

Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут інформатики та радіоелектроніки
Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, назва факультету)

Кафедра захисту інформації
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти (освітній ступінь))

на тему "Аналіз захищеності мереж мобільного зв'язку на основі технології SS7"

Виконав: студент 6 курсу, групи РТ-713м
спеціальності (напряму підготовки)
125 – Кібербезпека (Системи технічного
захисту інформації, автоматизація її
обробки)

(код і назва напряму підготовки, спеціальності)

Кошель О.А.

(прізвище та ініціали)

Керівник Романенко С.М.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

м.Запоріжжя
2018 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет
 (повне найменування вищого навчального закладу)

Інститут, факультет _____ **ІРЕ,**
ФРЕТ _____

Кафедра _____ захисту
 інформації _____

Ступінь вищої освіти (освітній ступінь) _____ магістр

Спеціальність _____ **125**
Кібербезпека _____

(код і назва)

Напрямок підготовки Системи технічного захисту інформації, автоматизація її
обробки

(код і назва)

ЗАТВЕРДЖУЮ
 Завідувач кафедри захисту
 інформації
проф., д.т.н., Карпуков

Л.М. _____

“ ”

_____ 20 ____ року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

_____ Кошелю Олександр
 Андрійовичу _____
 (прізвище, ім'я, по батькові)

1. Тема проекту (роботи) аналіз захищеності мереж мобільного зв'язку на
основі _____ технології
SS7 _____

керівник проекту (роботи) Романенко Сергій Миколайович, канд. фіз.-мат.
наук, доцент кафедри захисту
інформації _____
 (прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “7”
листопада 2018 року № 329

2. Строк подання студентом проекту (роботи) 4 грудня 2018 року

3. Вихідні дані до проекту (роботи) Архітектура мереж мобільного зв'язку GSM, специфікація стека протоколів SS7.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) вивчити стек протоколів SS7, вивчити підсистему MAP, знайти уразливості та можливі напрями атак на підсистему MAP, аналіз сучасних засобів захисту мереж мобільного зв'язку.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Схема реєстрація абонента в мережі мобільного зв'язку, схема здійснення вихідного дзвінка, схема надсилання SMS – повідомлення, атака на розкриття конофіденційного ідентифікатора абонента.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основний	Романенко С.М., доцент кафедри захисту інформації		
Охорона праці	Коробко О.В., старший викладач кафедри ОПНС		
Економічна частина	Левченко Н.М., проф. кафедри ПТБД		
Нормо- контроль	Нікуліщев Г.І., старший викладач кафедри захисту інформації		

7 . Д а т а в и д а ч і з а в д а н н я _ _ _ _ _ 5
ЖОВТНЯ _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з літературою	05.10-08.10	
2	Вивчення стеку протоколів SS7	09.10-17.10	
3	Вивчення підсистеми MAP	18.10-23.10	
4	Складання профілю зловмисника	24.10-28.10	
5	Можливі атаки на SS7	29.10-10.11	
6	Аналіз сучасних засобів захисту мобільних мереж	11.11-21.11	
7	Діагностика потреб інвестування досліджень з захищеності мереж мобільного зв'язку	22.11-24.11	
8	Охорона праці та безпека у надзвичайних ситуаціях	25.11-26.11	
9	Оформлення пояснювальної записки	27.11-30.11	

Студент _____

 ініціали)

(підпис)

(прізвище та

Керівник проекту (роботи) _____

(підпис)

(прізвище та ініціали)

РЕФЕРАТ

ПЗ: 94с., 35 рисунків, 5 таблиць, 20 джерел.

Об'єкт дослідження – мережі мобільного зв'язку на основі технології SS7.

Мета роботи – дослідження та аналіз можливих потенційних атак і сучасних засобів захисту мереж мобільного зв'язку на основі технології SS7.

Метод дослідження – моделювання можливих потенційних атак на мережі мобільного зв'язку на основі технології SS7.

У роботі вивчається стек протоколів SS7, та історія розвитку сигнальної мережі. Вивчаються основні блоки та ланки з яких складається мережа. Вивчається архітектура стека протоколів SS7 та призначення кожної з підсистем архітектури. Аналізується підсистема MAP. Вивчаються об'єкти мережі підсистеми та ідентифікатори. Складається профіль злоумисників. Аналізуються можливі потенційні атаки та потенційно уразливі повідомлення примітиви, де описується їх призначення, відправники та отримувачі при нормальній поведінці в роботі. Представляються напрямки рішення проблем захищеності мереж мобільного зв'язку, представляються та аналізуються актуальні на сьогоднішній день засоби забезпечення безпеки мереж мобільного зв'язку.

МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ, СТЕК ПРОТОКОЛІВ SS7, ПІДСИСТЕМА MAP, АТАКИ, ПОВІДОМЛЕННЯ ПРИМІТИВИ, СУЧАСНІ ЗАСОБИ ЗАХИСТУ.

ЗМІСТ

Список скорочень	7
Вступ	8
1. Стек протоколів SS7	11
2. Підсистема MAP	16
3. Профіль зловмисника	23
4. Можливі потенційні атаки на мережі мобільного зв'язку	28
4.1. Атака на розкриття конфіденційного ідентифікатора абонента	32
4.2. Атака на розкриття інформації про розташування абонента	33
4.3. Атака на порушення доступності абонента	34
4.4. Атака на перехоплення вхідних SMS – повідомлень	35
4.5. Атака маніпуляцій з USSD – запитами	36
4.6. Атака на зміну профілю VLR	37
4.7. Атака на прослуховування вихідних викликів	38
4.8. Атака на перенаправлення вхідних викликів	39
4.9. Атака на відмову в обслуговуванні для вхідних викликів	40
1. Потенційно уразливі повідомлення примітиви	41
5. Аналіз сучасних засобів захисту мобільних мереж	52
6. Діагностика потреб інвестування досліджень з захищеності мереж мобільного зв'язку на основі технології SS7	64
6.1. Загальні положення	64

6.2.Короткий опис аналізу	65
6.3.Визначення вартості аналізу	65
6.3.1. Основна заробітна плата виконавців, єдиний соціальний внесок, непрямі витрати.....	66
6.3.2. Витрати на матеріал	68
6.3.3. Витрати на послуги сторонніх організацій	69
6.3.4. Витрати на утримання, експлуатацію та амортизацію обладнання	69
6.3.5. Загальний кошторис витрат на аналіз	72
6.4.Економічна оцінка роботи	73
6.5.Висновок по главі шість	73
7. Охорона праці та безпека у надзвичайних ситуаціях	74
7.1.Аналіз потенційних небезпек	74
7.2.Заходи забезпечення безпеки	75
7.3.Заходи щодо виробничої санітарії та гігієни праці.....	76
7.4.Заходи з пожежної безпеки	84
7.5.Заходи забезпечення безпеки у надзвичайних ситуаціях	86
Висновки	92
Список використаних джерел	93

СПИСОК СКОРОЧЕНЬ

- BSS - Base Station Subsystem - система базових станцій
- GGSN - Gateway GPRS Support Node – шлюзовий вузол підтримки GPRS
- GMSC - Gateway Mobile Switching Center - шлюзовий комутатор мобільної мережі
- GSMSCF - GSM Service Control Function - вузол управління послугами GSM
- HLR - Home Location Register - домашній реєстр місцеположення
- IMSI - International Mobile Subscriber Identity - міжнародний ідентифікатор мобільного абонента
- MSC - Mobile Switching Center - комутатор мереж мобільного зв'язку
- MSISDN - Mobile Station ISDN Number - номер мобільної станції
- MSRN - Mobile Station Roaming Number - роумінговий номер мобільної станції
- SGSN - Serving GPRS Support Node - вузол обслуговування абонентів пакетної мережі передачі даних
- SMS - C - Short Message Service Centre - центр коротких повідомлень
- STP - Signal Transfer Point - сигнальний комутатор
- VLR - Visitor Location Register - гостьовий реєстр місцеположення
- ПК - персональний комп'ютер

ВСТУП

На сьогоднішній день мережі мобільного зв'язку займають найактивнішу частину критично важливої інформаційної структури і є ключовим інструментом у багатьох сферах життя суспільства, починаючи від управління банківськими рахунками і закінчуючи переговорами на рівні лідерів світових держав. Незважаючи на твердження про захищеність мобільного зв'язку, ми часто можемо спостерігати цілком протилежні приклади: все частіше за останні роки в інтернеті публікуються записи приватних телефонних розмов людей, чий статус зазвичай асоціюється з підвищеними заходами безпеки.

В якості відповідей на ці витoki інформації часто висуваються версії про сучасних, складних і дорогих технологіях прослуховування, які можуть використовуватися тільки спецслужбами. Дана точка зору належить людям, які представляють мобільний зв'язок, як набір найсучасніших найбільш захищених технологій. А саме таку картину і створює реклама сучасних пристроїв і послуг. Насправді ж телекомунікаційна мережа являє собою складну систему з безліччю підсистем різного технологічного рівня. У таких випадках рівень безпеки всієї мережі визначається рівнем найслабшої ланки.

У мобільних мережах, процес встановлення голосових викликів досі заснований на технології ЗКС 7 (Загальний канал сигналізації # 7) або як кажуть в Європі про SS7 (Signaling System # 7), яка була створена в 70-і роки минулого століття.

У сучасних мережах зв'язку SS7 позиціонується як система, що дозволяє станціям з програмним управлінням, мережевим базам даних і іншим вузлам обмінюватися повідомленнями, що відносяться до процесів встановлення, підтримки і роз'єднання з'єднань, а також інформацією, необхідною для виконання розподілених прикладних процесів і управління мережевими ресурсами.

До 60-х службові команди для з'єднання абонентів і доставки інформаційних пакетів передавалися по розмовному каналу. Такий підхід був неефективним [17]. А основна безпека протоколів в ті часи ґрунтувалася на захисті вузлів і каналів зв'язку. З метою усунення недоліків і з деяких інших причин виникла потреба в розробці нової системи в класі систем сигналізації по загальному каналу. В кінці 70-х роках була розроблена технологія SS7. Це був прорив в плані безпеки, тому що для сигналізації, тобто для передачі службових команд під час встановлення телефонного з'єднання, став використовуватися окремий канал, фізично недоступний абоненту [6]. Отже, і отримання доступу до мережі SS7 за коштами несанкціонованого окремого вузла була нездійсненна.

Розроблена в 70-х роках минулого століття система містить певні недоліки в плані захищеності, а саме відсутнє шифрування і перевірка справжності сервісних повідомлень. Довгий час це не представляло небезпеки ні для абонентів, ні для операторів, - мережа SS7 була замкнутою системою, в яку підключалися тільки оператори фіксованого зв'язку. Однак науковий прогрес не стоїть на місці, і мережа еволюціонувала для підтримки потреб мобільного зв'язку і надання додаткових послуг. На початку 2000-х років була запропонована специфікація SIGTRAN (Signaling Transport), що дозволяє передавати службову інформацію SS7 по IP-мережі [6]. Сигнальна мережа перестала бути ізольованою. При цьому збереглася і передалася вся слабкість безпеки верхніх рівнів протоколів SS7, адже їх розробники виходили з того, що до сигнального каналу ніхто фізично не добереться, тому визнали недоцільним все ускладнювати. В результаті чого зловмисники мають можливість безконтрольно створювати, надсилати, перехоплювати і змінювати повідомлення протоколів SS7, здійснюючи різні атаки не тільки на мобільні мережі та їх абонентів, але й також на користувачів швидкозростаючої промисловості IoT (Internet of Thing) - пристроїв. Які використовуються не тільки вдома, а й у виробництві, добувній промисловості, енергетиці та в життєво важливих системах міста, як

світлофори, дороги. В яких людина приймає мінімальну участь в роботі. В такому випадку компрометація навіть одного з пристроїв може привести к дуже серйозним непередбаченим наслідкам.

1 СТЕК ПРОТОКОЛІВ SS7

Стек протоколів SS7 або Signaling System No. 7 (сигнальна система №7) — набір сигнальних телефонних протоколів, позиціонується як система, що дозволяє станціям з програмним управлінням, мережевим базам даних і іншим вузлам обмінюватися повідомленнями, що відносяться до процесів встановлення, підтримки і роз'єднання з'єднань, а також інформацією, необхідною для виконання розподілених прикладних процесів і управління мережевими ресурсами. У Європі систему зазвичай називають SS7, в Росії вона відома як ОКС-7, а в Північній Америці називають CCS7 [7].

Стек протоколів SS7 розроблявся фірмою AT&T, починаючи з 1975 року, і був визначений як стандарт Міжнародним союзом електрозв'язку в 1981 році у вигляді рекомендацій серії Q.7xx. SS7 був призначений, щоб замінити системи сигналізації SS5, SS6 і R2, які раніше використовувалися в усьому світі як стандарти, визначені ITU (International Telecommunication Union) [7].

SS7 замінив SS6, SS-5 і R5, за винятком деяких варіантів R2, які іноді використовуються. SS-5 і більш ранні версії використовували принцип сигналізації в лінії, де інформація, необхідна для з'єднання, передавалася спеціальними тонами у телефонній лінії. Такий тип сигналізації створював вразливість в безпеці протоколу, оскільки зломисник міг емулювати набір службових тонів своїм абонентським пристроєм. Фахівці, яких називають фрікерами, експериментували з телефонними станціями, посилаючи їм нестандартні сигнальні тони за допомогою маленьких електронних приладів, які називаються BlueBox [7].

SS7 представляє універсальну структуру для організації сигналізації, повідомлень, мережевої взаємодії і технічного обслуговування телефонної мережі. Починаючи з установки з'єднання, протокол працює для обміну користувальницької інформації, маршрутизації дзвінків, взаємодії з білінгом і підтримки інтелектуальних послуг [7].

В процесі зміни технології і для збереження її функціональної гнучкості з'явилася концепція розділених сервісних рівнів, реалізована в інтелектуальних телефонних мережах. Сервіс, який надає інтелектуальна мережа - це послуга перетворення телефонного номера (наприклад, коли безкоштовний номер перетвориться в звичайний абонентський номер телефонної мережі загального користування). Іншими послугами інтелектуальної мережі - є автоматичне визначення номера абонента, блокування номерів абонентів, автоматична переадресація виклику (дзвінка), утримання виклику (дзвінка), конференція, передплачені дзвінки. Різні постачальники обладнання надають різні сервіси для абонентів. SS7 також важливий при стикуванні VoIP-мереж і телефонної мережі загального користування [7].

Мережа SS7 складається з декількох типів ланок (A, B / D, C, E, і F) і трьох типів пунктів - пункти комутації SSP (Service Switching Point), пункти передачі сигналізації STP (Signal Transfer Point) і пункти контролю сигналізації SCP (Service Control Point) [8].

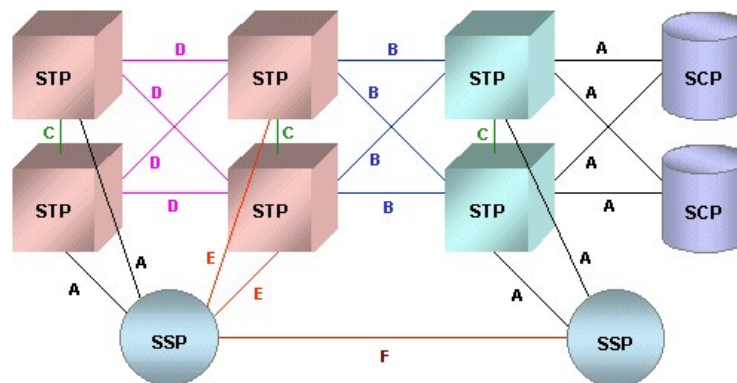


Рисунок 1.1 - Схема пунктів сигналізації та типів ланок

Ланки типу А (access, «доступ») - з'єднують STP з SSP або з SCP. Використовуються для доставки сигнальних повідомлень до або від кінцевих пунктів сигналізації, можуть так само доставляти і до початкового пункту сигналізації.

Ланки типу B/D (bridge «міст», diagonal «діагональ») - об'єднуються в дві з'єднані пари STP. Використовуються для перенесення сигнальних повідомлень від початкової точки входу в сигнальну мережу до місця призначення.

Ланки типу C (cross «перехресні») - з'єднують взаємопов'язані STP. Призначені підвищувати надійність мережі, якщо одне або кілька ланок недоступні.

Ланки типу E (extended «розширений») - підключають SSP до STP додатковим комплектом ланок до другої пари STP, вони являються розширеними і забезпечують резервну зв'язаність мережі.

Ланки типу F (fully associated «повністю асоційовані») - з'єднують два кінцевих пункту сигналізації.

Для ідентифікації кожного пункту, мережа SS7 визначає унікальний номер, який отримав назву код пункту сигналізації SPC (Signaling Point Code) [16].

Архітектура моделі протоколів SS7 має рівневу структуру, аналогічну моделі OSI (Open Systems Interconnection). На рисунку 1.2 представлена сучасна архітектура стека протоколів SS7 і показані її відповідності рівням моделі OSI. Частина стека протоколів SS7, відповідна першим трьом рівням моделі OSI - фізичного, канального і мережевого. Четвертий рівень стека протоколів відповідає прикладному рівню моделі OSI. Функції транспортного, сеансового і представницького рівнів в моделі SS7 не вимагають реалізації [16].

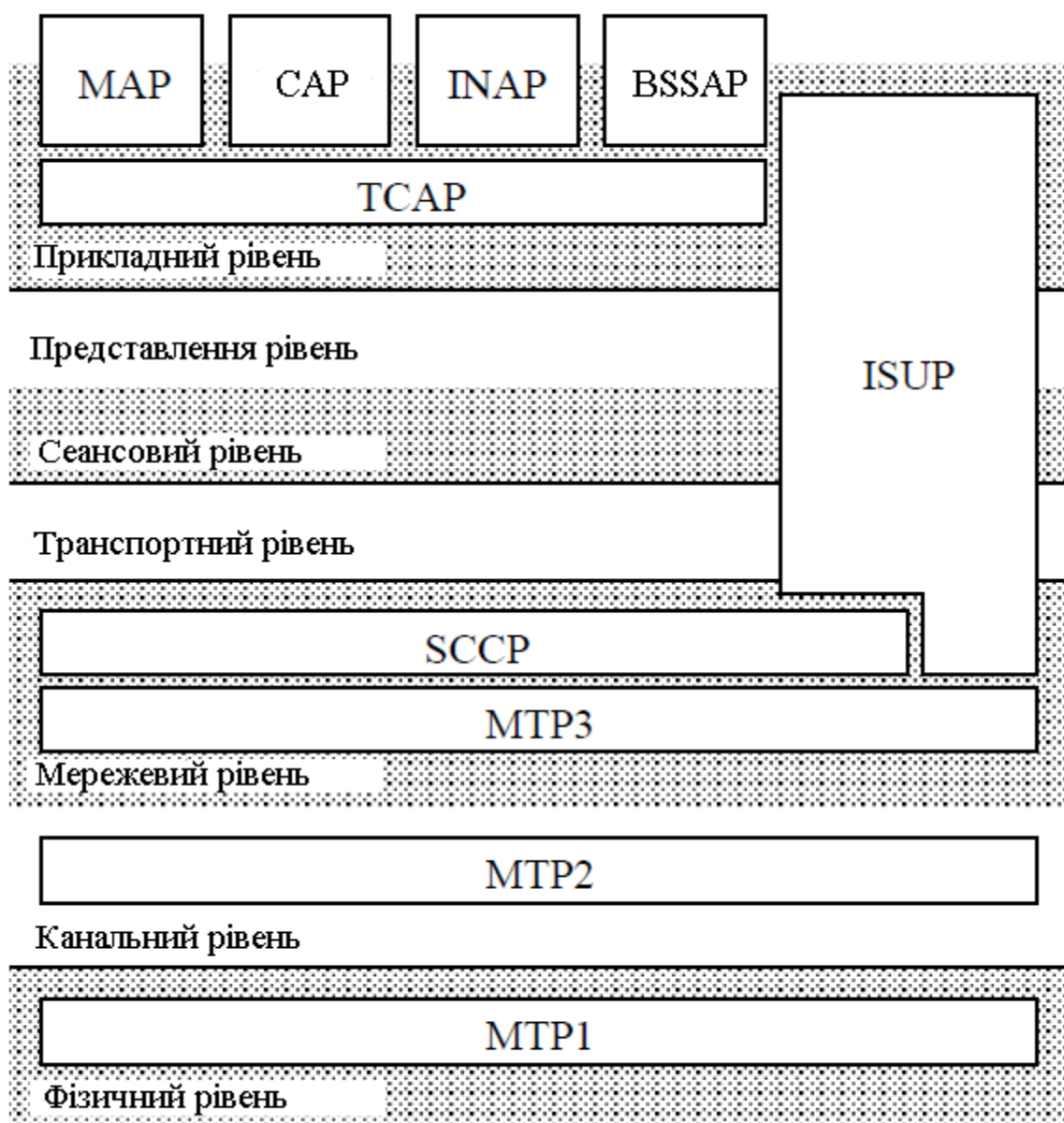


Рисунок 1.2 - Архітектура стека протоколів SS7

Рівні мають назву MTP (Message Transfer Part) 1, MTP 2 і MTP 3 - підсистеми передачі повідомлень, вона виконує функції обміну даними, обробку повідомлень і маршрутизацію, управління сигнальним трафіком, управління ланкою сигналізації (призначене для перенесення сигнальних повідомлень між двома пунктами сигналізації), управління сигнальними шляхами. Четвертий рівень моделі SS7 містить рівні, які призначені для користувача, SCCP (Signaling Connection Control Part) - підсистема управління

сигнальними з'єднаннями. Разом з МТР розділяють функції мережевого рівня, їх називаються підсистемою мережевих послуг NSP (Network Services Part) [16]. NSP виконують функції адресації і маршрутизації повідомлень і надають сервіс управління для четвертого рівня стека протоколів SS7. ISUP (Integrated Services Digital Network User Part) - канално-орієнтований протокол для установки, підключення і завершення з'єднання при дзвінку. TCAP (Transaction Capabilities Application Part) - забезпечує інтерфейс прикладних підсистем того чи іншого користувача з підсистемою мережі, а, точніше, з підсистемою SCCP. Створює запити до бази даних від віддаленого об'єкта, може використовуватися як протокол зв'язку для обміну компонентами між процесами, які встановили зв'язок, так і для зв'язку з інтелектуальними мережами INAP (Intelligent Network Application Part), інтелектуальними мережами мобільного зв'язку CAP (CAMEL Application Part), мобільними службами MAP (Mobile Application Part). BSSAP (Base Station System Application Part) - прикладна підсистема базових станцій BSS (Base Station Subsystem) GSM (Global System for Mobile Communications). Складається з DTAP (Direct Transfer Part) та BSSMAP (BSS Management Application Part). DTAP - прикладна підсистема обміну сигнальними повідомленнями між мобільною станцією та MSC (Mobile Switching Center). BSSMAP - прикладна підсистема взаємодії BSC (Base Station Controller) та MSC.

В ході розгляду першої глави було представлено історію розвитку сигнальної мережі. Представлені основні блоки та ланки з яких складається мережа. Представлено архітектуру стека протоколів SS7 і показані відповідності рівням моделі OSI, та визначено призначення кожної з підсистем архітектури.

