ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему **«ВДОСКОНАЛЕННЯ ЗАСОБІВ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ ТЕЛЕФОННИХ МЕРЕЖ СТВОРЕНИХ НА БАЗІ ПРОТОКОЛІВ ЗКС-7»**

Виконав: студент групи 6 курсу, групи АРДМ-61
спеціальності 172 Телекомунікації і радіотехніка
(шифр і назва спеціальності)

Корольов Д.В.
(прізвище та ініціали)

Керівник Дакова Л.В.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтроль _____
(прізвище та ініціали)

Київ – 2022

ВСТУП

Актуальність дипломної роботи обумовлена тим, що сьогодні більшість сервісів інтернет-банкінгу використовують SMS-повідомлення для підтвердження банківських операцій. Для доставки цих повідомлень використовується SMS-шлюз телефонних мереж. В основі роботи цих мереж лежить стек протоколів ЗКС-7.

Протоколи ЗКС-7 забезпечують маршрутизацію дзвінків, взаємодію з білінгом та підтримку USSD-послуг. Ці протоколи підтримують використання як в цифрових, так і в аналогових мережах, забезпечуючи високу швидкість встановлення з'єднання і передачі даних (без втрат і дублювання) та можливість перемикання трафіку на альтернативні маршрути в разі відмов. Серед переваг ЗКС-7 також можна виділити високу економічність. Але в стека ЗКС-7 є важливий недолік пов'язаний з можливістю проникнення в мережу зловмисників.

Цю вразливість зловмисники можуть використати для перехоплення SMS, прослуховування телефонних розмов, викрадення коштів з рахунку абонента за допомогою USSD-запиту, встановлення місцезнаходження абонента.

Метою дипломної роботи «Вдосконалення засобів захисту передачі даних телефонних мереж створених на базі протоколів ЗКС-7» є визначення засобів, що дозволяють підвищити рівень безпеки телефонних мереж створених на базі протоколів ЗКС-7.

Для досягнення цієї мети були поставлені завдання:

- проаналізувати принципи телефонної комутації;
- розглянути нормативно-правові акти із сфери телекомунікації;
- дослідити дії зловмисників, що проникають в телефонну мережу;
- дослідити існуючі засоби захисту телефонних мереж створених на базі протоколів ЗКС-7;
- розробити рекомендації щодо вдосконалення засобів захисту телефонних мереж створених на базі протоколів ЗКС-7.

Об'єкт дослідження: процес захисту передачі даних в телефонних мережах створених на базі протоколів ЗКС-7.

Предмет дослідження: механізми, що підвищують рівень безпеки телефонних мереж створених на базі протоколів ЗКС-7.

Практична цінність одержаних результатів: запропоновано рекомендації щодо вдосконалення засобів захисту телефонних мереж створених на базі протоколів ЗКС-7. Запропоновані рекомендації можуть бути використані операторами для підвищення рівня безпеки телефонних мереж.

1. ОПИС ТЕЛЕФОННОЇ КОМУТАЦІЇ

1.1 Поняття комутації телефонного виклику

Комутація телефонного виклику - процес визначення, яким чином має бути встановлено з’єднання між абонентом телефонної мережі, який ініціював виклик і абонентом, що викликається.

В рамках завдання комутації виконується маршрутизація і вибір каналу зв’язку (комутація каналу), лінії зв’язку узгодження принципів взаємодії відповідно до застосовуваної телефонної сигналізацією.

У телефонній мережі загального користування в рамках проходження одного виклику можуть застосовуватися різні підходи до його комутації, в залежності від особливостей проміжних вузлів зв’язку та сполучених телефонних мереж. Проте, в ТМЗК застосовується єдиний підхід до телефонної нумерації, загальний для всіх з’єднаних телефонних мереж усього світу.

Найперші телефонні комутатори були ручними; оператори використовували електричний розподільний щит та дротові шнури для підключення та відключення всіх дзвінків. Перший дзвінок за допомогою такої комутації відбувся в 1878 році в штаті Коннектикут. В 1879 році зі збільшенням кількості телефонних абонентів, користувачів стали ідентифікувати за номерами, а не за іменами[1].

В той час процес встановлення телефонного зв’язку між абонентами виглядав так: абонент, який був підключений до ручного перемикача, відправляв попереджувальний сигнал, який запалював лампочку на розподільному щиті оператора. Далі оператор підключав телефон абонента до телефонної лінії та попросив вказати номер, за яким необхідно було зателефонувати. Далі оператор відправляв сигнал адресату за вказаним номером. Якщо адресат відповідав на дзвінок, то оператор встановлював з’єднання, підключаючи шнур між двома

клемними гніздами на розподільному щиті. На розподільному щиті кожен роз'єм терміналу представляв абонента.

За даними журналу Scientific American в 1890-х роках правоохоронні органи вже починають прослуховувати телефонні розмови[2]. Теоретично можливими також були прослуховування з боку зловмисників, адже в перших телефонних мережах засобів захисту не існувало.

Так винахід першого автоматизованого комутатора пов'язаний з необхідністю усунути людський фактор під час встановлення з'єднання.

Власник патенту "US Patent No. 447918 10/6/1891", патенту на перший автоматизований комутатор, Алмон Браун Строуджер був власником похоронного бюро. В один момент він помітив, що кількість його клієнтів чомусь різко впала[3].

Виявилось, що телефоністка міського ручного комутатора була дружиною власника іншого похоронного бюро. Використовуючи своє службове становище, вона перенаправляла телефонні дзвінки родичів небіжчиків своєму чоловікові.

Строуджер вирішив усунути оператора з ланцюга "абонент — адресат", для цього він найняв декількох електромеханіків, які створили автоматизований телефонний комутатор. В основі роботи пристрою лежала ідея двоходових селекторів для встановлення з'єднання між абонентами. Кожен імпульс, що надходив в обмотку обертаючого електромагніта, повертав храповий напівциліндр, а разом з ним і щітку навколо осі на один крок в обраній декаді. При відпуску електромагніта собачка, ковзаючи, перескакувала на наступний зуб напівциліндра, число імпульсів визначало номер ламелі в декаді, на якій зупиниться щітка. Тим самим вхід комутатора (щітка) виявлявся сполученим з певним виходом декади. Через свій засоб роботи пристрій також став відомим як покроковий перемикач.

Перша станція з покроковим перемикачем в США відкрилася в Ла-Порті в штаті Індіана в 1892 році, її комутаційна здатність складала 99 абонентів. Циферблатний телефон Строуджера вважається попередником сучасного телефонного апарату. Цей пристрій мав три кнопки: одна на сотні, одна на

десятки і одна на одиниці. Щоб зателефонувати за номером 322, абоненту необхідно було тричі натиснути кнопку сотень, двічі кнопку десятків та двічі кнопку одиниць.

У 1896 році компанія Automatic Electric Company розробила поворотний циферблат для генерації імпульсів. Цей спосіб передачі набраних цифр став відомим як імпульсний набір і широко застосовувався до другої половини XX століття.

Цікаво зауважити, що деякі абоненти відмовлялись користуватись набором імпульсних телефонів, оскільки вважали, що виконують "роботу телефонної компанії".

У наступні десятиліття з’явилась можливість здійснювати дзвінки між абонентами, яких обслуговували сусідні комутатори. Таким чином, вимога до мережевої телесигналізації зростала.

Вже в 1940-х роках більшість великих міст США мали виключно автоматизовані телефонні станції.

Прямий набір на відстань був запроваджений у США в 1950-х роках. DDD дозволяв здійснювати національні міжміські дзвінки без допомоги оператора, тобто будь-який комутатор у Сполучених Штатах міг направити телефонний сигнал до будь-якого іншого комутатора в країні.

Міжнародний прямий набір на відстань став можливим у 1960-х роках, створивши таким чином необхідність телесигналізації між міжнародними комутаторами[4].

З 1889 по 1976 рік телесигналізація мала три основні характеристики[5]:

- телесигналізація була досить простою. Все, що потрібно від системи сигналізації - це налаштування та створення каналу між двома абонентами;
- сигналізація завжди була пов’язана з фізичною топологією; тобто всі сигнали, безпосередньо пов’язані з налаштуванням або зайнятістю лінії;
- використовувався детермінований зв’язок, також відомий як передача сигналів по виділеному каналу (англ. Channel Associated Signaling).

Слід зазначити, шо більшість національних мереж електрозв’язку в усьому світі до сих пір включають в собі обладнання, що базується на сигналізації по виділеному каналі. Тому під час впровадження більш сучасних станцій, потрібно передбачувати можливість взаємодії вже з існуючими системами сигналізації або можливість заміни застарілого обладнання.

Так кількість абонентів найбільшого в Україні оператора фіксованого зв’язку «Укртелеком» складає близько 2,2 мільйона абонентів[7]. В 2015 році «Укртелеком» утилізував три старі аналогових АТС радянського виробництва і мідний кабель на суму 237 мільйонів гривень[14]. Ці гроші було спрямовано на модернізацію обладнання[15].

1.2 Злом мереж, що використовують сигналізацію по виділеному каналу

Оскільки передача сигналів по виділеному каналу передбачає, що службова інформація про маршрутизації кодується і передається в тому ж каналі, що і корисне навантаження, то виникає загроза втручання в роботу мережі.

Через обмежені можливості для генерації сигналів, сигналізацією по виділеному каналу можна управляти лише при встановленні з’єднання і роз’єднання. Так в 1980-х роках на основі цих особливостей систем сигналізації по виділеному каналі був розроблений пристрій Blue Box, що дозволяв зловмисникам шляхом натискання на кнопки посилати в телефонну лінію службові сигнали, що використовувалися для управління процесом встановлення з’єднань на міжміських лініях.

Процес злому телефонних мереж виглядав так: зловмисник спершу набирає телефонний номер, який обслуговується іншою телефонною станцією. Виклик проходить через комутатори «домашньої» і «зовнішньої» станції. Під час встановлення з’єднання, зловмисник за допомогою Blue box посилає службовий сигнал частотою 2600 герц. Цей сигнал вказує, що дзвінок закінчено з ініціативи абонента («абонент повісив трубку»). Надіславши такий сигнал, абонент

повідомляє комутатор «зовнішньої» станції, що дзвінок припинено і телефонна лінія вільна. Проте комутатор «домашньої» станції ігнорує цей сигнал та важає, що лінія все ще зайнята.

Після цього зловмисник може за допомогою звукових сигналів Blue Box здійснювати дзвінок на новий телефонний номер, адже комутатор «домашньої» станції вважає, що абонент все ще здійснює початковий дзвінок, хоча фактично зловмисник дзвонить на зовсім інший номер. Таким чином, зловмисник міг безкоштовно або за меншу плату здійснювати міжміські та міжнародні дзвінки[6].

1.3 Створення загальноканальних систем сигналізації

В 1976 році був створений новий спосіб телесигналізації - загальноканальна сигналізація (англ. Common Channel Signaling). В загальноканальній сигналізації, на відміну від сигналізації по виділеному каналу, службові повідомлення передаються по окремо виділених каналах.

Загальноканальна сигналізація мала наступні переваги перед сигналізацією по виділеному каналу:

- швидкість - в більшості випадків час встановлення з’єднання не перевищує однієї секунди;
- висока продуктивність - один канал сигналізації здатний одночасно обслужити безліч телефонних розмов;
- економічність - у порівнянні з традиційними системами сигналізації скорочується обсяг обладнання комутаційної станції;
- надійність - існує можливість альтернативної маршрутизації в мережі в разі відмови одного з каналів;
- гнучкість - можливість передачі будь-яких даних (телефонії, цифрових мереж з інтеграцією служб, мереж рухомого зв’язку, інтелектуальних мереж і т.д.)[8];
- захищеність - звичайний абонент не може генерувати службові сигнали для комутаторів.

Набір протоколів ЗКС-7 - це сучасна система загальноканальної сигналізації. Для неї характерні такі основні особливості:

- відповідність міжнародним стандартам (будуть розглянуті в Розділі 2);
- можливість використання як на національному так і міжнародному рівні мереж;
- придатність для різних послуг зв’язку, наприклад, телефонних послуг, послуг передачі тексту;
- сумісність з цифровою мережею інтегрального обслуговування (ISDN);
- постійна доступність вузлів сигналізації, навіть під час дзвінків;
- використання ланок сигналізації також і для передачі призначених для користувача даних;
- використання різних середовищ передачі інформації: кабелю (мідь, світловод), радіорелейних ліній, супутникових ліній зв’язку (до 2 супутникових ліній зв’язку);
- при необхідності ЗКС-7 може використовуватися для більш низьких швидкостей передачі інформації і для аналогових вузлів сигналізації;
- автоматичний контроль і управління мережею сигналізації.

