Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: " Аналіз вразливостей протоколу SS7: загрози та методи захисту"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Новосад Володимир Дмитрович
підпис (прізвище та ініціали)

Керівник Оробчук О.Р.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Новосаду Володимиру Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз вразливостей протоколу SS7: загрози та методи захисту

Керівник роботи Оробчук Олександра Романівна.,
доктор філософії., старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» 11 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 12.12.2023

3. Вихідні дані до роботи Вимоги до операційної системи Kali
.

4. Зміст роботи (перелік питань, які потрібно розробити)
ОБРУНТУВАННЯ АКТУАЛЬНОСТІ ДОСЛІДЖЕННЯ. Обгрунтування необхідності захисту телекомунікаційних мереж, що працюють на основі протоколу SS7. ОГЛЯД ДОСПУНИХ ІНСТРУМЕНТІВ. Аналіз інструментів для виявлення та усунення вразливостей протоколу SS7. ТЕСТУВАННЯ ТА АНАЛІЗ СИГНАЛЬНОЇ МЕРЕЖІ Підготовка інструментів для тестування вразливостей у протоколі SS7 в середовищі Kali Linux. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ. Дотримання вимог охорони праці під час роботи з телекомунікаційними системами та тестовими середовищами
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета та задачі дослідження. Загрози для сигнальних мереж SS7. Інструменти для тестування сигнального трафіку. Огляд алгоритму тестування сигнального трафіку у сигнальних мереж SS7. Перехоплення тестування сигнального трафіку у протоколі SS7. Демонстрація тестування сигнальної мережі SS7. Аналіз знайдених загроз. Розробка механізму фільтрації. Підсумковий аналіз

Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Підбір джерел про вразливості та захист протоколу SS7	23.09 – 02.10	Виконано
3.	Опрацювання джерел та аналіз сучасних досліджень	03.10 – 16.10	Виконано
4.	Оформлення розділу « Аналітичний огляд вразливостей та захисту протоколу SS7»	17.10 – 23.10	Виконано
5.	Оформлення розділу « Загальні підходи та основні методи досліджень »	24.10 – 29.10	Виконано
6.	Оформлення розділу « Практичні завдання з протоколом SS7»	30.10 – 18.11	Виконано
7.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	19.11 – 24.11	Виконано
8.	Оформлення кваліфікаційної роботи	25.11 – 07.12	Виконано
9.	Нормоконтроль	08.12 – 10.12	Виконано
10.	Перевірка на плагіат	12.12 – 14.12	Виконано
11.	Попередній захист кваліфікаційної роботи	20.12 – 15.12	Виконано
12.	Захист кваліфікаційної роботи	28.12.2023	Виконано

Студент _____ Новосад В.Д.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Оробчук О.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз вразливостей протоколу SS7: загрози та методи захисту // ОР «Магістр» // Новосад Володимир Дмитрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-61 // Тернопіль, 2024 // С. 77, рис. – 29, табл. – - , кресл. – -, додат. – 4.

Ключові слова: SS7, СИГНАЛЬНІ МЕРЕЖІ, ВРАЗЛИВОСТІ ПРОТОКОЛУ, КІБЕРБЕЗПЕКА, ТЕЛЕКОМУНІКАЦІЇ, DIAMETER, ЗАХИСТ ІНФОРМАЦІЇ.

У кваліфікаційній роботі виконано аналіз вразливостей протоколу SS7, які створюють значні ризики для безпеки телекомунікаційних мереж. Проведено огляд функцій та архітектури SS7, розглянуто основні вразливості, зокрема перехоплення SMS, локаційне відстеження. Виконано детальний аналіз сучасних атак із використанням тестових кейсів, що демонструють серйозні ризики для операторів зв'язку та їхніх клієнтів.

У ході виконання роботи було запропоновано ефективні методи захисту сигнальних мереж, включаючи впровадження SS7 Firewall, сегментування мережі, моніторинг трафіку та перехід на протокол Diameter. Результати роботи спрямовані на зменшення ризиків несанкціонованого доступу, підвищення кіберстійкості телекомунікаційних систем та захист конфіденційних даних абонентів.

Результати досліджень можуть бути використані для створення більш безпечних телекомунікаційних мереж та вдосконалення існуючих систем.

ABSTRACTS

SS7 protocol vulnerability analysis: threats and protection methods // Thesis of educational level "Master"// Volodymyr Novosad // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-61 // Ternopil, 2024 // P. 77, figs. 29, tables -, drawings -, added. – 4.

Keywords: SS7, SIGNALING NETWORKS, PROTOCOL VULNERABILITIES, CYBERSECURITY, TELECOMMUNICATIONS, DIAMETER, INFORMATION SECURITY.

The qualification thesis focuses on analyzing vulnerabilities of the SS7 protocol, which pose significant risks to the security of telecommunication networks. The research includes a review of the functions and architecture of SS7, as well as an analysis of its primary vulnerabilities, such as SMS interception and location tracking. A detailed examination of modern attacks is presented using test cases that demonstrate substantial risks for telecom operators and their clients.

In the course of the research, effective methods for securing signaling networks were proposed, including the implementation of an SS7 Firewall, network segmentation, traffic monitoring, and migration to the Diameter protocol. The results aim to mitigate the risks of unauthorized access, enhance the cybersecurity resilience of telecommunication systems, and protect subscribers' confidential data.

The findings of this research can be utilized to develop more secure telecommunication networks and improve existing systems.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

СС7 (SS7)	–	Система сигналізації №7
МТР (MTP)	–	Частина передачі повідомлень
СККЧ (SCCP)	–	Система контролю сигнальних з'єднань
МАП (MAP)	–	Частина прикладних повідомлень
СТП (STP)	–	Точка передачі сигналів
МСЦ (MSC)	–	Центр комутації мобільного зв’язку
ГМЦ (HLR)	–	Головний регістр місцезнаходжень
ВРЦ (VLR)	–	Відвідуваний регістр місцезнаходжень
ГТР (GMSC)	–	Головний транзитний центр комутації
СМСЦ (SMSC)	–	Центр обміну повідомленнями SMS
ОД (OTP)	–	Одноразовий пароль
ДОП (Diameter)	–	Протокол Diameter
МНД (IPX)	–	Інтернет-пакетний обмін
КСЗІ (SIEM)	–	Система управління інформаційною безпекою
МПК (PKI)	–	Інфраструктура відкритих ключів
ЗСШ (TLS)	–	Захищений транспортний рівень
ММД (API)	–	Міжмодульний доступ
СФ (Firewall)	–	Мережевий екран
ЗМС (IMS)	–	Система мультимедійних підключень
ТШП (IPSec)	–	Технологія шифрування протоколів
НІКБ (NIST)	–	Національний інститут стандартів і технологій
РЗК (RFC)	–	Рекомендації робочої групи з Інтернету

ЗМІСТ

ВСТУП

Телекомунікаційні мережі є фундаментом сучасного суспільства, забезпечуючи зв’язок мільярдів людей і підтримуючи роботу ключових секторів економіки, державного управління та соціальної взаємодії. Їхнє значення постійно зростає в умовах глобальної цифровізації, коли все більше послуг, таких як онлайн-банкінг, електронна торгівля чи управління розумними пристроями, залежить від стабільної та безпечної роботи мереж. У цьому контексті захист телекомунікаційних систем є важливим завданням, оскільки вони служать критичною інфраструктурою, від якої залежить стабільність економічних і соціальних процесів у глобальному масштабі [1].

Протокол SS7 (Signaling System No. 7), розроблений у 1970-х роках, став однією з основ для функціонування сучасних телекомунікаційних мереж. Він був створений для вирішення задачі уніфікованого управління сигналізацією в телефонних мережах, забезпечуючи маршрутизацію дзвінків, передачу текстових повідомлень, підтримку роумінгу та реалізацію інших послуг. Завдяки своїй ефективності та функціональності SS7 швидко став глобальним стандартом, який підтримує взаємодію операторів зв’язку в усьому світі.

Однак, протокол SS7 спроектований у часи, коли питання кібербезпеки не були настільки актуальними, як сьогодні. Його архітектура базується на принципі довіри між вузлами мережі, що стало джерелом численних вразливостей. Відсутність шифрування, автентифікації та сучасних механізмів контролю трафіку створюють можливості для зловмисників здійснювати різні атаки, які ставлять під загрозу конфіденційність, цілісність і доступність даних. Найпоширенішими серед таких загроз є перехоплення SMS, локаційне відстеження користувачів і маніпуляції з маршрутизацією дзвінків.

Загрози, пов’язані з SS7, мають масштабні наслідки. Зловмисники можуть використовувати ці вразливості для викрадення OTP-кодів, які надсилаються через SMS для двофакторної автентифікації. Це створює ризики для фінансової безпеки користувачів, оскільки отримання доступу до таких кодів може

призвести до несанкціонованих транзакцій. Локаційне відстеження через SS7 дозволяє зловмисникам отримувати інформацію про місцезнаходження користувачів у реальному часі, що є серйозним порушенням приватності. Маніпуляції з маршрутизацією дзвінків можуть призводити до переадресації дзвінків на зловмисницькі вузли, що відкриває можливість для перехоплення конфіденційних розмов або доступу до платних послуг.

Ці загрози впливають не лише на індивідуальних користувачів, а й на операторів зв'язку, які змушені витрачати значні ресурси на усунення наслідків атак. У масштабах держави це може мати серйозні наслідки для національної безпеки, оскільки телекомунікаційні мережі забезпечують зв'язок державних установ, силових структур і аварійних служб. Проблема ускладнюється тим, що SS7 досі широко використовується, навіть попри появу сучасніших протоколів, таких як Diameter. Для багатьох операторів зв'язку перехід на нові стандарти є складним і витратним процесом.

Метою цього дослідження є детальний аналіз вразливостей протоколу SS7, їхнього впливу на безпеку телекомунікаційних мереж і розробка практичних рекомендацій щодо підвищення їхньої захищеності. У межах роботи будуть досліджені архітектура протоколу SS7, його функціональні можливості та основні вразливості. Особливу увагу приділено вивченню найпоширеніших атак на SS7, зокрема перехоплення SMS, локаційного відстеження та шахрайства в роумінгу.

Крім того, буде проведено аналіз сучасних методів захисту, включаючи SS7 Firewall, моніторинг трафіку, сегментування мереж і перехід на протоколи нового покоління, такі як Diameter. Важливим аспектом є розробка практичних рекомендацій для операторів зв'язку, які стикаються з викликами захисту своїх мереж. У дослідженні будуть використані методи моделювання, емпіричний аналіз і аналіз літератури, що дозволять отримати цілісну картину проблематики протоколу SS7 та запропонувати реалістичні рішення.

Результати цього дослідження мають практичне значення для операторів зв'язку, фахівців із кібербезпеки та розробників телекомунікаційних протоколів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XII науково-технічна конференція «Інформаційні моделі, системи та технології» (м.Тернопіль, Україна).