2 ПІДСИСТЕМА MAP

Архітектура SS7 представляє набір протоколів, які виконують свою певну роль в сигнальній системі. У дипломній роботі буде розглянуто питання захищеності мереж мобільного зв'язку на основі технології SS7, на прикладному рівні моделі OSI, а саме підсистеми MAP. Це пояснюється тим що, підсистема MAP забезпечує функціонування мобільного зв'язку і надає такі послуги як комутація та обслуговування викликів, підтримка мобільності, відправка коротких SMS-повідомлень і технічна експлуатація.

Підтримка перерахованих вище послуг підсистемою MAP, забезпечує такі відомі важливі процедури в мережах мобільного зв'язку, як роумінг та хендовер.

Роумінг - це надання послуг зв'язку мобільному абоненту, що знаходиться поза зоною дії домашньої мережі або зони обслуговування домашнього центру комутації мобільного зв'язку, шляхом використання ресурсів іншої мережі або іншого центру комутації мобільного зв'язку [4].

Хендовер - це передача обслуговування мобільних станцій в процесі розмови з одного стільника в інший без переривання зв'язку [4].

Забезпечення мобільності абонентів мереж мобільного зв'язку та надання послуг, виконується при взаємодії між об'єктами мережі, за допомогою спеціальних повідомлень. Об'єкти мережі можуть реалізовані, в різному обладнанні або інтегровані в одному. Об'єктами в підсистемі MAP є:

- BSS (Base Station Subsystem) - це система базових станцій мереж мобільного зв'язку [18]. У систему базових станцій входять контролер базових станцій BSC (Base Station Controller), базові приймально-передавальні станції BTS (Base Transceiver Station) і транскодер TRAU (Transcoding Rate and Adaptation Unit). BSC - керує радіоресурсами між мобільними станціями і BTS, відповідає за встановлення з'єднань з BTS/TRAU/SGSN (Serving GPRS Support Node), маршрутизує пакетні дані між BTS і SGSN і вибирає швидкість передачі мовних даних по BSS.

BTS - забезпечують покриття мережі мобільного зв'язку. TRAU - відповідає за зміну швидкості передачі голосових даних [18]. Для економії транспортних ресурсів в BSS мова стискається, з невеликою втратою якості і передається до мобільної станції в стислому вигляді, а для передачі в CN (Core Network) стислий потік розгортається до швидкості основного цифрового каналу 64 кбіт/сек.;

- EIR (Equipment Identification Register) - база даних, яка містить список IMEI (International Mobile Equipment Identity) або IMEISV (International Mobile Equipment Identity and Software Version) всіх мобільних станцій, користувачів які підписалися на послуги оператора мережі мобільного зв'язку [4]. Функціональний блок EIR інтегрований з HLR (Home Location Register) в одне обладнання, але розділений функціонально. У EIR міжнародні ідентифікатори обладнання розділені на три списки. Білий список включає ідентифікатори всього обладнання, допущеного для роботи в даній мережі. Чорний список включає IMEI (IMEISV) обладнання, яке не допущено для роботи в даній мережі. Сірий список містить ідентифікатори обладнання, якому не заборонена робота в даній мережі (за винятком тих випадків, коли воно міститься в чорному списку або не міститься в білому списку);

- HLR (Home Location Register) - це база даних в якій зберігається інформація абонентів. У реєстрі містяться всі обов'язкові постійні і опціональні змінні дані, про клієнтів, які отримують послуги мобільного зв'язку у оператора;

- VLR (Visitor Location Register) - це база даних, в якій зберігається і оновлюється інформація абонентів, які знаходяться в зоні дії центру комутації мобільного зв'язку, до якого відноситься даний VLR [4]. Функціональний блок VLR інтегрований з MSC в одне обладнання, але розділений функціонально;

- MSC (Mobile Switching Center) - це комутатор мережі GSM/UMTS (Universal Mobile Telecommunications System), реалізований з

використанням технології комутації каналів. MSC відповідає за управління з'єднань, додатковими послугами (передача коротких повідомлень SMS, переадресація), за збір інформації про оплату наданих послуг, всередині області, яку обслуговують базові станції, підключені до MSC [4];

- GMSC (Gateway Mobile Switching Center) - це шлюзовий комутатор, через який здійснюється взаємодія мережі оператора, з телефонними мережами фіксованого та мобільного зв'язку інших операторів [4]. На сьогоднішній день практично всі MSC, є GMSC. Це пов'язано з тим, що GMSC, комутує не тільки внутрішнє навантаження як MSC, а й комутує зовнішнє навантаження мережі [18];

- STP (Signal Transfer Point) - це комутатор сигналізації, що приймає повідомлення на межах своїх мереж або всередині мережі і передає його без обробки змісту [16];

- SGSN (Serving GPRS Support Node) - це вузол обслуговування абонентів пакетної мережі передачі даних мереж GSM/UMTS [18]. SGSN виступає точкою з'єднання між системою базових станцій (BSS) мережі радіодоступу RAN (Radio access network) і ядром мережі CN (Core Network) [20]. SGSN можна назвати аналогом комутатора MSC мережі GSM;

- GGSN (Gateway GPRS Support Node) - це шлюзовий вузол підтримки GPRS, забезпечує передачу і маршрутизацію пакетних даних SGSN з зовнішньої IP (Internet Protocol) - мережею, для мереж мобільного зв'язку стандартів GSM/UMTS;

- GSMSCF (GSM Service Control Function) - це вузол, який забезпечує виконання послуг інтелектуальної мережі, зазначених у профілі абонента;

- SC (Service Centre) або SMS - C - відповідає за прийом, зберігання і передачу коротких повідомлень від до мобільних станцій. Він також сповіщає абонента про успішну доставку коротких повідомлень або про

відсутність можливості доставити SMS (Short Message Service) адресату [4];

- AuC (Authentication Center) зберігає і обробляє інформацію, яка потрібна для аутентифікації MS (Mobile Station). AuC представляє захищену базу даних, в якій зберігаються копії записаних в SIM (Subscriber Identification Module) - картах абонентів секретних ключів і алгоритмів, призначених для обчислення даних для аутентифікації і шифрування інформації радіоканалів. Функціональний блок AuC інтегрований з HLR в одне обладнання, але розділений функціонально. AuC містить генератор випадкових чисел RAND (Random Number), для кожного абонента мережі GSM в AuC, зберігаються ключ ідентичності iK (identity key), алгоритм обчислення ключа шифрування Kc (Cipherring Key) - A8 і алгоритмів обчислення відгуку SRES (Signed Response) - A3. За допомогою алгоритмів A3 і A8, з використанням iK і генерованого числа RAND, що є вхідним параметром для вказівки алгоритмів, в AuC обчислюються SRES і Kc, які разом з RAND зберігаються в HLR і VLR. Набір трьох чисел отримав назву триплет [4].

В мережах рухомого зв'язку у кожного абонента та вузлів існує набір ідентифікаторів, які виконують функції ідентифікації, адресації та нумерації в підсистемі MAP.

IMSI (International Mobile Subscriber Identity) - міжнародний ідентифікатор мобільного абонента, зберігається в SIM - карті. Структура IMSI показана на рисунку 2.1.

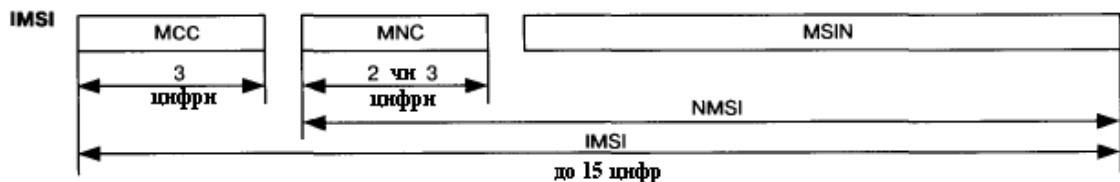


Рисунок 2.1 - Структура IMSI

IMSI складається з трьох частин:

- MCC (Mobile Country Code) - ідентифікує код країни, де постійно знаходиться мобільний абонент, код для України - 255;
- MNC (Mobile Network Code) - ідентифікує код мережі мобільного абонента;
- MSIN (Mobile Station Identification Number) - ідентифікаційний номер абонента в середині мережі мобільного зв'язку.

MSISDN (Mobile Station ISDN Number) - це номер мобільної станції абонента. Структура MSISDN показана на рисунку 2.2.

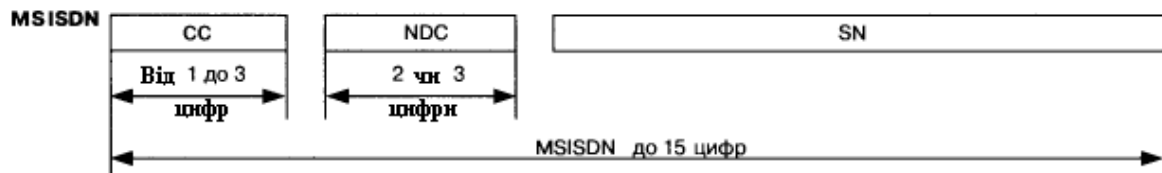


Рисунок 2.2 - Структура MSISDN

MSISDN складається з наступних елементів:

- Код країни (Country Code, CC), для України - +380;
- Національного коду мережі призначення NDC (National Destination Code), що складається з MNC та номера абонента SN (Subscriber Number).

MSRN (Mobile Station Roaming Number) - роумінговий номер мобільної станції, використовується для маршрутизації виклику до мобільної станції при роумінгу [4]. MSRN має структуру, ідентичну MSISDN.

LA (Location Area) - це та область, в якій абонент може переміщатися без оновлення даних в VLR [4]. Структура показана на рисунку 2.3.

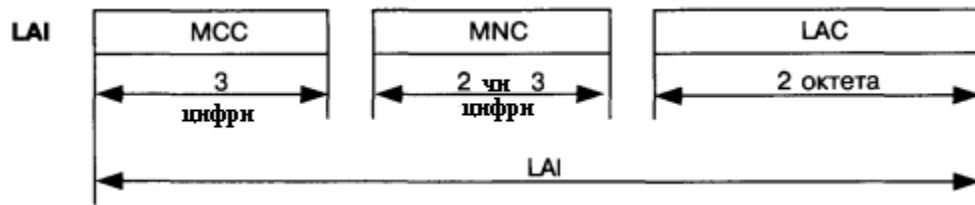


Рисунок 2.3 - Структура LAI

LAI складається з наступних складових:

- код країни (MCC);
- код мережі (MNC);
- код зони місцезнаходження (LAC), який являє собою код довжиною в 2 октету, що ідентифікує зону місцезнаходження мобільної станції.

CGI (Cell Global ID) - ідентифікатор зони в якій в останній раз встановлено радіозв'язок з мобільною станцією. Структура показана на рисунку 2.4.

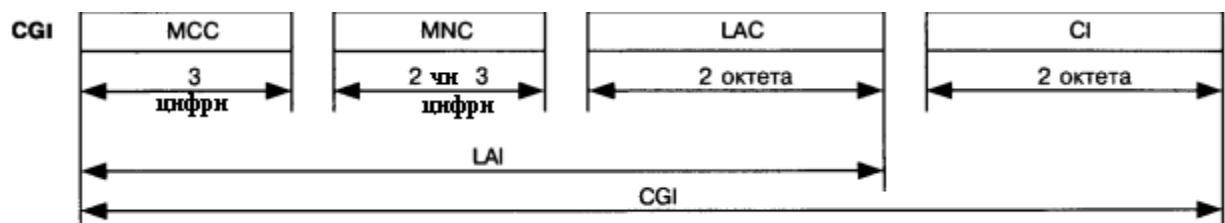


Рисунок 2.4 - Структура CGI

LAI складається з наступних складових:

- код країни (MCC);
- код мережі (MNC);
- код зони місцезнаходження (LAC);
- номер стільника (Cell Identity, CI).

MGT (Mobile Global Title) - глобальна адреса, використовується в протоколі SCCP для маршрутизації повідомлень MAP. Адрес формується з IMSI способом, який показаний на рисунку 2.5.

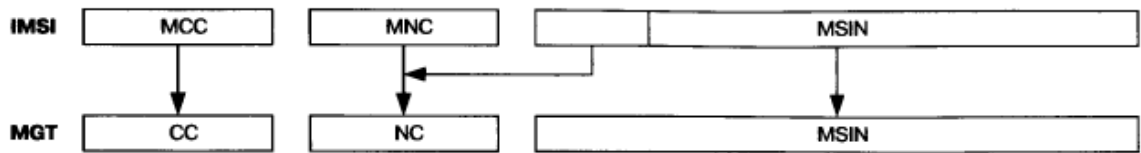


Рисунок 2.5 - Формування MGT з IMSI

В ході розгляду другої глави було представлено підсистему MAP. Було розглянуто об'єкти мережі підсистеми та представлені ідентифікатори, які виконують свою певну функцію в ідентифікації, нумерації чи адресації для абонентів чи вузлів підсистеми MAP.

3 ПРОФІЛЬ ЗЛОВМИСНИКА

В даному розділі складемо профіль зловмисника, який використовує уразливості мереж мобільного зв'язку на основі SS7, а саме протоколу MAP, і виконує серйозні атаки, в результаті яких може бути витік конфіденційних даних, втрата фінансових коштів, порушення доступності абонентів і елементів мережі.

Всіх зловмисників розділимо на два основних типи:

- зовнішні зловмисники - особи або група осіб, що не мають доступу до інформаційної системи і до окремих її компонентів;
- внутрішні зловмисники - особи або група осіб, що мають доступ до інформаційної системи і до окремих її компонентів.

В якості зловмисників виділимо наступні види:

- спецслужби іноземних держав;
- терористичні і злочинні угруповання;
- користувачі інформаційної системи і зовнішні фізичні особи;
- конкуруючі організації;
- виробники і постачальники програмних засобів і технічного обладнання;
- обслуговуючий персонал, найманий, для монтажу, налагоджувальних та інших видів робіт;
- обслуговуючий персонал інформаційної системи (охорона, прибиральники);
- адміністратори інформаційної системи і адміністратори безпеки.

Всіх зловмисників розділимо за рівнем підготовки, який необхідний для реалізації загроз безпеки інформації:

- зловмисники, які мають низький рівень знань при реалізації загроз безпеки інформації в інформаційній системі;
- зловмисники, які мають середній рівень знань при реалізації загроз безпеки інформації в інформаційній системі;

– зловмисники, які мають високий рівень знань при реалізації загроз безпеки інформації в інформаційній системі.

Розглядаючи види зловмисників, ми можемо прибрати такий вид зловмисників, як «користувачі інформаційної системи і зовнішні фізичні особи». Дану пару ми можемо прибрати, так як зовнішні фізичні особи не мають, як достатніх знань для реалізації загроз безпеки інформації в інформаційній системі, так і доступу до внутрішньої мережі мобільного зв'язку оператора. А мобільні станції користувачів інформаційної системи, які обслуговуються у даного оператора мобільного зв'язку, розділені фізично від сигнальної системи.

Розглядаючи зловмисників, можемо об'єднати в пару «виробників і постачальників програмних засобів і технічного обладнання» і «конкуруючі організації». Це пояснюється тим, що цій парі не вигідно виробляти атаки. Якщо атаки з боку виробників і постачальників буду сприйняті як неполадки в програмних засобах або технічному обладнанні, а атаки з боку конкурентів будуть виявлені, то обидві сторони даної пари понесуть як фінансові втрати, так і репутаційні. Устаткування і програмні засоби перестануть купуватися інформаційними системами, а виявив атаку з боку конкурентів, оператор мережі мобільного зв'язку може відмовити в обслуговуванні абонентів, мобільного зв'язку конкурента. Слід пам'ятати про те, що в якості майданчика для атак, структуру оператора зв'язку конкурентів або інших операторів можуть використовувати спецслужби іноземних держав, так як, отримавши доступ до мережі оператора зв'язку, атаки можуть проводитися з будь-якої точки планети, що є найбільш перспективним для зловмисника, та відстежити його місце розташування практично неможливо.

Також не розглядаємо як потенційних зловмисників такий вид, як «обслуговуючий персонал інформаційної системи» (охорона, прибиральники), через те що, вони не володіють достатніми знаннями для реалізації загроз безпеки інформації в інформаційній системі, і не мають прямого доступу до обладнання.

Розглядаючи вид «адміністратори інформаційної системи і адміністратори безпеки» до них додаємо вид зловмисників як «обслуговуючий персонал, найманий, для монтажу, налагоджувальних та інших видів робіт», Тим самим створивши групу дійсно актуальних зловмисників, що представляють загрозу безпеки інформації в інформаційній системі. Це пояснюється тим, що в якості об'єднаної групи можуть виступати, як спецслужби іноземних держав, так і терористичні та злочинні угруповання або окремі особи, які мають свої зацікавленості в проведенні цілеспрямованих атак на інформаційну систему. Вони мають безпосередній доступ до обладнання та мають середній або високий рівень знань при реалізації загроз безпеки інформації в інформаційній системі. Цю групу зловмисників можна позначити як «технічні фахівці».

Обробивши і проаналізувавши інформацію про всіх видів зловмисників можемо виділити 3 актуальних виду зловмисників, які представляють реальні загрози безпеки інформації в інформаційній системі:

- спецслужби іноземних держав;
- терористичні і злочинні угруповання;
- технічні фахівці.

Зовнішніми зловмисниками будемо вважати спецслужби іноземних держав і терористичні і злочинні угруповання. Атаки їх будуть проводитися з зони, яка не контролюється, з мереж зв'язку конкурента або інших операторів зв'язку, крім цього атаки можуть бути реалізовані з внутрішніх вузлів, які були скомпрометовані атакуючим. Внутрішніми зловмисниками будемо вважати технічних фахівців, так як вони виробляють атаки з контрольованої зони, шляхом можливості підключення свого обладнання до мережі або скориставшись легітимним набором функцій в існуючому обладнанні інформаційної системи.

За рівнем підготовки, для реалізації загроз безпеки інформації, технічні фахівці і спецслужби іноземних держав мають високий рівень знань і мають безпосередній доступ до обладнання. Рівень підготовки

терористичних і злочинних угруповань можемо вважати середнім, внаслідок того, що перед проведенням цілеспрямованих атак, вони здійснюють підготовку та вивчення підсистеми.

В ході розгляду третьої глави було складено профіль зловмисника, даний профіль допоможе нам зрозуміти від кого нам потрібно захищатись. За профілем зловмисника складаємо остаточну таблицю 3.1, яка містить інформацію про види зловмисників, про групи відносно контрольованої зони, про рівень підготовки і передумов для реалізації загроз безпеки інформації.

Таблиця 3.1 - Профіль зловмисників для мереж мобільного зв'язку

Вид зловмисників	Тип зловмисників	Рівень підготовки	Передумови для реалізації загроз безпеки інформації
Спецслужби іноземних держав	Зовнішній	Високий рівень знань	Завдання збитків державі. Компрометація і підривання діяльності органів державної влади.
Терористичні і злочинні угруповання	Зовнішній	Середній рівень знань	Завдання збитків державі. Скоєння терористичних актів. Підрив діяльності органів державної влади. Нанесення матеріального збитку і отримання особистої матеріальної вигоди шляхом шахрайства, виявлення вразливостей і подальшого їх продажу та іншими злочинними шляхами.

Вид зловмисників	Тип зловмисників	Рівень підготовки	Передумови для реалізації загроз безпеки інформації
Технічні фахівці	Внутрішній	Високий рівень знань	Нанесення матеріального збитку і отримання матеріальної особистої вигоди, зловживання довірою.

Продовження таблиці 3.1 - Профіль зловмисників для мереж мобільного зв'язку

4 МОЖЛИВІ ПОТЕНЦІЙНІ АТАКИ НА МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ

Для кращого розуміння атак з боку зловмисника, необхідно розглянути нормальну поведінку в роботі системи при реєстрації абонента в мережі мобільного зв'язку, при здійсненні вихідного дзвінка і надсилання повідомлення.

Коли мобільна станція має намір увійти в мережу в ході включення вона формує список сусідніх стільників і вибирає з них кращу, використовуючи загальний канал стільника, повідомляє, що його поточне місце розташування обслуговується даним стільником. Ця інформація разом з повідомленням примітивом «LocationUpdate» і IMSI передається на BSC. Після цього, повідомлення примітив «LocationUpdate» і IMSI передається на MSC/VLR в зоні якого, базові станції обслуговують мобільного абонента, який подав запит про реєстрацію в мережі. По мобільному ідентифікатором IMSI, VLR/MSC визначає домашню мережу мобільного абонента який хоче зареєструватися і пов'язує її з HLR, куди в подальшому передається повідомлення примітив «SendAuthenticationInfo» і IMSI. Наприклад початок мобільного ідентифікатора 25599 ... відповідає українському мобільному оператору Vodafone (255 - код країни Україна, 99 - цифри визначають домашню мережу Vodafone). Після чого HLR робить перевірку, звертаючись до реєстру EIR, з'ясовує чи є даний користувач в базі даних і до якого списку він належить. Якщо перевірка пройшла успішно, реєстр HLR запитує у AuC вектори аутентифікації і пересилає триплет і IMSI в VLR/MSC, де гостьовий реєстр зберігає і використовує ці дані як параметри аутентифікації і шифрування. Після того як VLR/MSC отримав ці дані, VLR/MSC посилає RAND з триплетів на мобільну станцію абонента. Отримавши дані RAND і маючи в SIM - карті ключ ідентичності iK, обчислюють SRES, який відправляє в VLR/MSC. Якщо SRES, обчислений в мобільній станції, збігається зі SRES, розрахованих в AuC процес авторизації вважається успішним [10]. Якщо авторизація пройшла успішно VLR/MSC відправляє на

HLR повідомлення примітив «UpdateLocation», щоб HLR мав інформацію, в зоні якого MSC/VLR обслуговується мобільна станція. Повідомлення містить в собі IMSI і MGT VLR/MSC. Отримавши повідомлення, HLR відправляє профіль абонента за допомогою примітив повідомлення «InsertSubscriberData», на VLR/MSC, який запитав цю інформацію. Після того як VLR/MSC отримає цю інформацію, процедура «UpdateLocation» буде завершено і HLR збереже в профілі абонента адресу MSC/VLR. Після цих процедур, абонент вважається, зареєстрований в мережі.