Висновки за розділом 1

В Розділі 1 були розглянуті базові принципи телефонної комутації та процес її еволюції. Вже на початку розвитку телефонії існували загрози інформаційної безпеки. Ці загрози були одним з важливих факторів, які змушували вдосконалювати телефонні мережі. Так винахід першого автоматизованого телефонного комутатора пов’язаний з бажанням усунути людський фактор з процесу комутації. А однією з причин розробки загальноканальної сигналізації була загроза втручання в службові сигнали сигналізації по виділеному каналу.

Також в розділі було порушене питання модернізації застарілого обладнання оператором фіксованого зв’язку «Укртелеком».

2. НОРМАТИВНО-ПРАВОВА БАЗА У СФЕРІ ТЕЛЕКОМУНІКАЦІЇ

2.1 Створення міжнародних стандартів зв'язку

Електрична телеграфія стала доступною для загального користування в кінці 1850-х років. Але телеграфний зв'язок не був міжнародним, оскільки кожна країна використовувала різні системи кодування.

17 травня 1865 року, після двох з половиною місяців переговорів, 20 країн-засновниць підписали в Парижі першу Міжнародну телеграфну конвенцію. Ця конвенція заклала основи для стандартизації телеграфного обладнання, розробки єдиних інструкцій по експлуатації та встановлення єдиних міжнародних правил тарифікації[9].

Міжнародний телеграфний союз був створений для подальшого регулювання цієї угоди. Через десять років з поширенням послуг телефонії, Міжнародний телеграфний союз почав розробляти законодавство, що регулює використання телефонії.

У 1934 році Міжнародний телеграфний союз змінив свою назву на сучасну — Міжнародний союз електрозв'язку. На той час МСЕ охоплював усі форми дротового та бездротового зв'язку. У 1947 році МСЕ став спеціалізованим агентством ООН.

Раніше майже всі національні мережі управлялися урядовими установами. Але в 1980-х роках в деяких країнах відбулася дерегуляції ринку телефонії. Це змусило МСЕ змінюватись та адаптуватись до нових вимог.

У грудні 1992 р. на позачерговій женевській конференції була проведена структурна реформа ITU. Були створені три сектори:

- радіозв'язку (ITU-R),
- стандартизації телекомунікації (ITU-T),
- розвитку телекомунікацій (ITU-D).

Раніше членство в МСЕ було відкрите тільки для урядів, що входять до ООН. З 1992 року постачальники обладнання, телекомунікаційні наукові установи та регіональні телекомунікаційні організації також набули право членства. Наприклад, Cisco Systems та Європейський інститут телекомунікаційних стандартів є членами постачальників та регіональних організацій.

2.2 Міжнародні стандарти ЗКС-7

Детальні специфікації систем загальноканальної сигналізації, що включають SDL-діаграми, структури даних, часові параметри сигналів, сценарії розробляються й удосконалюються фахівцями ITU-T, та публікуються в кольорових книгах ITU-T, зокрема, Рекомендації Q.7xx у випусках Жовтої, Червоної та Блакитної книги (1981, 1985 та 1989 роки) і Білої книги ITU-T (1993 рік). Ці специфікації є загальнодоступними. Вони повинні виконуватись всіма операторами, які хочуть підключитись до міжнародної мережі ЗКС-7. Список рекомендацій Q.7xx наведений у Додатку А.

МСЕ допускає використання національних та регіональних стандартів, наприклад, стандарти ETSI використовуються в країнах Європи. Але якщо абонент буде здійснювати міжнародний дзвінок, дзвінок повинен буде виконуватись відповідно до міжнародних стандартів.

Також слід зазначити, що SDL-діаграми, таблиці тайм-аутів, сценарії обміну сигналів та інші розробки, створені компаніями для власного використання в програмно-керованій комутаційній техніці, у відкритих джерелах не публікуються[10].

Ці специфікації можна поділити відповідно до рівнів ЗКС-7, які вони регулюють. Рівень 1 – це фізичний рівень, що працює з бітовим потоком даних. Залежно від способу передачі даних використовуються різні стандарти. В той час як розподіл рівнів 2, 3, 4 наведений в Таблиці 1.1. Призначення цих рівнів буде розглянуто в Розділі3.

Таблиця 1.1

Рівні ЗКС-7 та стандарти, що їх регулюють

Рівень ЗКС-7	**Стандарти**
Рівень 2	Q.701 – Q.703, Q.781
Рівень 3	Q.704 – Q.707, Q.782
Рівень 4 (підсистема SCCP)	Q.711 – Q.714, Q.786
Рівень 4 (підсистема TUP)	Q.721 – Q.724, Q.783
Рівень 4 (підсистема ISUP)	Q.761 – Q.764, Q.785
Рівень 4 (підсистема TCAP)	Q.771 – Q.775

2.3 Законодавство України в сфері телекомунікації

Відносини суб'єктів ринку телекомунікацій щодо надання та отримання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування в Україні регламентуються Законом України «Про телекомунікації». Так в пункті 3 статті 9 зазначено, що оператори, провайдери телекомунікацій зобов'язані вживати технічні та організаційні заходи із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами[11].

В Постанові Кабінету Міністрів від 11 квітня 2012 р. № 295 затверджено «Правила надання та отримання телекомунікаційних послуг». В цих правил зазначені наступні обов'язки оператора:

…22) вживати відповідні до законодавства заходи із забезпечення таємниці телефонних розмов, іншої інформації, що передається телекомунікаційними мережами, а також із захисту відомостей про споживача, отриманих під час укладання договору, надані чи замовлені ним послуги, іншої інформації з обмеженим доступом;

…30) вживати заходи для недопущення несанкціонованого доступу до телекомунікаційних мереж, технічних засобів провайдерів та інформації, що передається ними[12].

Також в пункті 47 цих правил вказано, що дані про місцезнаходження кінцевого обладнання абонента не можуть передаватися оператором, провайдером без його згоди третім особам, крім випадків, встановлених законом.

Слід зазначити, що вимоги НД ТЗІ 1.1–001–99 «Технічний захист інформації на програмно-керованих АТС загального користування» не поширюються на захист:

- міжстанційних каналів синхронізації, сигналізації та передачі абонентської інформації;
- від зловмисних дій авторизованих користувачів у межах наданих їм повноважень, що наносять збиток власникам інформаційних ресурсів[13].

Висновок за розділом 2

В розділі була розглянута нормативно-правова база зі сфери телекомунікації. Було з’ясовано, що законодавство України покладає на оператора відповідальність за створення та підтримку роботи захищеної телефонної мережі, але не визначає способи цього захисту. Оператори повинні самі обирати та впроваджувати необхідні рішення для захисту своїх мереж та інформації, що в них циркулює.

Також в розділі 2 було встановлено, що для здійснення міжнародних дзвінків виклик повинен відповідати рекомендаціям Q.7xx, які розроблені ITU-T.

3. АНАЛІЗ РОБОТИ ЗКС-7

3.1 Ланки сигналізації та пункти сигналізації

Ланка сигналізації ЗКС-7 з'єднують пункти сигналізації в мережі зв'язку. Пункти сигналізації і ланки сигналізації утворюють незалежну мережу сигналізації, яка накладається на мережу каналів передачі.

Слід зазначити відмініть між пунктами сигналізації (SP) та транзитними пунктами сигналізації (STP). Пункти сигналізації являють собою джерела (вихідні пункти) і приймачі (пункти призначення) трафіку сигналізації. У мережі зв'язку - це, перш за все, мережеві вузли. Транзитні пункти сигналізації, відповідно до адреси пункту призначення, направляють прийняті сигнальні повідомлення в інший транзитний або приймальний пункт сигналізації. В транзитному пункті сигналізації обробка викликів для сигнальних повідомлень не виконується. Транзітний пункт сигналізації може бути інтегрований в пункт сигналізації або може формувати власний вузол в мережі сигналізації. Залежно від розміру мережі сигналізації може існувати один або кілька рівнів транзитних пунктів сигналізації. Всі пункти сигналізації в мережі сигналізації визначаються кодом в структурі відповідного плану нумерації і, отже, можуть безпосередньо адресуватися в сигнальному повідомленні.

Ланка сигналізації складається з ланки даних сигналізації (два канали передачі даних, що функціонують спільно в протилежних напрямках з однаковою швидкістю передачі) і функціональних блоків управління передачею даних. В якості ланки даних сигналізації може використовуватися канал існуючої лінії передачі. З метою резервування між двома пунктами сигналізації зазвичай існує кілька ланок сигналізації. У разі відмови одного з цих ланок функції ЗКС-7 забезпечують перенаправлення трафіку сигналізації по справним альтернативних маршрутах. Між двома пунктами сигналізації може підтримуватися різна

маршрутизація ланок сигналізації. Всі ланки сигналізації між двома пунктами сигналізації утворюють набір ланок сигналізації.

У мережі сигналізації ЗКС-7 можуть використовуватися два режими сигналізації. При пов’язаному режимі сигналізації маршрутизація ланки сигналізації здійснюється разом з группой̆ каналів передачі, прінадлежащей̆ цієї ланки. Іншими словами, ланка сигналізації безпосередньо підключається до пунктів сигналізації, які одночасно є і кінцевими пунктами групи каналів. Цей режим сигналізації рекомендується застосовувати в разі інтенсивного трафіку при обміні інформацией̆ між пунктами сигналізації А і В.

3.2 Підсистеми ЗКС-7

Структура системи ЗКС-7 розподілені між наступними підсистемами:

- підсистема передачі повідомлень (Message Transfer Part),
- підсистеми користувача (User Part).

Підсистема передачі повідомлень (MTP) підтримує нейтральні для користувача транспортні засоби обміну повідомленнями.

Кожна підсистема користувача (UP) реалізує функції, протоколи та кодування сигналізації ЗКС-7 для специфічного типу користувача (наприклад, послуга передачі даних, ISDN). Таким чином, підсистеми користувача керують встановленням і припиненням з’єднань по каналах передачі, обробкою послуг, а також функціями адміністративного управління і технічного обслуговування цих каналів передачі. Функції підсистеми передачі повідомлень і підсистем користувача системи ЗКС-7 поділяються на 4 рівня.

Рівні з 1 по 3 відносяться до підсистеми передачі повідомлень, в той час як підсистеми користувача утворюють рівень 4. Розподіл підсистем відповідно до рівнів зображений на Рисунку 3.1.

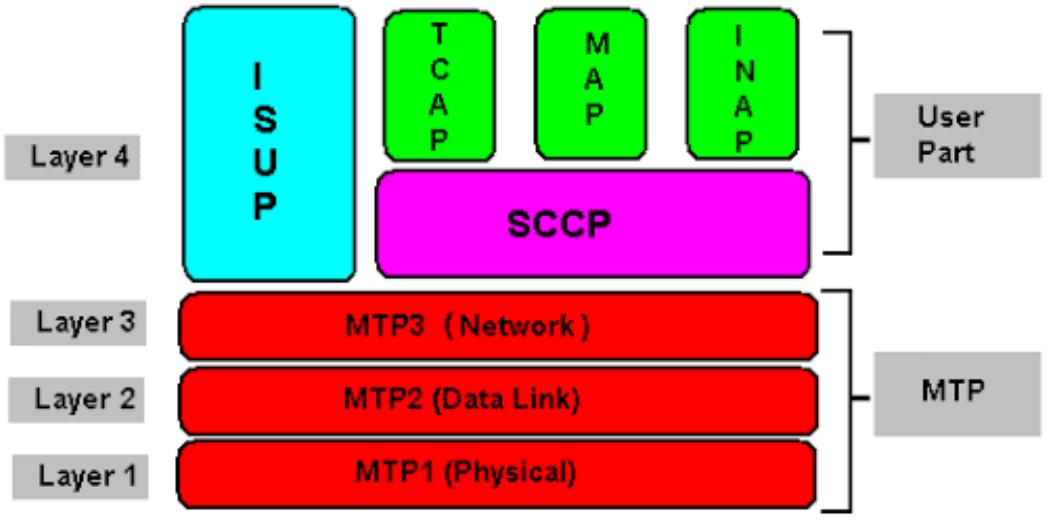


Рис. 3.1 – Розподіл підсистем ЗКС-7 відповідно до рівнів

При використанні сигналізації ЗКС-7 підсистема передачі повідомлень (МТР) застосовується всіма підсистемами користувача в якості транспортної системи для обміну повідомленнями. Повідомлення, що передаються з однієї підсистеми користувача в іншу, надходять в підсистему передачі повідомлень. Підсистема передачі повідомлень забезпечує доставку повідомлень в адресовану підсистему користувача в правильному порядку, без втрати інформації, без дублювання або зміни послідовності і без бітових помилок.