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ВРАЗЛИВОСТЕЙ ТА ЗАХИСТУ ПРОТОКОЛУ SS7

1.1 Протокол SS7: основні функції та призначення

Протокол SS7 (Signaling System No. 7) є основою сучасних телекомунікаційних мереж другого та третього поколінь (2G і 3G). Його історія починається у 1970-х роках, коли він був створений для забезпечення ефективної взаємодії між телефонними мережами. У міру розвитку мобільного зв'язку цей протокол зазнав значних змін і адаптації для підтримки нових функцій, таких як роумінг, передача SMS, а також різноманітні додаткові сервіси.

Однією з головних функцій SS7 є координація роботи мережі, що охоплює встановлення, підтримку та завершення викликів. Наприклад, під час здійснення телефонного дзвінка між двома абонентами протокол передає інформацію про їх місцезнаходження, дозволяючи маршрутизувати виклик відповідно до топології мережі. Завдяки цьому забезпечується безперебійний зв'язок навіть у випадках, коли абоненти знаходяться в різних країнах.

Іншою важливою функцією є обробка та доставка текстових повідомлень. SS7 відповідає за маршрутизацію повідомлень між вузлами мережі, а також за підтвердження їх доставки. Це робить можливим обмін SMS навіть у найвіддаленіших куточках світу. Крім того, SS7 підтримує додаткові сервіси, такі як голосова пошта, переадресація викликів і визначення номера абонента, що значно покращує користувацький досвід.

Протокол SS7 є складним багаторівневим механізмом управління телекомунікаційними послугами, що поєднує у собі як маршрутизацію дзвінків, так і забезпечення передачі SMS. Однак через відсутність сучасних методів захисту він стає об'єктом численних атак.

Ключовим аспектом роботи SS7 є підтримка роумінгу, який дозволяє абонентам використовувати свої мобільні послуги за межами домашньої мережі. Завдяки SS7 оператори обмінюються інформацією про абонентів, що дає змогу

здійснювати дзвінки, надсилати SMS і користуватися мобільним інтернетом навіть у роумінгу. Ця функція є особливо важливою для бізнесу, подорожей і міжнародного співробітництва.

Архітектура протоколу SS7 базується на багаторівневій моделі, яка забезпечує ефективний обмін даними. Основні рівні включають MTP (Message Transfer Part), який відповідає за передачу даних між вузлами; SCCP (Signaling Connection Control Part), що забезпечує адресацію і маршрутизацію сигналів; і MAP (Mobile Application Part), який надає сервіси для мобільних мереж, такі як управління викликами і передача SMS. Ця багаторівнева структура дозволяє SS7 інтегруватися з різними системами та технологіями.

Попри всі свої переваги, SS7 має низку обмежень, зокрема в питаннях безпеки. Його архітектура була розроблена в часи, коли питання кібербезпеки не були пріоритетними. Протокол функціонує на основі довіри між вузлами мережі, що створює вразливості, які можуть бути використані зловмисниками. Наприклад, недостатня автентифікація і відсутність шифрування роблять можливим перехоплення трафіку або маніпуляцію даними.

SS7 залишається критично важливим компонентом телекомунікаційної інфраструктури, який забезпечує роботу мільйонів користувачів у всьому світі. Його роль особливо значуща у глобальному масштабі, оскільки протокол дозволяє інтегрувати мережі різних операторів і забезпечувати сумісність технологій. Це сприяє розвитку міжнародного співробітництва, економічної взаємодії та доступності зв’язку для широкого загалу.

Сучасні дослідження спрямовані на вдосконалення SS7 шляхом впровадження додаткових механізмів захисту та інтеграції з новими протоколами, такими як Diameter. У перспективі ці заходи мають забезпечити ще більш високу стабільність і безпеку телекомунікаційних мереж, адаптуючи їх до нових викликів і потреб сучасного світу. [2]

1.2 Архітектура та принцип роботи

Архітектура та принцип роботи протоколу SS7 є важливими аспектами для розуміння його функціональності, ефективності та вразливостей. Як одна з основ телекомунікаційних мереж, SS7 складається з багаторівневої структури, яка дозволяє забезпечувати передачу сигналів між вузлами мережі. Ця архітектура розроблена для роботи у складних мережевих середовищах, де необхідна швидка і надійна маршрутизація сигналів.

Протокол SS7 побудований на основі кількох основних компонентів, кожен з яких має свої унікальні функції. Центральним елементом є точки сигналізації (Signaling Points), які використовуються для генерації або обробки сигнального трафіку. Вони можуть бути класифіковані як точки початку, кінця або транзиту, залежно від їх ролі у мережі.

Трансферні точки сигналізації (STP) відіграють важливу роль у маршрутизації трафіку. Вони відповідають за перенаправлення сигналів між різними сегментами мережі, забезпечуючи безперебійну комунікацію між вузлами. STP також використовуються для оптимізації маршрутизації, що дозволяє зменшити затримки і підвищити ефективність мережі. Цей компонент є критично важливим для великих телекомунікаційних операторів, які обслуговують мільйони абонентів.

Багаторівнева архітектура SS7 включає кілька рівнів протоколів, кожен з яких виконує специфічні функції. Рівень Message Transfer Part (MTP) відповідає за доставку повідомлень між вузлами мережі. Цей рівень забезпечує фізичну і логічну передачу даних, включаючи маршрутизацію і відновлення в разі збоїв.

Рівень Signaling Connection Control Part (SCCP) використовується для управління адресацією і з'єднаннями. Він дозволяє ідентифікувати абонентів і послуги, використовуючи додаткові дані, такі як унікальні ідентифікатори або адреси. SCCP також забезпечує підтримку розширених функцій, таких як комутація повідомлень.

Mobile Application Part (MAP) є ключовим рівнем для мобільних мереж, оскільки він забезпечує підтримку таких послуг, як роумінг, передача SMS і управління викликами. Цей рівень інтегрує різні функції SS7, забезпечуючи злагоджену роботу мобільних мереж.

Принцип роботи SS7 базується на ієрархічній структурі, де кожен компонент виконує свою роль для забезпечення безперебійного зв'язку. Наприклад, під час встановлення виклику між двома абонентами, сигнал проходить через кілька вузлів мережі, кожен з яких виконує свою специфічну функцію. Це дозволяє забезпечити високу швидкість і надійність зв'язку.

SS7 також підтримує обмін інформацією між мережами різних операторів, що робить його незамінним у глобальному масштабі. Наприклад, у роумінгу протокол передає дані про місцезнаходження абонента, дозволяючи забезпечувати зв'язок навіть за межами домашньої мережі. Така інтеграція є основою для сучасного мобільного зв'язку.

Проте архітектура SS7 має свої обмеження, особливо в аспектах безпеки. Відсутність сучасних механізмів автентифікації і шифрування робить мережу вразливою до атак. Зловмисники можуть використовувати ці слабкі місця для перехоплення трафіку або маніпуляції даними, що підкреслює важливість розробки нових методів захисту.

Попри ці виклики, SS7 залишається критично важливим компонентом телекомунікаційних систем, забезпечуючи високу продуктивність і універсальність. Його архітектура і принцип роботи створюють надійну основу для реалізації нових послуг і технологій у сфері мобільного зв'язку.

1.3 Основні проблеми безпеки

Протокол SS7, який був розроблений для телекомунікаційних мереж ще в 1970-х роках, на сьогодні є однією з найуразливіших частин інфраструктури мобільного зв'язку. Основною проблемою безпеки SS7 є те, що його архітектура базується на принципі довіри між вузлами. На момент створення протоколу

вважалося, що всі учасники мережі є добропорядними та дотримуються встановлених стандартів. У сучасному цифровому середовищі такий підхід створює значні ризики для конфіденційності та цілісності даних.

Однією з найбільших вразливостей SS7 є відсутність автентифікації вузлів. Це дозволяє зловмисникам підроблювати сигнальні запити та отримувати доступ до конфіденційної інформації. Наприклад, за допомогою підробленого запиту ProvideSubscriberInfo зловмисники можуть дізнатися місцезнаходження абонента, що є серйозним порушенням приватності.

Друга критична проблема — відсутність шифрування даних. Усі повідомлення, що передаються мережею SS7, надсилаються у вигляді відкритого тексту. Це дозволяє зловмисникам перехоплювати трафік та отримувати доступ до важливої інформації, такої як текстові повідомлення або OTP-коди для двофакторної автентифікації. Наприклад, атаки з використанням команди SendRoutingInfoForSM дозволяють перехоплювати SMS, що може бути використано для компрометації банківських акаунтів або інших захищених сервісів.

Ще однією проблемою є можливість маніпуляції маршрутизацією викликів. Зловмисники можуть використовувати команду UpdateLocation для зміни місця доставки викликів або повідомлень. Це дозволяє перенаправляти дзвінки на підставний номер, отримуючи доступ до конфіденційної інформації або здійснюючи фінансове шахрайство.

Вразливості SS7 також включають можливість перевантаження мережі через надсилання великої кількості сигнальних запитів. Такий тип атак, відомий як DoS (Denial of Service), може вивести з ладу мережу, зробивши її недоступною для звичайних користувачів.

Сучасні дослідження також демонструють, що зловмисники можуть здійснювати складні атаки, комбінуючи кілька вразливостей протоколу SS7. Наприклад, перехоплення трафіку може бути поєднано з маніпуляцією маршрутизацією для створення більш складних сценаріїв атак.

Попри серйозність цих проблем, оператори зв’язку часто стикаються з труднощами у впровадженні захисних механізмів. Більшість мереж використовує застаріле обладнання, яке не підтримує сучасні методи шифрування та автентифікації. Крім того, оновлення мережі вимагає значних фінансових витрат та технічних ресурсів. [3]

Основними шляхами вирішення проблем безпеки SS7 є впровадження SS7 Firewall, використання систем моніторингу трафіку для виявлення аномалій, а також поступовий перехід до протоколу Diameter, який є більш безпечним завдяки вбудованим засобам шифрування та автентифікації. Однак ці заходи потребують активної участі як операторів зв’язку, так і регуляторів, які повинні забезпечити дотримання стандартів безпеки.

Таким чином, хоча SS7 залишається основою сучасних телекомунікаційних мереж, його вразливості створюють серйозні ризики для конфіденційності та безпеки користувачів. Тому модернізація протоколу та впровадження сучасних методів захисту є нагальними завданнями для операторів зв’язку та регуляторів у всьому світі.

1.4 Аналіз сучасних досліджень

Сучасні дослідження, присвячені протоколу SS7, демонструють високу актуальність теми, особливо у контексті забезпечення безпеки телекомунікаційних мереж. У світлі зростаючої кількості кібератак, дослідники зосереджують свою увагу на вивченні вразливостей, оцінці ризиків і розробці ефективних заходів захисту. Наукові публікації, практичні кейси та звіти телекомунікаційних компаній стають джерелами цінної інформації про природу загроз і способи боротьби з ними.