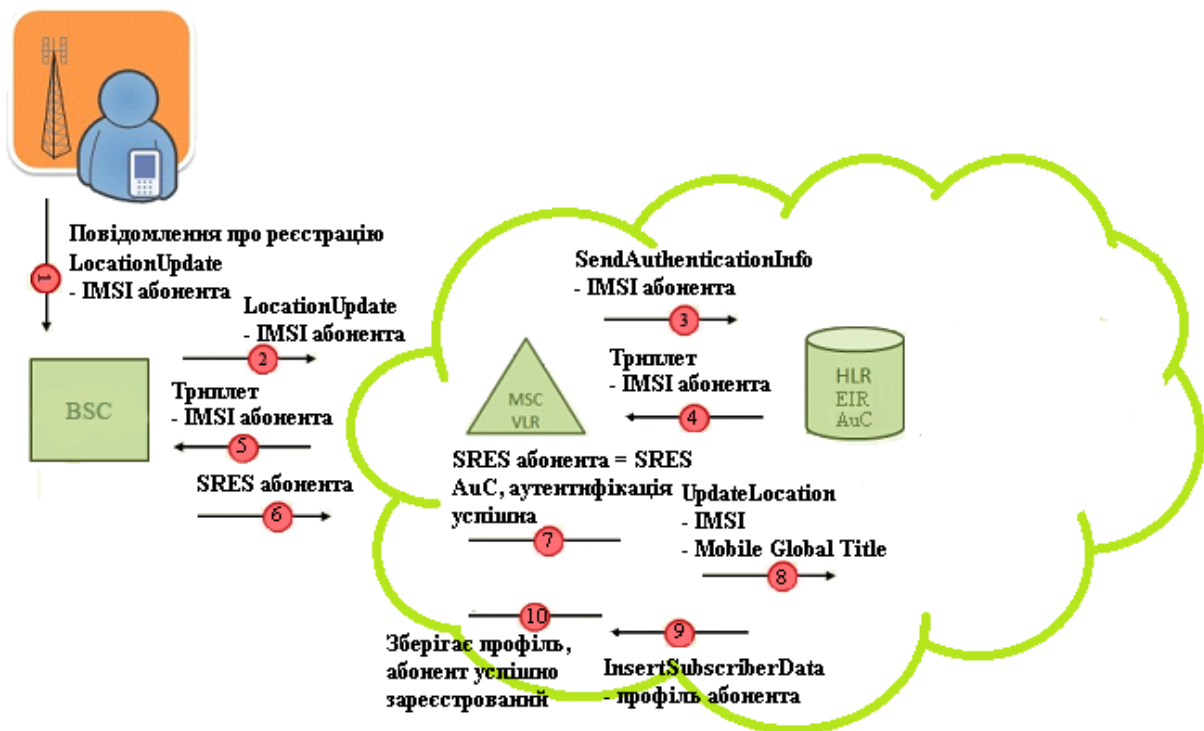


Рисунок 4.1 - Схема реєстрація абонента в мережі мобільного зв'язку

Абонент «А», збирається зробити вихідний дзвінок абоненту «В». Коли абонент «А» здійснює дзвінок абоненту «В» його мобільна станція звертається до MSC/VLR, яка обслуговує абонента «А». Отримавши виклик від мобільної станції, MSC/VLR по MSISDN абонента «В» визначає домашню мережу мобільного абонента і пов'язує її з HLR, після чого відправляє повідомлення примітив «SendRoutingInfo» і MSISDN абонента

«B» на HLR, щоб отримати інформацію про локалізацію абонента. Після чого HLR перевіряє підписку абонента на послуги та відсутність у абонента заборон, та відправляє повідомлення примітив «ProvideRoamingNumber» і IMSI абонента «B» на VLR/MSC, який обслуговує його в даний момент. Отримавши повідомлення примітив від HLR, VLR/MSC вибирає вільний номер MSRN з бази даних номерів і відправляє його на HLR. Отримавши номер MSRN, HLR відправляє його MSC/VLR, який обслуговує абонента «A». В результаті чого, MSC/VLR робить дзвінок на отриманий номер MSRN. Як тільки абоненти встановили зв'язок, VLR/MSC, який видав номер звільняє його і знову вносить в базу даних вільних номерів.

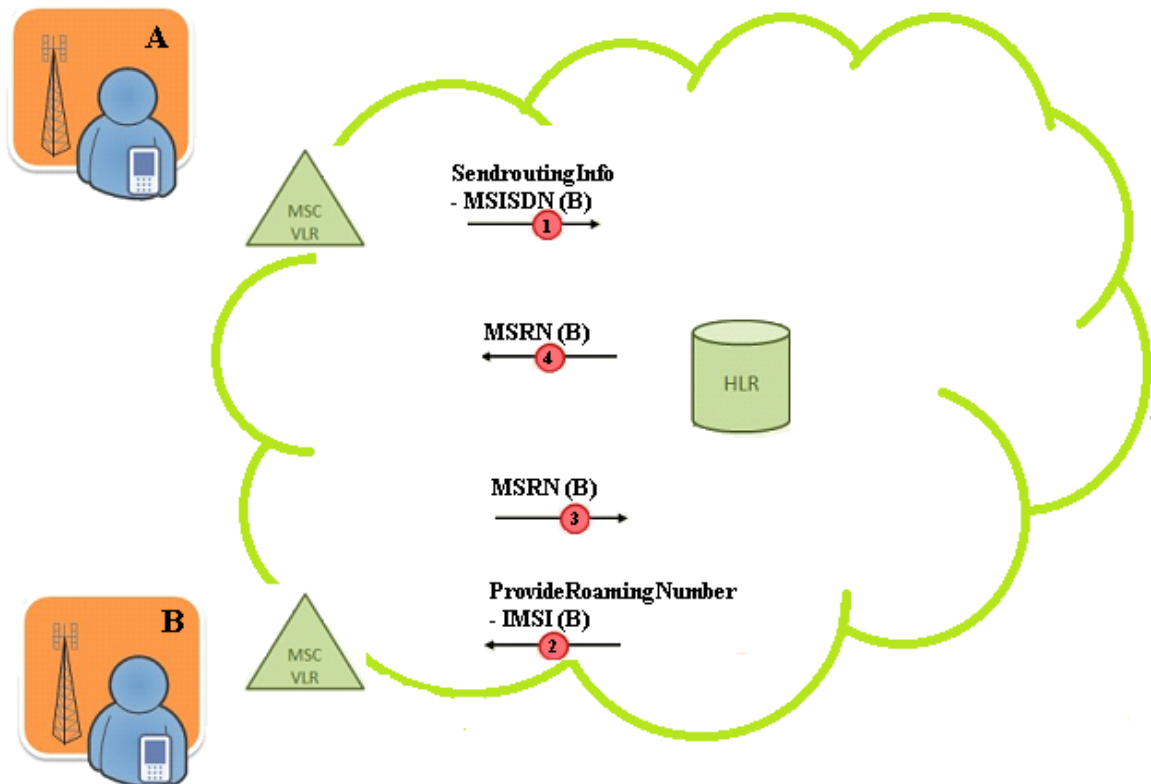


Рисунок 4.2 - Схема здійснення вихідного дзвінка

Абонент «А», збирається надіслати SMS - повідомлення абоненту «В». Коли абонент «А» відправляє SMS - повідомлення, воно передається в MSC/VLR, який обслуговує абонента «А». Після чого VLR/MSC перевіряє

підписку абонента на послуги відправлення повідомлень та відсутність у абонента заборон, після чого відправляє в SC повідомлення примітив «MO-ForwardSM», яке містить MSISDN абонента «В» і безпосередньо SMS-повідомлення, яке потрібно йому відправити. Потім SC по MSISDN абонента «В» визначає домашню мережу мобільного абонента і пов'язує її з HLR, після чого відправляє в HLR повідомлення примітив «SendRoutingInfoForSM» і MSISDN «В», для того щоб отримати інформацію про локалізацію абонента одержувача при доставці SMS - повідомлення. У відповідь HLR відправляє в SC, IMSI абонента одержувача і адресу MSC/VLR, який обслуговує його. SC відправляє повідомлення примітив «MT-forwardSM» і IMSI одержувача на адресу MSC/VLR абонента «В». Володіючи інформацією об адресі MSC/VLR, який обслуговує абонента «В» з відповідним IMSI, SC надсилає SMS - повідомлення.

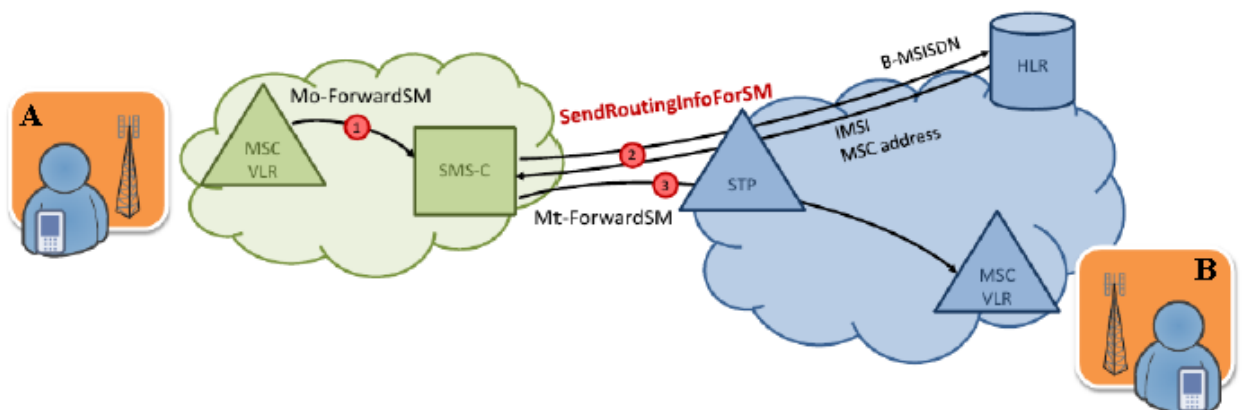


Рисунок 4.3 - Схема надсилання SMS - повідомлення

Розглянули нормальне функціонування системи, тепер розглянемо дії злоумисника, спрямовані на розкриття конфіденційного ідентифікатора абонента, розкриття інформації про розташування абонента, порушення доступності мережі, перехоплення вхідних SMS - повідомлень, маніпуляції з USSD - запитами, зміни профілю VLR, прослуховування вихідних дзвінків,

перенаправлення вхідних викликів і відмова в обслуговуванні вхідних викликів.

4.1 Атака на розкриття конфіденційного ідентифікатора абонента

Початковими даними для реалізації атаки є MSISDN абонента жертви. В атаці зловмисник посилає повідомлення примітив «SendRoutingInfoForSM» і MSISDN абонента жертви від імені SC на STP. Повідомлення примітив «SendRoutingInfoForSM» використовується для запиту маршрутної інформації для локалізації абонента одержувача при доставці SMS - повідомлення [17]. Коли повідомлення примітив надходить на STP, по MSISDN визначається домашня мережа мобільного абонента і пов'язує її з HLR, STP передає його далі на HLR, де домашній реєстр обробляє запит, збирає всю необхідну інформацію і передає її зловмисникові.

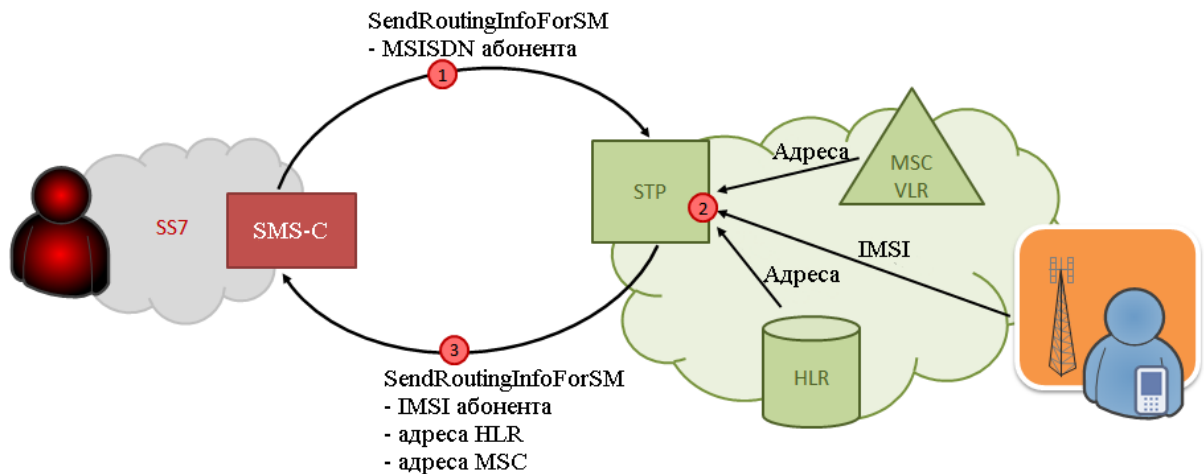


Рисунок 4.3 - Схема «розкриття конфіденційного ідентифікатора»

При успішній реалізації атаки зловмисник отримає IMSI абонента жертви, адресу HLR в якому зберігаються дані абонента і адресу MSC/VLR, які обслуговують абонента в даний момент.

4.2 Атака на розкриття інформації про розташування абонента

Початковими даними для реалізації атаки є IMSI абонента і адреса поточного MSC/VLR. В атаці зловмисник посилає повідомлення примітив «ProvideSubscribeInfo» з IMSI абонента жертви на адресу поточного MSC/VLR, від імені HLR. Повідомлення примітив протоколу MAP, «ProvideSubscribeInfo» використовується для отримання інформації про місцезнаходження абонента в роумінгу від оператора іншої мережі [17]. MSC/VLR обробляє запит, збирає всю необхідну інформацію і передає її зловмисникові.

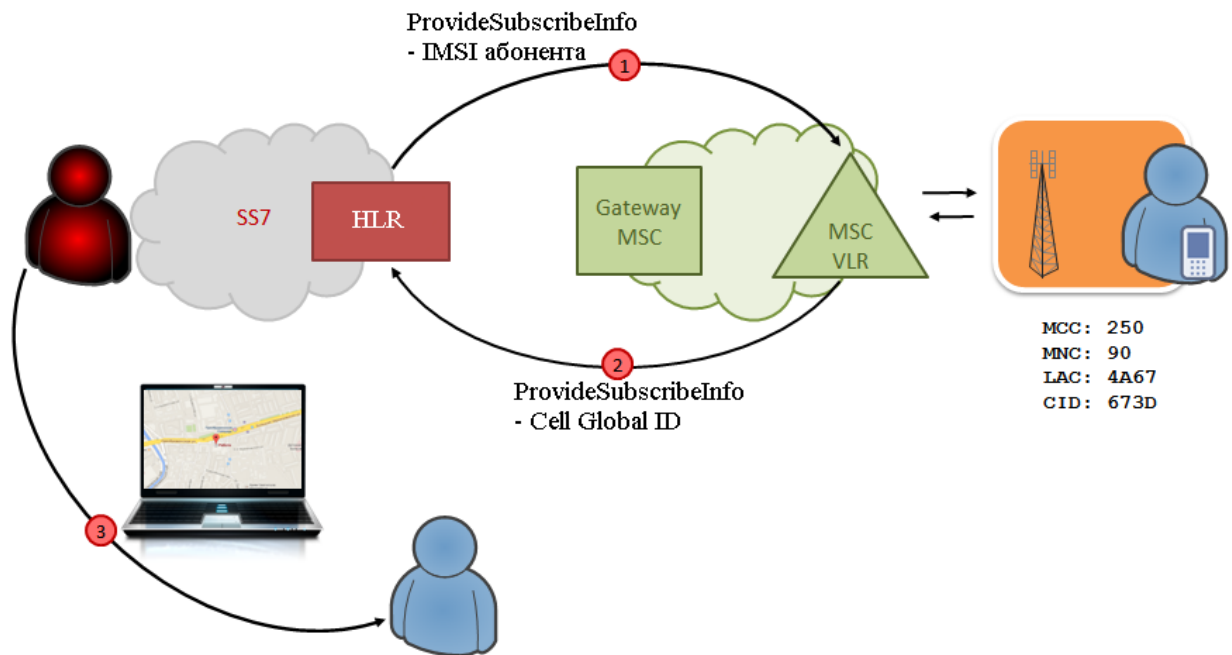


Рисунок 4.4 - Схема «розкриття інформації про розташування абонента»

При успішній реалізації атаки зловмисник отримає CGI, в який входить MCC, MNC, LAC, CI. Використовуючи загальнодоступні ресурси в інтернеті за даними ідентифікаторів можна визначити місце розташування абонента жертви.

4.3 Атака на порушення доступності абонента

Початковими даними для реалізації атаки є IMSI абонента жертви і адреса поточного MSC/VLR. В атаці зловмисник посилає повідомлення примітив «UpdateLocation» з IMSI абонента жертви і адресом не існуючого MSC/VLR на HLR від імені MSC/VLR, який на даний момент обслуговує його. Повідомлення примітив протоколу MAP, «UpdateLocation» використовується для запиту реєстрації в зоні дії нового MSC/VLR [17]. HLR отримавши запит обробляє його і оновлює в профілі абонента жертви адресу MSC/VLR на не існуючу.

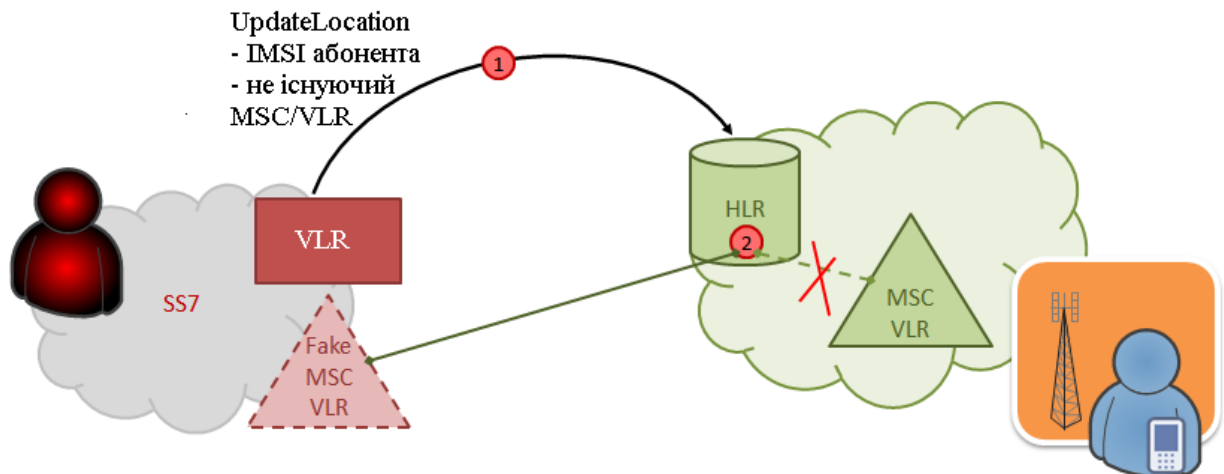


Рисунок 4.5 - Схема «порушення доступності мережі»

При успішній реалізації атаки, абонент жертва перестане отримувати вхідні дзвінки та SMS повідомлення. Мобільна станція абонента жертви буде відображати, що він знаходиться в зоні дії мережі мобільного зв'язку свого оператора. Абонент буде недоступний до тих пір, поки не переміститься в зону дії іншого MSC/VLR, не проведе перезавантаження мобільної станції або не виконає вихідний дзвінок.

4.4 Атака на перехоплення вхідних SMS - повідомлень

Атака є продовженням атаки з порушенням доступності. Зловмисник робить всі ті ж дії, що і в минулій атаці, але вказує вже MSC/VLR, який знаходиться під його контролем.

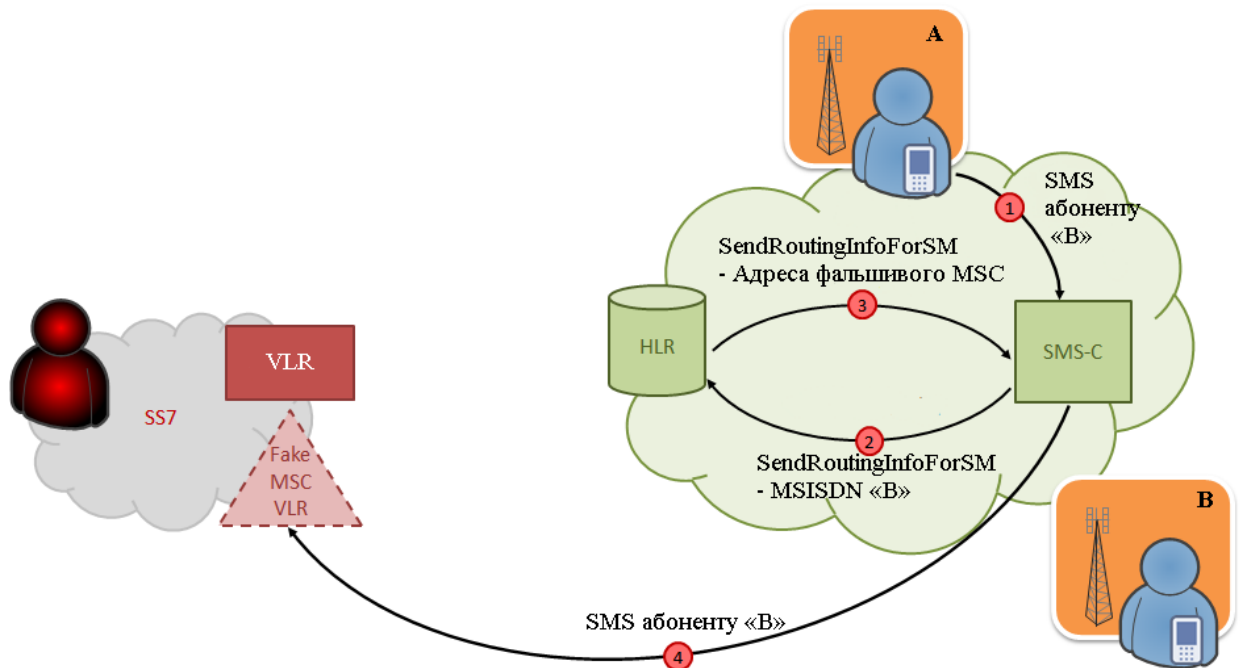


Рисунок 4.6 - Схема «перехоплення вхідних SMS - повідомлень»

При успішній реалізації атаки, всі вхідні SMS - повідомлення, будуть направлятися на вказаний зловмисником вузол. Атакуючий має ряд можливостей, так як SMS - повідомлення вимагають від MSC/VLR, підтвердження його доставки. Зловмисник може надіслати відповідь, що він отримав повідомлення (адресат не отримає вхідне повідомлення, а його отримає тільки атакуючий); не відправляти звіт і перереєструвати абонента на колишню адресу (повідомлення буде надіслано вдруге і адресат отримає повідомлення); відправити звіт про отримання, перереєструвати абонента на колишній адресу і відправити змінене повідомлення.

4.5 Атака маніпуляцій з USSD - запитами

Початковими даними для реалізації атаки є MSISDN і IMSI абонента жертви, адреса HLR і USSD запит, який необхідно виконати зловмиснику. Найбільш поширеним є запит переказу грошових коштів. Все USSD запити, як правило, вказані на сайті оператора мобільного зв'язку.

В атаці зловмисник посиляє повідомлення примітив «ProcessUnstructuredSS-Request» з MSISDN і IMSI абонента жертви і командою USSD запитом на адресу HLR від імені VLR/MSC. Повідомлення примітив протоколу MAP, «ProcessUnstructuredSS-Request» використовується для того щоб забезпечити виконання неструктурованих додаткових послуг [17]. HLR отримавши запит, передає його в білінгову платформу з усією необхідною інформацією для виконання USSD запиту. Після чого білінгова платформа виконує USSD запит і відправляє у відповідь повідомлення про підтвердження виконання USSD запиту.

