднання пристрою до базової станції, за для протидії емуляції фальшивої базової станції. Слід розуміти що кожної секунди тисячі операторів з’єднуються з базовими станціями, не лише вмикаючи телефон, а і під час кожного хендоверу, що передає пристрій від однієї базової станції до іншої, то ж перевірка не має бути дуже ретельної та масивною, оскільки це

буде нести величезне навантаження на мережу мобільного оператора, збільшить затримки у зв’язку, та спричинить більше аварій на стороні оператора мобільного зв’язку.

Пропоную розглянути Блок-схему алгоритму додаткової перевірки




## 3.1 Перевірка затримки з’єднання

Під час запиту на підключення MU завжди відправляє певну інформацію до базової станції, таку як своє місцезнаходження, IMSI, рівень

сигналу та інше, перший етап перевірки складається з достовірності переданих даних, а саме рівня сигналу.

У випадку якщо між пристроєм на справжньою базовою станцією існує базова станція зловмисника, вона буде отримувати інформацію від пристрою, обробляти та передавати на справжню базову станцію, що несе за собою збільшення затримки у з'єднанні, але пристрій буде бачити лише затримку між собою та базовою станцією зловмисника, то ж у випадку якщо базова станція фіксуватиме затримку більше ніж на 50% від рівня сигналу пристрою, алгоритм буде переходити на наступні етапи перевірки. Якщо такої затримки не буде зафіксовано, то пристрій буде передаватись на подальшу звичайну автентифікацію і підключення до послуг оператора мобільної мережі.

При невдачі пристрій відправлятиметься для більш ретельної перевірки на наступні етапи.

Приклад реалізації логіки перевірки, за вийнятком того що в прикладі будут статичні змінні, а не ті що передаються пристроєм в реальному часі.

```
using namespace std;

class Mobile_info
{
private:
    long long IMSI = 23014462961098;
    long long  KIkey = 0x5F30D6FFDFDF3486;

    /*0x5F30D6FFDFDF3486*/
public:
    bool forwarding = 1;
    time_t time_forward(time_t* time_forward);
    uint64_t forward_time()
    {
        using namespace std::chrono;
        uint64_t t_forward =
            duration_cast <milliseconds>
            (system_clock::now().time_since_epoch()).count() - 1686578800500;
        return t_forward;

    };
    long long Number = 380965045692;
    string BS_connection = "UZ9032_GSM_2100";
    /*50.42290762817396, 30.433538804285796 */
    double x = 50.42290762817396;
    double y = 30.433538804285796;
    double get_x()
    {
```

```
        return Mobile_info::x;
    }
    long long get_y()
    {
        return Mobile_info::y;
    }
    long long getki()
    {
        return KIkey;
    }
    long long ping = 300;
    long long get_ping()
    {
        return Mobile_info::ping;
    }
    uint64_t mobile_time()
    {
        using namespace std::chrono;
        uint64_t ms_phone =
            duration_cast <milliseconds>
            (system_clock::now().time_since_epoch()).count() - 1686578800500;
        return ms_phone;

    };
};

class System_info
{
public:
    string BS_info[6]{ "UZ9032_GSM_2100", "UZ9021_LTE_1800", "UZ9012_UMTS_1800",
"UZ2812_GSM_0900", "UZ2810_LTE_2700", "UZ2808_GSM_1800" };
    uint64_t system_time()
    {
        using namespace std::chrono;
        uint64_t ms_system =
            duration_cast <milliseconds>
            (system_clock::now().time_since_epoch()).count() - 1686578800000;
        /*std::cout << ms_system << " milliseconds in system\n";*/
        return ms_system;
    };
};

/*Перша перевірка відбувається за такою логікою:*/
for (int i = 0; i < 2; i++) {
        if (((Mobile.mobile_time() + Mobile.get_ping()) >=
(System.system_time() - (Mobile.get_ping() * 0.5))) &&
((Mobile.mobile_time() + Mobile.get_ping()) <=
(System.system_time() + (Mobile.get_ping() * 0.5))))
        {
            ch1 = 1;
            break;
        }
        else
        {
            cout << "Repeat " << Mobile.mobile_time() +
Mobile.get_ping() << "  " << System.system_time() << "\n";
        }
    }
```

## 3.2 Перевірка бачення мережі

Інформація що до назв та конфігурацій базових станцій відсутня у відкритому доступі, то ж логічно буде звірити цю інформацію між тою що надає базова станція пристрою, та актульною інформацією, але проблема також  в тому що зловмисник може спробувати також з'єднатись з тією самою базовою станцією, і з деякою вірогідністю у нього це вийде, особливо якщо атака відбувається у малолюдному місці де може бути в рази менше базових станцій.