Одна з ключових тем, що досліджується в рамках SS7, — це перехоплення повідомлень. У своїх роботах автори акцентують увагу на тому, що атаки на основі запитів, таких як SendRoutingInfoForSM, дозволяють зловмисникам отримати доступ до текстових повідомлень, які можуть містити конфіденційну

інформацію, наприклад OTP-коди. Практичні дослідження демонструють, що цей вид атак є особливо небезпечним для банківських систем та інших платформ, які використовують SMS для автентифікації.

Іншим важливим напрямком є локаційне відстеження абонентів. Дослідники підкреслюють, що запити ProvideSubscriberInfo дозволяють зловмисникам дізнатися про місцезнаходження користувачів, створюючи ризики як для їхньої приватності, так і для фізичної безпеки. Експерименти показали, що така інформація може бути отримана навіть без доступу до закритих сегментів мережі.

Сучасні дослідження також охоплюють механізми, які викликають ризики у протоколі SS7. Наприклад, вивчаються команди, які не мають достатньої автентифікації, або ті, що можуть бути використані для маніпуляції маршрутизацією викликів. У цьому контексті розробляються інструменти для автоматизованого сканування мереж на предмет використання таких команд, що дозволяє операторам ідентифікувати слабкі місця та оперативно їх усувати.

Дослідники також активно працюють над розробкою захисних технологій для SS7, зокрема SS7 Firewall. Аналіз ефективності фільтрації трафіку показує, що виявлення і блокування небезпечних запитів значно знижує ризики. Однак, як підкреслюється у багатьох роботах, ефективність таких систем залежить від їхньої коректної конфігурації та регулярного оновлення.

Одним із перспективних напрямків є перехід до протоколів нового покоління, таких як Diameter. У наукових дослідженнях зазначається, що Diameter надає вищий рівень безпеки завдяки використанню шифрування, автентифікації та механізмів контролю доступу. Проте його впровадження потребує значних фінансових інвестицій, а також технічної підтримки для забезпечення сумісності зі старими мережами.

У сфері практичних рекомендацій для операторів зв’язку дослідники пропонують впроваджувати системи моніторингу аномалій. Завдяки таким системам можна оперативно виявляти підозрілу активність у мережі, наприклад надмірну кількість однотипних запитів або відхилення у структурі трафіку.

Багато авторів наголошують на необхідності створення централізованих платформ для обміну даними між операторами, що дозволить швидко реагувати на нові загрози.

Крім того, аналіз показує, що успішний захист мереж SS7 потребує не лише технологічних рішень, але й підвищення обізнаності персоналу операторів. Впровадження тренінгів, регулярних аудиторських перевірок і стандартів безпеки є важливим компонентом стратегії захисту.

Отже, сучасні дослідження вказують на складність та багатогранність проблеми безпеки SS7, водночас пропонуючи комплексний підхід до її вирішення. Зважаючи на швидкий розвиток технологій і зростання загроз, подальші дослідження та інноваційні рішення залишаються ключем до забезпечення надійної та безпечної роботи телекомунікаційних мереж.

1.5 Підхід до захисту мереж

Захист мереж, побудованих на базі протоколу SS7, є критично важливим завданням для сучасних телекомунікаційних операторів. Це обумовлено широким використанням цього протоколу в мережах 2G і 3G, а також його вразливостями, які можуть використовуватися зловмисниками для атаки. Сучасний підхід до захисту базується на впровадженні низки заходів, які забезпечують багаторівневу безпеку та мінімізують ризики.

Одним із ключових інструментів є SS7 Firewall, який виконує функцію бар’єра між зовнішніми мережами і внутрішньою інфраструктурою оператора. Основна ідея використання такого фаєрвола полягає у перевірці вхідного та вихідного трафіку на рівні протоколу. Всі запити аналізуються на предмет їхньої легітимності, а ті, що не відповідають встановленим правилам безпеки, блокуються. Наприклад, запити ProvideSubscriberInfo, які часто використовуються для відстеження місцезнаходження абонентів, можуть бути відфільтровані ще до потрапляння в мережу. Завдяки таким рішенням оператори

можуть запобігти несанкціонованому доступу до своїх систем і забезпечити захист критичної інформації.

Ще одним важливим напрямком є шифрування трафіку, яке дозволяє захистити дані від перехоплення. Незважаючи на те, що SS7 спочатку не підтримував шифрування, сучасні рішення дозволяють інтегрувати захищені канали зв'язку, такі як VPN-тунелі, між вузлами мережі. Це особливо актуально для міжнародного роумінгу, де трафік проходить через декілька операторів. Захищені канали допомагають забезпечити конфіденційність даних, знижуючи ймовірність їх перехоплення та маніпуляцій з боку зловмисників.

Використання систем моніторингу трафіку, заснованих на аналізі аномалій, є ще одним ефективним методом захисту. Такі системи дозволяють виявляти підозрілі патерни в трафіку, що свідчать про потенційні атаки. Наприклад, надмірна кількість запитів із одного джерела або використання команд, нехарактерних для нормальної роботи мережі, можуть бути ознакою спроби атаки. Виявлення таких аномалій у реальному часі дозволяє операторам оперативно реагувати, блокуючи загрози ще до їх реалізації.

Багаторівнева автентифікація також є важливим елементом сучасного підходу до захисту. У протоколі SS7, який базується на довірі між вузлами, відсутні механізми автентифікації. Сучасні технології дозволяють впроваджувати процедури перевірки кожного запиту перед його обробкою. Наприклад, використання цифрових сертифікатів або криптографічних ключів для автентифікації вузлів мережі допомагає знизити ризики підробки запитів.

Перехід до більш сучасних стандартів, таких як Diameter, також є перспективним напрямком. Diameter був розроблений з урахуванням уроків, отриманих під час експлуатації SS7, і включає в себе вбудовані механізми шифрування, автентифікації та контролю доступу. Проте впровадження Diameter є довгостроковим завданням, яке потребує значних інвестицій і часу. Крім того, для забезпечення сумісності між різними поколіннями мереж (2G, 3G, LTE) необхідно підтримувати роботу SS7 паралельно з новими стандартами. [4]

Важливим аспектом захисту є навчання персоналу операторів і користувачів. Багато атак на основі SS7 можливі через людський фактор, такий як неправильно налаштовані системи або недостатня обізнаність співробітників. Регулярне проведення навчань, розробка політик безпеки і їх впровадження дозволяють знизити ймовірність помилок і забезпечити відповідність сучасним стандартам.

Комплексний підхід, який поєднує технологічні, організаційні та регуляторні заходи, є найбільш ефективним у забезпеченні безпеки мереж SS7. Наприклад, впровадження національних і міжнародних стандартів, розроблених організаціями, такими як GSM Association, дозволяє гармонізувати підходи до захисту між операторами різних країн. Завдяки цьому не лише мінімізуються ризики, але й підвищується довіра до операторів зв’язку, що важливо для користувачів.

Таким чином, багаторівнева стратегія, що включає шифрування, фільтрацію, моніторинг і автентифікацію, дозволяє значно знизити вразливість мереж, побудованих на базі SS7. Крім того, інвестування в сучасні технології та навчання персоналу допомагає операторам залишатися на передовій захисту телекомунікаційних систем

РОЗДІЛ 2 ЗАГАЛЬНІ ПІДХОДИ ТА ОСНОВНІ МЕТОДИ ДОСЛІДЖЕНЬ

2.1 Вразливості протоколу SS7

Протокол SS7, який був створений для забезпечення глобальної інтеграції телекомунікаційних мереж, спочатку проектувався у середовищі, де основною передумовою була довіра між операторами. Цей підхід привів до того, що базові функції безпеки, такі як шифрування і автентифікація, були або взагалі відсутні, або недостатньо розвинуті. У сучасному контексті це створює численні вразливості, які можуть бути використані зловмисниками.

Вразливості протоколу SS7, такі як перехоплення SMS, локаційне відстеження та маніпуляція маршрутизацією, можуть бути представлені у вигляді інтегрованої онтології ризиків [3]. Такий підхід може бути адаптований для аналізу команд SS7, наприклад, SendRoutingInfo та UpdateLocation. Він дозволяє створити знання, зрозумілі як технічним експертам, так і фахівцям із забезпечення безпеки.

Однією з ключових проблем протоколу SS7 є відсутність шифрування даних між вузлами мережі. Це дозволяє перехоплювати сигнальний трафік, включаючи запити та відповіді, у відкритому вигляді. Уразливість до так званих "людина-в-середині" атак стає критичною в умовах глобального трафіку між операторами, які фізично розташовані у різних країнах.

Іншою серйозною проблемою є недостатня автентифікація запитів. Протокол SS7 працює на основі довіри між операторами, що дозволяє зловмисникам імітувати законні запити, такі як SendRoutingInfoForSM або ProvideSubscriberInfo. Це відкриває двері для атак, спрямованих на перехоплення повідомлень, визначення локації абонентів або перенаправлення дзвінків.

Надмірно довірливий доступ до функцій SS7 є ще однією значною вразливістю. Будь-який вузол, що отримує доступ до мережі SS7, може надсилати запити або модифікувати сигнальний трафік. Це створює ризики у

випадках, коли доступ до протоколу мають недостатньо захищені або зловмисні вузли.

Ще однією важливою проблемою є відсутність фільтрації трафіку. Багато операторів не використовують спеціалізовані SS7 Firewall, що робить їхні мережі вразливими до надмірного обсягу запитів або до експлуатації уразливих команд. Відсутність чіткого моніторингу і фільтрації дозволяє зловмисникам непомітно здійснювати атаки протягом тривалого часу.

Крім того, дослідники зазначають ризики, пов’язані з роумінгом, оскільки SS7 відіграє ключову роль у підтримці міжнародного зв’язку. Уразливості під час роумінгу дозволяють зловмисникам використовувати різницю в налаштуваннях безпеки між операторами, щоб здійснювати фінансові шахрайства або перехоплювати трафік.

Особливу увагу також приділяють помилкам у конфігурації мереж. Навіть у випадках, коли оператори впроваджують базові засоби захисту, неправильна конфігурація може зробити їх неефективними. Вразливості часто виникають через відсутність узгодженості між налаштуваннями обладнання різних виробників.

Таким чином, вразливості SS7 обумовлені його архітектурою, що не була розрахована на сучасні вимоги до безпеки. Вони становлять серйозну загрозу як для конфіденційності користувачів, так і для стабільності роботи телекомунікаційних операторів. Подальші розділи роботи присвячені детальному аналізу атак, які експлуатують ці вразливості, та методам їхнього нейтралізування.

2.2 Популярні атаки на SS7

Атаки на протокол SS7 активно використовують його структурні вразливості, що дозволяє зловмисникам отримувати доступ до конфіденційної інформації, порушувати конфіденційність користувачів і виконувати шахрайські

дії. Наведені нижче приклади ілюструють основні механізми експлуатації цих вразливостей.