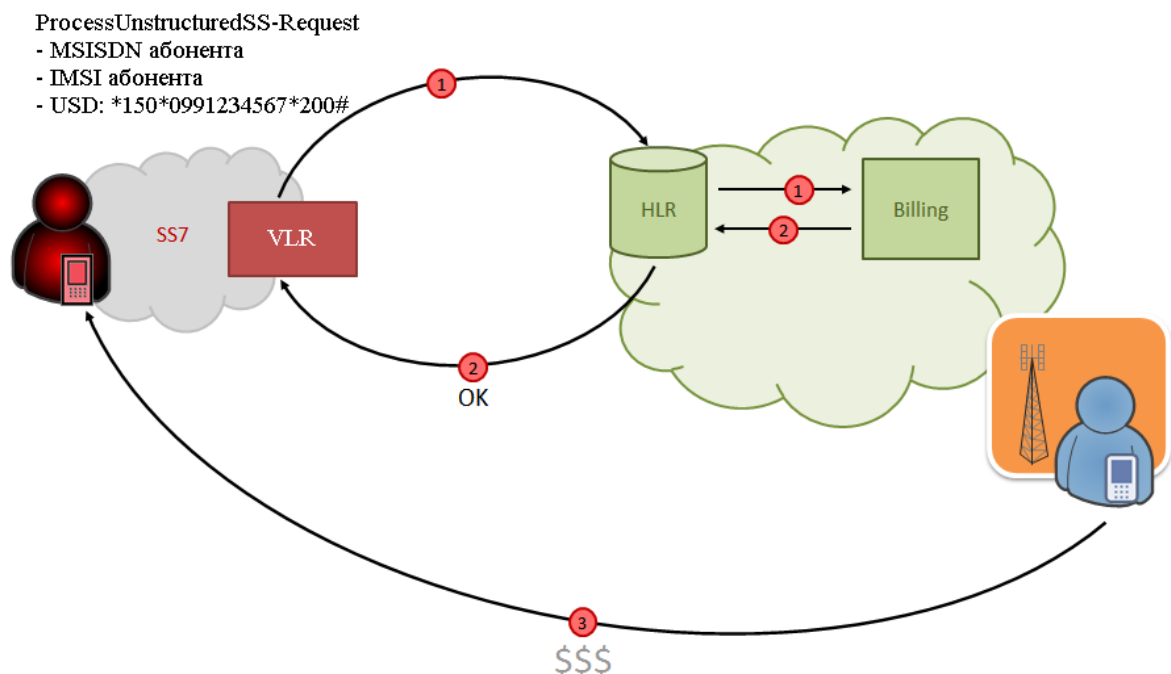


Рисунок 4.7 - Схема «маніпуляцій з USSD - запитами»

При успішній реалізації атаки з USSD запитом на переказ грошових коштів. Абонент жертва може нічого не запідозрити, навіть якщо у нього підключена послуга сповіщень при операціях пов'язаних з його грошовими коштами, так як разом із цією атакою зловмисник може провести перехоплення вхідних повідомлень і операція з переказу грошових коштів залишиться непомітною.

4.6 Атака на зміну профілю VLR

Початковими даними для реалізації атаки є MSISDN і IMSI абонента жертви і адреса поточного VLR/MSC.

В атаці зловмисник посилає повідомлення примітив «InsertSubscriberData» з MSISDN і IMSI абонента жертви на адресу VLR/MSC від імені HLR. повідомлення примітив протоколу MAP, «InsertSubscriberData» використовується для зміни профілю абонента в базі даних VLR [17]. Отримавши повідомлення примітив від HLR, VLR/MSC оновлює профіль абонента жертви в своїй базі даних.

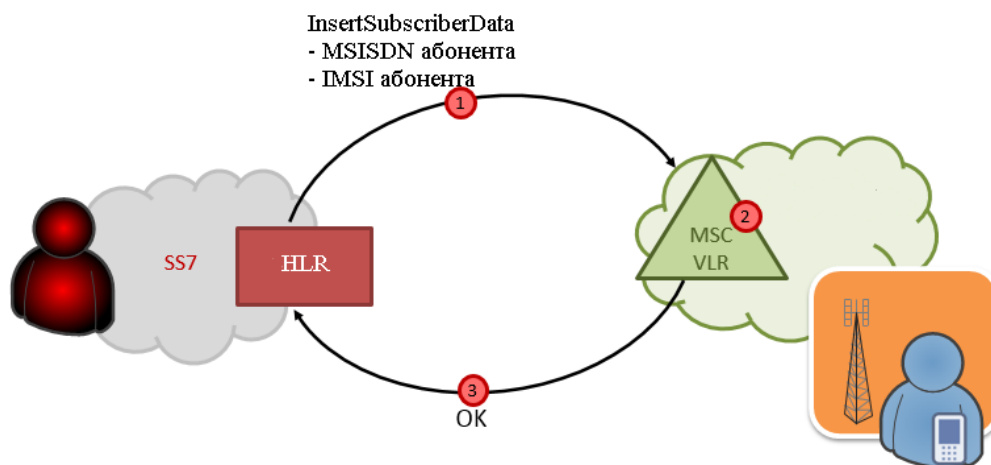


Рисунок 4.8 - Схема «зміна профілю VLR»

При успішній реалізації атаки, зловмисник змушує VLR/MSC обслуговувати змінений профіль абонента.

4.7 Атака на прослуховування вихідних викликів

Атака є розширеною версією атаки зі зміною профілю VLR. Зловмисник робить всі ті ж дії, що і в минулій атаці, але змінює в профілі абонента жертви адреса платформи тарифікації і вказує адресу обладнання, яке знаходиться під контролем зловмисника. Коли абонент жертва «А» захоче зробити вихідний виклик абоненту «В», запит на тарифікацію потрапить на адресу обладнання зловмисника, в цьому запиті знаходиться номер абонента, що викликається. Коли зловмисник направив виклик на своє обладнання, і створив конференц зв'язок, зловмисник додає до конференції абонента «В». Між абонентами «А» і «В» встановлюється зв'язок і відбувається розмова.

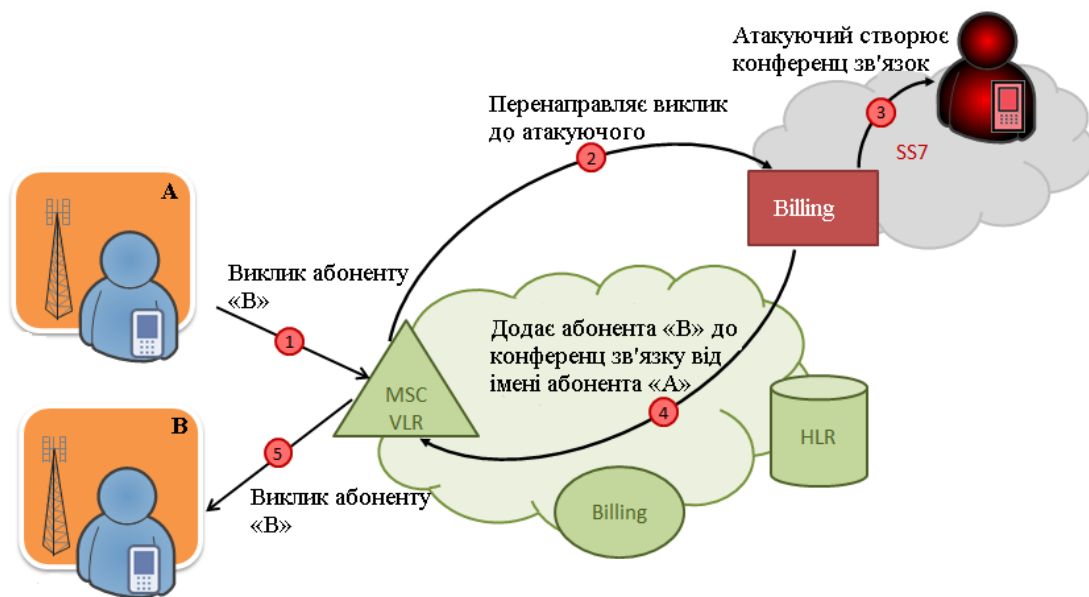


Рисунок 4.9 - Схема «прослуховування вихідних дзвінків»

При успішній реалізації атаки, розмова між абонентами «А» і «В» відбудеться, але голосовий трафік пройде через обладнання зловмисника.

4.8 Атака на перенаправлення вхідних викликів

Атака є продовженням атаки з порушенням доступності. Зловмисник робить всі ті ж дії, але вказує вже MSC/VLR, який знаходиться під його контролем. Коли абонент «А» здійснює виклик абоненту «В» його мобільна станція звертається до GMSC, яка обслуговує абонента «А». Отримавши виклик від мобільної станції, GMSC по MSISDN абонента «В» визначає домашню мережу мобільного абонента і пов'язує її з HLR, та відправляє повідомлення примітив «SendRoutingInfo» на HLR, щоб отримати інформацію про локалізацію абонента. Після чого HLR відправляє повідомлення примітив «ProvideRoamingNumber» і IMSI абонента «В» на VLR/MSC, який під контролем зловмисника. У відповідь зловмисник на HLR відправляє номер MSRN, на який він хоче направити вхідний виклик. Отримавши номер MSRN, HLR відправляє його на GMSC, який обслуговує абонента «А». В результаті чого, GMSC виклик на отриманий номер MSRN.

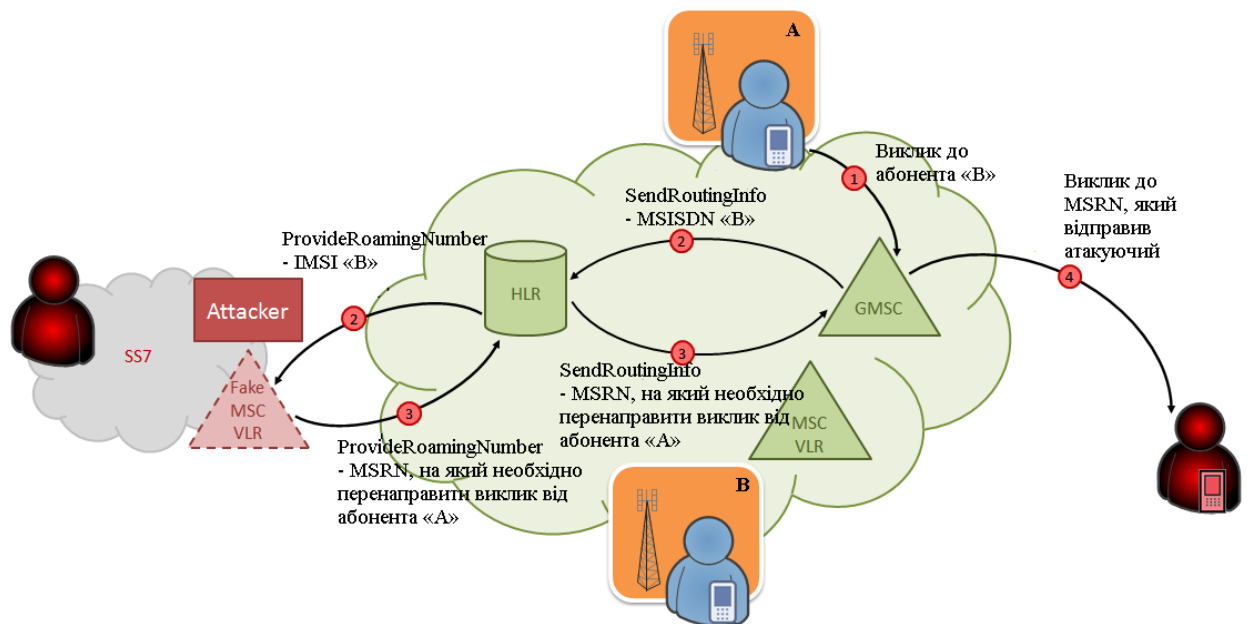


Рисунок 4.10 - Схема «перенаправлення вхідних викликів»

При успішній реалізації атаки, зловмисник направляє вхідний виклик абоненту жертви на свій довільний номер.

4.9 Атака на відмову в обслуговуванні для вхідних викликів

Початковими даними для реалізації атаки є IMSI і адреса поточного VLR/MSC абонента жертви. В атаці зловмисник масово посиляє повідомлення примітив «ProvideRoamingNumber» і IMSI абонента жертви на VLR/MSC від імені HLR. Повідомлення примітив протоколу MAP, «ProvideRoamingNumber» використовується для отримання роумінгового номера від операторів іншої мережі для абонентів у роумінгу [17]. Коли зловмисник масово посиляє запити, на надання номера, він досить швидко можна вичерпати базу даних номерів. Безпосередньо робота номера становить частку секунд, проте таймер утримання номера в обладнанні становить близько хвилини.

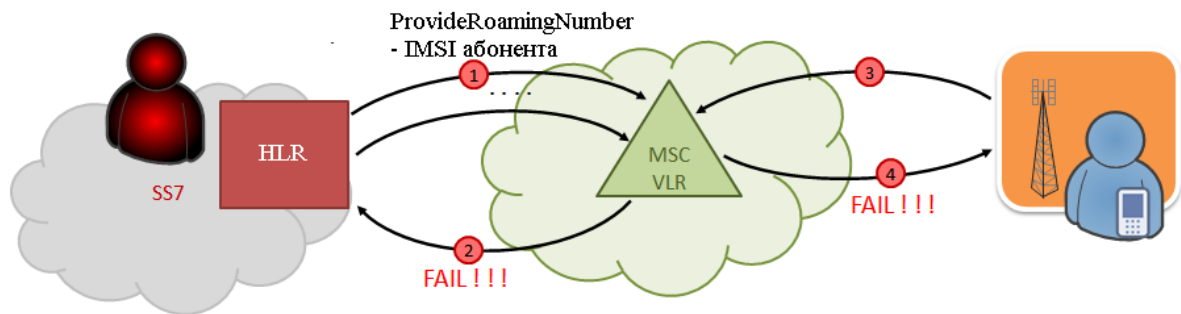


Рисунок 4.11 - Схема «відмови в обслуговуванні для вхідних викликів»

При успішній реалізації атаки, MSC/VLR абонента жертви не зможе приймати вхідні мобільні виклики.

4.10 Потенційно уразливі повідомлення примітиви

Крім тих повідомлень, які були використані в атаках, зловмисник може використовувати інші потенційно небезпечні повідомлення примітиви. Для них розглянемо призначення в роботі системи, та можливі маніпуляції з боку зловмисника, використовуючи які, він може домогтися певного типу атаки. В якості небезпечних повідомлень примітивів розглянемо лише малу частину серед усіх існуючих повідомлень в підсистемі MAP, до яких ми можемо віднести наступні повідомлення:

- FailureReport;
- SendParameters;
- RemoteUserFree;
- NoteSubscriberDataModified;
- ReportSMDeliveryStatus;
- ResumeCallHandling.

«FailureReport» - це повідомлення примітив використовується для відправки звіту про помилку від GGSN або SGSN на HLR, коли абонент недоступний або при обробці запиту сталася помилка.

Використовуючи повідомлення примітив «FailureReport» зловмисник має можливість виконати атаку на порушення доступності абонента та атаку на відмову в обслуговуванні для сервісу пакетної передачі.

Атаку на порушення доступності абонента має можливість виконати зловмисник, якщо має IMSI абонента. Він відправляє повідомлення примітив «FailureReport» на HLR від імені GGSN, GGSN припиняє комутувати з'єднання та абонент тимчасово стає недоступним для прийому та передачі трафіку, бо саме GGSN та SGSN відповідають за пакетну передачу, зокрема за надання абонентам послуги мобільного інтернету.

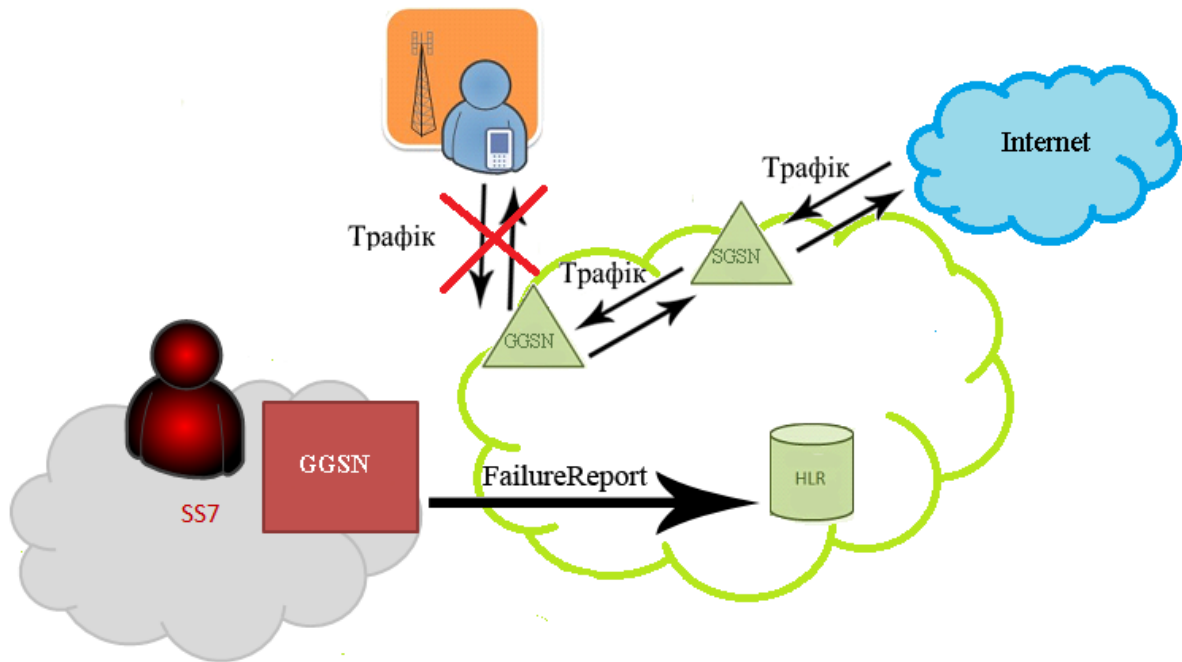


Рисунок 4.12 - Схема атаки на порушення доступності абонента за допомогою повідомлення примітива «FailureReport»

DoS атаку на відмову в обслуговуванні для сервісу пакетної передачі зломисник може виконати, якщо він має більшу частину IMSI абонентів, які обслуговуються одним GGSN. Масово відправляючи повідомлення «FailureReport», HLR буде вважати їх недоступними. Масові запити не залишаться непоміченими з боку працездатності мережі. Мережа відключить даний вузол та направить трафік на інший GGSN. Продовжуючи посилати повідомлення від імені інших GGSN, зломисник виконає DoS атаку, тим самим погіршуючи весь сервіс пакетної передачі для абонентів мережі мобільного зв'язку оператора.

«SendParameters» - це повідомлення примітив використовувалось для отримання IMSI абонента, для отримання ключів шифрування радіосигналу і GSM-триплета при аутентифікації, для реєстрування абонента в зоні обслуговування іншого MSC/VLR та для отримання профіля абонента. Повідомлення примітив зберіглося з перших версій підсистеми MAP. На сьогоднішній день це повідомлення примітив рідко використовується, але

його все ще підтримує обладнання мереж мобільного зв'язку. Відправником цього повідомлення є MSC/VLR та SGSN, приймачем цього повідомлення є HLR. При реєстрації абонента в мережі MSC/VLR запитує у HLR ISMI абонента, його профіль та GSM-триплет для аутентифікації його в мережі. Крім того його може відправляти VLR/MSC, коли абонент змінив місцеположення та знаходиться в зоні обслуговування іншого MSC/VLR. Для того щоб знову не реєструвати абонента в мережі, а лише запитати у попереднього VLR/MSC ключі шифрування та повідомити HLR о зміні MSC/VLR абонентом.

Використовуючи повідомлення примітив «SendParameters» зломисник має можливість виконати атаки на розкриття мобільного ідентифікатора, розкриття профілю абонента, розкриття ключів шифрування радіосигналу, атаку на порушення доступності абонента та атаку, яка дає можливість направити вхідні виклики.

Атака на розкриття мобільного ідентифікатора є найголовнішою, тому що без мобільного ідентифікатора зломисник не зможе виконувати більш складні атаки. Атака на розкриття профілю виконується за допомогою аргументу примітива «SendParameters», в якому передається бітовий масив з повідомленням «RequestInfo» з запитом на отримання профілю абонента. Атака на розкриття профілю абонента може служити продовженням атак для зломисника, змінивши профіль абонента він дуже легко зможе маніпулювати з дзвінками та повідомленнями абонента. Атаки на розкриття ключів шифрування, дає можливість зломиснику прослуховувати дзвінки. Атака, яка дає можливість направити вхідні виклики та атака на порушення доступності абонента. В поточній версії підсистеми MAP використовується повідомлення примітив «UpdateLocation», для того щоб повідомити HLR, що абонент хоче зареєструватись в мережі мобільного зв'язку або змінив базову станцію і знаходиться в зоні нового MSC/VLR. В першій версії підсистеми MAP ці процедури виконувало повідомлення «SendParameters». Тому і попередні атаки, які використовували повідомлення примітив

«UpdateLocation», можуть бути виконані зломисником за допомогою повідомлення «SendParameters».

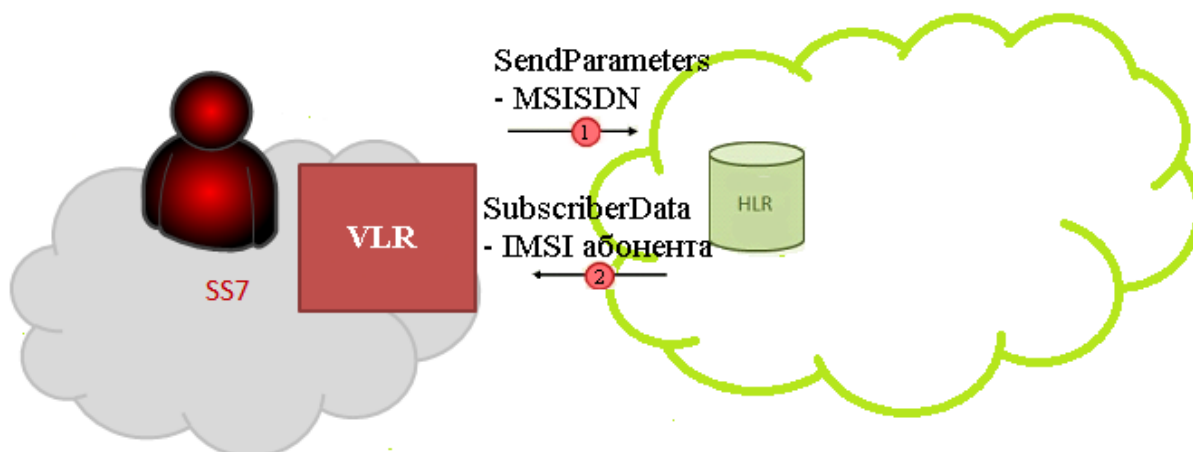


Рисунок 4.13 - Схема атак на розкриття мобільного ідентифікатора та розкриття профілю абонента за допомогою повідомлення примітива «SendParameters»

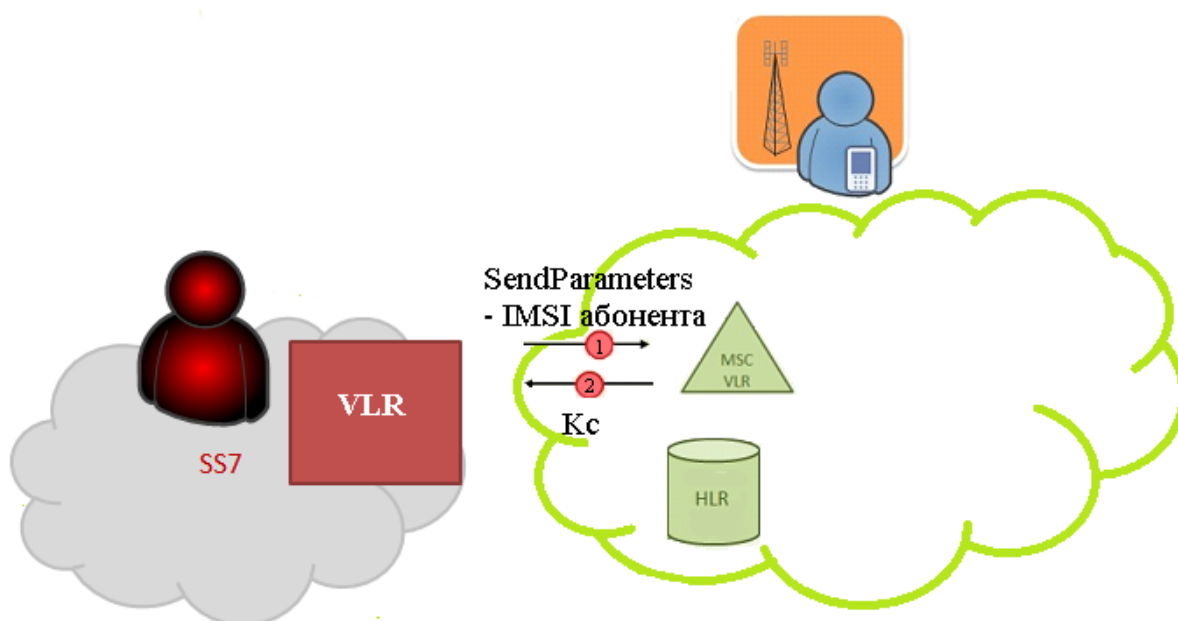


Рисунок 4.14 - Схема атак на розкриття ключів шифрування за допомогою повідомлення примітива «SendParameters»

«RemoteUserFree» - це повідомлення примітив використовується для видалення абонентської інформації з бази даних. Це повідомлення відправляє HLR, коли абонент змінив зону обслуговування на інший VLR/MSC, а інформацію про абонента з попереднього VLR/MSC потрібно видалити.