Підсистема передачі повідомлень призначена для передачі і прийому сигнальних одиниць, виправлення помилок передачі, управління мережею сигналізації і синхронізації. Її функції розподілені по функціональним рівням 1, 2 і 3.

Рівень 1 (ланка даних сигналізації) визначає фізичні, електричні і функціональні характеристики ланки даних сигналізації і блоків доступу. Рівнем 1 представлена функція перенесення інформації для ланки сигналізації..

Рівень 2 (ланка сигналізації) визначає функції і процедури для правильного обміну повідомленнями користувачів по ланці сигналізації. На рівні 2 необхідно виконувати такі функції:

- обмеження сигнальних одиниць прапорами;
- видалення зайвих прапорів;

- виявлення помилок з використанням контрольних бітів;
- виправлення помилок шляхом повторної передачі сигнальних одиниць;
- контроль інтенсивності помилок в ланці даних сигналізації;
- відновлення нормального режиму роботи.

Рівень 3 (мережа сигналізації) визначає процедуру взаємодії окремих ланок сигналізації. Розрізняють такі дві функціональні області:

- обробка повідомлень, тобто напрямок повідомлень в потрібне ланка сигналізації або в потрібну підсистему користувача;
- управління мережею сигналізації, тобто управління трафіком повідомлень, за допомогою, наприклад, перемикання ланок сигналізації при виявленні збою і переходу до звичайного режиму роботи після усунення збою.

Різні функції рівня 3 взаємодіють один з одним, з функціями інших рівнів і з відповідними функціями інших пунктів сигналізації.

Кожна підсистема користувача (UP) підтримує функції, що дозволяють застосовувати підсистему передачі повідомлень для певного типу користувача. В даний час в ITU-T визначено наступні підсистеми користувачів:

- підсистема ISDN-користувача (ISUP),
- підсистема управління сигнальними з’єднаннями (SCCP).

Завдяки своїй модульній структурі, система сигналізації ЗКС-7 може адаптуватися, в залежності від висунутих до неї вимог. Можливо також розширення для майбутніх видів застосування. Кожен користувач ЗКС-7 може вказати власну підсистему користувача; наприклад, підсистема користувача рухомого зв’язку (MUP) являє собою власну специфікацію компанії Siemens для мережі рухомого телефонного зв’язку[16].

Підсистема ISDN-користувача (ISUP) виконує функції сигналізації для управління викликами, обробки послуг і додаткових видів обслуговування, а також для адміністрування каналів в мережі ISDN. Для транспортування сигнальних одиниць повідомлення підсистема ISUP підтримує інтерфейси з

підсистемою передачі повідомлень і підсистемою управління сигнальними з'єднаннями (SCCP).

Мітка маршрутизації містить код пункту призначення, код вихідного пункту і поле вибору ланки сигналізації.

Код ідентифікації каналу (CIC) призначає повідомленням конкретний канал. Кожному каналу присвоюється постійний код ідентифікації каналу.

Тип повідомлення визначає функцію і формат ISUP-повідомлення. Існують різні типи повідомлень для встановлення з'єднання, звільнення з'єднання і адміністративного управління каналами.

Типи повідомлень для встановлення з'єднань (приклади):

- Повідомлення "Initial address" (далі IAM) є першим повідомленням, переданим в процесі встановлення з'єднання в наступний мережевий вузол. Воно використовується для заняття каналу і містить всю інформацію, необхідну для виконання маршрутизації в кінцевий мережевий вузол.
- Повідомлення "Subsequent address" (далі SAM). За допомогою нього здійснюється транспортування цифр, які ще не були відправлені в повідомленні IAM.
- Повідомлення "Address complete" (далі ACM). За допомогою повідомлення ACM викликає мережевий вузол інформується про досягнення кінцевого мережевого вузла.
- Повідомлення "Answer" (далі ANM) інформує мережевий вузол, що викликає, про відповідь адресата. Зазвичай повідомлення ANW ініціює процедуру обліку тарифікації дзвінка.

Типи повідомлень для звільнення з'єднання (приклади):

- Повідомлення "Release" ініціює звільнення з'єднання каналів. Кожне невдало встановлене з'єднання по каналу також звільняється за допомогою повідомлення REL. Крім того, це повідомлення містить інформацію про причини невдалого встановлення з'єднання.
- Повідомлення "Release complete" (далі RLC) За допомогою повідомлення RLC фіксується роз'єднання встановленого по каналу з'єднання.

Прийом повідомлення RLC підтверджується. Після передачі або прийому повідомлення RLC канал звільняється і стає доступним для встановлення нового з’єднання [20].

Типи повідомлень для адміністративного управління каналами (приклади):

- Повідомлення "Blocking" (далі BLO) використовується для блокування каналу.
- Повідомлення "Unblocking" (далі UBL) використовується для розблокування заблокованих каналу.

Фіксована обов’язкова частина ISUP-повідомлення включає в себе параметри, необхідні для певного типу повідомлення і мають фіксовану довжину. Для повідомлення IAM, наприклад, це такі параметри:

- тип з’єднання (наприклад, з’єднання через супутникову лінію зв’язку),
- вимоги до каналу передачі,
- вимоги до системи сигналізації (наприклад, наскрізна підсистема ISUP),
- тип абонента (ISDN-абонент = звичайний абонент).

Змінн обов’язкова частина ISUP-повідомлення включає в себе параметри змінної довжини. Одним з таких параметрів повідомлення IAM є номер абонента або, принаймні, його частина номера, необхідна для маршрутизації в кінцевий мережевий вузол.

Якщо повідомлення має необов’язкову частина, то в цій частині повідомлення можуть передаватися певні параметри. Це можуть бути параметри фіксованою або змінною довжини. Приклади для повідомлення IAM:

- телефонний номер абонента,
- параметри для типу повідомлення,
- призначена для користувача інформація,
- процедури сигналізації.

Як приклади процедур сигналізації для ISUP нижче більш детально описується встановлення та звільнення з’єднання.

Встановлення з’єднання починається після надходження в вихідний мережевий вузол достатньої кількості цифр від абонента. Спочатку виконується маршрутизація і займається вільний канал. Для встановлення з’єднання ISUP витікаючого мережевого вузла спочатку посилає т повідомлення IAM . Початкове адресне повідомлення (IAM) містить усі отримані цифри. В подальшому адресному повідомленні (SAM) ISUP передає наступні цифри.

Після прийому IAM транзитний мережевий вузол виконує маршрутизацію. У разі успішного виконання цієї процедури транзитний мережевий вузол займає вільний канал, і ISUP посилає повідомлення IAM в кінцевий мережевий вузол. Повідомлення IAM підсистеми ISUP транзитного мережевого вузла містить весь набраний до даного моменту часу номер (цифри якого містяться в прийнятому повідомленні IAM і в подальшому повідомленні SAM, якщо воно надійшло). Повідомлення SAM, що надходять в транзитний мережевий вузол після посилки IAM, передаються підсистемою ISUP без змін.

Кінцевий мережевий вузол аналізує набраний номер, що міститься в IAM, і при необхідності очікує подальші цифри, що надходять в повідомленні SAM. При наявності всієї інформації визначається викликається лінія, опитується її стан і виконується перевірка повноважень, необхідних для використання запитуваної послуги. За допомогою повідомлення "address complete" (ACM) кінцевий мережевий вузол інформує вихідний мережевий вузол про успішне встановлення з’єднання з кінцевим мережевим вузлом.

У разі телефонної послуги, по каналу від кінцевого мережевого вузла до абонента надсилається сигнал виклику, за умови що абонент вільний. Після встановлення з’єднання сигнал виклику відключається, і відбувається проключеніе виклику. Згодом ISUP кінцевого мережевого вузла посилає у відповідь повідомлення (ANW) в вихідний мережевий вузол, який потім починає процедуру обліку вартості викликів.

Звільнення з’єднання може бути ініційовано викликають або абонентом. З цією метою ISUP мережевого вузла-ініціатора надсилає повідомлення про звільнення (REL) в транзитний мережевий вузол. Транзитний мережевий вузол

відразу ж передає повідомлення REL в відповідний кінцевий мережевий вузол. Кожне прийняте повідомлення REL підтверджується повідомленням "release complete" (RLC) після звільнення задіяного каналу.

Підсистема управління сигнальними з’єднаннями (SCCP) використовується як доповнення до підсистеми передачі повідомлень. Ця підсистема виконує додаткові функції передачі повідомлень між мережевими вузлами і між мережевими вузлами та іншими пунктами сигналізації, такими як банки даних. З точки зору підсистеми передачі повідомлень, SCCP є користувачем, що має власний індикатор послуги. Комбінація підсистеми SCCP і підсистеми передачі повідомлень називається підсистемою мережевих послуг (NSP).

Підсистема SCCP забезпечує передачу повідомлень двох типів:

- без логічного сигнального з’єднання,
- з логічним сигнальним з’єднанням.

Без встановлення логічного сигнального з’єднання користувач SCCP може передавати поодинокі повідомлення іншим користувачам SCCP.

Логічне сигнальне з’єднання дозволяє здійснювати обмін повідомленнями між двома користувачами SCCP. Логічне сигнальне з’єднання встановлюється через взаємний мережевий вузол кодів вихідних пунктів між підсистемами SCCP пунктів сигналізації, обробних потік сигналізації. Таким чином, повідомлення, призначені для іншого користувача SCCP, можуть бути особливим чином. Важливо тут те, що SCCP може посилати повідомлення через MTP-мережу.

Підсистема SCCP має власну функцію маршрутизації. Як адресних параметрів підсистемою SCCP можуть використовуватися такі параметри:

- код пункту призначення,
- глобальний заголовок,
- номер підсистеми.

Код пункту призначення просто передається в підсистему MTP, яка потім виконує маршрутизацію. Проте глобальна заголовок містить цифри або іншу адресну інформацію, яка не є стандартною для мережі сигналізації. З цієї причини для передачі повідомлення в пункт призначення підсистема SCCP повинна

спочатку визначити його код (трансляція глобальних заголовків). Номер підсистеми визначає функцію користувача; наприклад, у вхідному повідомленні цей номер ідентифікує SCCP-користувача (такого як прикладна підсистема IN, INAP), для якого призначено повідомлення.

Мітка маршрутизації включає в себе код пункту призначення, код вихідного пункту і поле вибору ланки сигналізації. SCCP визначає код пункту призначення на основі адресних параметрів, що містяться в призначеній для користувача інформації.

Фіксована обов’язкова частина повідомлення підсистеми SCCP містить параметри фіксованої довжини, які повинні бути представлені в повідомленнях певного типу. Для повідомлення "connection request" (далі CR), наприклад, це такі параметри: локальне посилання; клас протоколу, який використовується для передачі повідомлень

Змінна обов’язкова частина SCCP-повідомлення містить параметри змінної довжини. Для повідомлення CR, наприклад, це такі параметри: телефонний номер абонента, що викликається; ідентифікатор SCCP-користувача (наприклад, ISUP, TCAP)

Додаткова (необов’язкова) частина SCCP-повідомлення містить параметри, які можуть використовуватися в повідомленні будь-якого типу. Розглянуті параметри можуть мати або фіксовану, або змінну довжину. Для повідомлення CR, наприклад, це такі параметри: телефонний номер абонента; повідомлення, написані, що підлягають передачі

Для встановлення логічного сигнального з’єднання підсистеми SCCP пунктів сигналізації відповідного потоку сигналізації посилають один одному свої власні коди вихідних пунктів. Крім того, вони призначають локальні посилання на процес, для якого здійснюється встановлення логічного сигнального з’єднання (наприклад, для користування послугою в процесі обробки існуючого з’єднання), і аналогічним чином інформують про це одна одну. Після цього можливий обмін повідомленнями. Кожна підсистема SCCP за допомогою локальної посилання може привласнювати вхідні повідомлення відповідного процесу.