Для цього слід зазначити що такий метод буде ефективний у випадку якщо реалізувати відображення на пристрої і передачу відкритих конфігурацій базової станції зашифровану тим самим ki ключем,

то інформація від кожного пристрою до базової станції буде надходити в унікальному виді, і не міститиме загрози оскільки не буде містити відповіді від базової станції

Реалізація даної перевірки складається з співставлення наданої інформації про базову станцію від пристрою з базою даних що знаходиться в мережі мобільного оператора. За для прискорення алгоритму перевірки можуть бути розроблені  окремі масиви з базовими станціями, які теоретично можуть добивати до пристрою для кожного району, для відсутності необхідності перевіряти конкретну базову станцію зі всіма базовими станціями населеного пункту.

Також неможливо вирахувати математично чи дістане сигнал базової станцій до пристрою оскільки є велика кількість факторів яка впливає на цей показник, такі як рівень напруги на базовій станції, погодні умови, завантаження мережі, модель телефону та інше.

Реалізація 2 етапу перевірки відбувається таким чином:

```
if (ch1 == 1)
{
    Mobile.getki();
    ch2 = 1;
    ch3 = 1;
}
else /*друга перевірка*/
{
    cout << "Check base stations\n";
    if ((Mobile.get_x() >= 48.600572) && (Mobile.get_x() <=
48.622935) && (Mobile.get_y() >= 22.257013) && (Mobile.get_y() <=
22.304838))/*координати належать одному із районів Ужгорода, таким
чином мають бути зафіксовані у базі даних масиви із базовими
станціями району де визначені координати користувача*/
    {
        for (int i = 0; i < sizeof(System.BS_info) /
sizeof(System.BS_info[0]); i++)
        {
            if (Mobile.BS_connection == System.BS_info[i])
            {
                ch2 = 1;
                break;
            }
        }
    }
}
```

У випадку якщо пристрій проходить другий етап, він відправляється на третій етап перевірки, де перевіряється підозра на вже здійснену атаку, та ввімкнення переадресації даних користувача  з недавнього часу в умовах підозрілої затримки мережі. Якщо пристрій не проходить цю перевірку то відбувається видалення та блокування IMSI пристрою на всіх VLR та HLR.

## 3.3 Перевірка наявності переадресації трафіку

Реалізація третього етапу перевірки в моєму випадку є чисто формальною, оскільки перевірка має відбуватись в налаштуваннях контроллерів, та перевірка службового каналу SS7, що знаходиться за межами кваліфікації бакалавра.

У випадку якщо фіксується ввімкнення переадресації менше ніж як 2 години та зафіксовано збільшену затримку з першого етапу перевірки, то також відбувається процедура видалення та блокування IMSI.

Реалізація 3 етапу перевірки

```
if (ch2 == 0)
{
    cout << "Your IMSI was deleted from VLRs and HLR for your
security, please contact any of our stores with your SIM card.\n";
}
else
{
    if (System.system_time() - Mobile.forward_time() <= 7.2e+6)
    {
        cout << "Your IMSI was deleted from VLRs and HLR for your
security, please contact any of our stores with your SIM card.\n";
        ch3 = 0;
    }
    else
    {
        Mobile.getki();;
        ch3 = 1;
    }
     }
```

Слід зазначити що блокування IMSI є необхідною мірою, оскільки в разі простого видалення з HLR та VLR, при перезавантаженні пристрою, і новій спробі з’єднання відбувається повторна реєстрація сім карти у базах даних, то ж у випадку крадіжки ваших персональних даних для аутентифікації абонента, єдине що може вам допомогти це заміна сім карти.