Використовуючи повідомлення примітив «RemoteUserFree», зломисник має можливість виконати атаку на порушення доступності абонента. Відправляючи це повідомлення від імені HLR на VLR/MSC в зоні якого обслуговується абонент, VLR/MSC видаляє інформацію про абонента і вважає, що він вийшов з зони його обслуговування. Тепер коли інші абоненти будуть викликати абонента жертву, вони отримають відповідь, що абонент недоступний.



Рисунок 4.15 - Схема атаки на порушення доступності абонента за допомогою повідомлення примітива «RemoteUserFree»

«NoteSubscriberDataModified» - це повідомлення примітив використовується HLR, для того щоб повідомити платформі GSMSCF про зміни в профілі абонента, за якими він повинен обслуговувати абонента.

Використовуючи повідомлення примітив «NoteSubscriberDataModified», зломисник має можливість виконати атаки на зміну профілю абонента, на порушення доступності абонента та атаку, яка дає можливість направляти вхідні виклики.

Атаку на зміну профілю зломисник може використовувати для своїх корисних цілей, змінивши в своєму профілі тарифи та доступні для нього послуги. Атака, яка дає можливість направити вхідні дані, використовується разом з атакою на зміну профілю. Додавши у профіль абонента послугу безумовної переадресації, зломисник має можливість отримувати всі вхідні дані абонента жертви через себе. Атака на порушення доступності, використовується разом з атакою на зміну профілю для того, щоб змінити профіль абонента таким чином, щоб GSMSCF блокував всі вхідні та вихідні дані, що зробить його недоступним для інших абонентів.

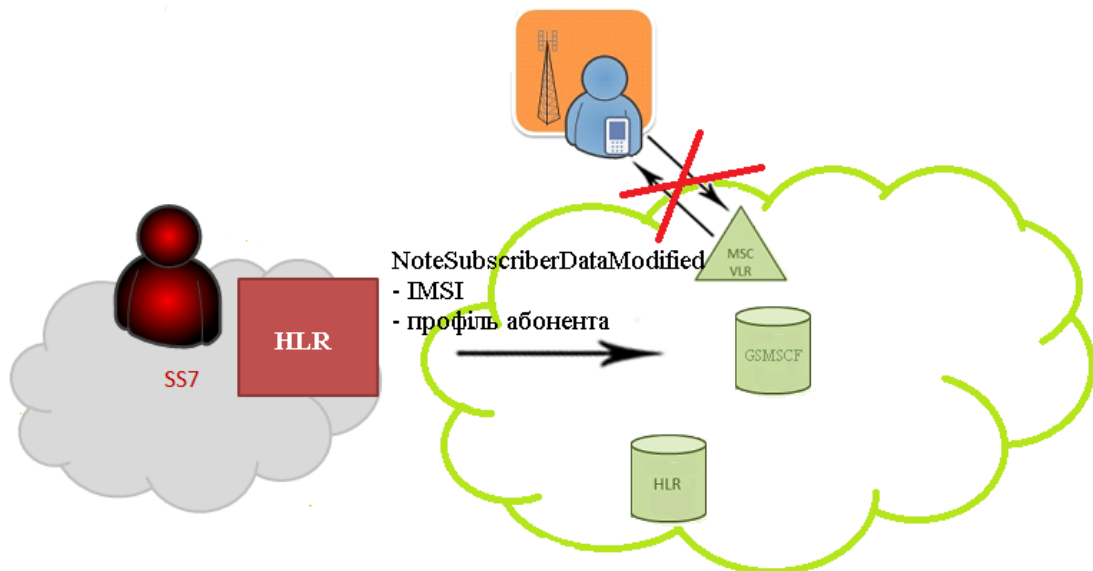


Рисунок 4.16 - Схема атаки на порушення доступності абонента за допомогою повідомлення примітива «NoteSubscriberDataModified»

«ReportSMDeliveryStatus» - це повідомлення примітив використовується SMS-GMSC для того, щоб повідомити HLR, що повідомлення не може бути доставлено. Після чого HLR відмічає абонента як тимчасово недоступного і встановлює флаг очікування для повторної передачі повідомлення.

Повний процес повідомлення примітива «ReportSMDeliveryStatus» на рисунку 4.17. Якщо SC не може доставити повідомлення абоненту, він відповідає в SMS-GMSC. Після того як SMS-GMSC отримує відповідь, що повідомлення не може бути доставлено, він посилає повідомлення примітив «ReportSMDeliveryStatus» на HLR, який після чого встановлює флаг очікування повідомлення. Після чого посилає повідомлення примітив «alertServiceCentre» до SMS-IWMSC з інформацією про те, що повідомлення не може бути доставлено, та очікує коли абонент буде в мережі доступний. Коли VLR/MSC отримує інформацію про те що абонент в мережі та доступний він відправляє повідомлення примітив «readforSM» в HLR. Отримавши повідомлення примітив, HLR відправляє повідомлення примітив «alertServiceCentre» до SMS-IWMSC, який в свою чергу інформує про це SC. Після чого процес доставки повідомлення починається знову з повідомлення «forwardSM».

Використовуючи повідомлення примітив «ReportSMDeliveryStatus», зломисник має можливість виконати атаку на порушення доступності абонента. Схема атаки представлена на рисунку 4.18. Відправляючи це повідомлення від імені SMS-GMSC на HLR, домашній реєстр відмічає в профілі абонента, що він тимчасово недоступний, таким чином абонент не зможе приймати вхідні SMS - повідомлення, бо всі повідомлення будуть чекати коли абонент знову буде доступним.

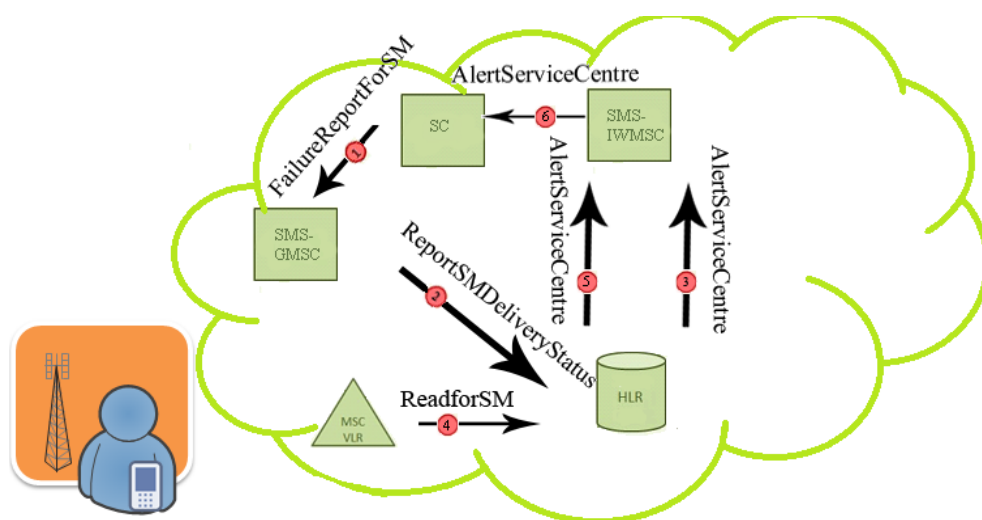


Рисунок 4.17 - Схема роботи повідомлення примітива «ReportSMDeliveryStatus»

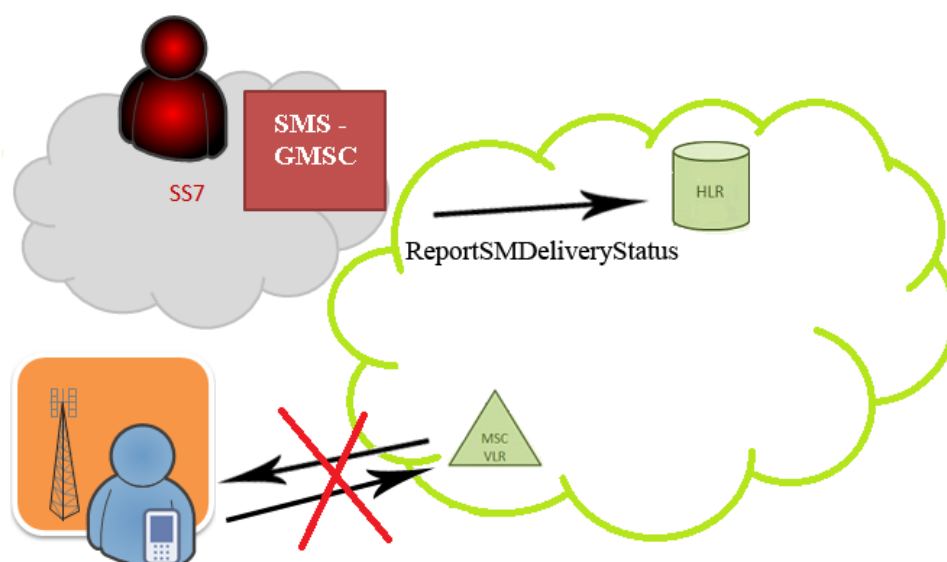


Рисунок 4.18 - Схема атаки на порушення доступності абонента за допомогою повідомлення примітива «ReportSMDeliveryStatus»

«ResumeCallHandling» - це повідомлення примітив використовується для передачі управління виклику між MSC/VLR та GMSC. Це повідомлення відправляє HLR на GMSC для того, щоб виконати переадресацію, якщо абонент недоступний і ця послуга була активована абонентом раніше.

Використовуючи повідомлення примітив «ResumeCallHandling», зловмисник має можливість виконати атаку на порушення доступності абонента, та виконати атаку, яка дає можливість направити вхідні виклики.

Виконуючи атаку, яка дає можливість направити вхідні виклики, зловмисник відправляє повідомлення примітив «ResumeCallHandling» від імені HLR на GMSC. Цим повідомленням він активує переадресацію вхідних викликів на адресу GMSC, який знаходиться під його контролем. Після цього зловмисник має ряд можливостей, заблокувати вхідний виклик, зробити абонента недоступним, або направити виклик на MSC і мати можливість прослуховувати його.

Атака на порушення доступності абонента є варіантом атаки, яка дає можливість направляти вхідні виклики. Зловмисник вказує адресу на інший GMSC, який не має інформацію про абонента і таким чином буде ігнорувати вхідні виклики до абонента.

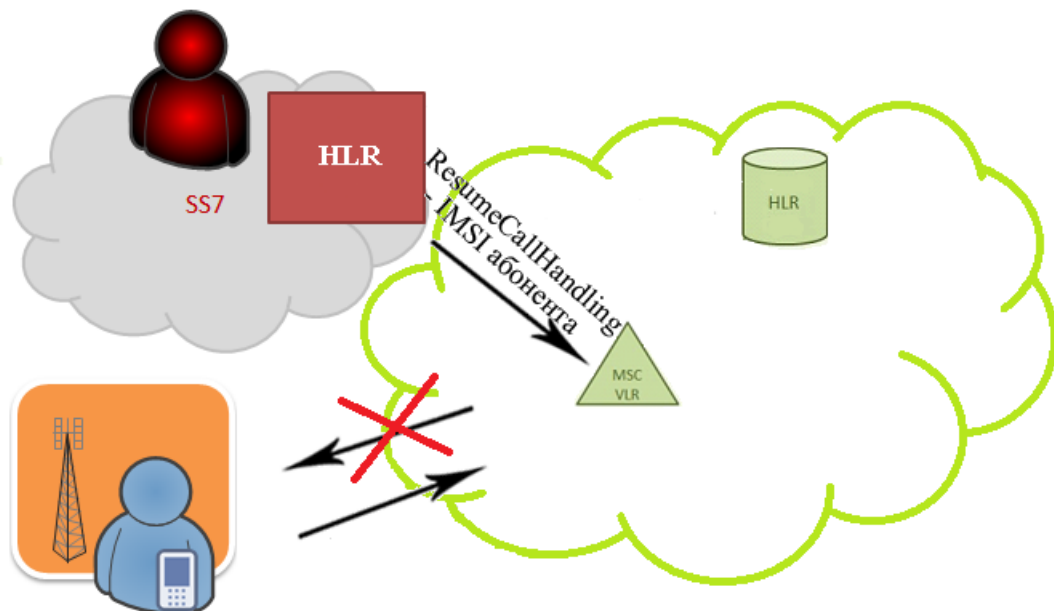


Рисунок 4.19 - Схема атаки на порушення доступності абонента за допомогою повідомлення примітива «ResumeCallHandling»

Таким чином була розглянута лише мала частина атак, які злоумисник може здійснити, отримавши доступ до мережі мобільного зв'язку. Та розглянута лише мала частина небезпечних повідомлень примітивів підсистеми MAP, використовуючи які, злоумисник також може домогтися тих самих атак, але вже іншим способом. Завдяки атакам та повідомленням примітивів злоумисник має можливість:

- розкрити конфіденційний ідентифікатор абонента;
- розкрити розташування абонента;
- порушити доступності абонента;
- перехопити вхідні SMS - повідомлення;
- маніпулювати USSD - запитами;
- розкрити профіль абонента;
- змінити профіль абонента у VLR;
- розкрити ключі шифрування;
- прослуховувати вихідні виклики;
- направляти вхідні виклики;
- направляти вхідні дані;
- відмовити в обслуговуванні сервіс пакетної передачі;
- відмовити в обслуговуванні MSC/VLR для вхідних викликів.

В ході розгляду четвертої глави було розглянуто нормальну поведінку в роботі системи при реєстрації абонента в мережі мобільного зв'язку, при здійсненні вихідного дзвінка і надсилання повідомлення. Для розуміння проблем захищеності мереж мобільного зв'язку були приведені основні атаки. Найбільшу загрозу представляє атака на розкриття конфіденційного ідентифікатора абонента, бо саме всі дані отримані при успішній реалізації цієї атаки, можуть використовуватись злоумисником в більш складних атаках. Була представлена мала частина потенційно уразливих повідомлень примітивів, було описано їх призначення, відправники та отримувачі при нормальній поведінки в роботі. Проаналізувавши профілі злоумисників та нормальну поведінку уразливих повідомлень, це допомогло для кожного

небезпечного повідомлення сформувані можливі потенційні атаки з боку атакуючого.

5 АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ МОБІЛЬНИХ МЕРЕЖ

Продemonструвавши атаки на мережі мобільного зв'язку в попередньому розділі, можна стверджувати, що безпека мереж мобільного зв'язку операторів перебуває під загрозою. Вирішити проблеми безпеки мереж мобільного зв'язку на основі технології SS7, можна за допомогою двох напрямків. Перший напрямок полягає у створенні та впровадженні нового стека протоколів, який буде забезпечувати безпеку мереж мобільного зв'язку. Даний напрямок є дуже дорогим і для його створення і впровадження потрібно дуже багато часу. Крім того потрібно перетворення всієї інфраструктури мереж мобільного зв'язку під новий стек протоколів. Другим напрямком у вирішенні даної проблеми є створення засобів захисту на основі існуючої інфраструктури мережі, які будуть забезпечувати безпеку мереж мобільного зв'язку.

Актуальними на сьогоднішній день можна виділити наступні засоби забезпечення безпеки мереж мобільного зв'язку:

- SMS Home Routing;
- Системи моніторингу SS7;
- SS7 Firewall;
- SS7 IDS/IPS.

«SMS Home Routing» - це апаратно-програмний комплекс, призначений для приховування реальних IMSI абонентів і адрес мережевого обладнання. Принцип роботи «SMS Home Routing» представлений на рисунку 5.1. Коли SC передає повідомлення примітив «SendRoutingInfoForSM» з номером MSISDN абонента. STP передає запит і MSISDN абонента далі на «SMS Home Routing». У відповідь обладнання «SMS Home Routing» посилає випадково сгенерованное число IMSI і в якості адреси MSC/VLR абонента він відправляє свою адресу. Отримавши інформацію, SC передає SMS - повідомлення на отриману адресу, тобто

знову відправляє в «SMS Home Routing». Отримавши SMS - повідомлення, «SMS Home Routing» посилає повторно повідомлення примітив «SendRoutingInfoForSM» в HLR, але вже з метою дізнатися реальний IMSI і адресу MSC/VLR абонента. Отримавши достовірну інформацію, «SMS Home Routing» здійснює відправку SMS - повідомлення абоненту [14].

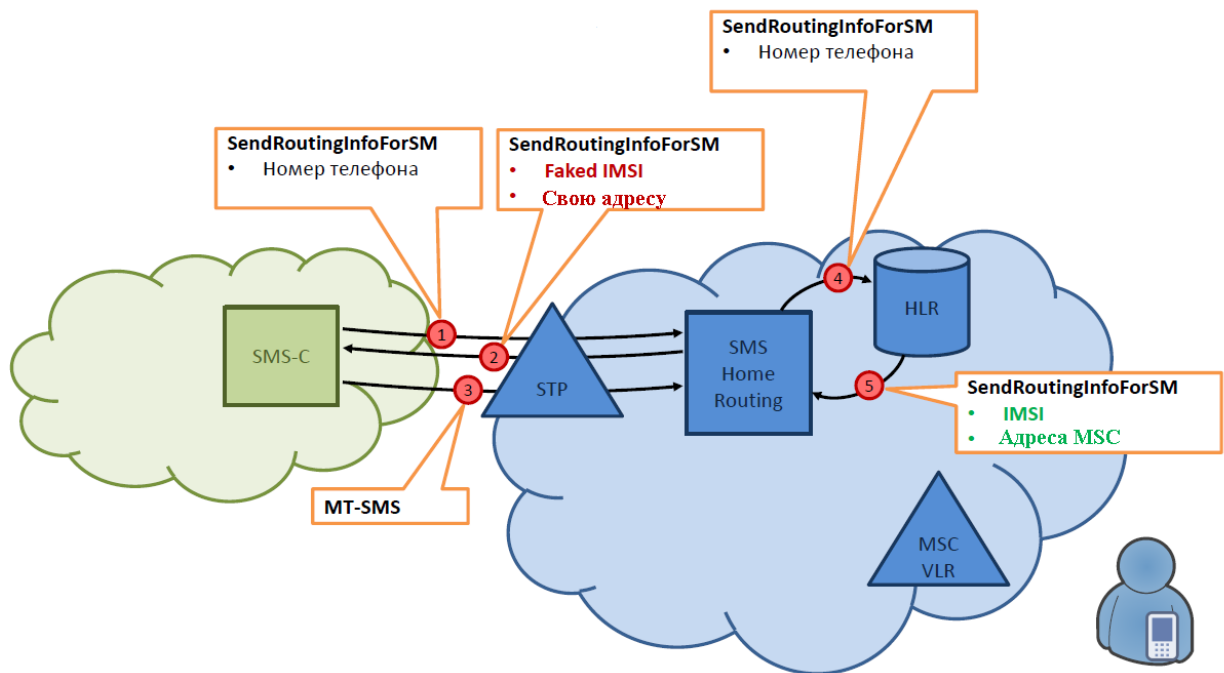


Рисунок 5.1 - Схема роботи «SMS Home Routing»

Перевагою «SMS Home Routing» є те, що засіб захисту запобігає розкриття IMSI абонента, який є ключовим для реалізації більш складних схем атак.

Недоліком цього засобу захисту є те, що воно не дозволяє повністю забезпечити приховування конфіденційних даних абонентів і мережі. Це пов'язано з такими причинами як:

- помилки конфігурації «SMS Home Routing»;
- помилки конфігурації STP;
- інші повідомлення примітиви для отримання IMSI абонента.

За перерахованими перевагами і недоліками, можна зробити висновок про те, що засіб захисту «SMS Home Routing» є обов'язковим для установки у всіх мережах мобільного зв'язку, однак навіть при правильному налаштуванні і конфігурації системи і устаткування, воно є недостатнім для забезпечення безпеки мережі мобільного зв'язку.

«Системи моніторингу SS7» - це апаратно-програмний комплекс, в який входять пристрої «Probe», впроваджені на стиках мережі, які збирають, передають і записують копії сигнального трафіку на виділений сервер моніторингу в базу даних, де інформація аналізується на наявність мережових проблем [15].

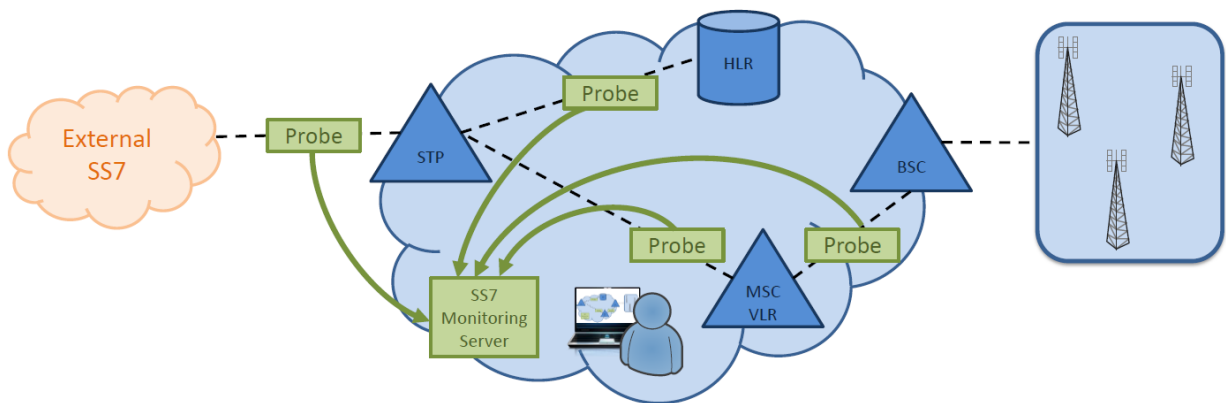


Рисунок 5.2 - Схема роботи «систем моніторингу SS7»

Як перевагою так і головним недоліком «систем моніторингу SS7» є те, що основне призначення систем моніторингу - це аналіз мережових проблем, отримання інформації про якість роботи і експлуатації мережі. Крім цього, функціонал аналізу нелегітимного трафіку може мати відчутні відмінності, що безпосередньо пов'язано з технічною реалізацією виробників «систем моніторингу SS7». Також важливим є те, що для отримання інформації про атаки, оператору системи необхідно буде провести велику кількість запитів, що займають досить багато часу. Це відбувається внаслідок

того що, в мережі циркулює великий обсяг трафіку, який накладає обмеження на термін зберігання копій.