Прикладна підсистема можливостей транзакцій (TCAP) є прикладним протоколом сигналізації (7 рівень моделі OSI). TCAP взаємодіє безпосередньо з SCCP, так як підсистема проміжного обслуговування (ISP) в цьому випадку не використовується. Підсистема TCAP і її послуги використовуються, наприклад, в таких застосуваннях, як прикладна підсистема рухомого зв'язку (MAP)[17].

Приклади застосувань TCAP:

- передача в опорний мережевий вузол рухомого телефонного зв'язку повідомлення про місцезнаходження мобільного абонента;
- перевірка достовірності і транзакцій при обслуговуванні по кредитних картах;
- додаткові послуги мережевого вузла, що використовує незв'язану з каналом сигнальну інформацію (ISDN), такі як встановлення з'єднання з зайнятим абонентом (CCBS) і завершення викликів при відсутності відповіді (CCNR) в замкнутих групах користувачів (CUG);
- опитування робочих станів або ініціювання дій по експлуатації та технічного обслуговування у віддалених мережевих вузлах.

Повідомлення, якими обмінюються між собою TCAP-користувачі, можуть включати в себе один або кілька індивідуальних компонентів. Компонент повідомлення може містити, наприклад:

- запит на виконання дії TCAP-користувачем віддаленого вузла,
- запит даних або стану,
- відповідь на виклик операції або на запит.

TCAP-користувач передає в TCAP компоненти повідомлення окремо, при цьому пов'язаним компонентам повідомлення присвоюються однакові ідентифікатори діалогу. Користувач починає передачу зі спеціального запиту. Потім TCAP об'єднує всі компоненти повідомлення з однаковим ідентифікатором діалогу в одне закінчене повідомлення і передає його в підсистему SCCP для пересилання необхідному адресату.

Для передачі повідомлень TCAP-користувачеві доступні два способи діалога: стуктурний і неструктурний.

Неструктурована діалог: ТСАР-користувач передає поодинокі компоненти повідомлення в ТСАР, і ТСАР посилає їх необхідному адресату окремо або в групі, відповідно до запиту користувача. При цьому відповідність між переданим компонентом повідомлення та будь-яким прийнятим підсистемою ТСАР відповіддю не встановлюється.

Структурована діалог: ТСАР-користувач встановлює діалог з віддаленим ТСАРпользователем і обмінюється з ним повідомленнями в процесі діалогу. Таким чином, може бути встановлено пряме відповідність між компонентом повідомлення та відповіддю на нього.

ТСАР-повідомлення включає в себе наступні поля:

- тип повідомлення,
- загальну довжину повідомлення,
- інформаційний елемент (елементи) транзакції,
- довжину частини компонентів повідомлення,
- компонент (компоненти) повідомлення.

Тип повідомлення визначає функцію ТСАР-повідомлення. ТСАР-користувачеві доступні наступні типи повідомлень:

- "unidirectional" (односпрямоване) використовується для передачі повідомлень в режимі неструктурованого діалогу;
- "begin" (початкове) використовується на початку діалогу, встановленого в режимі структурованого діалогу;
- "continue" (продовження) виконується обмін завданнями, звітами і даними в режимі діалогу;
- «end" (кінець) використовується в режимі структурованого діалогу для закінчення діалогу;
- "abort" (примусове переривання) використовується в режимі структурованого діалогу для переривання діалогу після помилки.

В поле загальної довжини повідомлення міститься кількість октетів повідомлення.

Інформаційні елементи транзакції використовуються тільки для структурованого діалогу. Вони містять, наприклад:

- ідентифікатор транзакції. Вихідна підсистема TCAP призначає діалогу ідентифікатор і передає його підсистемі TCAP віддаленого кінця. Потім підсистеми TCAP можуть призначати вхідні повідомлення відповідного діалогу;
- причину примусового переривання. Однією з причин раптового завершення транзакції може бути невідомий тип повідомлення або невідомий ідентифікатор транзакції.

Частина компонентів повідомлення містить один або кілька компонентів повідомлення. У частині компонентів повідомлення повинно знаходитися поле довжини частини компонентів повідомлення.

TCAP-користувачеві доступні наступні типи компонентів:

- "invoke" (виклик) - за допомогою цього типу компонента, наприклад, ініціюється операція, яка виконується на віддаленому мережевому вузлі;
- "return result" (повертається результат) - цей тип компонента використовується для передачі результату виконання запиту;
- "return error" (яка повертається помилка) - цей тип компонента використовується для передачі інформації про невдалий виконанні операції;
- "reject" (відмова) - за допомогою даного типу компонента відхиляється обробка певного компонента повідомлення.

Поле «Довжина компонента» містить кількість октетів в компоненті повідомлення.

Інформаційні елементи залежать від типу компонента. Ось деякі приклади інформаційних елементів:

- "invoke ID" (ідентифікатор виклику) - ідентифікатор виклику використовується для того, щоб встановити відповідність між результатами і запитами на виконання операцій. Він присутній в кожному компоненті повідомлення;
- "operation code" (код операції) - код операції визначає підлягає виконанню операцію. Він міститься в компоненті повідомлення типу "invoke";

- "error code" (код помилки) - код помилки вказує причину невдалого виконання операції. Цей код включається в компонент повідомлення типу "return error";
- "problem code" (код проблеми) - код проблеми вказує причину, по якій був відхилений компонент повідомлення. Цей код включається в компонент повідомлення типу "reject";
- "parameter" (параметр) - це поле містить додаткову інформацію користувача.

Неструктурований діалог дозволяє виконувати передачу одного або декількох компонентів повідомлення віддаленого TCAP-користувачеві. В цьому випадку TCAP-користувач спочатку посилає підлягають передачі компоненти повідомлення в підсистему TCAP. Ці компоненти ідентифікуються загальним індикатором діалогу. TCAP-користувач, використовуючи односпрямований запит, ініціює посилку компонентів повідомлення з ідентичними індикаторами діалогу. У запиті міститься як інформація про адресу, так і індикатор діалогу підлягають передачі компонентів повідомлення. TCAP з відповідних компонентів повідомлення формує односпрямоване повідомлення. Потім, для транспортування заданої адресату, це повідомлення разом з відповідною адресною інформацією передається підсистемою TCAP в підсистему SCCP. TCAP на стороні прийому приймає односпрямовані повідомлення і передає їх адресуемому TCAP-користувачеві.

Структурований діалог дозволяє TCAP-користувачеві для обміну повідомленнями почати діалог з іншим TCAP-користувачем і, після закінчення обміну, завершити діалог.

TCAP-користувач починає новий діалог шляхом посилки в підсистему TCAP запиту на початок діалогу. Цей запит містить інформацію про адресу та індикатор діалогу підлягають обміну компонентів повідомлення. Запит на початок діалогу може надсилатися в TCAP перед передачею компонентів повідомлення. Компоненти повідомлення, надісланого TCAP перед запитом на початок діалогу з відповідним індикатором, надсилаються необхідному партнеру

з допомогою повідомлення "begin" (початок). Повідомлення "begin" також містить ідентифікатор транзакції, який в процесі діалогу використовується для встановлення відповідності між компонентами повідомлення і діалогом. TCAP разом з відповідною адресною інформацією передає повідомлення "begin" в підсистему SCCP, яка посилає їх необхідному адресату. Підсистема TCAP адресата отримує повідомлення "begin" і інформує адресується TCAP-користувача про початок нового діалогу.

Діалог може бути продовжений обома TCAP-користувачами. З цією метою TCAP-користувач посилає в TCAP повідомлення "continue". Повідомлення "continue" може містити, наприклад, компоненти повідомлення з подальшими запитами операцій. Крім того, дане повідомлення може містити повідомлення з результатами виконання раніше отриманого запиту.

Існують наступні можливості завершення діалогу:

- TCAP-користувачі заздалегідь вказують на необхідність завершення діалогу; обмін повідомленнями не відбувається, повідомлення "end" (закінчення діалогу) надсилати не потрібно. базовий спосіб завершення: TCAP-користувач в потрібний момент закінчує діалог і посилає повідомлення "end" поточному партнеру по діалогу;
- TCAP-користувач за допомогою повідомлень "end" як і раніше може передавати компоненти повідомлення віддаленого TCAP-користувачеві, оголосивши в той же самий час кінець діалогу.

Примусове переривання: TCAP-користувач завершує діалог через помилку і посилає повідомлення "abort" (примусове переривання) іншому абоненту. У повідомлення "abort" може також включатися інформація про причину переривання діалогу.

3.3 Адресація сигнальних одиниць

Кожному пункту сигналізації в мережі сигналізації призначається унікальний код. Підсистема передачі повідомлень використовує цей код для маршрутизації повідомлень.

Код пункту призначення в сигнальної одиниці повідомлення визначає пункт сигналізації, в який повинно бути передано це повідомлення.

Код вихідного пункту вказує, з якого пункту сигналізації передано повідомлення. Вміст поля вибору ланки сигналізації визначає маршрут сигналізації, за яким має передаватися повідомлення. Таким чином, поле вибору ланки сигналізації використовується на ланках сигналізації для поділу навантаження між двома пунктами сигналізації.

Октет службової інформації (SIO) містить додаткову інформацію про адресу. За допомогою індикатора послуги, цільова підсистема передачі повідомлень визначає підсистему користувача, для якої призначено повідомлення.

Національні коди пунктів визначають вузли в межах національної мережі, а міжнародні коди пунктів ідентифікують вузли в межах міжнародної телефонної мережі. У всьому світі в вузлах, які є частиною міжнародної сигнальної мережі, використовуються коди пунктів ITU-T ISPC.

3.4 Процес підключення абонента до мережі під час роумінгу

Роумінг – це послуга, що дозволяє абонентам здійснювати дзвінки, користуватися послугою передачі даних, що надаються оператором, перебуваючи в мережах інших операторів, в тому числі і зарубіжних, з якими оператор абонента має роумінг-угоду. При цьому номер телефону абонента залишається незмінним.

Перша дія, яке відбувається при спробі зареєструватися в мережі оператора-партнера – це перевірка абонента на «валідність». Цим займається VLR/MSC, в зоні дії якого знаходиться абонент. Після отримання службової команди

«UpdateLocation» та IMSI від абонента, VLR/MSC відправляє за допомогою підсистеми MAP повідомлення «SendAuthenticationInfo» до HLR; HLR в свою чергу перевіряє, що абонент і отриманий IMSI дійсні.

Після цієї перевірки VLR/MSC відправляє на домашній HLR повідомлення «UpdateLocation». Це повідомлення відправляється для того, щоб в HRL була інформація, в зоні дії якого VLR/MSC знаходиться його абонент. Повідомлення «UpdateLocation» містить в собі IMSI абонента і ідентифікатор VLR/MSC . HLR, отримавши дані, перевірить, чи підключена послуга роумінг. Якщо у абонента немає заборони, то HLR видалить профіль абонента з того VLR/MSC , де був абонент зареєстрований до цієї процедури, відправивши повідомлення «CancelLocation». Також HLR за допомогою повідомлення «InsertSubscriberData» пересилає профіль абонента на запитав цю інформацію VLR/MSC. Після того як VLR/MSC отримає цю інформацію, запит «Updatelocation» буде завершено, і HLR збереже у себе в профілі абонента адресу VLR/MSC, що відправив запит «UpdateLocation». При надходженні виклику або SMS в HLR є інформація, якому VLR/MSC направити його.

Після цих процедур абонент вважається зареєстрованим в мережі, тобто він може здійснювати і приймати виклики, SMS, користуватися додатковими послугами[22].

Якщо проаналізувати роботу підсистем ЗКС-7 та зіставити їх з базовою еталонною моделлю взаємодії відкритих систем (моделлю OSI), як це показано на Рисунку 3.2, то можна зрозуміти, що в підсистемах ЗКС-7 п’ятий (сеансовий) рівень лише частково представлений підсистемою ISUP, що виконує функції сигналізації в цифровій мережі інтегрального обслуговування. Але ця підсистема не виконує завдання автентифікації абонентів, що є вразливістю протоколів ЗКС-7.