Перехоплення SMS є однією з поширених форм атак. Зловмисники використовують команду SendRoutingInfoForSM, яка дозволяє отримати інформацію про маршрут доставки SMS. Після цього повідомлення перенаправляються на підроблені вузли мережі. Основними цілями такої атаки є отримання одноразових паролів для двофакторної автентифікації або компрометація конфіденційної інформації, надісланої через SMS. Реалізація передбачає надсилання запитів на вузли HLR або MSC з використанням підроблених ідентифікаційних даних. Як приклад, у 2022 році в Європі група хакерів використовувала цю вразливість для перехоплення OTP-кодів банківських транзакцій, що дозволило їм виконувати несанкціоновані перекази коштів із рахунків клієнтів [5].

Локаційне відстеження використовує команду ProvideSubscriberInfo, що надає можливість отримати поточне місцезнаходження абонента. Ця інформація може використовуватися для шпигунства, переслідування або фізичного відстеження. Механізм атаки полягає у надсиланні численних запитів на вузли HLR для отримання географічних координат абонента. Наприклад, у 2021 році дослідники з Positive Technologies зафіксували випадки, коли зловмисники використовували цю вразливість для відстеження політиків і журналістів, відправляючи численні запити для визначення їхнього місцезнаходження [6].

Переадресація дзвінків здійснюється за допомогою команди UpdateLocation, яка дозволяє змінювати маршрут викликів жертви. Це дає змогу зловмисникам перенаправляти дзвінки на підроблені номери, отримуючи доступ до конфіденційної інформації під час розмов. Реалізація включає зміну записів у HLR, щоб виклики проходили через вузол зловмисників. У 2023 році в Південній Америці хакери використовували цей метод, перенаправляючи виклики банківських клієнтів на свої номери, що дозволило їм отримувати фінансову інформацію для несанкціонованих операцій.

Шахрайство в роумінгу використовує команди SS7 для маніпуляцій із роумінговими параметрами, що дозволяє зловмисникам користуватися послугами зв'язку без оплати. Вони змінюють дані про роумінг у HLR/VLR, перенаправляючи трафік через неофіційні вузли. Наприклад, у 2020 році в Південно-Східній Азії оператор зазнав значних збитків через маніпуляції з роумінговими даними, що дозволило хакерам безкоштовно користуватися міжнародними викликами протягом тривалого періоду [7].

Сучасні атаки на SS7 стають дедалі складнішими, оскільки зловмисники комбінують кілька методів для досягнення своїх цілей. Наприклад, локаційне відстеження може поєднуватися із шахрайством у роумінгу, а перехоплення SMS із переадресацією викликів. Глобальна природа SS7 ускладнює впровадження універсальних заходів безпеки, а висока вартість модернізації мереж затримує перехід на сучасніші протоколи, такі як Diameter.

Попри зусилля урядів і телекомунікаційних компаній, повністю усунути загрози SS7 наразі неможливо. Це робить питання захисту мереж критично важливим як для безпеки користувачів, так і для стабільності роботи операторів.

2.3 Механізми та команди SS7, які викликають ризики

Протокол SS7 включає низку механізмів і команд, які забезпечують передачу даних та управління телекомунікаційними послугами. Однак їхня початкова архітектура, орієнтована на довіру між вузлами, створює серйозні вразливості. Описані нижче компоненти є найбільш ризикованими у використанні.

MAP (Mobile Application Part) – це основний компонент протоколу SS7, що відповідає за управління критично важливими послугами в телекомунікаційних мережах, такими як роумінг, обмін SMS і автентифікація абонентів. Він забезпечує передачу сигналів між базами даних HLR (Home Location Register) і VLR (Visitor Location Register), які зберігають інформацію про абонентів та їх місцезнаходження.

MAP (Mobile Application Part) виконує ключову роль у роботі телекомунікаційних мереж, забезпечуючи функціональність роумінгу, SMS, голосових послуг та автентифікації абонентів. Він слугує основою для обміну критично важливими даними між компонентами мережі.

Роумінг є однією з найважливіших функцій MAP. Команди MAP дозволяють абонентам користуватися зв'язком за межами їхньої домашньої мережі. Наприклад, команда **UpdateLocation** забезпечує реєстрацію абонента в зоні дії нової мережі, передаючи дані про місцезнаходження з VLR до HLR.

MAP також підтримує SMS і голосові послуги. Команди протоколу забезпечують маршрутизацію цих послуг через HLR, який зберігає інформацію про те, який MSC обслуговує абонента. Це дозволяє доставляти повідомлення та виклики навіть у складних мережевих умовах.

Автентифікація є ще одним ключовим аспектом MAP. Команди цього протоколу забезпечують обмін автентифікаційними ключами між елементами мережі, що дозволяє перевіряти легітимність абонента перед наданням доступу до послуг.

Попри свою функціональність, MAP має значні вразливості, які зловмисники можуть використовувати для атак. Наприклад, команда **SendRoutingInfo** дозволяє отримувати маршрутну інформацію для доставки SMS або виконання викликів. Через відсутність автентифікації вузлів зловмисники можуть використовувати цю команду для доступу до конфіденційної інформації. У 2022 році ця вразливість була використана для перехоплення OTP-кодів банківських клієнтів, що дозволило виконувати несанкціоновані перекази коштів [8].

Інша ризикована команда — InsertSubscriberData, яка використовується для внесення змін до записів про абонента в HLR. Зловмисники можуть використовувати її для зміни параметрів абонента, наприклад, перенаправлення дзвінків на свої номери або активації небажаних послуг. У 2023 році хакери змогли перенаправляти дзвінки банківських клієнтів, отримуючи конфіденційну інформацію для шахрайських дій [9].

Для захисту від атак через MAP оператори можуть застосовувати кілька заходів. Використання SS7 Firewall дозволяє блокувати підозрілі запити, такі як SendRoutingInfo або InsertSubscriberData, а також вести логування для аналізу загроз. Моніторинг трафіку за допомогою SIEM-систем допомагає виявляти аномальну активність, наприклад, численні запити з одного вузла. Впровадження автентифікації між вузлами забезпечує перевірку їх легітимності, а шифрування даних захищає інформацію під час передачі.

MAP-команди є основою роботи телекомунікаційних мереж, але їхня вразливість до атак робить критично важливим впровадження сучасних заходів безпеки. Це дозволяє забезпечити конфіденційність абонентів, захист даних і стабільність роботи мереж.

SCCP (Signaling Connection Control Part) виконує критичну функцію в телекомунікаційних мережах, забезпечуючи передачу сигналів і даних між різними вузлами. Цей компонент підтримує ключові операції, необхідні для ефективної роботи мережі.

Однією з головних функцій SCCP є маршрутизація сигналів. Він забезпечує логічну передачу повідомлень між вузлами мережі та різними рівнями сигналізації. Наприклад, SCCP використовується для передачі даних між HLR і VLR, необхідних для обробки запитів роумінгу [10]. Це дозволяє підтримувати зв'язок між різними частинами мережі.

SCCP також забезпечує можливість створення віртуальних з’єднань між вузлами, що значно спрощує обмін даними. Віртуальні канали дозволяють операторам і абонентам обмінюватися інформацією в реальному часі. Це критично важливо для забезпечення якісного зв’язку, особливо під час голосових викликів, передачі даних або роботи з базами даних.

Ще однією важливою функцією SCCP є обробка адрес. Він дозволяє транслювати адреси для доставки повідомлень у різні сегменти мережі. Наприклад, SCCP перетворює номер телефону в MSC або VLR, які відповідають за маршрутизацію викликів, що забезпечує коректне спрямування сигналів.

Попри свою функціональність, SCCP має значні вразливості. Одна з них — недостатня перевірка запитів. У SCCP відсутні вбудовані механізми автентифікації вузлів, через що система приймає запити без перевірки їхнього джерела. Це дозволяє зловмисникам надсилати фальшиві команди, які система обробляє як легітимні. Наслідки таких дій включають доступ до конфіденційної інформації абонентів і порушення нормальної роботи мережі. Наприклад, зловмисники можуть надсилати фальшиві запити для отримання інформації про маршрутизацію або місцезнаходження абонента.

Ще одна проблема — можливість обходу мережевих правил. Зловмисники можуть використовувати SCCP для створення фальшивих маршрутів сигналізації, що дозволяє приховувати їхню діяльність або проводити DoS-атаки. Це може призвести до перевантаження вузлів мережі, викликаючи їхню нестабільну роботу. Наприклад, створення маршрутів через підроблені вузли може спрямовувати великий обсяг трафіку на певний MSC, що викликає його перевантаження і виводить із ладу [11].

Ризики, пов’язані із SCCP, включають компрометацію даних, порушення цілісності мережі та масштабні DoS-атаки. Відсутність автентифікації робить SCCP вразливим до нелегітимних запитів, які можуть спричиняти збої в роботі мережі та значні фінансові збитки для операторів.

Для мінімізації цих загроз існує кілька ефективних контрзаходів. Впровадження SS7 Firewall дозволяє перевіряти джерела запитів і блокувати підозрілі команди. Моніторинг активності за допомогою SIEM-систем забезпечує виявлення аномальної сигналізації в реальному часі. Встановлення механізмів автентифікації для вузлів дозволяє перевіряти їх легітимність перед обробкою запитів. Шифрування з’єднань забезпечує захист критичних сигналів, а сегментування мережі обмежує можливості доступу до вузлів SCCP.

Хоча SCCP є важливим компонентом для передачі даних і сигналів, його вразливості створюють серйозні ризики для телекомунікаційних мереж. Для забезпечення безпеки оператори повинні впроваджувати сучасні методи захисту, такі як Firewall, шифрування даних, автентифікація та постійний моніторинг

активності мережі. Це дозволить мінімізувати ризики атак і забезпечити стабільну роботу мережевої інфраструктури.

CAMEL (Customized Applications for Mobile networks Enhanced Logic) є розширенням протоколу SS7, яке дозволяє операторам мобільних мереж впроваджувати послуги з доданою вартістю. Його основна функція полягає у забезпеченні взаємодії між різними системами, такими як голосова пошта, платні сервіси та переадресація дзвінків. Завдяки CAMEL оператори можуть створювати спеціалізовані послуги для своїх клієнтів і підтримувати їх навіть у роумінгу.

Серед основних функцій CAMEL можна виділити переадресацію дзвінків. Ця функція дозволяє автоматично перенаправляти дзвінки на голосову пошту або інші номери. Наприклад, дзвінки абонента можуть бути автоматично перенаправлені на номер служби підтримки для отримання консультації [12]. Ще одна важлива функція CAMEL — підтримка послуг у роумінгу. Це дозволяє абонентам користуватися спеціальними послугами, такими як платна переадресація викликів або голосові послуги, без необхідності зміни налаштувань. Оператори також можуть впроваджувати платні сервіси з доданою вартістю, наприклад, інтерактивні голосові меню (IVR), що дозволяють абонентам легко взаємодіяти із системою.