За перерахованими перевагами і недоліками «систем моніторингу SS7», можна зробити висновок, що даний засіб захисту не зможе забезпечити безпеку мережі мобільного зв'язку по ряду причин:

- призначення «систем моніторингу SS7» - це аналіз мережевих проблем, отримання інформації про якість роботи мережі і експлуатації мережі;
- можливість моніторингу нелегітимного SS7 трафіку залежить від технічної реалізації системи;
- необхідно зробити багато окремих запитів для отримання інформації про атаки;
- термін зберігання даних обмежений до 1 місяця.

«SS7 Firewall» - це апаратно-програмний комплекс, який впроваджується на кордонах мережі і здійснює фільтрацію небажаного трафіку [15]. Комплекс «SS7 Firewall», як правило, може впроваджуватися перед прикордонним STP, паралельно STP і безпосередньо в STP.

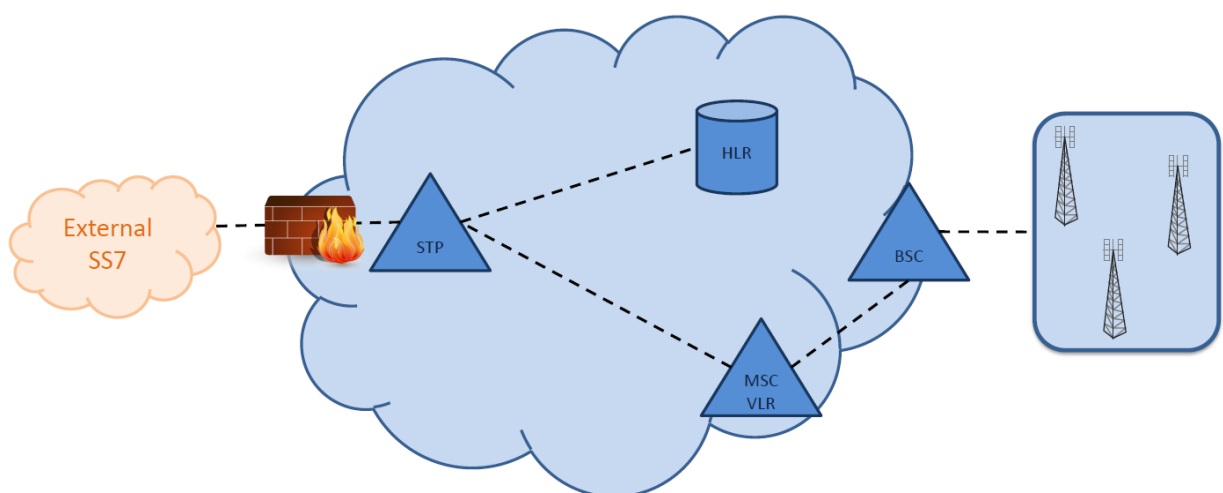


Рисунок 5.3 - Схема впровадження «SS7 Firewall» перед STP

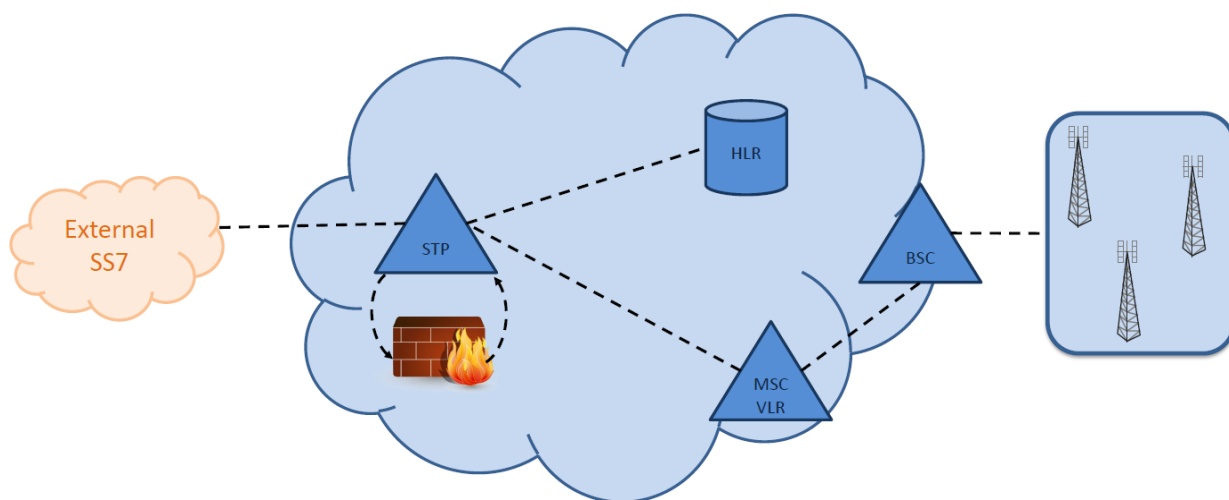


Рисунок 5.4 - Схема впровадження «SS7 Firewall» паралельно STP

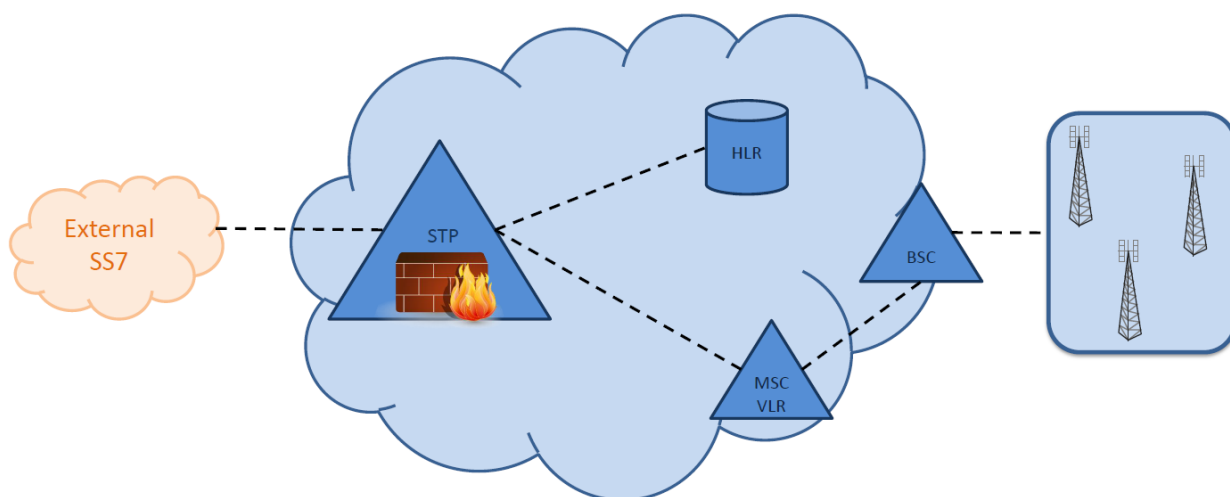


Рисунок 5.5 - Схема впровадження «SS7 Firewall» безпосередньо в STP

Системи «SS7 Firewall» здійснюють фільтрацію трафіку за чорно-білими списками. Дану базу даних задає оператор системи в ручну. Істотним недоліком в цьому всьому є те, що некоректна конфігурація системи «SS7 Firewall» може чинити негативний вплив на працездатність сервісу мережі мобільного зв'язку. Даний фактор має суттєвий вплив при наданні роумінгу своїм абонентам або абонентам іншої мережі. Так як запити з їхнього боку до

оператора мережі мобільного зв'язку системою «SS7 Firewall» можуть розцінюватися як небажаний трафік, що в подальшому призведе до блокування абонентів і їх трафіку в роумінгу. Внаслідок чого оператор мережі мобільного зв'язку понесе як фінансові втрати, так і репутаційні.

Про системи «SS7 Firewall» можна зробити наступний висновок, що даний засіб захисту використовується в мережах мобільного зв'язку, однак з великою обережністю, що і привертає зловмисників, так як даний засіб захисту не може в повній мірі забезпечити безпеку мережі мобільного зв'язку.

«SS7 IDS» (Intrusion Detection System) - це апаратно-програмний комплекс, Виявлення вторгнень в мережу мобільного зв'язку оператора. Комплекс «SS7 IDS» зазвичай впроваджується паралельно STP. Принцип роботи SS7 IDS полягає в наступному, комплекс бере копію сигнального трафіку STP, аналізує трафік по базі даних, яка закладена в комплексі і робить висновок про наявність атак і нелегітимних дій. Якщо система виявляє атаку або нелегітимну дію, то повідомляє оператору мережі [15].

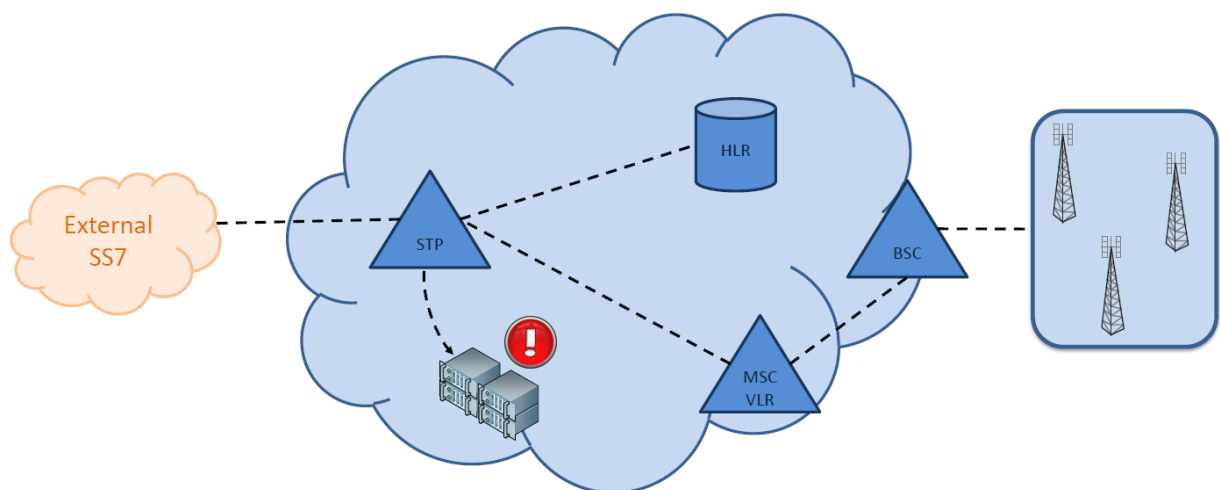


Рисунок 5.6 - Схема впровадження «SS7 IDS» паралельно STP

«SS7 IDS/IPS» (Intrusion Prevention System) - це апаратно-програмний комплекс. Виявлення і запобігання вторгнень в мережу мобільного зв'язку

оператора [15]. Комплекс «SS7 IDS/IPS», як правило, може впроваджуватися перед прикордонним STP, або паралельно STP.

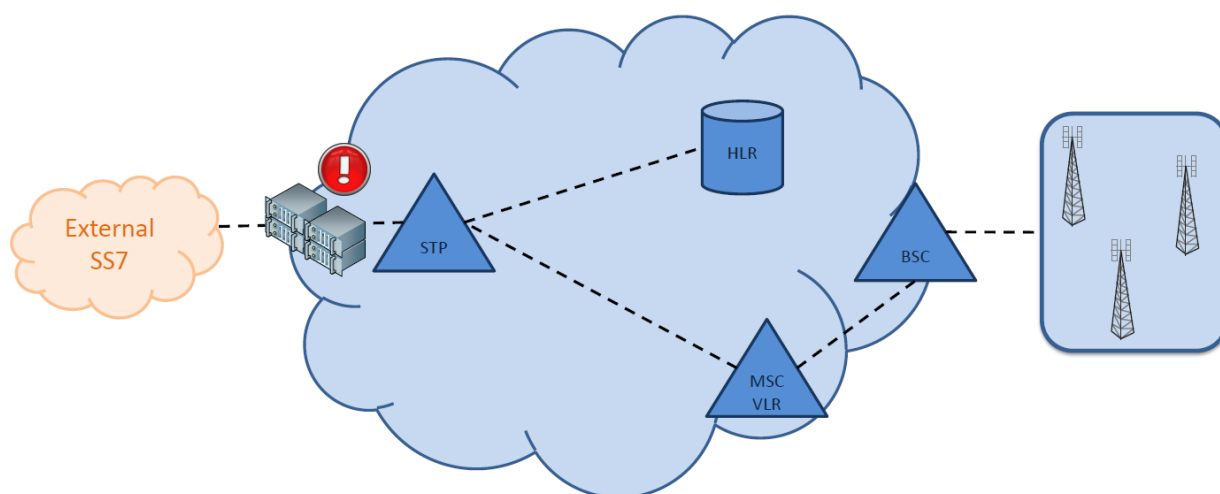


Рисунок 5.7 - Схема впровадження «SS7 IDS/IPS» перед STP

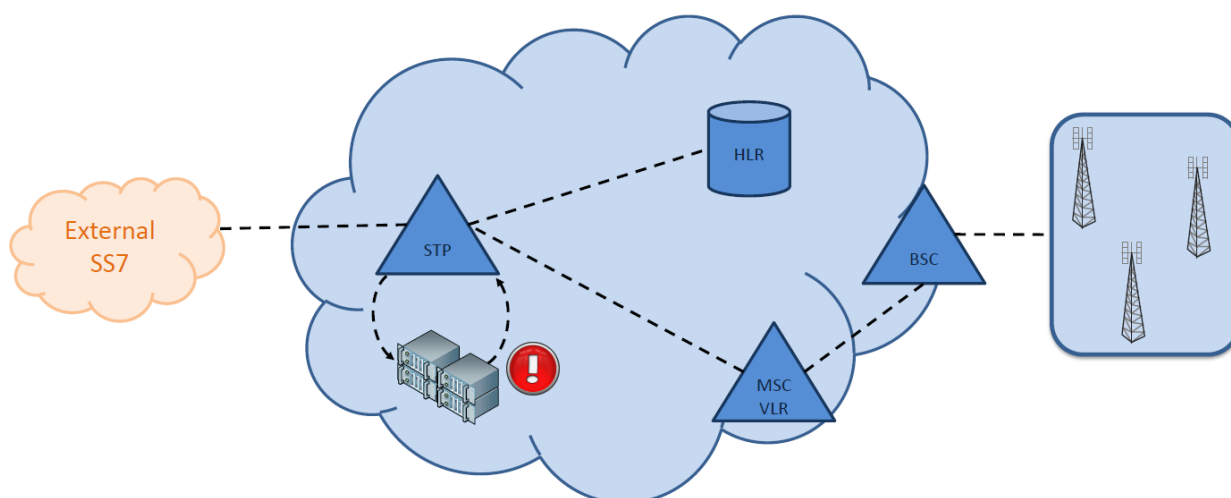


Рисунок 5.8 - Схема впровадження «SS7 IDS/IPS» паралельно STP

Принцип роботи «SS7 IDS/IPS» полягає в наступному, комплекс бере копію сигнального трафіку STP, аналізує трафік по базі даних, яка закладена в комплексі і робить висновок про наявність атак і нелегітимних дій. Якщо система виявляє атаку або нелегітимну дію, то повідомляє оператору мережі, а після чого блокує [15].

Всі повідомлення в системі «SS7 IDS/IPS» поділяються на три великі групи:

- неприпустимі;
- умовно неприпустимі;
- з попередньою перевіркою розташування.

Неприпустимі повідомлення - повідомлення з кодами операцій, які ні за яких умов не повинні приходити в мережу оператора з боку зовнішніх підключень. Наприклад, до таких повідомлень можна віднести:

- «SendIMSI» - повідомлення протоколу MAP, яке використовується для запиту ідентифікатора IMSI абонента за його номером мобільної станції [17];
- «AnyTimeInterrogation» - повідомлення протоколу MAP, яке використовується для запиту за номером мобільної станції абонента ідентифікатора базової станції, де в даний момент знаходиться абонент [17].

Умовно неприпустимі - повідомлення з кодами операцій, які не повинні приходити в мережу оператора з боку зовнішніх підключень, адресовані абонентам своєї мережі. Наприклад, до таких повідомлень можна віднести:

- «ProviderSubscriberInfo» - повідомлення протоколу MAP, яке використовується для отримання інформації про місцезнаходження абонента в роумінгу від оператора іншої мережі [17];
- «ProviderRoamingNumber» - повідомлення протоколу MAP, яке використовується для отримання роумінгового номера від операторів інших мереж для абонентів у роумінгу [17].

З попередньою перевіркою розташування - повідомлення з кодами операцій, які не повинні приходити в мережу оператора з боку зовнішніх підключень, адресовані абонентам своєї мережі, якщо абонент в цей момент зареєстрований в домашній мережі. Наприклад, до таких повідомлень можна віднести:

- «ProcessUnstructuredSS-Reques» - повідомлення для передачі USSD запитів [17];
- «RegisterSS» - повідомлення дозволяє управляти додатковими послугами.

Роблячи висновки по системам «SS7 IDS/IPS», можна зазначити, що даний засіб захисту є найбільш ефективним рішенням забезпечення безпеки мереж мобільного зв'язку. Перевагами даної системи є те, що головне призначення системи - це виявлення та запобігання вторгнень в мережах мобільного зв'язку. Системи мають зручний моніторинг, який визначає і реагує на нелегітимні дії пов'язані з безпекою системи на відміну від «систем моніторингу SS7». Іншою перевагою «SS7 IDS/IPS» є те, що система не робить негативного впливу на сигнальний трафік і на надані оператором послуги, оскільки система аналізує копії трафіку, чого не може забезпечити «SS7 Firewall». Рішення комплексу IPS дозволяє з'ясувати причину підозрілого трафіку, а в разі атак і нелегітимних дій, зовсім запобігти їх на початковому етапі.

Таким чином система «SS7 IDS/IPS» має ряд наступних переваг щодо інших засобів захисту:

- не впливає на трафік SS7;
- показує наявність або відсутність реальних атак з сигнальної мережі;
- можливість з'ясування причин і джерел підозрілого SS7 трафіку;
- глибокий аналіз стека протоколів SS7;
- кореляція параметрів на різних рівнях SS7;
- можливість блокування повідомлень SS7 по гнучко - формованому шаблону.

Роблячи висновки за засобами захисту мобільних мереж, складаємо порівняльну таблицю 5.1. В якості оцінок введемо умовні позначення:

- «+» - повністю забезпечує безпеку мережі мобільного зв'язку від даного типу атаки;
- «+-» - забезпечує безпеку мережі мобільного зв'язку від більшості реалізацій даного типу атаки;
- «-+» - забезпечує безпеку мережі мобільного зв'язку від деяких реалізацій атак даного типу;
- «-» - не забезпечує безпеку мережі мобільного зв'язку від даного типу атаки.

Таблиця 5.1 - Порівняння засобів захисту мереж мобільного зв'язку

Атаки	«SMS Home Routing»	«Системи моніторингу SS7»	«SS7 Firewall»	«SS7 IDS/IPS»
Розкриття конфіденційного ідентифікатора абонента	-+	-	-+	-+
Розкриття розташування абонента	-+	-	-+	-+
Порушення доступності абонента	-	-	-	-+

Продовження таблиці 5.1 - Порівняння засобів захисту мереж мобільного зв'язку

Атаки	«SMS Home Routing»	«Системи моніторингу SS7»	«SS7 Firewall»	«SS7 IDS/IPS»
Перехоплення вхідних SMS - повідомлень	-	-	-	-+
Маніпулювання USSD - запитами	-	-	-+	-+
Зміна профілю абонента	-	-	-	-+
Прослуховування вихідних викликів	-	-	-	-+
Перенаправлення вхідних викликів	-	-	-	-
Відмова в обслуговуванні для вхідних викликів	-	-+	-+	-+
Розкриття профіля абонента	-	-	-	-
Відмова в обслуговуванні для сервісу пакетної передачі	-	-	-	-
Перенаправлення вхідних даних	-	-	-	-
Розкриття ключів шифрування	-	-	-	-

В ході розгляду п'ятої глави було представлено напрямки у рішенні захищеності мереж мобільного зв'язку. Були представлені актуальні на сьогоднішній день засоби забезпечення безпеки мереж мобільного зв'язку до

яких відносять «SMS Home Routing», «системи моніторингу SS7», «SS7 Firewall» та «SS7 IDS/IPS». Для кожного засобу захисту представлено загальний принцип роботи. За всіма засобами захисту було виконано порівняльний аналіз. За яким маємо можливість зазначити, що найбільш ефективним засобом захисту є «SS7 IDS/IPS». Даний засіб захисту має найбільш гнучкі модулі виявлення і запобігання вторгнень в мережу мобільного зв'язку. Однак вбудовані модулі захисту використовують для аналізу вже досліджені повідомлення примітиви стека протоколів SS7, що робить мережі мобільного зв'язку та засоби захисту мереж все ще уразливими перед атаками, коли зломисник має можливість використовувати інші потенційно небезпечні повідомлення примітиви, маніпулюючи ними і посилаючи їх на той чи інший елемент мережі мобільного зв'язку. В підрозділі 4.10 було розглянуто лише малу частину серед усіх існуючих повідомлень в підсистемі MAP, які потрібно вивчати та розширювати список небезпечних повідомлень для того щоб розширити область засобів захисту та запобігти серйозних подальших атак.

6 ДІАГНОСТИКА ПОТРЕБ ІНВЕСТИВАННЯ ДОСЛІДЖЕНЬ З ЗАХИЩЕНОСТІ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЇ SS7

6.1 Загальні положення

Інвестиції - це сукупність витрат, спрямованих у формі цілеспрямованого вкладу коштів в різні сфери і галузі діяльності для подальшого отримання прибутку і досягнення певного результату. Інвестиціями є всі види майнових та інтелектуальних цінностей, що вкладуються в об'єкти підприємницької та інших видів діяльності, в результаті якої створюється прибуток або досягається економічний чи соціальний ефект [12].

Об'єктами інвестиційної діяльності можуть бути будь-яке майно, в тому числі основні засоби і оборотні активи в усіх галузях та сферах народного господарства, цінні папери, цільові грошові вклади, науково-технічна продукція, інтелектуальні цінності, інші об'єкти власності, а також майнові права [12].

Суб'єктами інвестиційної діяльності можуть бути громадяни і юридичні особи України та іноземних держав, а також держави [12].