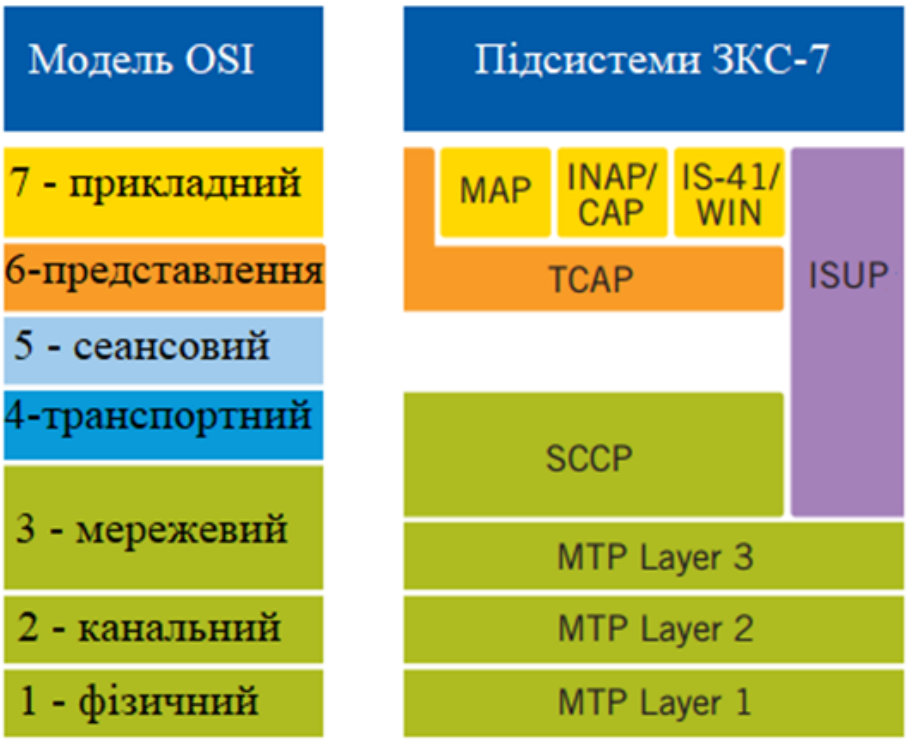


Рис. 3.2 – Співставлення моделі OSI та підсистем ЗКС-7

3.5 Модель зловмисника

Уразливості протоколів ЗКС-7 дозволяють зовнішньому зловмисникові навіть з невисокою кваліфікацією проникати в мережу та проводити серйозні атаки, результатом яких може бути викрадення коштів з рахунків абонентів, витік конфіденційних даних абонентів, перехват SMS, прослуховування дхвінків та порушення доступності абонентів чи елементів мережі.

Зловмисником може бути людина або група людей з кваліфікацією, достатньою для побудови вузла, що емулює роботу оператора стільникового зв’язку. Для доступу до мережі ЗКС-7 зловмисники можуть придбати на чорному ринку підключення у існуючого оператора або отримати дозвіл на діяльність в якості оператора зв’язку в країнах з лояльним законодавством у сфері регулювання зв’язку.

Так в 2017 році німецька газета Süddeutsche Zeitung оприлюднила статтю[17], в якій було підняте питання безпеки банківських операцій, що використовують SMS-автентифікацію. Виявилось, що доступ до комутатора ЗКС-7 можна придбати всього за 1000 євро, а за допомогою корупційних схем в країнах «третього світу» можна дістати ліцензію мобільного оператора.

Якщо учасник хакерської групи працює технічним фахівцем в компанії - операторі зв'язку, то у нього також є можливість забезпечити підключення свого обладнання до мережі ЗКС-7. Технічному фахівця для здійснення деяких атак досить скористатися легітимним набором функцій існуючого обладнання мережі зв'язку.

Існує також можливість проникнути в мережу оператора через зламані прикордонний пристрій, наприклад, GGSN вузол, що забезпечує маршрутизацію даних між GPRS Core network (GTP) та зовнішніми IP-мережами.

Цілями зловмисника можуть бути:

- реалізація шахрайських схем,
- отримання конфіденційних даних абонентів,
- порушення роботи окремих елементів або всієї мережі.

3.5 Огляд атак на стек протоколів ЗКС-7:

Загальні особливості атак на стек протоколів ЗКС-7:

- зловмисникам не потрібне складне устаткування: достатньо ПК на базі ОС сімейства Linux з встановленим SDK для формування пакетів ЗКС-7;
- зловмисник, який успішно здійснив одну з атак, може провести інші атаки тими ж засобами. Наприклад, якщо зловмисник зміг визначати місце розташування абонента, то йому залишилося виконати лише декілька простих дій, щоб отримувати можливість перехоплювати SMS;
- атаки базуються на легітимних командних повідомленнях мережі, тому не можна просто відфільтрувати їх, оскільки це може мати негативний вплив на весь сервіс.

Атаки на телефонні мережі, що створені на основі протоколів ЗКС-7, використовують особливість сучасних телефонних мереж — мобільності абонентів. По-перше, місцезнаходження абонента завжди повинно відслідковуватись для встановлення з'єднання. Саме ця інформація може бути об'єктом атаки. По-друге, мобільність абонента передбачає можливість здійснення дзвінків у будь-якій точці світу за допомогою роумінгу.

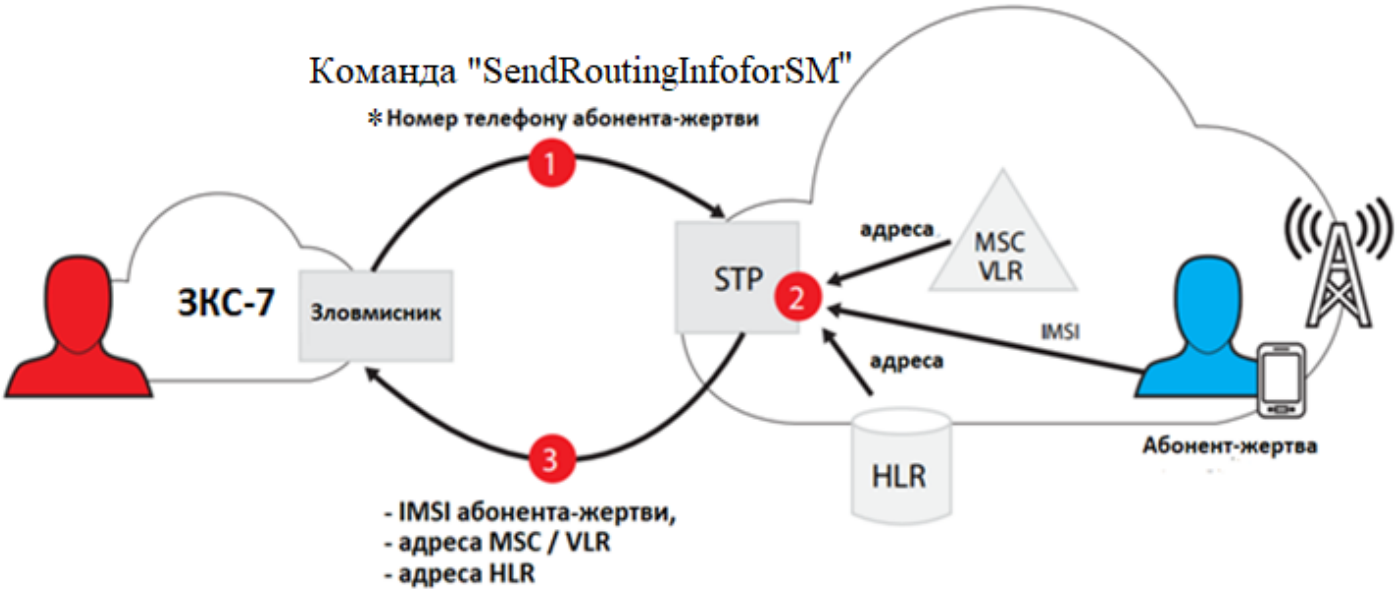
Взаємодія між мережевими підсистемами оператора здійснюється за допомогою стандартизованих запитів. ТМЗК, до якої підключені майже всі світові оператори, базується на протоколах ЗКС-7. Тому запити можуть бути відправлені з будь-якої країни світу. А неправильні налаштування фільтрація запитів можуть призвести до порушення роботи роумінгу.

Далі в роботі будуть розглянуті атаки, що використовують тільки вразливість стеку протоколів ЗКС-7 та інформацію з відкритих джерел. Хоча існують комбінації атак на ЗКС-7 із застосуванням шкідливого ПЗ та/чи соціальної інженерії. Наприклад, ідентифікатор IMSI можна дізнатись за допомогою шкідливого ПЗ.

Атака «Розкриття ідентифікатора IMSI»

Мета атаки: дослідження мережі оператора на можливість проникнення, отримання даних про абонентів.

Опис атаки. Зловмисник підключається до сигнальної мережі ЗКС-7 за допомогою спеціального комутатору та комп'ютера на базі ОС Linux і відправляє



службову команду «SendRoutingInfoforSM» в мережевий канал, вказуючи номер телефону абонента-жертви в якості параметра. Домашня мережа, в якій зареєстрований абонент-жертва, відправляє у відповідь на запит: IMSI жертви та адресу MSC/VLR та HLR[20]. Схема атаки зображена на рис. 3.3.

Рис. 3.3 – Схема атаки з розкриття ідентифікатора IMSI

Результат. У разі успішної атаки зловмисник отримує наступну інформацію:

- IMSI абонента,
- адреса MSC/VLR , який обслуговує абонента,
- адреса HLR (БД), в якому зберігається підписка абонента.

За адресою MSC/VLR можна визначити місце розташування абонента, як правило, з невисокою точністю, але отримані дані зловмисник може використовувати в більш складних атаках, опис яких наводиться далі.

Атака «Розкриття місцезнаходження абонента»

Мета: визначення місцезнаходження абонента телефонної мережі.

Опис. Атака заснована на легітимному запиті місцеположення абонента. Зловмисник відправляє службову команду «ProvideSubscribeInfo», вказуючи в якості параметра IMSI абонента. Цей запит адресований MSC/VLR, до якого підключений абоент-жертва. Дані для цієї атаки можна отримати в результаті проведення атаки «Розкриття ідентифікатора IMSI».

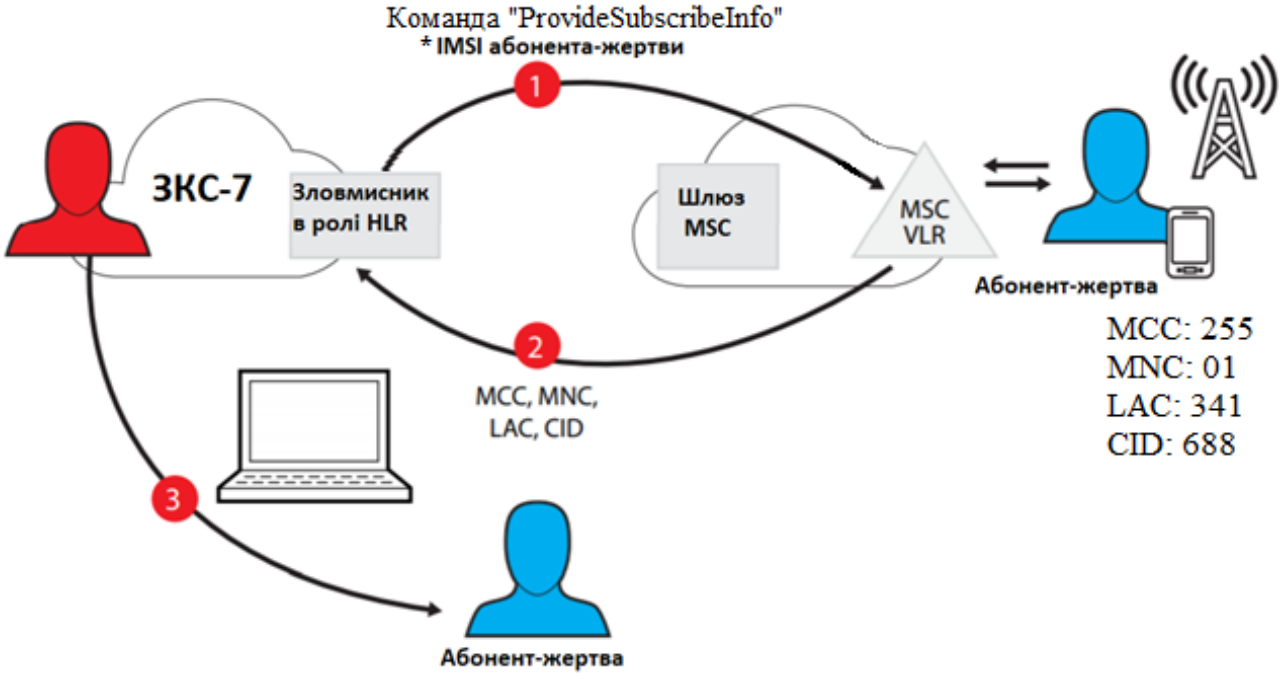


Рис. 3.4 – Схема атаки з визначення місцезнаходження абонента

Результат. Зловмисник отримує глобальний ідентіфікатор Cell Global Identity, який складається з чотирьох параметрів:

- Mobile Country Code,
- Mobile Network Code,
- Location Area Code,
- Cell Identity.