Однак CAMEL має низку вразливостей, які можуть бути використані зловмисниками для шахрайських дій. Однією з таких є маніпуляція параметрами послуг. Зловмисники можуть змінювати маршрутизацію дзвінків або активувати небажані послуги, перенаправляючи дзвінки на свої номери. Це дозволяє їм отримувати доступ до конфіденційної інформації, яка передається під час розмов. Інша загроза — безкоштовне використання послуг. Зловмисники можуть отримувати доступ до платних сервісів без оплати, завдаючи оператору фінансових збитків. Крім того, через CAMEL можливо створення фальшивих платних сервісів. Зловмисники перенаправляють дзвінки абонентів на преміум-номери, зареєстровані на підставних осіб, отримуючи прибуток за кожен дзвінок [13].

Ризики шахрайства через CAMEL включають фінансові втрати для операторів, компрометацію конфіденційної інформації та шкоду для репутації компанії. Наприклад, у 2021 році в Європі було виявлено групу зловмисників, які використовували CAMEL для створення фальшивих преміум-сервісів. Вони перенаправляли дзвінки на платні номери, отримуючи значний прибуток, що призвело до багатомільйонних збитків для операторів.

Для захисту CAMEL необхідно впроваджувати сучасні заходи безпеки. Використання SS7 Firewall дозволяє фільтрувати запити до CAMEL та обмежувати доступ до послуг для неперевірених вузлів. Моніторинг трафіку допомагає виявляти аномальну активність, наприклад, різке збільшення дзвінків на преміум-номери. Встановлення механізмів автентифікації між вузлами забезпечує перевірку їхньої легітимності. Регулярний аудит платних послуг та контроль преміум-номерів дозволяють уникнути їх використання зловмисниками.

CAMEL відіграє важливу роль у впровадженні послуг із доданою вартістю, але його вразливості потребують уваги. Впровадження ефективних заходів захисту є критично важливим для забезпечення безпеки клієнтів, фінансової стабільності операторів і довіри до їхніх послуг.

CAMEL є корисним інструментом для надання послуг із доданою вартістю, але його вразливості створюють серйозні ризики шахрайства та компрометації конфіденційності. Операторам необхідно впроваджувати сучасні заходи захисту, такі як SS7 Firewall, моніторинг трафіку та автентифікацію вузлів, щоб мінімізувати ризики та забезпечити надійну роботу своїх послуг.

Протокол SS7, хоч і забезпечує ключові функції для роботи телекомунікаційних мереж, має вразливості, що створюють значні ризики. Без належних захисних заходів оператори стикаються з такими проблемами, як перехоплення даних, компрометація конфіденційності та фінансові збитки. [14]

Для мінімізації загроз необхідно впроваджувати сучасні засоби захисту. Одним із ключових інструментів є SS7 Firewall, який дозволяє фільтрувати небажані запити, обмежувати доступ до критичних вузлів та контролювати

трафік у режимі реального часу. Моніторинг трафіку забезпечує виявлення аномальної активності та потенційних атак завдяки аналізу сигналізації та виявленню відхилень від нормального функціонування мережі. Вдосконалені механізми автентифікації, такі як впровадження сертифікатів або токенів, додають додатковий рівень захисту, запобігаючи доступу до вузлів SS7 з боку недовірених джерел.

Ці заходи, застосовані у комплексі, дозволяють зменшити ризики, покращити безпеку телекомунікаційної інфраструктури та забезпечити стабільність роботи мереж у сучасних умовах

2.4 Методи захисту

Захист протоколу SS7 включає впровадження систем моніторингу, фільтрації трафіку та модернізацію на основі альтернативних протоколів, таких як Diameter. Однак ці методи не завжди можуть бути швидко реалізовані через технічні та фінансові обмеження.

Можна використати також аксіоматично-дедуктивний підхід для організації знань у складних системах. Це дозволяє структурувати процеси моніторингу та автоматизувати аналіз аномалій у трафіку SS7. Впровадження цього підходу в системи телекомунікацій забезпечить більш надійний контроль за підозрілою активністю та дозволить швидко реагувати на кіберзагрози [4].

Для зменшення ризиків, пов’язаних із вразливостями протоколу SS7, оператори телекомунікацій застосовують різні методи захисту. Вони дозволяють забезпечити базовий рівень безпеки шляхом ізоляції критичних вузлів, контролю доступу та моніторингу мережевого трафіку. Одним із ключових підходів є мережеве сегментування.

Мережеве сегментування передбачає розділення телекомунікаційної інфраструктури на логічно та фізично ізольовані сегменти, щоб обмежити доступ до критичних компонентів мережі та запобігти розповсюдженню атак.

Механізм сегментування мережі SS7 є важливим етапом забезпечення її безпеки. Він передбачає ізоляцію вузлів, контроль доступу та захист точок входу, що мінімізує ризики несанкціонованого доступу та атак. Ізоляція вузлів SS7 полягає в розділенні компонентів, які відповідають за обробку сигналізації, від загальної IP-мережі. Це можна здійснити за допомогою фізичного або логічного розділення. Фізичне розділення передбачає використання окремих серверів або комутаторів, які функціонують виключно для вузлів SS7. Логічне розділення реалізується шляхом створення віртуальних локальних мереж (VLAN). Такі VLAN забезпечують ізоляцію певних сегментів мережі навіть у межах однієї фізичної інфраструктури.

Контроль доступу є наступним важливим етапом, що забезпечує захист мережі SS7. У цьому процесі налаштовуються спеціальні правила, які визначають взаємодію тільки між перевіреними вузлами. Це дозволяє значно обмежити можливості несанкціонованого доступу до критичних компонентів мережі. Для ще більшої безпеки застосовуються міжмережеві екрани (firewalls). Вони виконують функцію блокування трафіку, що надходить із зовнішніх IP-адрес до сегментів, у яких розташовані вузли SS7. Це значно знижує ризик проникнення зовнішніх загроз.

Сегментування мережі має низку значних переваг. Завдяки цьому механізму зловмисникам стає складніше отримати доступ до вузлів SS7 навіть у випадку проникнення до загальної IP-мережі оператора. Сегментація також дозволяє локалізувати атаки, ізолюючи їх у межах певного сегмента мережі. Це запобігає поширенню загроз на інші частини інфраструктури, що забезпечує стабільну роботу всіх компонентів. Крім того, сегментування підвищує гнучкість в управлінні мережею. У разі виникнення інцидентів це дозволяє оперативно реагувати на загрози без необхідності масштабних змін у мережевій інфраструктурі [15].

Прикладом реалізації сегментування є успішний досвід одного з телекомунікаційних операторів. У рамках цього підходу вузли SS7 були ізольовані від основної IP-мережі, яка використовується для надання інтернет-

послуг. Це було досягнуто шляхом налаштування VLAN-конфігурації, у якій вузли SS7 розмістили у VLAN 10, а користувацькі сервери — у VLAN 20. Між цими сегментами було встановлено міжмережевий екран. Він дозволяв проходження лише критично важливого трафіку, наприклад, запитів від довірених вузлів. Такий підхід забезпечив додатковий рівень захисту мережі, дозволив ефективно ізолювати вузли SS7 та запобігти потенційним загрозам.

Обмеження сегментування мережі SS7 пов’язані з низкою технічних і організаційних факторів. Одним із основних обмежень є складність реалізації. Впровадження сегментації вимагає ретельного планування архітектури мережі, детальної конфігурації обладнання та узгодження всіх змін із поточною інфраструктурою. Це може бути особливо складно для великих операторів зв’язку, де мережі мають складну структуру і численні взаємозалежності між компонентами.

Ще одним важливим аспектом є вартість реалізації. Для досягнення фізичної ізоляції вузлів SS7 необхідно використовувати додаткове обладнання, зокрема комутатори та сервери, що створює фінансове навантаження на компанію. Крім того, залучення кваліфікованих фахівців для налаштування та підтримки сегментованої мережі може також збільшити витрати.

Попри свою ефективність у мінімізації ризиків, сегментація не усуває всіх потенційних загроз. Вона не здатна захистити від внутрішніх атак у випадках, коли зловмисник уже отримав доступ до ізольованого сегмента. Це обмеження підкреслює необхідність застосування додаткових заходів безпеки, таких як моніторинг трафіку, управління доступом та інші методи виявлення аномальної активності.

Таким чином, сегментація є корисним, але не всеосяжним інструментом забезпечення безпеки мережі SS7, який потребує комплексного підходу для досягнення максимального ефекту.

Мережеве сегментування є одним із ключових методів базового захисту телекомунікаційної інфраструктури. Воно значно ускладнює доступ до критичних вузлів і локалізує потенційні загрози в межах окремих сегментів

мережі. Попри деякі обмеження, сегментація є важливим етапом у побудові комплексної системи безпеки SS7.

Фільтрація сигналів є одним із ключових методів захисту протоколу SS7. Цей підхід базується на контролі та обмеженні доступу до команд протоколу на основі визначених правил, що дозволяє значно зменшити ризик використання вразливостей для атак.

Механізм фільтрації сигналів є важливим інструментом для забезпечення безпеки мережі SS7. Його основною функцією є аналіз і обробка запитів, що надходять до мережі, з метою виявлення та блокування потенційно небезпечних дій. Усі запити аналізуються на відповідність встановленим правилам фільтрації, що дозволяє обмежувати доступ до критичних вузлів або команд. Наприклад, команда SendRoutingInfo, яка відповідає за маршрутизацію SMS, може бути заблокована для вузлів, які не мають дозволу на її виконання. Сигнали приймаються та відправляються виключно від перевірених джерел, що входять до списку довірених вузлів оператора.

Фільтрація сигналів здійснюється за декількома типами. Фільтрація за типом команд дозволяє встановлювати обмеження на виконання певних команд, які можуть бути використані зловмисниками. Наприклад, виконання команди SendRoutingInfo може бути заборонено для вузлів, які не є частиною роумінгової системи, або команда InsertSubscriberData обмежується тільки внутрішніми вузлами. Це значно знижує ймовірність атак, пов’язаних із критичними командами [16].

Фільтрація за джерелом запитів передбачає обробку тільки тих запитів, що надходять від вузлів зі списку довірених джерел. Наприклад, дозволяється обробка запитів лише від внутрішніх вузлів оператора або його партнерів у роумінгу, тоді як усі інші запити блокуються або відхиляються. Це ефективно зменшує ризик атак із зовнішніх джерел.

Як приклад реалізації фільтрації сигналів, оператор телекомунікацій може налаштувати SS7 Firewall із чіткими правилами. Команда SendRoutingInfo блокується для запитів від зовнішніх вузлів, які не належать до списку

роумінгових партнерів. Команда UpdateLocation дозволяється лише для вузлів із певними IP-адресами, які входять до внутрішньої мережі. Команда InsertSubscriberData забороняється для вузлів, які не пройшли автентифікацію. Такий підхід дозволяє ефективно контролювати потік сигналів у мережі та мінімізувати ризики небажаних дій.

Фільтрація сигналів має численні переваги. Вона є ефективним засобом запобігання атакам, оскільки дозволяє блокувати небажані команди ще на етапі надсилання запиту до вузла. Обмеження доступу за джерелом запиту локалізує загрози, не дозволяючи зовнішнім вузлам виконувати небажані дії в мережі оператора. Крім того, механізм фільтрації забезпечує гнучкість налаштувань, що дає змогу адаптувати правила до специфічних потреб оператора [17].