Метою дипломної роботи є аналіз захищеності мереж мобільного зв'язку на основі технології SS7. Даний аналіз в майбутньому допоможе доповнювати засоби захисту операторів мереж мобільного зв'язку та звертати увагу на уразливі місця та повідомлення мережі SS7. Все це робить аналіз захищеності мереж мобільного зв'язку на основі технології SS7 економічно доцільним.

Далі представлена економічна оцінка аналізу захищеності:

- короткий опис аналізу;
- визначення вартості аналізу;
- економічна оцінка роботи;
- висновки.

6.2 Короткий опис аналізу

В ході аналізу вивчається стек протоколів SS7, вивчається підсистема MAP. Аналізується нормальна поведінка роботи об'єктів мережі при процесах реєстрації абонента в мережі, при здійсненні вихідного дзвінка і надсилання повідомлення. Складається профіль зловмисника. Аналізуються знайдені уразливості та можливі напрямки атак. Аналізуються сучасні засоби захисту для мереж мобільного зв'язку.

6.3 Визначення вартості аналізу

Вартість аналізу визначається за фактичними витратами. В основі визначення вартості лежить перелік виконаних робіт та її трудомісткість.

Трудомісткість - показник, що характеризує витрати робочого часу на виробництво певної споживної вартості або на виконання конкретної операції.

Для визначення трудомісткості виконання робіт визначимо перелік основних етапів та видів робіт. По кожному виду робіт визначається також кваліфікаційний рівень виконавців.

Трудомісткість виконання аналізу визначимо за сумою трудомісткості етапів і видів робіт, оцінюваних в людях на день. Розподіл робіт за видами і кваліфікаційним рівнем виконавців, та величини трудомісткості для проведеного проекту наведені в Таблиці 6.1.

Таблиця 6.1 - Розрахунок трудомісткості

№	Етапи виконуваних робіт	Трудомісткість, люд./дні	
		Головний інженер	Інженер
1.	Розробка та уточнення технічного завдання	1	1

2.	Вивчення стека протоколів SS7	1	3
3.	Вивчення підсистеми MAP	1	2
4.	Аналіз можливих атак на мережу SS7	2	3
5.	Аналіз сучасних засобів захисту мобільних мереж	2	2
6.	Оформлення звіту	0	3
7.	Здача аналізу	1	1
8.	Підсумок	8	15

На основі трудомісткості виконання робіт буде розраховані витрати на оплату праці її виконавців.

6.3.1 Основна заробітна плата виконавців, єдиний соціальний внесок, непрямі витрати

Основна заробітна плата - це винагорода за виконання роботи відповідно до встановлення норм праці (годині, виробітку, обслуговування, посадових обов'язків) [3].

Основна заробітна плата виконавців аналізу розраховується на підставі наступних даних:

- трудомісткість виконання робіт $T_{гол.інж.}$ та $T_{інж.}$;
- оклад керівника проекту, головного інженера, за місяць (двадцять два робочих дня) складає 8 000 грн., денна ставка восьми часового робочого дня керівника проекту складає $C_{гол.інж.} = 363 \text{ грн.}$;
- оклад інженера за місяць (двадцять два робочих дня) складає 6 000 грн., денна ставка восьми часового робочого дня інженера складає $C_{інж.} = 273 \text{ грн.}$;
- єдиний соціальний внесок $ЄСВ = 22\%$;
- відсоток додаткової заробітної плати = 15%;
- накладні витрати = 40 %.

Основна заробітна плата виконавців ($Z_{осн.з/пл}$) розраховується за формулою:

$$Z_{осн.з/пл} = T_{гол.інж.} \times C_{гол.інж.} + T_{інж.} \times C_{інж.} \quad (6.1)$$

$$Z_{осн.з/пл} = 8 \times 363 + 15 \times 273 = 6999 \text{ грн.}$$

Додаткова заробітна плата — це винагорода за понаднормативну працю, трудові успіхи та винахідливість і за особливі умови праці. Вона включає доплати, надбавки, гарантії та компенсації, передбачені чинним законодавством, премії, пов'язані з виконанням виробничих завдань та функцій [3].

Додаткова заробітна плата виконавців ($Z_{додат.з/пл}$) розраховується за формулою:

$$Z_{додат.з/пл} = Z_{осн.з/пл} \times \frac{15}{100} \quad (6.2)$$

$$Z_{додат.з/пл} = 5979 \times 0,15 = 1049,85 \text{ грн.}$$

Єдиний соціальний внесок - обов'язковий платіж до системи загальнообов'язкового державного соціального страхування, що справляється в Україні з метою забезпечення страхових виплат за поточними видами загальнообов'язкового державного соціального страхування [5].

Внески розраховуються за формулою:

$$B_{соц.} = (Z_{осн.з/пл} + Z_{додат.з/пл}) \times \frac{ЄСВ}{100} \quad (6.3)$$

$$B_{соц.} = (5979 + 896,85) \times 0,22 = 1770,75 \text{ грн}$$

Накладні витрати - це витрати не пов'язані безпосередньо з технологічним процесом на виготовлення продукції, а утворюються під впливом певних умов роботи з організації, управління та обслуговування виробництва [19].

Накладні витрати розраховуються за формулою:

$$NB = (Z_{осн.з/п.л} + Z_{додат.з/п.л}) \times \frac{40}{100} \quad (6.4)$$

$$NB = 6999 + 1049,85 \times 0,4 = 3219,54 \text{ грн.}$$

6.3.2 Витрати на матеріал

Вартість витратних матеріалів, необхідних для виконання роботи, визначається виходячи з величини їх витрат, діючих цін і транспортних витрат. В даному розрахунку відносяться використані при виконанні аналізу матеріалів. Калькуляція витрат - Таблиця 6.2.

Таблиця 6.2 - Калькуляція витрат за матеріалом

Матеріал	Одиниця виміру	Кількість	Ціна, грн.	Сума, грн.
Папір для принтера	пачка	1	115	115
Картридж для принтера	штука	1	438	438
Транспортні витрати			14	
Загалом				567

6.3.3 Витрати на послуги сторонніх організацій

Для розробки використовувалась одна стороння організація: інтернет провайдер «Київстар».

Розмір тарифу інтернету від компанії «Київстар» - $C_{інтер.} = 140 \text{ грн/місяц.}$

Податок на додану вартість (ПДВ) - це непрямий податок, який входить в ціну товарів (робіт, послуг) і сплачується покупцем, але його облік і перерахування до державного бюджету здійснює продавець (податковий агент). ПДВ складає 20 %.

Для розрахунку витрат на інтернет ($B_{інтер.}$), скористаємося формулою:

$$B_{інтер.} = T_{інтер.} \times \frac{C_{інтер.}}{1,2}; \quad (6.5)$$

де $T_{інтер.}$ - це кількість місяців використання Інтернету; 1,2 - це коефіцієнт для розрахунку коштів не враховуючи 20% ПДВ.

$$B_{інтер.} = 3 \times 117 = 351 \text{ грн.}$$

У підсумку, витрати на послуги сторонніх організацій ($B_{стор.орг.}$) є рівними витратам на оплату Інтернету.

$$B_{стор.орг.} = B_{інтер.} \quad (6.6)$$

$$B_{стор.орг.} = 351 \text{ грн.}$$

6.3.4 Витрати на утримання, експлуатацію та амортизацію обладнання

Витрати, пов'язані з утриманням техніки, є складовою всіх витрат підприємства. Усі витрати на утримання техніки поділяють на постійні і змінні. Постійні витрати - це витрати, які не залежать від інтенсивності використання техніки - кількості годин роботи або виконаного обсягу робіт [2].

Змінні витрати на техніку безпосередньо пов'язані з її експлуатацією. До них відносять витрати на паливо і мастила, ремонт техніки, оплату праці робітників, які її обслуговують, інші витрати [2].

При розробці методики використовувалося обладнання у вигляді двох комп'ютерів з первісною вартістю 11 700 грн. кожен. Для них необхідно прорахувати витрати на електроенергію і амортизаційні відрахування.

Так само буде враховуватися освітлення, необхідне для роботи. Всі ці витрати розраховуються на підставі наступних даних:

- розмір тарифу споживання електроенергії $C_{ел.} = 0,9$ грн кВт × ч;
- розмір споживання комп'ютером за 8 годин роботи $K_{ел.} = 1,76$ кВт;
- розмір споживання освітленням за 8 годин роботи $O_{ел.} = 2,88$ кВт;
- первісна вартість комп'ютера $B_{комп.} = 11\,700$ грн.;
- час використання основного засобу інженером $T_{вик.інж.} = 2$ місяці;
- час використання основного засобу головним інженером $T_{вик. гол.інж.} = 1$ місяць;
- термін амортизації комп'ютера = 36 місяців, норма амортизації комп'ютера за 3 місяці $H_a = 8\%$;
- коефіцієнт для розрахунку коштів не враховуючи 20 % ПДВ = 1.2.

Для розрахунку витрат на електроенергію на комп'ютери ($Z_{ел.комп.}$), скористаємося формулою:

$$B_{ел.комп.} = (T_{гол.інж.} + T_{інж.}) \times K_{ел.} \times \frac{C_{ел.}}{1,2} \times 8 \quad (6.7)$$

$$B_{ел.комп.} = (8 + 15) \times 1,76 \times 0,75 \times 8 = 242,88 \text{ грн.}$$

Для розрахунку витрат на електроенергію освітлення ($B_{ел.осв.}$), скористаємося формулою:

$$B_{ел.осв.} = (T_{гол.інж.} + T_{інж.}) \times O_{ел.} \times \frac{C_{ел.}}{1,2} \times 8 \quad (6.8)$$

$$B_{ел.осв.} = (8 + 15) \times 2,88 \times 0,75 \times 8 = 397,44 \text{ грн.}$$

Загальні витрати на електроенергію ($B_{заг.ел.}$) є сумою витрат електроенергії, що пішла на комп'ютери ($B_{ел.комп.}$) і освітлення ($B_{ел.осв.}$):

$$B_{заг.ел.} = B_{ел.комп.} + B_{ел.осв.} \quad (6.9)$$

$$B_{заг.ел.} = 242,88 + 397,44 = 640,32 \text{ грн.}$$

Амортизаційні відрахування - процес поступового перенесення вартості основних засобів на продукт, що виготовляється з їх допомогою. Для заміщення зношеної частини основних засобів виробництва підприємства роблять амортизаційні відрахування, тобто відрахування певних грошових сум відповідно до розмірів фізичного і морального зносу засобів виробництва [1].

Розрахуємо амортизаційні відрахування по основному засобу за 3 місяці:

$$A_{комп.} = B_{комп.} \times \frac{H_a}{100} \quad (6.10)$$

$$A_{комп.} = 11\,700 \times 0,08 = 936 \text{ грн.}$$

Обчислимо амортизаційні відрахування по основному засобу для кожного з виконавця щодо часу його використання:

$$A_{інж.} = A_{комп.} \times \frac{T_{вик.інж.}}{12} \quad (6.11)$$

$$A_{інж.} = 936 \times \frac{2}{12} = 156 \text{ грн.}$$

$$A_{\text{гол.інж.}} = A_{\text{комп.}} \times \frac{T_{\text{вик.гол.інж.}}}{12} \quad (6.12)$$

$$A_{\text{гол.інж.}} = 936 \times \frac{1}{12} = 78 \text{ грн.}$$

Загальна амортизація є сумою амортизації інженера і головного інженера:

$$A = A_{\text{гол.інж.}} + A_{\text{інж.}} \quad (6.13)$$

$$A = 78 + 156 = 234 \text{ грн.}$$

6.3.5 Загальний кошторис витрат на аналіз

Кошторис витрат являє собою зведений план усіх витрат підприємства виробничо-фінансової діяльності за певний календарний період. До кошторису включаються витрати основного і допоміжного виробництва, пов'язані з виготовленням та продажем продукції, товарів і послуг, а також на утримання адміністративно-управлінського персоналу, виконання різних робіт і послуг, у тому числі і не входять в основну виробничу діяльність підприємства [11].

Таблиця 6.3 - Загальний кошторис витрат

№	Найменування статті	Сума, грн.
1.	Витрати на оплату праці	8048,85
2.	Єдиний соціальний внесок	1770,75
3.	Витрати на матеріали	567
4.	Витрати на послуги сторонніх організацій	351
5.	Витрати на утримання, експлуатацію та амортизацію обладнання	640,32
6.	Амортизаційні відрахування	234
7.	Накладні витрати	3219,54
Загалом витрат		14831,46

6.4 Економічна оцінка роботи

Витрати на аналіз захищеності мереж мобільного зв'язку на основі технології SS7 вважаю доцільним. Даний аналіз в майбутньому допоможе доповнювати засоби захисту операторів мереж мобільного зв'язку та звертати увагу на уразливі місця та повідомлення мережі SS7. Завдяки вивченню аналізу збільшиться рівень забезпечення безпеки операторів мереж мобільного зв'язку, що дозволить їм уникнути великих фінансових і репутаційних втрат.

6.5 Висновок по главі шість

В ході діагностики потреб інвестування досліджень з захищеності мереж мобільного зв'язку було встановлено наступне:

- аналіз захищеності мереж мобільного зв'язку на основі технології SS7 дає змогу організувати більш надійний захист мереж від можливих атак зловмисників;
- дозволить операторам мереж мобільного зв'язку уникати великих фінансових і репутаційних втрат. Даний аналіз надасть конкурентну перевагу на ринку конкурентів мобільних операторів серед захищеності мереж мобільного зв'язку.

Виходячи з цього, можемо зробити висновок що, аналіз захищеності мереж мобільного зв'язку на основі технології SS7 економічно доцільний і необхідний.

7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1 Аналіз потенційних небезпек

Робоче приміщення являє собою офіс, розташований на другому поверсі чотирьохповерхової офісної будівлі. Габарити приміщення складають $8\text{ м} \times 8\text{ м} \times 3\text{ м}$. Площа приміщення складає 56 м^2 . У приміщенні знаходиться шість робочих місць, обладнаних персональними комп'ютерами.

Основними потенційними небезпеками при роботі в офісі є [9]:

- небезпека ураження електричним струмом, внаслідок недотримання правил електробезпеки або виходу з ладу електроприладів;
- порушення роботи кістково-м'язового апарату внаслідок тривалих статичних навантажень при роботі з ПК;
- нервово-психічні перевантаження внаслідок постійного контакту з клієнтами, колегами по роботі, керівництвом при вирішенні робочих питань, які можуть носити конфліктний характер і призвести до емоційного дискомфорту, внутрішнього роздратування, емоційної нестабільності та захворювань нервової системи;
- незадовільні ергономічні характеристики робочого місця внаслідок нераціонального планування робочого місця, що може призвести до механічних травм, уражень електричним струмом та порушень кістково-м'язового апарату;
- негативний вплив недостатнього освітлення робочої зони на зір та продуктивність роботи працюючого, внаслідок несправності освітлювальних приладів або неправильного проектування освітлювальної системи;
- негативний вплив незадовільних параметрів повітряного

середовища робочої зони на здоров'я працюючого, внаслідок неправильного проектування системи вентиляції або несправності її несправності;

- негативний вплив підвищеного рівня шуму на психоемоційний стан працюючого, який пов'язаний з використанням застарілої периферійної техніки, кондиціонерів, копіювальної техніки, освітлювальних приладів;

- небезпека загоряння у зв'язку із несправністю електричного обладнання, недотримання, або порушення правил протипожежної безпеки обслуговуючим персоналом, що може призвести до пожежі;

- неправильні дії персоналу у надзвичайних ситуаціях.

Для створення безпечних і комфортних умов праці були використані нормативно-правові документи: Конституція України, Законодавства України про охорону здоров'я, Основи земельного законодавства України, Закон про трудові колективи, Закон України про охорону праці та ін. Єдиними правилами і нормами, що поширюються на всі галузі народного господарства, є вимоги державних стандартів ССБТ.

7.2 Заходи забезпечення безпеки

Приміщення офісу, в якому перебувають працівники, відносяться до приміщень без підвищеної небезпеки ураження електричним струмом.

Обладнання, що використовується в приміщенні є споживачем електроенергії, що живиться від змінного струму 220 В від мережі з заземленою нейтраллю, та відноситься до електроустановок до 1000В закритого виконання. За способом захисту людини від ураження електричним струмом відповідає згідно з ГОСТ 12.2.007.0-75* (2001) «ССБТ. Вироби електротехнічні. Загальні вимоги безпеки» I (стаціонарні комп'ютери,) та II (освітлювальні прилади, кондиціонери, опалювальні пристрої, ноутбуки, сканери) класу захисту.

Основними причинами ураження персоналу електричним струмом є:

- дотик до струмопровідних частин, що знаходяться під напругою (оголені кабелі живлення, розетки 220В);
- дотик до металевих не струмопровідних частин після переходу на них напруги з струмоведучих частин.

Згідно «Правилам улаштування електроустановок» (ПУЕ) виконані такі групи заходів з електробезпеки:

Згідно з ГОСТ 12.1.009-76 (1999) «ССБТ. Електробезпека. Терміни та визначення» у приладах II класу захисту використовується подвійна ізоляція - електрична ізоляція, що складається з робочої і додаткової ізоляції.

Так як згідно з НПАОП 40.1-1.32-01 «Правила улаштування електроустановок. Електрообладнання спеціальних установок» офісні приміщення у більшості своїй відносяться до класу пожежонебезпечної зони П-Па (приміщення, в яких містяться тверді горючі речовини), тому передбачений ступінь захисту ізоляції обладнання IP44.

Згідно з ГОСТ 12.1.030-81 (2001) «ССБТ. Електробезпека. Захисне заземлення, занулення» у приміщенні встановлене занулення, призначене для зменшення часу замикання, та захисне заземлення, яке, згідно з ПУЕ, забезпечує опір не більше 4 Ом.

Експлуатація електроустановок і електроустаткування проводиться відповідно до НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок» (далі «ПБЕЕ») та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів».

Розетки марковані попереджувальними мітками з зазначенням напруги (~220 В) згідно з ПБЕЕС 6.11.6.

Проведено навчання з правил електробезпеки, перевірка знань та атестація персоналу на кваліфікаційну групу з електробезпеки, згідно НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;

7.3 Заходи щодо виробничої санітарії та гігієни праці

Показники мікроклімату в офісному приміщенні відповідають встановленим санітарно-гігієнічним вимогам ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005-88 (1991) «ССБТ. Загальні санітарно-гігієнічні вимоги до повітря робочої зони» і ГН 2152-80 «Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих та громадських приміщень».

Робота в приміщеннях, належать до категорії Іб - легка робота, тому встановлені наступні оптимальні значення параметрів мікроклімату:

- у холодний період року: температура 21-23°; відносна вологість: 40-60%; швидкість переміщення повітря: 0,1 м/с;
- у теплий період року: температура 22-24°; відносна вологість: 40-60%; швидкість переміщення повітря: 0,2 м/с.

Дотримання вимог цих документів досягається оснащенням приміщень пристроями кондиціонування і вентиляції, дезодорації повітря, опалювання згідно вимог ДБН В.2.5-67:2013 «Опалення, вентиляція та кондиціонування».

Згідно ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення» в офісних приміщеннях використовується природне та штучне освітлення. Природне освітлення здійснено через світлові прорізи, які забезпечують коефіцієнт природної освітленості (КПО) не нижче 1,5%. Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски на поверхні екранів і клавіатури, використовуються сонцезахисні пристрої, на вікнах встановлені жалюзі.

Штучне освітлення в приміщенні здійснено у вигляді комбінованої системи освітлення з використанням люмінесцентних джерел світла у світильниках загального освітлення.

Величина освітленості при штучному освітленні люмінесцентними лампами відповідає в горизонтальній площині не нижче 300 лк - для системи

загального освітлення і не нижче 750 лк - для систем комбінованого освітлення згідно з ДБН В.2.5-28-2006.

Проведено розрахунки для системи загального освітлення.

Як джерела загального освітлення використані люмінесцентні лампи типу ЛВП. Ступінь захисту світильників IP 54 (захист від пилу та бризок).

Числове значення коефіцієнта світильника $[L/h] = 1.3$.

Розрахунок кількості рядів світильників у приміщенні N_p :

$$N_p = \frac{B}{(H - h_p) \times [L/h]} \quad (7.1)$$

де B - ширина приміщення, м; H - висота приміщення, м; h_p - висота робочої поверхні.

$$\text{Таким чином } N_p = \frac{8}{(3 - 0,725) \times 1,3} = 2,70 = 3(\text{шт}).$$

Визначення максимально припустимої відстані між рядами світильників L_{max} :

$$L_{max} = \frac{B}{N_p} \quad (7.2)$$

де B - ширина приміщення, м; N_p - кількість рядів світильників у приміщенні, шт.

$$\text{Виходячи з (7.2) } L_{max} = \frac{8}{3} = 2,6 (\text{м}).$$

Розрахунок висоти підвісу світильника над робочою поверхнею h :

$$h = \frac{L_{max}}{[L/h]} \quad (7.3)$$

де L_{max} - максимально припустима відстань між рядами світильників,

м; $[L/h]$ - числове значення коефіцієнта світильника.

$$\text{Згідно з (7.3) } h = \frac{2,6}{1.3} = 2(\text{м}).$$

Знаходження висоти звисання світильника зі стелі h_3 :

$$h_3 = H - h_p - h \quad (7.4)$$

де H - висота приміщення, м; h_p - висота робочої поверхні, м; h - висота підвісу світильника над робочою поверхнею, м.

$$\text{Відповідно до (7.4) } h_3 = 0,27(\text{м}).$$

Визначення значення індексу приміщення i , що характеризує співвідношення розмірів освітлювального приміщення і висоти розміщення світильників:

$$i = \frac{A \times B}{h \times (A + B)} \quad (7.5)$$

де A - довжина приміщення, м; B - ширина приміщення, м; h - висота підвісу світильника над робочою поверхнею, м.

$$\text{Таким чином } i = \frac{8 \times 8}{2 \times (8 + 8)} = 2$$

Коефіцієнт використання світлового потоку, створюваного світильниками вибраного типу $\eta = 54\%$. Коефіцієнт відбиття стелі $\rho_c = 70\%$, стін $\rho_{ст} = 50\%$ та підлоги $\rho_{п} = 30\%$.

Визначення сумарного світлового потоку освітлювальної установки у даному приміщенні Φ_{Σ} . Для офісного приміщення коефіцієнт запасу приймається рівним $k_3 = 1.5$. Коефіцієнт нерівномірності освітлення $z = 1.1$. У приміщенні розміром $8\text{м} \times 8\text{м} \times 3\text{м}$ потрібно створити освітленість $E_n = 300$ лк.

$$\Phi_{\Sigma} = \frac{E_n \times A \times B \times k_3 \times z}{\eta} \quad (7.6)$$

де E_n - рівень нормованого загального освітлення, лк; A - довжина приміщення, м; B - ширина приміщення, м; k_3 - коефіцієнт запасу; z - коефіцієнт нерівномірності (мінімальної) освітленості; η - коефіцієнт використання світлового потоку.

$$\text{Відповідно до (7.6) } \Phi_{\Sigma} = \frac{300 \times 8 \times 8 \times 1,5 \times 1,1}{0,54} = 58666(\text{лм}).$$

Визначення умовної загальної кількості світильників у приміщенні N_{cv}^* :

$$N_{cv}^* = \frac{A \times B}{L_{max}^2} = \frac{8 \times 8}{6,76} \quad (7.7)$$

де A - довжина приміщення, м; B - ширина приміщення, м; L_{max} - максимально припустима відстань між рядами світильників, м. Результат округлений до цілого значення, кратного кількості рядів N_p .