Як результат модель поведінки відсіюватиме з’єднання що мають вірогідність на спробу атаки, або вже атаковані з крадіжкою конфіденційної

інформації та перехопленням трафіку за допомогою службового каналу SS7 та включенням переадресації трафіку.

Інтегрування алгоритму такої перевірки у загальну систему протоколу з’єднання до базових станцій має значно знизити ефективність використання нелегальних базових станцій, та посилити конфіденційність абонентів від несанкціонованого втручання.

## Висновки

У даній дипломній роботі було проведено комплексний аналіз проблеми безпеки в мережі телефонного зв'язку та мереж мобільного оператора з метою виявлення основних загроз і розробки ефективних заходів захисту. Результати дослідження підтверджують те, що зростання використання мобільних пристроїв та послуг зв'язку приводить до збільшення загроз безпеці, які можуть вплинути на конфіденційність, цілісність та доступність інформації.

Основними загрозами безпеці в мережі телефонного зв'язку та мереж мобільного оператора є шпигунське програмне забезпечення, атаки на базові станції, фішинг, перехоплення даних та злам паролів. Ці загрози можуть призвести до негативних наслідків, включаючи несанкціонований доступ до особистої інформації користувачів, крадіжку даних, втрату конфіденційності та порушення приватності.

У роботі було проаналізовано різні методи та технології, які можуть бути використані для захисту мережі телефонного зв'язку та мереж мобільного оператора. Серед них варто відзначити застосування сильних шифрувальних алгоритмів, механізмів аутентифікації, систем контролю доступу на прикладі розробленого у цій роботі та оновлення програмного

забезпечення і апаратних засобів. Ці заходи можуть допомогти уникнути більшості загроз безпеці та забезпечити високий рівень захисту для користувачів мережі.

З метою покращення безпеки в мережі телефонного зв'язку та мереж мобільного оператора рекомендується впроваджувати цілісну стратегію безпеки, яка включає не лише технічні заходи, але й організаційні та правові аспекти. Важливо забезпечити своєчасне навчання та освіту персоналу щодо безпеки, встановити політику безпеки, яка враховує вимоги законодавства та міжнародних стандартів.

Висновок дипломної роботи підкреслює необхідність постійного моніторингу і оновлення заходів безпеки в мережі телефонного зв'язку та мереж мобільного оператора, оскільки загрози безпеці постійно еволюціонують. Тільки завдяки поєднанню технологічних, організаційних і правових заходів можна забезпечити надійний захист і забезпечити безпеку користувачів в цифровому світі.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


3. http://celnet.ru/4G.php
4. http://celnet.ru/3G.php
5. https://habr.com/ru/articles/403649/
6. https://habr.com/ru/companies/ruvds/articles/531138/
7. https://www.firstpoint-mg.com/blog/ss7-attack-guide/
8. https://ss7.info/ss7-flaw/

9. https://ru.wikipedia.org/wiki/%D0%9E%D0%9A%D0%A1-7
10. https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html
11. https://www.sciencedirect.com/science/article/abs/pii/S1353485817300144
12. https://en.wikipedia.org/wiki/IMSI-catcher
13. https://www.smtechub.com/ss7-attack/
14. https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