Однак цей підхід має і певні недоліки. Одним із них є необхідність регулярного оновлення правил фільтрації, оскільки загрози в мережі постійно змінюються. Це вимагає активного моніторингу та швидкої адаптації до нових типів атак. Неправильно налаштовані правила можуть викликати затримки в обробці сигналів або навіть блокувати легітимні запити, що може негативно вплинути на функціонування мережі. Крім того, впровадження фільтрації сигналів є складним завданням, яке потребує високого рівня технічної експертизи та регулярного контролю. Таким чином, для ефективної роботи цього механізму необхідний комплексний підхід, що включає постійний моніторинг і оптимізацію правил.

Фільтрація сигналів є ефективним методом захисту протоколу SS7, оскільки дозволяє запобігати атакам ще на етапі обробки запитів. Вона забезпечує контроль за доступом до критичних команд і вузлів, що мінімізує ризики для телекомунікаційної мережі. Проте її ефективність залежить від правильної реалізації та постійного оновлення правил.

Обмеження доступу за географією є одним із підходів до захисту протоколу SS7, який спрямований на зменшення ризику атак із зовнішніх джерел. Цей метод базується на аналізі географічного походження вхідних запитів і дозволяє блокувати потенційно небезпечні запити з недовірених регіонів.

Механізм обмеження доступу за географією є важливим інструментом для підвищення безпеки мережі SS7, дозволяючи оператору контролювати джерела запитів на основі їхнього географічного розташування. Усі вхідні запити до вузлів перевіряються на відповідність визначеним географічним зонам. Це забезпечує можливість блокування небажаних запитів із регіонів, які не входять до списку довірених зон. Список довірених регіонів може включати лише ті країни, де оператор має бізнес-партнерів або роумінгові угоди. Наприклад, доступ дозволяється лише вузлам, що належать операторам із країн Європи та Північної Америки. Усі запити з регіонів, які не входять до списку, автоматично блокуються.

Географічні обмеження мають значні переваги. Вони знижують рівень зовнішніх загроз, обмежуючи запити з регіонів, де оператор не має партнерів. Це зменшує ризик атак від зловмисників, які використовують слабкі правила безпеки в певних країнах. Локалізація доступу дозволяє оператору зосередитися на обробці запитів лише від перевірених вузлів, що покращує загальну безпеку мережі. Крім того, цей підхід забезпечує гнучкість, оскільки географічні обмеження можуть бути налаштовані відповідно до змін у бізнес-стратегії або партнерській мережі [18].

Проте географічні обмеження мають і свої недоліки. Для забезпечення ефективності цього механізму необхідний постійний моніторинг і оновлення списку дозволених регіонів, щоб враховувати зміни в партнерській мережі. Такий підхід не може повністю захистити від атак, які виконуються через компрометовані вузли у дозволених зонах. Крім того, реалізація обмежень потребує використання спеціалізованих інструментів для аналізу IP-адрес, таких як GeoIP-сервіси, що може призвести до додаткових витрат.

Приклад реалізації обмеження доступу за географією включає кілька етапів. Оператор телекомунікацій може скласти список дозволених регіонів, надавши доступ до вузлів SS7 лише з IP-адрес перевірених партнерів у визначених країнах, наприклад, Європи та Північної Америки. Запити з регіонів із високим рівнем активності зловмисників автоматично блокуються. Для додаткового

захисту оператор може використовувати SIEM-системи, які аналізують аномальні запити навіть із дозволених регіонів, щоб виявити компрометовані вузли.

Для підвищення ефективності географічних обмежень рекомендується інтегрувати цей підхід з іншими методами, такими як фільтрація сигналів і SS7 Firewall. Навіть вузли із дозволених регіонів повинні перевірятися на наявність аномальної активності, щоб запобігти потенційним загрозам. Списки дозволених регіонів та IP-адрес слід регулярно оновлювати відповідно до змін у партнерських відносинах.

Географічні обмеження є важливим елементом захисту мережі SS7, оскільки вони мінімізують ризики атак із зовнішніх джерел. Однак для забезпечення комплексного захисту мережі цей підхід повинен використовуватися разом із сучасними технологіями, такими як SS7 Firewall та системи моніторингу, що забезпечує багаторівневий захист інфраструктури.

2.5 Сучасні підходи до захисту

Захист телекомунікаційних мереж, що базуються на протоколі SS7, є багатовекторною задачею, яка потребує застосування інноваційних підходів і технологій. Враховуючи широту та складність мереж SS7, сучасні методи захисту орієнтовані на багаторівневий контроль і активну протидію загрозам.

Одним із найважливіших підходів є впровадження захисної архітектури на основі політик безпеки. Цей підхід передбачає використання так званих сигнальних міжмережевих екранів (SS7 Firewall), які аналізують вхідний і вихідний трафік у реальному часі. Такі системи можуть застосовувати кілька рівнів фільтрації: від базового аналізу сигнатур до контекстної обробки, яка враховує історію дій у мережі. Наприклад, запит на локацію абонента з невідомого джерела може бути заблокований, а інформація про нього — надіслана оператору для розслідування.

Сучасні технології шифрування даних у протоколах зв’язку стали стандартом у багатьох галузях, але в SS7 це залишається викликом. Проте розробка адаптивних механізмів шифрування є пріоритетом для операторів зв’язку. Наприклад, впровадження TLS (Transport Layer Security) у каналах обміну сигналами може значно ускладнити перехоплення інформації зловмисниками. [19]

Додатково до цього, використання систем аналізу поведінки трафіку дозволяє виявляти аномальні дії, які можуть свідчити про спробу атаки. Ці системи здатні автоматично генерувати попередження або навіть блокувати підозрілий трафік. Наприклад, раптовий сплеск запитів ProvideSubscriberInfo може бути автоматично позначений як потенційна загроза.

Інтеграція штучного інтелекту (ШІ) та машинного навчання у системи захисту мереж SS7 також є перспективним напрямком. Використання ШІ дозволяє створювати моделі, які прогнозують поведінку зловмисників і виявляють навіть приховані загрози. Наприклад, алгоритми можуть виявляти аномалії у патернах трафіку, які звичайна система моніторингу може пропустити.

Значну увагу приділяють створенню регуляторних стандартів та норм, які забезпечують уніфікований підхід до захисту мереж SS7. Це включає вимоги до використання захищених каналів зв’язку, обов’язкову автентифікацію вузлів і аудит дій у мережі. Впровадження таких стандартів, як GSMA FS.11 (SS7 Interconnect Security), допомагає операторам знижувати ризики і підвищувати рівень безпеки.

У контексті інтеграції SS7 з мережами четвертого та п’ятого поколінь, особливу увагу приділяють гібридним рішенням, які забезпечують сумісність між різними протоколами і одночасно підвищують безпеку. Наприклад, використання Diameter як заміни для SS7 у LTE-мережах дозволяє зменшити вразливості, характерні для старого протоколу, і водночас забезпечити зворотну сумісність.

Крім технічних заходів, важливо впроваджувати підвищення обізнаності операторів та персоналу. Регулярні тренінги та симуляції атак дозволяють персоналу оперативно реагувати на інциденти і впроваджувати захисні заходи. Успішний приклад такого підходу демонструють великі оператори зв’язку, які проводять регулярні тестування безпеки своїх мереж із залученням зовнішніх експертів.

Попри всі вжиті заходи, важливо пам’ятати, що жодна система захисту не є абсолютною. Тому сучасні підходи базуються на принципі "глибокого захисту", де використовується комбінація декількох рівнів безпеки, які забезпечують надійний захист навіть у випадку компрометації одного з компонентів системи.

2.6 Альтернативи SS7

Протокол SS7, хоч і залишається фундаментальним для мереж 2G і 3G, поступово втрачає свою актуальність через численні вразливості та обмеженість функціональних можливостей у сучасних умовах. У відповідь на виклики сучасних телекомунікаційних систем було розроблено кілька альтернатив, які пропонують більш надійні та адаптивні рішення. Вибір альтернативи залежить від потреб оператора, доступного обладнання та рівня безпеки, який потрібно забезпечити.

Однією з найпоширеніших альтернатив SS7 є протокол Diameter. Це покращений і масштабований варіант SS7, який був спеціально розроблений для роботи у мережах LTE та 5G. Diameter усуває основні проблеми SS7, такі як відсутність шифрування та автентифікації, завдяки інтеграції сучасних засобів безпеки. Наприклад, цей протокол включає вбудовані механізми шифрування трафіку між вузлами, що значно знижує ризик перехоплення даних. Diameter також підтримує більш гнучку архітектуру, яка легко адаптується до потреб оператора та дозволяє інтегруватися з існуючими IP-мережами.

Ще однією важливою альтернативою є IP Multimedia Subsystem (IMS). Ця платформа забезпечує передачу мультимедійного трафіку через IP-протоколи,

використовуючи сучасні засоби шифрування та автентифікації. IMS є невід'ємною частиною мереж 4G і 5G, забезпечуючи підтримку таких послуг, як голосові дзвінки, відеозв’язок та обмін мультимедійними повідомленнями. Особливість IMS полягає у використанні IPsec для шифрування трафіку, що забезпечує вищий рівень безпеки порівняно з SS7. Окрім того, IMS дозволяє операторам оптимізувати роботу своїх мереж і скоротити витрати на обслуговування завдяки автоматизації багатьох процесів.

Серед перспективних розробок варто відзначити Signal System No. 8 (SS8). Хоча цей протокол ще знаходиться на стадії розробки, він привертає увагу завдяки своїй спрямованості на безпеку та ефективність. SS8 інтегрує вдосконалені механізми виявлення та попередження атак, а також пропонує більшу гнучкість у налаштуванні мережевих параметрів. Це робить його привабливим для операторів, які прагнуть зменшити ризики, пов'язані з експлуатацією застарілих протоколів.

Перехід до сучасних альтернатив має важливі перспективи, але також стикається з низкою викликів. Найбільш значущими є висока вартість впровадження нових рішень, необхідність модернізації існуючого обладнання та забезпечення сумісності з поточними системами. Крім того, оператори стикаються з проблемами підготовки персоналу до роботи з новими протоколами та інтеграції цих рішень у вже існуючі мережі.

Однією з ключових переваг переходу на нові стандарти є можливість зниження витрат, пов’язаних із підтримкою та захистом мережі, а також значне зменшення вразливостей. Diameter, IMS та інші сучасні рішення дозволяють операторам забезпечити надійний захист даних, підвищити якість обслуговування абонентів та розширити спектр наданих послуг.

Зрештою, впровадження сучасних протоколів, таких як Diameter або IMS, є не лише технологічною необхідністю, але й стратегічною інвестицією в майбутнє телекомунікацій. Це забезпечує можливість ефективного функціонування мережі в умовах постійного розвитку технологій та зростання вимог до безпеки.