Таким чином $N_{cv}^* = 9,46 = 9(\text{шт})$.

Розрахунок світлового потоку умовного джерела світла $\Phi_{\text{л}}^*$:

$$\Phi_{\text{л}}^* = \frac{\Phi_{\Sigma}}{N_{cv}^* \times n} \quad (7.8)$$

де Φ_{Σ} - сумарний світловий потік освітлювальної установки, лм;
 $n=2$ - кількість ламп у світильнику, шт; N_{cv}^* - умовна загальна кількість світильників у приміщенні.

$$\text{Згідно з (7.8) } \Phi_{\text{л}}^* = \frac{58666}{9 \times 2} = 3259(\text{лм})$$

Вибір типу стандартної лампи з найближчим значенням фактичного світлового потоку лампи Φ_l , і знаходження коефіцієнту m (співвідношення між розрахунковим світловим потоком лампи Φ_l^* та фактичним світловим потоком вибраної стандартної лампи Φ_l):

Тип лампи - ЛБ потужністю 40Вт., $\Phi_l = 3200(лм)$.

$$m = \frac{\Phi_l^*}{\Phi_l} \quad (7.9)$$

$$\text{Таким чином } m = \frac{3259}{3200} = 1,01.$$

Визначення оптимальної (фактичної) кількості світильників у приміщенні $N_{св}$:

$$N_{св} = N_{св}^* \times m \quad (7.10)$$

де $N_{св}^*$ - умовна загальна кількість світильників у приміщенні, шт. m - співвідношення між розрахунковим світловим потоком лампи та фактичним світловим потоком вибраної стандартної лампи. Результат округлений до цілого значення, кратного кількості рядів N_p .

$$\text{Виходячи з (7.10) } N_{св} = 9 \times 1,01 = 9,09 = 9(шт)$$

Розрахунок загальної потужності освітлювальної установки P_{Σ} :

$$P_{\Sigma} = N_l \times P_l \quad (7.11)$$

де N_l - фактична кількість ламп у приміщенні, P_l - потужність однієї лампи.

$$\text{Відповідно до (7.11) } P_{\Sigma} = 9 \times 40 = 360(Вт)$$

Рівні звукового тиску в октавних смугах частот, рівні звуку та

еквівалентні рівні звуку на робочих місцях у приміщення не перевищують 45-50 дБ згідно ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» та ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

Вібрація (загальна) обладнання не перевищує гранично допустимих величин, встановлених Санітарними нормами вібрації робочих місць № 3044-84.

Для запобігання статистичного навантаження при користуванні ПК використовуються перерви в роботі 10 хв. через кожні дві години.

Загальні ергономічні вимоги встановлено ДСТУ ISO 9241-1:2003 «Ергономічні вимоги до роботи з відео терміналами в офісі. Частина 1. Загальні положення».

При організації робочих місць дотримані наступні вимоги:

- висота клавіатури від підлоги - 65-75 см;
- наявність ергономічних і зручних миші і клавіатури;
- можливість регулювання висоти і нахилу клавіатури (відстань від поверхні стола до середини клавіатури - не більше 30 мм, кут підйому клавіатури - від 2° до 15°);
- наявність у клавіатури підставки для рук;
- наявність килимка для миші з захистом від тунельного синдрому (спеціальний виступ забезпечує правильне положення кисті);
- наявність стільця або крісла з підлокітниками;
- наявність у стільця можливості регулювання висоти та куту нахилу спинки;
- ергономічна форма спинки для підтримки правильного положення спини при сидінні.

Для запобігання нервового напруження організоване правильне робоче місце, правильне робоче положення, ритм роботи, раціоналізовано трудовий процес, використовуються емоційні стимули, впроваджено

раціональні режими праці і відпочинку тощо.

Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» є неприпустимим розташування приміщень, призначених для роботи з відео дисплейними терміналами (ВДТ) у підвалах та цокольних поверхах. Також забороняється розташування вибухонебезпечних приміщень категорії А і Б (НАПБ Б. 03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною безпеки») та виробництв з мокрими технологічними процесами поряд з приміщенням, де розташовуються ЕОМ (ПЕОМ), а також над такими приміщеннями, або під ними. Окрім того, виробничі приміщення для роботи з ВДТ не повинні межувати з приміщеннями, у яких рівень шуму і вібрації перевищує допустимі значення.

Оскільки площа приміщення становить 64м^2 , а площа, на якій розташовується одне робоче місце з ВДТ, відповідно до вимог ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» повинна становити не менше 6м^2 , то в даному приміщенні можна розмістити щонайбільше 9 комп'ютеризованих робочих місць.

Відповідно до вимог ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» мінімальний об'єм приміщення на одне робоче місце з ВДТ становить 20м^3 . Об'єм приміщення становить 192м^3 , а об'єм, що припадає на одне комп'ютеризоване робоче місце - $21,3\text{м}^3$. Таким чином норматив щодо об'єму приміщення на одне робоче місце з ВДТ виконується.

Планування розміщення комп'ютеризованих робочих місць у приміщенні проведено із врахуванням наступних вимог:

- робочі місця з ВДТ розміщені на відстані не менше 1 м від стіни зі світловими прорізами;
- відстань між бічними поверхнями ВДТ складає не менше за 1,2 м;

- відстань між тильною поверхнею одного ВДТ та екраном іншого не менша за 2,5 м;
- прохід між рядами робочих місць не менший 1 м.

Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» рекомендовані розміри столу для робочого місця з ВДТ становлять: висота - 725 мм, ширина - 600-1400 мм, глибина - 800-1000 мм. Встановлені робочі столи мають такі розміри: висота - 725 мм, ширина - 1200 мм, глибина - 800 мм.

Комп'ютеризовані робочі місця розміщено рядами вздовж стіни з вікнами. Це дає змогу унеможливити дзеркальне відбиття на екрані ВДТ джерел природного світла (вікон) та потрапляння останніх у поле зору операторів, що погіршує умови їх зорової роботи.

7.4 Заходи з пожежної безпеки

Закон України «Про пожежну безпеку» визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності.

Пожежна безпека - стан об'єкта, при якому з регламентованою ймовірністю виключається можливість виникнення та розвиток пожежі і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей [9].

Для забезпечення пожежної безпеки в приміщенні проведено пожежну профілактику, яка включає в себе комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження її поширення, а також на створення умов для успішного гасіння пожежі.

Для ліквідації пожежі у початковій стадії її розвитку силами персоналу об'єктів застосовуються первинні засоби пожежогасіння. До них

відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, ящики з піском, пожежні відра, совкові лопати, ломи, сокири тощо), системи автоматичного пожежогасіння.

Первинні засоби пожежогасіння, в залежності від категорії приміщень, можуть розташовуватись як окремо, так і в складі пожежних щитів.

Залежно від агрегатного стану й особливостей горіння різних горючих речовин і матеріалів пожежі за ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва» поділяються на відповідні класи

В офісному приміщенні знаходиться дерев'яні меблі, електронна апаратура, паперові носії інформації.

Клас пожежі у офісному приміщенні (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») - пожежі твердих речовин, переважно органічного походження, горіння яких визначається як—супроводжується тлінням (деревина, пластмаси, папір) клас А та клас Е - займання електроустановок під напругою. Категорія приміщення (згідно із НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою») - визначається як категорії П-Па.

Визначення типу та розрахунок кількості первинних засобів пожежогасіння: (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») - для офісного приміщення площею 42м² категорій пожежонебезпеки А та Е застосовується 2 порошкових вогнегасника типу ВП-5, а також вуглецевий вогнегасник ВВ-5 (ВВК-5) (НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою», ДБН В. 1.1.7-2002 «Пожежна безпека об'єктів будівництва»).

Згідно з ДБН В.2.5-56:2014 «Системи протипожежного захисту» у приміщенні встановлені чотири комбінованих оптично-теплових датчика СПД-3.5. У разі спрацювання сигнал тривоги подається на ППКП і передається на звукові і світлові сповіщувачі будівлі.

Згідно з ДБН В.1.1-7-2002. "Пожежна безпека об'єктів будівництва" на випадок пожежі передбачені шляхи евакуації працюючих - проходи, проїзди, евакуаційні виходи. Два евакуаційні виходи розташовані розсереджено. Коридори і проходи, призначені для евакуації, мають якомога меншу довжину і мінімальна кількість поворотів. На всьому протязі проходу немає порогів або проміжних ступенів.

Згідно з п. 13 "Рекомендацій по складанню планів евакуації людей на випадок пожежі" план евакуації розміром формату А4 розміщено на видному місці під склом (плівкою).

Згідно з НАПБ Б.02.005-2003 "Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України" працівники пройшли інструктаж з пожежної безпеки та ознайомлені з евакуаційними заходами при пожежі.

7.5 Заходи забезпечення безпеки у надзвичайних ситуаціях

Організація навчання працюючого та не працюючого населення діям у надзвичайних ситуаціях проводиться відповідно до статті 39 Цивільного кодексу України, а також відповідної постанови Кабінету Міністрів України від 26 червня 2013 р. № 444 [13].

1. Порядок здійснення навчання населення діям у надзвичайних ситуаціях визначає механізм організації навчання населення діям у надзвичайних ситуаціях (далі - навчання населення), його структуру, види та форми.

2. Навчання населення здійснюється:

- за місцем роботи - працюючого населення;
- за місцем навчання - дітей дошкільного віку, учнів та студентів;
- за місцем проживання - непрацюючого населення.

3. Організація навчання населення покладається:

- для працюючого та непрацюючого населення - на ДСНС, Раду міністрів Автономної Республіки Крим, місцеві державні адміністрації, органи місцевого самоврядування;

- дітей дошкільного віку, учнів та студентів - на МОН.

4. Навчально-методичне забезпечення навчання населення здійснюється ДСНС разом з МОН.

5. Навчання населення складається з:

- навчання безпосередньо на підприємствах, в установах та організаціях;

- навчання за межами підприємств, установ та організацій керівного складу і фахівців з питань цивільного захисту та пожежної безпеки;

- практичної підготовки під час проведення спеціальних об'єктових навчань і тренувань з питань цивільного захисту;

- навчання під час здобуття відповідного освітнього рівня у навчальних закладах системи освіти;

- самостійного вивчення інформації про дії в умовах надзвичайних ситуацій.

6. Навчання працюючого населення здійснюється безпосередньо на підприємстві, в установі та організації згідно з програмами підготовки працівників до дій у надзвичайних ситуаціях, а також під час проведення спеціальних об'єктових навчань і тренувань з питань цивільного захисту.

7. Програми підготовки працівників до дій у надзвичайних ситуаціях розробляються і затверджуються підприємствами, установами, організаціями на підставі програм та організаційно-методичних вказівок з підготовки населення до дій у надзвичайних ситуаціях, що розробляються і затверджуються ДСНС, Радою міністрів Автономної Республіки Крим, місцевими державними адміністраціями, органами місцевого самоврядування.

Програми навчання з питань пожежної безпеки погоджуються із ДСНС.

8. Програми підготовки працівників до дій у надзвичайних ситуаціях поділяються на:

- загальної підготовки працівників підприємств, установ та організацій;
- спеціальної підготовки працівників, що входять до складу спеціалізованих служб і формувань цивільного захисту;
- додаткової підготовки з техногенної безпеки працівників об'єктів підвищеної небезпеки;
- пожежно-технічного мінімуму для працівників, зайнятих на роботах з підвищеною пожежною небезпекою;
- прискореної підготовки працівників до дій в особливий період.

9. Підготовка працівників до дій у надзвичайних ситуаціях передбачає вивчення та поглиблення знань:

- дії у надзвичайних ситуаціях;
- цивільний захист;
- техногенна безпека працівників об'єктів підвищеної небезпеки;
- пожежна безпека;
- способи захисту від наслідків надзвичайних ситуацій.

10. Навчання працівників на підприємстві, в установі та організації здійснюється шляхом курсового навчання, індивідуального навчання та шляхом проведення інструктажів за програмою загальної підготовки працівників, які проводяться особами з питань цивільного захисту, призначеними в межах штатної чисельності суб'єкта господарювання.

12. З метою належної організації навчального процесу, забезпечення послідовності теоретичного і практичного навчання на підприємствах, в установах та організаціях розробляються і ведуться планувальні, облікові та

звітні документи.

13. Для отримання працівниками відомостей про конкретні дії у надзвичайних ситуаціях на підприємстві, в установі та організації обладнується з урахуванням особливостей виробничої діяльності інформаційно-довідковий куточок з питань цивільного захисту.

14. Особи, що залучаються підприємствами, установами та організаціями (в тому числі на умовах договору) до проведення інструктажів, навчання і перевірки знань з питань цивільного захисту, пожежної та техногенної безпеки, зобов'язані пройти спеціальну підготовку на територіальних курсах, у навчально-методичних центрах цивільного захисту та безпеки життєдіяльності відповідно до вимог типового положення про них.

15. Навчання керівного складу підприємств, установ та організацій і фахівців, діяльність яких пов'язана з організацією і здійсненням заходів з питань цивільного захисту, здійснюється в установленому законодавством порядку.

16. Особи у разі прийняття на роботу та працівники щороку за місцем роботи проходять інструктаж з питань цивільного захисту, пожежної безпеки та дій у надзвичайних ситуаціях.

17. Спеціальні об'єктові навчання і тренування з питань цивільного захисту проводяться у порядку, затвердженому МВС.

18. Навчання працюючого населення здійснюється у робочий час за рахунок коштів підприємств, установ та організацій.

19. Організація навчання дітей дошкільного віку, учнів та студентів здійснюється МОН згідно із затвердженими ним і погодженими з ДСНС навчальними програмами з вивчення заходів безпеки, способів захисту від впливу небезпечних факторів, викликаних надзвичайними ситуаціями, надання до медичної допомоги.

20. Підготовка студентів вищих навчальних закладів до дій у надзвичайних ситуаціях здійснюється за нормативними навчальними

дисциплінами “Безпека життєдіяльності ” та “Цивільний захист”.

21. Підготовка учнів загальноосвітніх та професійно-технічних навчальних закладів до дій у надзвичайних ситуаціях, що передбачає здобуття знань і вмінь з питань особистої безпеки в умовах загрози та виникнення надзвичайної ситуації, користування засобами захисту від її наслідків, вивчення правил пожежної безпеки та основ цивільного захисту, здійснюється в рамках вивчення предметів “Основи здоров’я” та “Захист Вітчизни”.

22. Навчально-виховна робота з дітьми дошкільного віку проводиться згідно з вимогами базового компонента дошкільної освіти і спрямовується на формування достатнього та необхідного рівня знань і умінь дитини для безпечного перебування в навколишньому середовищі, елементарних норм поведінки у надзвичайних ситуаціях і запобігання пожежам від дитячих пустощів з вогнем.

23. З метою координації науково-методичної діяльності, узагальнення і поширення ефективних форм і методів організації навчально-виховного процесу з питань безпеки життєдіяльності та цивільного захисту визначаються:

- МОН - базові за галуззю знань кафедри з безпеки життєдіяльності у вищих навчальних закладах;
- місцевими органами управління освіти - територіальні базові (опорні) загальноосвітні та дошкільні навчальні заклади.

24. Позашкільна освітня робота з питань формування культури безпеки життєдіяльності серед дітей та молоді, формування здорового способу життя, оволодіння ними навичками самозахисту і рятування проводиться у позашкільних закладах, а також шляхом організації шкільних, районних (міських), обласних та всеукраїнських змагань з безпеки життєдіяльності.

25. МОН здійснює контроль і бере участь у моніторингу якості підготовки у навчальних закладах дітей дошкільного віку, учнів та студентів з

питань навчання діям у надзвичайних ситуаціях.

26. Навчання дітей дошкільного віку, учнів та студентів здійснюється під час навчально-виховного процесу за рахунок коштів, передбачених для фінансування навчальних закладів.

27. Навчання непрацюючого населення діям у надзвичайних ситуаціях здійснюється шляхом проведення інформаційно-просвітницької роботи за місцем проживання та самостійного вивчення загальної програми навчання населення діям у надзвичайних ситуаціях та інших інформаційно-довідкових матеріалів з питань цивільного захисту, правил пожежної безпеки у побуті та громадських місцях.

28. Інформаційно-просвітницька робота з питань поведінки в умовах надзвичайних ситуацій організовується місцевими органами виконавчої влади та органами місцевого самоврядування, в тому числі через утворені при них консультаційні пункти, та передбачає:

- інформування населення про методи реагування у разі виникнення надзвичайних ситуацій;
- створення в консультаційних пунктах умов для оволодіння громадянами навичками користування найбільш поширеними засобами захисту і надання першої само- та взаємодопомоги.

29. Для задоволення потреби у самостійному вивченні загальної програми навчання населення діям у надзвичайних ситуаціях місцеві органи виконавчої влади та органи місцевого самоврядування за методичного супроводження територіальних курсів, навчально-методичних центрів цивільного захисту та безпеки життєдіяльності видають навчальні, навчально-наочні посібники, брошури, розповсюджують інформаційні матеріали, буклети тощо.

Інформаційно-просвітницька робота з населенням щодо правил поведінки в умовах надзвичайних ситуацій проводиться шляхом запровадження постійних рубрик у засобах масової інформації, зокрема друкованих, а також за допомогою інформаційно-комунікаційних технологій,

аудіовізуальних та інтерактивних засобів та соціальної реклами.

Непрацююче населення має право отримувати від органів державної влади та органів місцевого самоврядування відомості про надзвичайні ситуації, у зоні яких або у зоні можливого ураження від яких може опинитися місце проживання непрацюючих громадян, а також про способи захисту від впливу небезпечних факторів, викликаних такими ситуаціями.

30. Пропаганда знань серед населення щодо власної та колективної безпеки у разі виникнення надзвичайної ситуації здійснюється за сприяння громадських організацій.

ВИСНОВКИ

В ході виконання дипломної роботи були вирішені наступні завдання:

- вивчено стек протоколів SS7;
- вивчена підсистема MAP;
- знайдені уразливості та можливі напрямки атак на підсистему;
- проаналізовані сучасні засоби захисту для мереж мобільного зв'язку.

При вивченні стека протоколів SS7 було представлено історію розвитку сигнальної мережі. Представлені основні блоки та ланки з яких складається мережа. Представлено архітектуру стека протоколів SS7 і показані відповідності рівням моделі OSI, та визначено призначення кожної з підсистем архітектури. В ході вивчення підсистеми MAP. Було розглянуто об'єкти мережі підсистеми та представлені ідентифікатори, які виконують функції в ідентифікації, нумерації чи адресації для абонентів чи вузлів підсистеми MAP. Для розуміння проблем захищеності мереж мобільного зв'язку були приведені можливі потенційні атаки. Була представлена мала частина потенційно уразливих повідомлень примітивів, було описано їх призначення, відправники та отримувачі при нормальній поведінки в роботі. Проаналізувавши профілі зловмисників та нормальну поведінку уразливих повідомлень, це допомогло для кожного небезпечного повідомлення

сформувати можливі потенційні атаки з боку атакуючого. Завдяки цьому ми маємо повне представлення про роботу і взаємодію усіх елементів мережі, а також про проблеми захищеності мереж мобільного зв'язку. В якості заключної частини були приведені напрямки рішення проблем захищеності мереж мобільного зв'язку, проаналізовано та представлено актуальні на сьогоднішній день засоби забезпечення безпеки мереж мобільного зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Амортизація [Електронний ресурс] - Режим доступу: <https://uk.wikipedia.org/wiki/%D0%90%D0%BC%D0%BE%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F>.
2. Андрійчук, В. Г. Економіка аграрних підприємств [Електронний ресурс] / В. Г. Андрійчук. - Режим доступу: <http://studentbooks.com.ua/content/view/743/39/1/2/>.
3. Види заробітної плати та їх характеристика [Електронний ресурс] – Режим доступу: https://pidruchniki.com/16400116/ekonomika/vidi_zarobit-noyi_plati_harakteristika.
4. Гойхман, В. Ю. Протоколи стека ЗКС7: підсистема MAP. Серія «Телекомунікаційні протоколи» [Текст] / В. Ю. Гойхман, Б. С. Гольдштейн, Н. Г. Сибірякова. – СПб.: БВХ - Петербург, 2012. – 200 с.
5. Єдиний соціальний внесок [Електронний ресурс] - Режим доступу : https://uk.wikipedia.org/wiki/%D0%84%D0%B4%D0%B8%D0%BD%D0%B8%D0%B9_%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%B2%D0%BD%D0%B5%D1%81%D0%BE%D0%BA.
6. Взлом стільникових мереж: не просто, а дуже просто [Електронний ресурс] - Режим доступу: <https://3dnews.ru/923316>.

7. ЗКС - 7 [Електронний ресурс] - Режим доступу: <https://ru.wikipedia.org/wiki/%D0%9E%D0%9A%D0%A1-7>
8. ЗКС № 7 [Електронний ресурс] - Режим доступу: <http://www.skunksworks.net/doc/DocATS/teledoc/oks7/index.php>
9. Катренко, Л.А. Охорона праці. Курс лекцій. Практикум: Навчальний посібник [Текст] / Л.А. Катренко, Ю.В. Кіт, І. П. Пістун. - Суми: Університетська книга, 2009. - 540 с.
10. Мережі GSM. Погляд зсередини. - Режим доступу: <https://www.ixbt.com/mobile/gsm-nets.html>
11. Непомнящий, С. Г. Планування на підприємстві [Електронний ресурс] / С. Г. Непомнящий // Таганрог: ТІУтаЕ. - 2011. - Режим доступу: http://www.aup.ru/books/m235/7_2.htm.
12. Об'єкти та суб'єкти інвестиційної діяльності [Електронний ресурс] – Режим доступу: https://pidruchniki.com/10561127/investuvannya/obyekti_subyekti_investitsiynoyi_diyalnosti.
13. Постанова Кабінету Міністрів України від 26 червня 2013 р. № 444 [Електронний ресурс] - Режим доступу: <http://zakon.rada.gov.ua/laws/show/444-2013-п>
14. Прослуховування українських мобільників: як це зроблено і як захиститися [Електронний ресурс] - Режим доступу: <https://habr.com/company/pt/blog/226977/>.
15. Пузанков, С. Моніторинг безпеки мереж SS7 [Електронний ресурс] / С. Пузанков. – Режим доступу: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/Webinar_03032016.pdf.
16. Самуйлов, К. Є. Методи аналізу і розрахунку мереж ЗКС 7: Монографія [Текст] / К. Є. Самуйлов. - М.: Вид-во РУДН, 2002. - 292 с.
17. Статистика основних загроз безпеки у мережах SS7 мобільного зв'язку. [Електронний ресурс] - Режим доступу: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SS7-Vulnerability-2016-rus.pdf>

18. Стільниковий зв'язок: історія, стандарти, технології [Електронний ресурс] - Режим доступу: <http://celnet.ru>
19. Що відноситься до прямих і непрямих витрат [Електронний ресурс] – Режим доступу: https://pidruchniki.com/1384072042810/buhgalter-skiy_oblik_ta_audit/scho_vidnositsya_pryamih_nepryamih_vitrat.
20. Як влаштована мережа стільникового зв'язку GSM/UMTS [Електронний ресурс] - Режим доступу: <https://m.habr.com/post/82757/>