## Додатки:

1. Код програми

```
#include <stdio.h>
#include <string>
#include <iostream>
#include <chrono>

using namespace std;
```

```
class Mobile_info
{
private:
    long long IMSI = 23014462961098;
    long long  KIkey = 0x5F30D6FFDFDF3486;

    /*0x5F30D6FFDFDF3486*/
public:
    bool forwarding = 1;
    time_t time_forward(time_t* time_forward);
    uint64_t forward_time()
    {
        using namespace std::chrono;
        uint64_t t_forward =
            duration_cast <milliseconds>
            (system_clock::now().time_since_epoch()).count() - 1686578800500;
        return t_forward;

    };
    long long Number = 380965045692;
    string BS_connection = "UZ9032_GSM_2100";
    /*50.42290762817396, 30.433538804285796 */
    double x = 50.42290762817396;
    double y = 30.433538804285796;
    double get_x()
    {
        return Mobile_info::x;
    }
    long long get_y()
    {
        return Mobile_info::y;
    }
    long long getki()
    {
        return KIkey;
    }
    long long ping = 300;
    long long get_ping()
    {
        return Mobile_info::ping;
    }
    uint64_t mobile_time()
    {
        using namespace std::chrono;
        uint64_t ms_phone =
            duration_cast <milliseconds>
            (system_clock::now().time_since_epoch()).count() - 1686578800500;
        return ms_phone;

    };
};

class System_info
{
public:
    string BS_info[6]{ "UZ9032_GSM_2100", "UZ9021_LTE_1800", "UZ9012_UMTS_1800",
"UZ2812_GSM_0900", "UZ2810_LTE_2700", "UZ2808_GSM_1800" };
    uint64_t system_time()
    {
        using namespace std::chrono;
        uint64_t ms_system =
            duration_cast <milliseconds>
            (system_clock::now().time_since_epoch()).count() - 1686578800000;
        /*std::cout << ms_system << " milliseconds in system\n";*/
        return ms_system;
```

```
    };
};


/*в даному вигляді передача інфомації базових станцій виглядає баззахостною, але в
разі якщо реалізувати відображення на пристрої і передачу зашифровану тим самим ki
ключем,
то інформація від кожного пристрою до базової станції буде надходити в уникальному
виді, і не міститиме загрози оскільки не буде містити відповіді від базової
станції*/


int main()
{

    Mobile_info Mobile;
    System_info System;
    bool ch1;
    bool ch2;
    bool ch3;
    /*System.system_time();*/
    /*Mobile.getki();*/
    /*Mobile.mobile_time();*/
    cout << "Check ping\n";
    /*cout << Mobile.forward_time();*/
    /*Перша перевірка*/
    for (int i = 0; i < 2; i++) {
        if (((Mobile.mobile_time() + Mobile.get_ping()) >= (System.system_time() -
(Mobile.get_ping() * 0.5))) && ((Mobile.mobile_time() + Mobile.get_ping()) <=
(System.system_time() + (Mobile.get_ping() * 0.5))))
        {
            ch1 = 1;
            break;
        }
        else
        {
            cout << "Repeat " << Mobile.mobile_time() + Mobile.get_ping() << "  " <<
System.system_time() << "\n";
        }
    }

    if (ch1 == 1)
    {
        Mobile.getki();
        ch2 = 1;
        ch3 = 1;
    }
    else /*друга перевірка*/
    {
        cout << "Check base stations\n";
        if ((Mobile.get_x() >= 48.600572) && (Mobile.get_x() <= 48.622935) &&
(Mobile.get_y() >= 22.257013) && (Mobile.get_y() <= 22.304838))/*координати належать
одному із районів Ужгорода, таким чином мають бути зафіксовані у базі даних масиви
із базовими станціями,
        які в теорії можуть добивати у йьому районі для того щоб не було
необхідності робити перевірку з усіма базовими станціями населеного пункту*/
        {
            for (int i = 0; i < sizeof(System.BS_info) / sizeof(System.BS_info[0]);
i++)
            {
                if (Mobile.BS_connection == System.BS_info[i])
                {
                    ch2 = 1;
                    break;
                }
```

```
                }
            }
        }

        if (ch2 == 0)
        {
            cout << "Your IMSI was deleted from VLRs and HLR for your security, please
contact any of our stores with your SIM card.\n";
        }
        else
        {
            if (System.system_time() - Mobile.forward_time() <= 7.2e+6)
            {
                cout << "Your IMSI was deleted from VLRs and HLR for your security,
please contact any of our stores with your SIM card.\n";
                ch3 = 0;
            }
            else
            {
                Mobile.getki();;
                ch3 = 1;
            }
        }
        cout << "Результати перевірки\nch1 = " << ch1 << "\nch2 = " << ch2 << "\nch3 = "
<< ch3;
    };
```

```
Check ping
Repeat 67545119  67545319
Repeat 67545119  67545319
Check base stations
Your IMSI was deleted from VLRs and HLR for your security, please contact any of our stores with your SIM card.
Результати перевірки
ch1 = 0
ch2 = 0
ch3 = 0

...Program finished with exit code 0
Press ENTER to exit console.
```