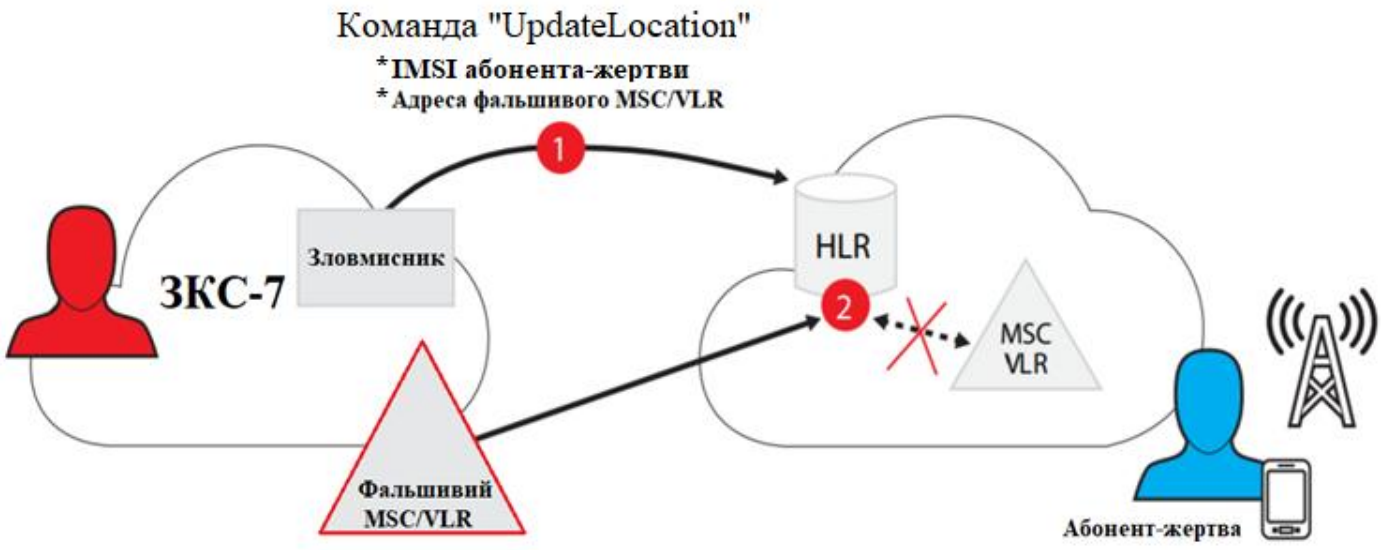
В мережі Інтернет є ряд загальнодоступних сервісів, які за вказаними ідентифікаторами визначають місцерозташування базової станції на карті місцевості. В умовах міської забудови точність визначення положення абонента складе кілька сотень метрів.

Атака «Порушення доступності абонента»

Мета: підключити абонента до фальшиво центру комутації, щоб унеможливити отримування ним дзвінків та SMS-повідомлень.

Опис. В основі атаки лежить підробка процесу реєстрації абонента в MSC/VLR. Така реєстрація може відбуватись, якщо абонент виїде за кордон та захоче підключитися до мережі роумінг-партнера.

Під час атаки зловмисник відправляє службова команда «UpdateLocation» адресовану HLR, що обслуговує абонента-жертву. В якості параметрів він вказує IMSI та адресу «фальшивого» MSC/VLR. Дані для цієї атаки можна отримати в результаті успішного проведення атаки «Розкриття ідентифікатора IMSI». Схема



атаки зображена на рис. 3.5.

Рис. 3.5 – Схема атаки з порушення доступності абонента

Результат. Абонент-жертва перестане отримувати вхідні дзвінки та SMS-повідомлення, при цьому телефон абонента буде показувати, що він знаходиться в зоні дії мережі. Абонент буде недоступний, поки він не переміститься в зону дії іншого MSC/VLR , не перевазантаже телефону або не зробе вихідний виклик.

Атака «Перехоплення вхідних SMS-повідомлень»

Мета: перехоплення вхідних SMS мобільного абонента

Опис. Атака є продовженням атаки «Порушення доступності абонента» і не вимагає додаткових дій з боку зловмисника. Схема атаки зображена на рис. 3.6.

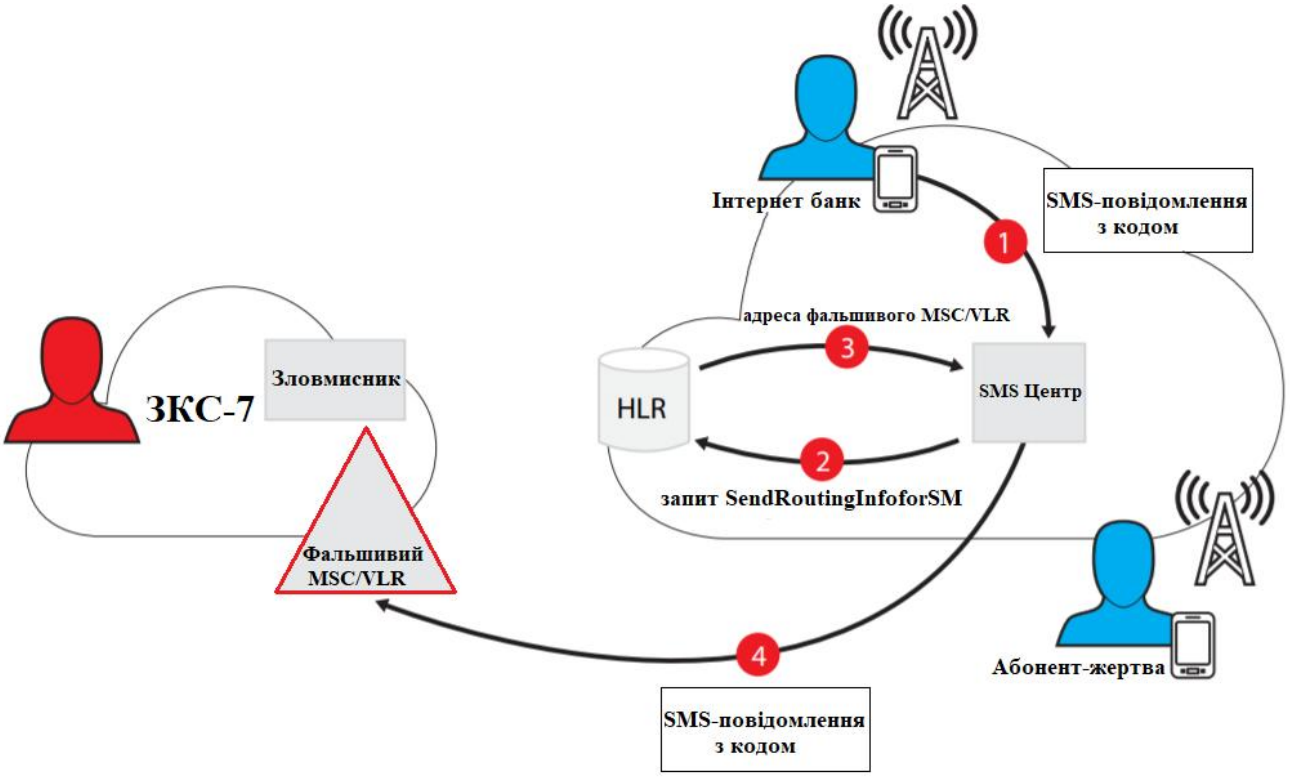


Рис. 3.6 – Схема атаки з перехоплення SMS -повідомлення

Результат. Після проведення реєстрації абонента-жертви на «фальшивому» MSC/VLR всі вхідні SMS-повідомлення будуть приходити на вузол зловмисника.

Зловмисник може:

- надіслати підтвердження про отримання SMS-повідомлення (SMS-центр буде вважати, що повідомлення доставлено);
- не відправляти звіт про отримання та зареєструвати абонента на початковий комутатор (через декілька хвилин SMS-повідомлення буде повторно надіслано абонту-жертві);
- надіслати підтвердження про отримання SMS-повідомлення SMS-центру, а абоненту жертві відправити підроблене SMS-повідомлення.

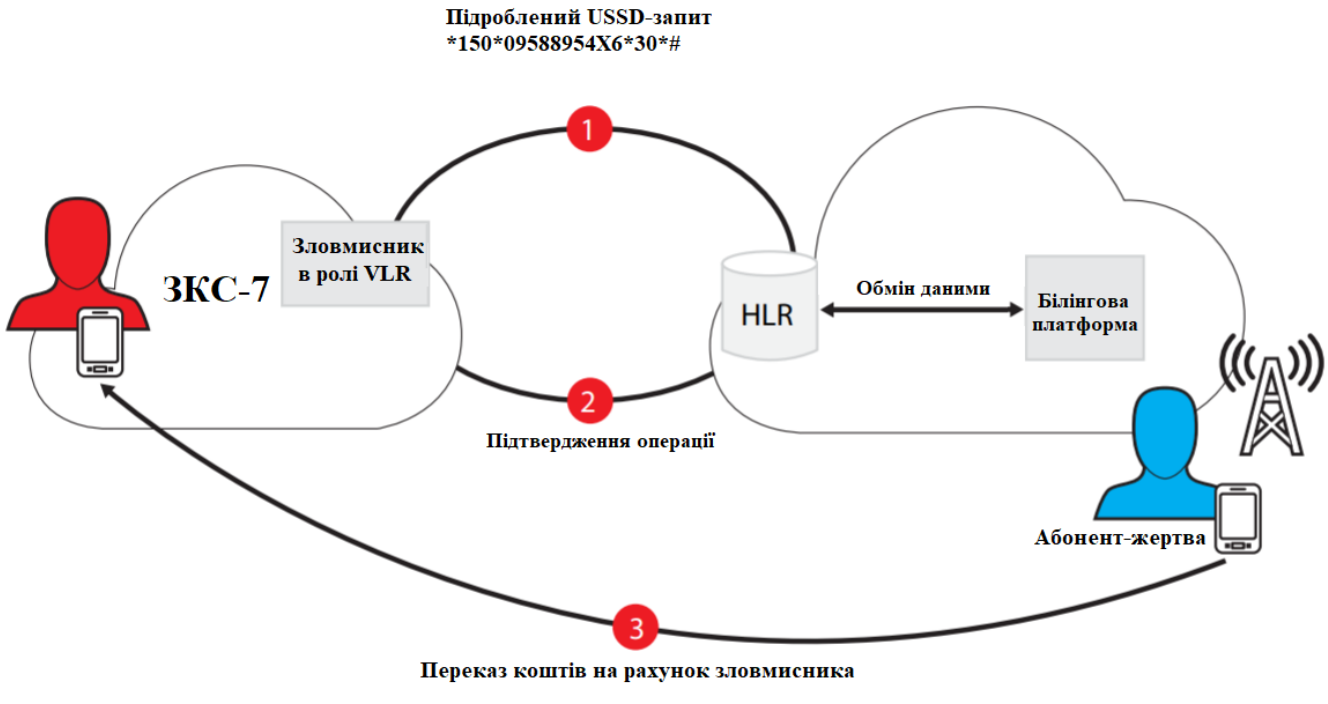
Дана атака може бути використана для:

- перехоплення одноразових паролів мобільного банку,
- перехоплення коду для відновлення паролів від інтернет-сервісів (елетронної пошти, соціальних мереж),
- отримання паролів для входу в особистий кабінет на сайті мобільного оператора (My Vodaphone, Мой Киевстар).