2.7 Практичні рекомендації для операторів зв’язку

Впровадження ефективного захисту телекомунікаційних мереж від загроз, пов’язаних із протоколом SS7, вимагає комплексного підходу. Оператори зв’язку повинні поєднувати технічні заходи з організаційними ініціативами, щоб забезпечити безпеку своїх мереж та захистити конфіденційність даних абонентів. Нижче наведено основні рекомендації для операторів зв’язку щодо забезпечення безпеки.

По-перше, впровадження SS7 Firewall є ключовим технічним заходом. Ці рішення дозволяють фільтрувати сигнальний трафік і блокувати потенційно небезпечні запити. SS7 Firewall здатен визначати аномальні активності, аналізувати вхідні та вихідні запити та зупиняти їх, якщо вони не відповідають політикам безпеки мережі. Це особливо важливо для запобігання атакам, таким як перехоплення SMS або відстеження місцезнаходження користувачів.

По-друге, рекомендується впроваджувати багаторівневий моніторинг трафіку. Використання систем моніторингу дозволяє виявляти підозрілу активність у реальному часі та вживати необхідних заходів для запобігання атак. Такі системи можуть аналізувати сигнали для виявлення аномалій, порушень у структурі трафіку або несанкціонованих запитів. Моніторинг забезпечує не тільки виявлення проблем, але й їх подальший аналіз для вдосконалення політик безпеки.

По-третє, важливим етапом є впровадження механізмів автентифікації вузлів у мережі. Протокол SS7 не передбачає механізмів автентифікації, тому додавання таких рішень, як Secure Diameter, може суттєво знизити ризики. Це дозволяє перевіряти легітимність запитів, які надходять до мережі, і забезпечувати доступ лише авторизованим вузлам. [20]

Крім того, перехід на сучасні протоколи, такі як Diameter, є одним із найефективніших стратегічних кроків. Diameter включає вбудовані механізми шифрування та автентифікації, які дозволяють захистити дані абонентів від

несанкціонованого доступу. Перехід на цей протокол також дозволяє інтегрувати мережі 4G та 5G, що є важливим у контексті розвитку телекомунікаційних технологій.

Організаційні заходи також відіграють значну роль. Оператори повинні періодично проводити аудити безпеки своїх мереж, перевіряючи відповідність протоколів сучасним стандартам. Навчання персоналу є ще одним важливим аспектом. Співробітники повинні мати навички виявлення та усунення загроз, а також знати, як працювати із сучасними засобами захисту.

Рекомендації для регуляторів також є невід'ємною частиною комплексного підходу. На національному рівні повинні впроваджуватися політики, які зобов'язують операторів забезпечувати належний рівень безпеки. Наприклад, регулятори можуть вимагати використання SS7 Firewall, регулярного моніторингу та звітності про інциденти безпеки.

Впровадження цих рекомендацій допоможе операторам підвищити стійкість мереж до атак, забезпечити захист даних абонентів і покращити довіру користувачів до їхніх послуг. Незважаючи на складність і витратність цих заходів, вони є критично важливими для забезпечення стабільної роботи телекомунікаційних систем у сучасних умовах.

2.8 Виклики впровадження захисту

Забезпечення безпеки протоколу SS7 залишається значним викликом для операторів зв'язку, особливо в умовах постійно зростаючих загроз і складності сучасних телекомунікаційних мереж. Попри наявність рішень, таких як SS7 Firewall, моніторинг трафіку, впровадження механізмів автентифікації та перехід на сучасні протоколи, їх застосування супроводжується низкою труднощів.

Першим і найбільш суттєвим викликом є висока вартість впровадження захисних заходів. Розгортання SS7 Firewall, інтеграція систем моніторингу та перехід на Diameter вимагають значних фінансових інвестицій. Це особливо складно для невеликих операторів, які мають обмежені бюджети. Крім того,

модернізація мереж може включати заміну обладнання, що додає додаткові витрати.

Другим викликом є складність інтеграції сучасних рішень у наявну інфраструктуру. Багато операторів використовують застаріле обладнання та технології, які важко поєднати з новими системами захисту. Цей процес вимагає ретельного планування, тестування та налаштування, щоб уникнути збоїв у роботі мережі.

Третім фактором є недостатній рівень підготовки персоналу. Інтеграція сучасних технологій безпеки вимагає висококваліфікованих фахівців, які здатні налаштовувати та обслуговувати такі системи. Оператори зв'язку часто стикаються з проблемою нестачі кадрів із необхідними знаннями та навичками. Це зумовлює необхідність інвестування в навчання та підвищення кваліфікації персоналу.

Ще однією проблемою є складність уніфікації стандартів і регуляторних вимог. У різних країнах використовуються різні підходи до забезпечення безпеки телекомунікаційних мереж. Це ускладнює інтеграцію міжнародних мереж і створює ризики для операторів, які працюють у кількох юрисдикціях. Регуляторні вимоги можуть бути недостатньо чіткими або застарілими, що гальмує впровадження сучасних рішень.

Крім того, оператори стикаються з опором користувачів і бізнес-партнерів, які не завжди готові до змін у роботі мереж. Наприклад, перехід на протокол Diameter може вимагати оновлення пристроїв абонентів або змін у роботі бізнес-додатків. Це може викликати незадоволення серед клієнтів і призвести до тимчасової втрати їхньої довіри.

Нарешті, постійна еволюція загроз і методів атак є ще одним викликом. Зловмисники швидко адаптуються до нових технологій і розробляють обхідні шляхи для впроваджених систем захисту. Це вимагає від операторів постійного оновлення засобів захисту та адаптації до нових викликів, що є як технічним, так і фінансовим тягарем.

Незважаючи на ці виклики, оператори зв’язку повинні докладати максимум зусиль для підвищення рівня безпеки своїх мереж. Рішення цих проблем є ключовим для забезпечення стабільності телекомунікаційної інфраструктури та захисту конфіденційності даних користувачів. Злагоджена співпраця між операторами, регуляторами та виробниками обладнання може суттєво прискорити впровадження ефективних рішень і мінімізувати ризики, пов’язані з використанням SS7.

РОЗДІЛ 3 ПРАКТИЧНІ ЗАВДАННЯ З ПРОТОКОЛОМ SS7

Практична частина роботи передбачає імітацію сигнального трафіку, аналіз його вразливостей та перевірку ефективності можливих заходів захисту. Основною метою є демонстрація реальних ризиків, пов’язаних із протоколом SS7, та перевірка сценаріїв, які можуть бути використані зловмисниками для реалізації атак.

На етапі виконання завдань було створено тестове середовище, яке дозволяє моделювати сигнальний трафік, аналізувати його структуру та оцінювати вплив атак на мережеву інфраструктуру. Крім того, в рамках роботи використовуються такі інструменти, як Wireshark, Scapy та Mininet, які забезпечують гнучкість у створенні тестових сценаріїв та відтворенні реальних загроз.

Практичний розділ складається з кількох етапів, починаючи від налаштування тестового середовища, яке дозволяє проводити безпечні експерименти, до моделювання типових атак, таких як перехоплення повідомлень або визначення місцезнаходження абонентів. Ці завдання спрямовані на демонстрацію вразливостей протоколу та перевірку можливостей впровадження захисних механізмів.

3.1 Підготовка до тестування

Для проведення практичного аналізу вразливостей протоколу SS7 необхідно створити тестове середовище, яке гарантуватиме безпеку експериментів і дозволить моделювати сигнальний трафік без впливу на реальні телекомунікаційні мережі. Це середовище створюється у кілька етапів і включає налаштування інструментів, віртуальної інфраструктури та спеціалізованого програмного забезпечення для роботи із сигнальним протоколом [21].

Обрано Kali Linux як основне середовище для експериментів. Ця операційна система пропонує широкий набір інструментів для аналізу мережевого трафіку та створення мережевих пакетів. Для забезпечення ізоляції тестового

середовища використовується віртуальна інфраструктура на основі VirtualBox, що дозволяє уникнути впливу на реальні телекомунікаційні мережі та забезпечує повний контроль над експериментальним середовищем.

На першому етапі створюється віртуальна машина з попередньо встановленим Kali Linux. Це дозволяє легко налаштовувати експериментальне середовище та встановлювати необхідні інструменти. Далі налаштовується віртуальна мережа, що складається з кількох вузлів, які імітують роботу телекомунікаційної інфраструктури. Ця мережа моделює взаємодію між вузлами HLR, VLR, MSC та іншими компонентами.

На наступному етапі завантажуються та встановлюються необхідні бібліотеки та інструменти. Серед них виділяються:

Для моделювання та аналізу вразливостей протоколу SS7 буде використано три ключові інструменти. Scapy дозволяє створювати, модифікувати та надсилати мережеві пакети, що ідеально підходить для моделювання атак і аналізу їх наслідків. Wireshark слугуватиме для захоплення мережевого трафіку, аналізу його структури та виявлення аномалій, забезпечуючи детальне розуміння поведінки протоколів. Mininet використовується для створення віртуальних мереж, що дозволяє моделювати складні топології та тестувати різні сценарії взаємодії між вузлами. Ці інструменти разом забезпечують повноцінне середовище для експериментів із сигнальним трафіком. топології.

Останнім етапом є налаштування інструментів для аналізу та моделювання трафіку. Це включає конфігурацію Scapy для генерації специфічних сигнальних пакетів, використання Wireshark для детального аналізу трафіку та створення мережевих сценаріїв за допомогою Mininet. Таке середовище дозволяє моделювати сигнальний трафік і досліджувати вразливості протоколу SS7 без ризику для реальних мереж.

Таким чином, поєднання Kali Linux, VirtualBox та спеціалізованих інструментів забезпечує безпечне, ізольоване та гнучке середовище для аналізу сигнальних протоколів. Це дає можливість ефективно вивчати вразливості SS7,

моделювати реалістичні атаки та розробляти контрзаходи для підвищення безпеки телекомунікаційних мереж.