Атака «Підробка USSD-запиту»

Мета: відправка USSD-запиту до HLR від імені абоненту.

Опис. Атака базується на підробці легітимного службого повідомлення «ProcessUnstructuredSS-Request», який VLR відсилає до HLR під час USSD-запиту абонента. Вихідними даними є телефонний номер абонента, адреса HLR і рядок самого USSD-запиту. Телефонний номер, як правило, відомий з самого початку, адресу HLR можна отримати в результаті успішної атаки «Розкриття



ідентифікатора IMSI», опис USS-запитів можна знайти на сайті оператора. Схема атаки зображена на рис. 3.7.

Рис. 3.7 – Схема атаки з підробкою з USSD-запиту

Результат. Найбільш небезпечним варіантом реалізації цієї атаки є підробка запиту на переказ коштів між рахунками абонентів. Якщо при знятті коштів з рахунку абонента оператор надсилає сповіщення за допомогою SMS-повідомлення, то проведення даної атаки спільно з атакою «Перехоплення вхідних SMS-повідомлень» дає зловмиснику можливість залишитися непоміченим.

Атака «Редагування профілю абонента в базі даних VLR»

Мета: редагування профілю абонента в базі даних VLR здійснюється для зміни тарифу чи підключення/відключення додаткових послуг

Опис. Під час підключення абонента до нового MSC дані його профіля копіюється з бази даних HLR в базу даних VLR . Зловмисник може призвести відправку в VLR фальшивого профілю абонента. Зловмисник в ролі HLR відправляє службову команду «InsertSubscriberData» вказуючи в якості параметра: IMSI абонента, його телефонний номер, відредагований профіль та адресу VLR. Телефонний номер, як правило, відомий з самого початку, адресу HLR та IMSI абонента можна отримати в результаті успішної атаки «Розкриття ідентифікатора IMSI». Схема атаки зображена на рис. 3.8.

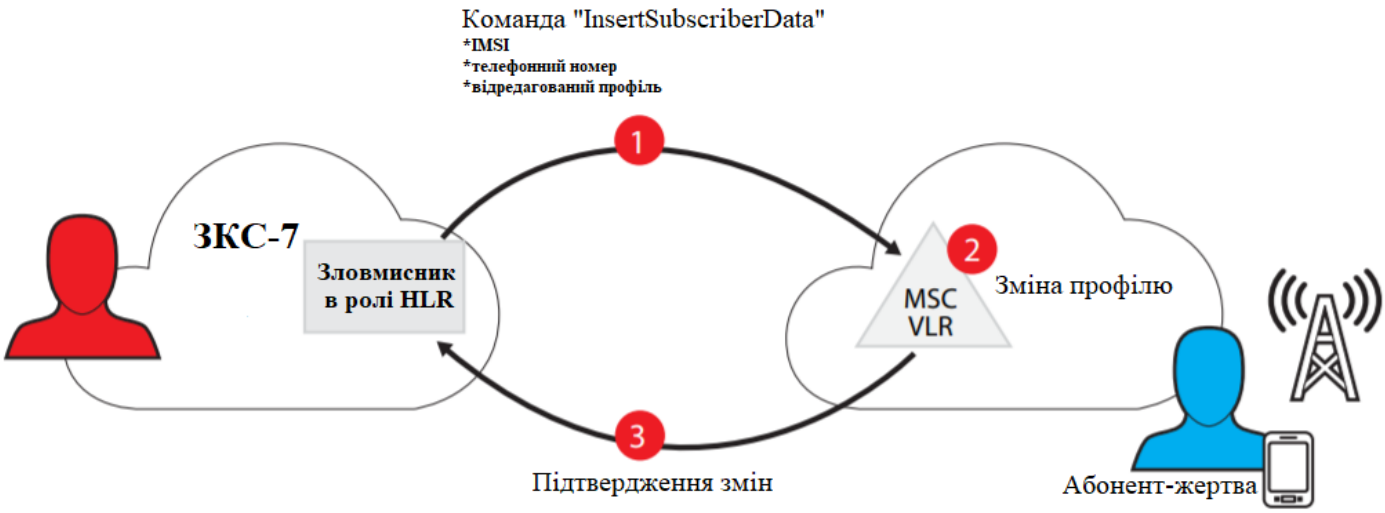


Рис. 3.8 – Схема атаки з редагування профілю абонента в базі даних VLR

Результат. Відреагувавши профіль абонента в базі VLR, зловмисник може здійснювати безкоштовні дзвінки, відключати/підключати додаткові посуги, наприклад, послугу оператора Vodaphone «ЗнайДе», що створена для пошуку місцезнаходження абонента іншим абонентом за допомогою USSD-запиту.

Висновок за розділом 3

В розділі 3 було проаналізовано роботу підсистем ЗКС-7 та розглянуто процес підключення абонентів до мережі в роумінгу. Недосконаліть процесу автентифікації абонентів, що відсилають службові запити до мережі, може бути використана для проведення атак, націлених на перехоплення SMS-повідомлень, підроблення USSD-запитів, редагування профілю абонента, встановлення його місцезнаходження. В розділі були наведені приклади таких атак.

4. ВДОСКОНАЛЕННЯ ЗАСОБІВ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ ТЕЛЕФОННИХ МЕРЕЖ

4.1 Методи захисту телефонних мереж

Існують наступні методи захисту телефонних мереж створених на базі протоколів ЗКС-7:

- фільтрування трафіку,
- контроль доступу до мережі,
- моніторинг та аудит мережі,
- приховування ідентифікатора абонента.

Фільтрування трафіку передбачає блокування неправомірних службових запитів згідно вставлених правил.

Контроль доступу до мережі передбачає аналіз та ведення журналів запитів до телефонної мережі.

Моніторинг та аудит – це процес постійного відстеження подій, які відбуваються в телефонній мережі. Моніторинг передбачає аналіз подій в режимі реального часу, а аудит - аналіз подій, що відбулися.

Кожен з цих методів реалізується апаратно-програмними засобами, які будуть розглянуті далі.

4.2 Мережеві екрани ЗКС-7

Мережеві екрани ЗКС-7 (англ. SS7 Firewall) – це апаратно-програмні комплекси, що виконують контроль зовнішнього ISUP-трафіку (збір інформації, модифікування і блокування підозрілих запитів із зазначенням причин відбою). Для визначення небажаного трафіку використовуються так звані «чорно-білі» списки.

Файерволи ЗКС-7 створені для блокування мережевих запитів в сторону вузлів сигнальної мережі оператора. Як правило, такі запити виконуються в сторону HLR з метою визначення MSC/VLR, що обслуговує абонента. Згідно досліджень компанії Enisa[21] мережеві екрани впроваджені приблизно у 28% операторів, що є досить низьким показником.

Схема роботи мережевого екрана показана на рис. 4.1.

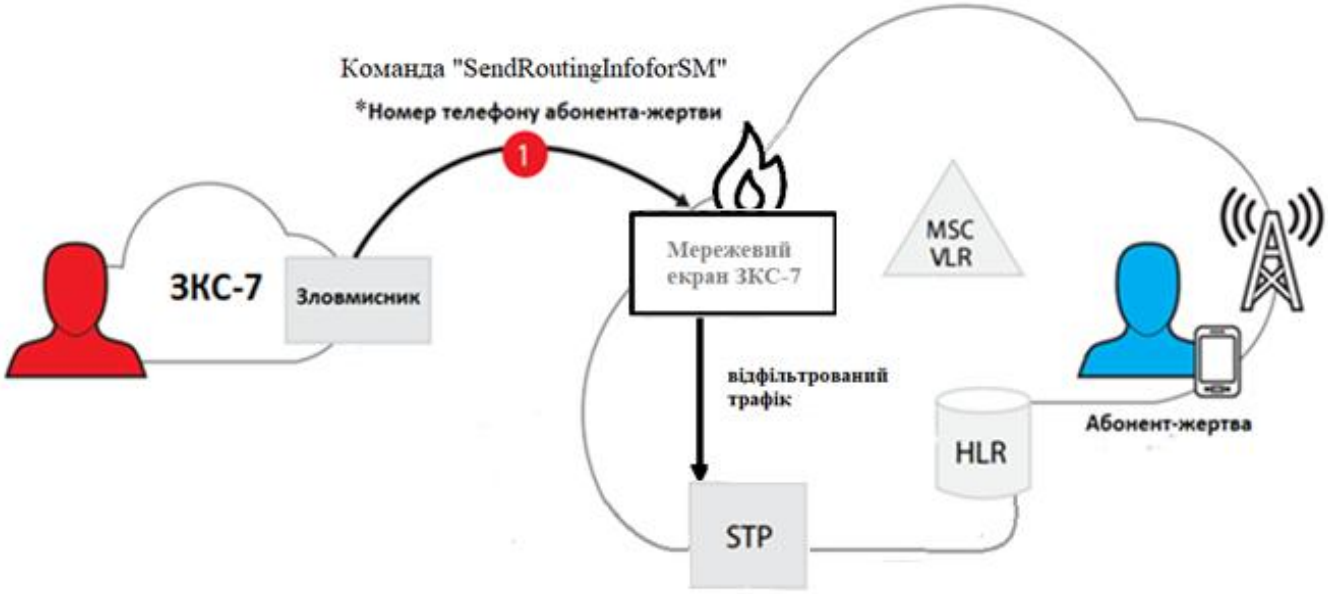


Рис. 4.1 – Схема роботи мережевого екрана ЗКС-7

Можна виділити наступні переваги мережевих екранів:

- Гнучке налаштування параметрів фільтрації. Можливість обробки тільки SMS-трафіку (в тому числі вихідного).
- В процесі впровадження структура мережі не зазнає істотних змін.
- Висока продуктивність і відмовостійкість системи.
- Підтримка роботи як в 2G/3G мереж, так і в CDMA.

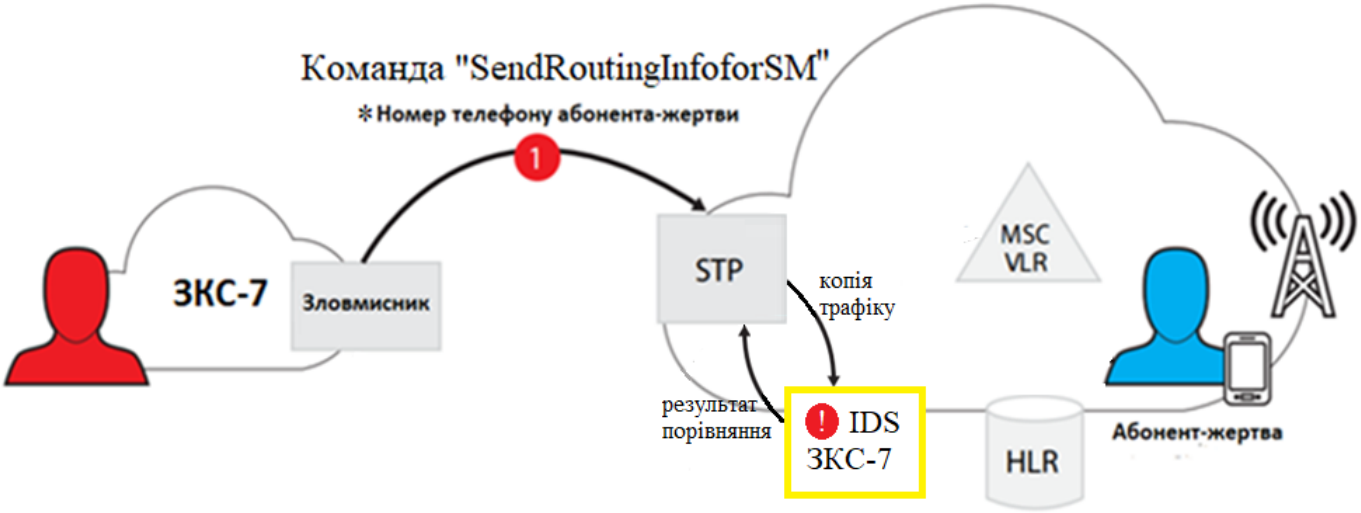
Але мережеві екрани мають і недоліки. Файерволи дозволяють захистити абонентів, що підключені до домашньої мережі. В той час як абоненти у роумінгу вразливі до атак: «Редагування профілю абонента в базі даних VLR», «Підробка USSD-запиту», «Порушення доступності абонента».

Крім того, помилкові налаштування файерволів можуть призвести до збоїв в роботі мережі та блокуванню трафіку.

4.3 Системи виявлення вторгнення ЗКС-7

Системи виявлення вторгнення ЗКС-7 (англ. Intrusion Detection System SS7) – це програмно-апаратнц комплекси, що створені для виявлення несанкціонованих запитів до телефонної мережі оператора.

Принцип роботи IDS полягає в тому, що комплекс бере копію сигнального трафіку STP, аналізує його по базі даних сигнатур та робить висновок про наявність атак чи нелегітимних дій. Схема роботи системи показана на Рисунку



4.2.

Рис. 4.2 – Схема роботи мережевого екрана ЗКС-7

Перевагою систем виявлення вторгнення є те, що вони не втручаються в абонентський трафік, оскільки IDS аналізує його копію. В разі виявлення загрози, дані про порушення записується в журнал подій, а на консоль адміністратора відправляється сигнал тривоги.

4.4 Системи моніторингу ЗКС-7

Системи моніторингу ЗКС-7 (англ. SS7 Protocol Analyzer) - це апаратно-програмні комплекси, що використовуються для аналізу трафіку мережі ЗКС-7 з

ціллю виявлення неправомірних дій. Згідно досліджень компанії Enisa[21] систему моніторингу використовують 69% операторів.

Перше покоління систем моніторингу було засновано на здатності станційних пристроїв формувати файли із записами про виклики (файли CDR). Даний функціонал досі використовується більшістю операторів зв'язку для абонентського білінгу і міжоператорських розрахунків. Проте, моніторинг, заснований на записах комутаційних станцій, має ряд недоліків:

- з інтерфейсу програмного забезпечення, встановленого на комутаційної станції, не завжди можна визначити маршрути і деталізацію проходження трафіку;
- комутаційні станції формують і враховують записи про виклики тільки в режимі реального часу. У разі збою або поломок станція перестає формувати записи в файлах. При цьому втрачається можливість дізнатися події, безпосередньо перед збоєм. Істотно ускладняється аналіз причини збоїв;
- у випадках, коли станція продовжує встановлювати з'єднання і передавати трафік, але припиняє формувати і враховувати записи про встановлення з'єднань, стає неможливою тарифікація з'єднань абонентів;
- формування файлів із записами про виклики є суттєвим навантаженням для обладнання. При пікових обсягах обслуговується телефонного трафіку станція припиняє забезпечення «непрофільних» процесів, до яких відноситься і формування файлів із записами про виклики. Тобто вона з'єднує абонентів, але на запис інформації про події потужності вже може не вистачити.

Друге покоління систем моніторингу засноване на використанні аналізатори, що підключаються до інтерфейсів комутаційних станцій або виділених каналах зв'язку. Такі аналізатори мали достатню обчислювальну потужність, щоб розбирати і записувати події, що відбуваються в рамках одного сигнального каналу, однак все ще не були здатні автоматично і в режимі реального часу зіставляти події, що відбуваються в різних точках мережі.

Третє покоління систем моніторингу відноситься до класу розподілених пасивних систем. Такі комплекси збирають і накопичують інформацію про події,

стан і активності станційного і канального устаткування, але робота йде за рахунок повністю пасивного збору даних, що не залежить від будь-якого обладнання мереж передачі. Крім того, такі системи моніторингу дозволяють встановлювати розподілену мережу датчиків даних і виробляти кореляції подій на різних ділянках. З огляду на засоби пасивного отримання даних, засоби моніторингу ні за яких умов не можуть вплинути на мережу оператора зв'язку. Що одночасно є перевагою і недоліком цих систем.

4.5 SMS Home Routing

Рішення SMS Home Routing являє собою апаратно-програмний комплекс, що використовуються для приховування реального IMSI абонента та адреси VLR/MSC, до якого він підключений, під час запиту «SendRoutingInfoForSM», що використовується для маршрутизації SMS-трафіку.

Згідно досліджень компанії Enisa[21] опитаних 87% операторів застосовують цю систему для захисту своїх мереж. Головним недоліком системи є те, що вона працює лише з SMS-трафіком. Як відомо IMSI абонента може бути розкрите не тільки під час запиту «SendRoutingInfoForSM». Схема роботи SMS Home Routing показана на рис. 4.3.

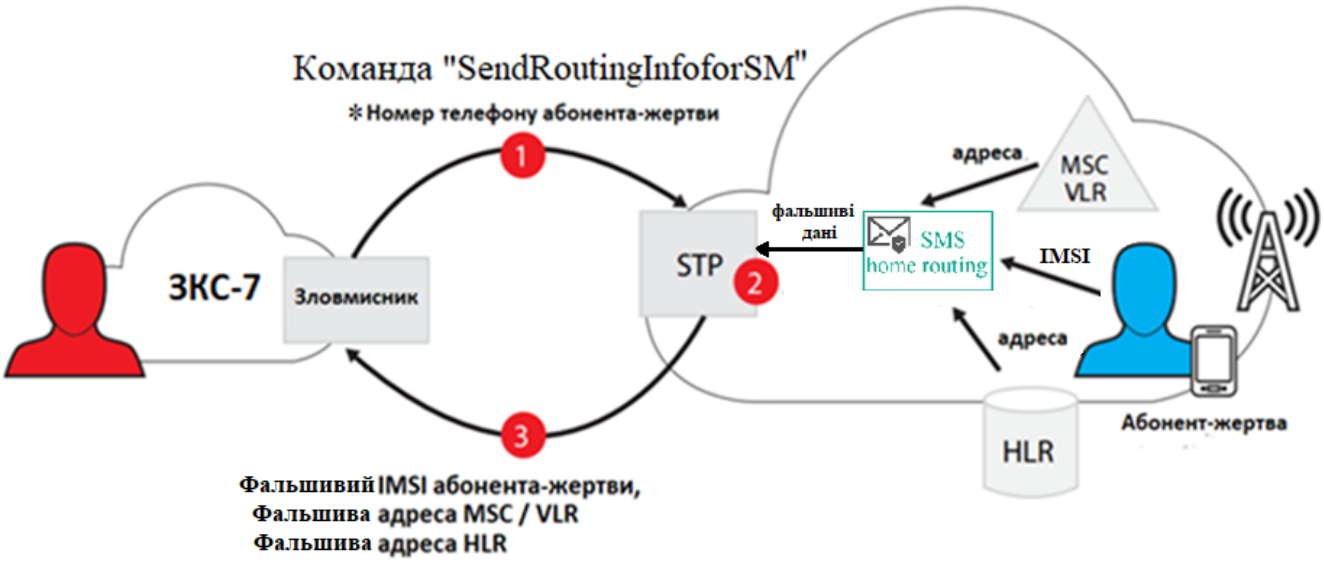


Рис. 4.3 – Схема роботи SMS Home Routing

4.6 Порівняння існуючих засобів захисту телефонних мереж

Засоби захисту телефонних мереж можна розділити на активні та пасивні. Активні засоби вносять зміни в абонентський трафік, в той час як пасивні лише виявляють несанкціоновані дії.

Було розглянуто частоту використання засобів серед телефонних операторів Європи[21]. Також було проаналізовано ефективність захисту мережі від різних типів атак існуючими засобами.

Порівняння засобів захисту телефонних мереж наведені в Таблиці 4.1.

Таблиця 4.1

Порівняння засобів захисту телефонних мереж

	Мережеві екрани	SMS Home Routing	IDS ЗКС-7	Системи моніторингу
Тип засобу захисту	Активний	Активний	пасивний	пасивний
Частота використання	28%	87%	49%	69%
Захист від підробки USSD-запитів	Частково	Ні	Частково	Ні
Захист від витоку IMSI	Частково	Частково	Частково	Ні
Захист від відключення абонентів від мережі	Ні	Ні	Ні	Частково
Захист SMS-трафіку	Частково	Так	Частково	Ні

4.6 Рекомендації щодо покращення засобів захисту

Вразливість протоколів ЗКС-7, що дозволяє здійснювати перехоплення SMS-повідомлень, може бути вирішена шляхом фільтрації небажаних повідомлень.

Однак не всі подібні повідомлення бувають небезпечними; при некоректному налаштуваннях фільтрації мережевих екранів ЗКС-7 з високою ймовірністю буде порушена робота легальних сервісів оператора.

Необхідно реалізувати фільтрацію таким чином, щоб блокувалися тільки повідомлення, які використовуються в рамках атак.

Тому мною запропоновано наступні рекомендації:

1. Розділити службові запити на 3 групи: небезпечні, підозрілі та інші.
2. До групи небезпечні запити віднести наступні запити: SendIMSI, SendRoutingInfoForLCS, AnyTimeInterrogation, Mt-ForwardSM, InsertSubscriberData.
3. Передбачити в налаштуваннях Мережевого екрану блокування запитів, що були віднесені до групи небезпечні.
4. До групи підозрілі запити віднести наступні запити: UpdateLocation, SendParameters, SendRoutingInfoForSM.
5. Передбачити в налаштуваннях Системи виявлення вторгнень детальну перевірку запитів від вузлів, що відсилають підозрілі запити.
6. Передбачити використання SMS Home Routing для захисту конфіденційності IMSI абонента та адреси мережевого обладнання оператора під час обміну SMS-трафіком між абонентами.
7. Проводити регулярний внутрішній аудит стану захищеності телефонної мережі. Під час нього аналізувати дані про стан мережі отримані від Системи моніторингу ЗКС-7.

Висновок за розділом 4

В розділі 4 було проаналізовано існуючі засоби захисту телефонних мереж створених на базі протоколів ЗКС-7, а саме мережевий екран ЗКС-7, система виявлення вторгнень ЗКС-7, Система моніторингу ЗКС-7. Була створена таблиця порівняння роботи цих засобів та частота їх використання телефонними операторами.

Були розроблені рекомендації щодо покращення засобів захисту телефонних мереж. В основі рекомендацій лежить комплексний підхід до безпеки телефонної мережі.

ВИСНОВКИ

В розділі 1 були розглянуті базові принципи телефонної комутації та процес її еволюції. Вже на початку розвитку телефонії існували загрози інформаційної безпеки. Ці загрози були одним з важливих факторів, які змушували вдосконалювати телефонні мережі. Так винахід першого автоматизованого телефонного комутатора пов'язаний з бажанням усунути людський фактор з процесу комутації. А однією з причин розробки загальноканальної сигналізації була загроза втручання в службові сигнали сигналізації по виділеному каналу.

Також в розділі було порушене питання модернізації застарілого обладнання оператором фіксованого зв'язку «Укртелеком».

В розділі 2 було з'ясовано, що законодавство України покладає на оператора відповідальність за створення та підтримку роботи захищеної телефонної мережі, але не визначає способи цього захисту. Оператори повинні самі обирати та впроваджувати необхідні рішення для захисту своїх мереж та інформації, що в них циркулює. Було встановлено, що для здійснення міжнародних дзвінків виклик повинен відповідати рекомендаціям Q.7xx, які розроблені ITU-T.

В розділі 3 було проаналізовано роботу підсистем ЗКС-7 та розглянуто процес підключення абонентів до мережі в роумінгу. Недосконаліть процесу автентифікації абонентів, що відсилають службові запити до мережі, може бути використана для проведення атак, націлених на перехоплення SMS-повідомлень, підроблення USSD-запитів, редагування профілю абонента, встановлення його місцезнаходження. В розділі були наведені приклади таких атак.

В розділі 4 було проаналізовано існуючі засоби захисту телефонних мереж створених на базі протоколів ЗКС-7, а саме мережевий екран ЗКС-7, система виявлення вторгнень ЗКС-7, Система моніторингу ЗКС-7. Була створена таблиця

порівняння роботи цих засобів та частота їх використання телефонними операторами.

Були розроблені рекомендації щодо покращення засобів захисту телефонних мереж. В основі рекомендацій лежить комплексний підхід до безпеки телефонної мережі.

Виходячи із поставленої мети дипломної роботи були виконані наступні завдання:

- проаналізовано принципи телефонної комутації;
- розглянуто нормативно-правові акти із сфери телекомунікації;
- досліджено дії зловмисників, що проникають в телефонну мережу;
- досліджено існуючі засоби захисту телефонних мереж створених на базі протоколів ЗКС-7;
- розроблено рекомендації щодо вдосконалення засобів захисту телефонних мереж створених на базі протоколів ЗКС-7.