Код для встановлення scapy (див. рисунок 3.1) та результат встановлення (див. рисунок 3.2)

```
sudo apt install scapy
```

Рисунок 3.1 – Код встановлення встановлення scapy

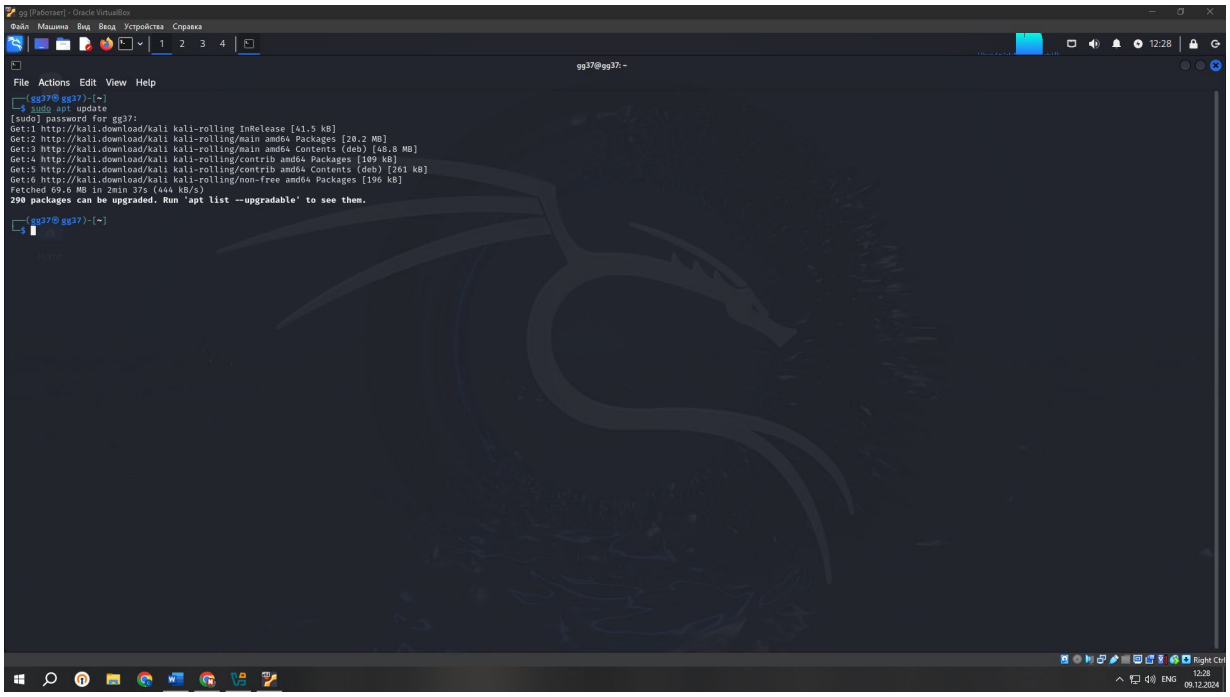

Рисунок 3.2 – Успішний результат встановлення scapy

Wireshark це інструмент для моніторингу мережевого трафіку та аналізу сигнальних пакетів. Код для встановлення wireshark (див. рисунок 3.3) та результат встановлення (див. рисунок 3.4)

```
sudo apt install wireshark
```

Рисунок 3.3 – Код встановлення встановлення wireshark

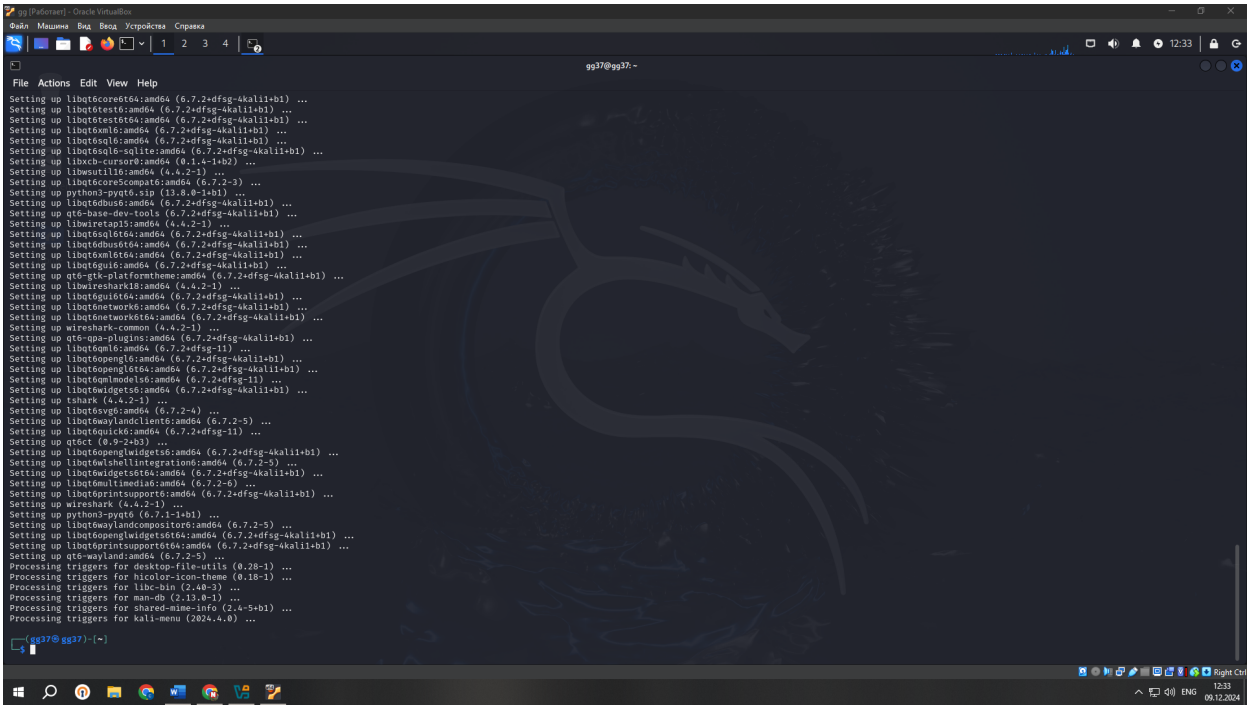

Рисунок 3.4 – Успішний результат встановлення wireshark

У налаштуваннях додаємо користувача до групи wireshark для зручності (див. рисунок 3.5)

```
sudo usermod -aG wireshark $(whoami)
```

Рисунок 3.5 – Код для додавання користувача в wireshark

Для симуляції мережевих вузлів використовується Mininet. Код для встановлення mininet (див. рисунок 3.6) та результат встановлення (див. рисунок 3.7).

```
sudo apt install mininet
```

Рисунок 3.6 – Код встановлення встановлення mininet

Рисунок 3.7 – Успішний результат встановлення mininet

Мережа залишається в стандартному режимі NAT з DHCP, що дозволяє автоматично отримувати IP-адресу та параметри маршрутизації. Це спрощує процес налаштування та мінімізує ризики конфліктів із системними конфігураціями.

3.2 Аналіз трафіку SS7 за допомогою Wireshark та Scapy

Для проведення аналізу трафіку протоколу SS7 використаємо два ключових інструменти: Wireshark для моніторингу мережевого трафіку та Scapy для моделювання сигнальних повідомлень. Ці інструменти дозволяють досліджувати структуру пакетів і перевіряти їхню взаємодію в ізольованому середовищі.

Відправлення тестового пакета SS7 за допомогою Scapy.

Для моделювання сигнального трафіку протоколу SS7 використовується Python-бібліотека Scapy. Пакет створено з використанням кастомного класу, який описує структуру M3UA-повідомлення (Message Transfer Part 3 User Adaptation Layer). Процес передбачає кілька основних етапів [22]. Спочатку створюється кастомний клас для пакета M3UA (див. рисунок 3.8), що дозволяє

моделювати специфічний сигнальний трафік. Далі виконується відправлення пакета через Scapy за допомогою коду (див. рисунок 3.9) та ми можемо побачити результат чи вдалось відправити пакет (див. рисунок 3.10). Після цього проводиться перевірка в Wireshark: запускається аналізатор трафіку, і налаштовується фільтр для відображення SCTP-трафіку. Ці дії забезпечують дослідження та валідацію створеного пакета в реальному середовищі.

```
from scapy.all import *

class M3UA(Packet):
    name = "M3UA"
    fields_desc = [
        ByteField("version", 1),
        ByteField("reserved", 0),
        ShortField("message_class", 1),
        ShortField("message_type", 1),
        IntField("message_length", 16),
        StrField("data", "Test SS7 packet")
    ]

bind_layers(SCTP, M3UA)
```

Рисунок 3.8 – Створення кастомного класу для пакета M3UA

```
pkt = IP(src="10.0.2.15", dst="10.0.2.1")/SCTP()
/M3UA(data="Test SS7 packet")
send(pkt)
```

Рисунок 3.9 – Код для відправлення тестового пакета через Scapy

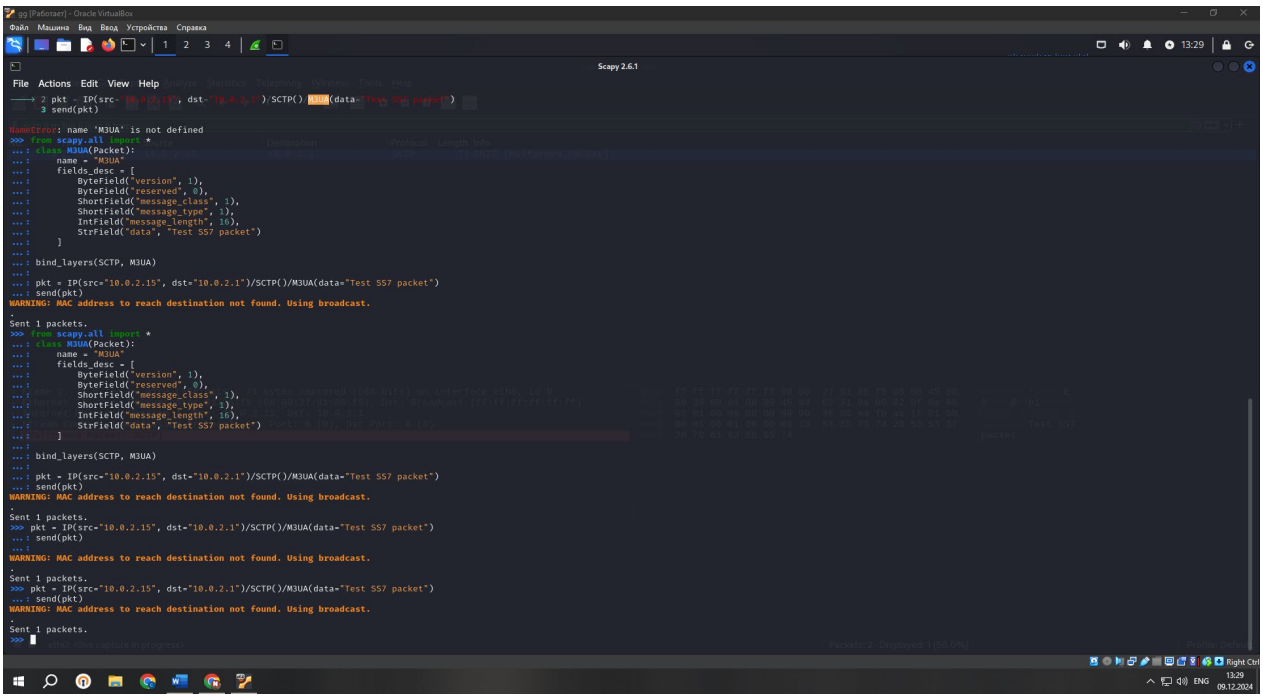

Рисунок 3.10 – Результат відправлення тестового пакета через scapy

Після відправлення пакета за допомогою Scapy він буде зафіксований у Wireshark (див. рисунок 3.11). На основі цього можна перевірити правильність формування пакета та його доставку. [23]

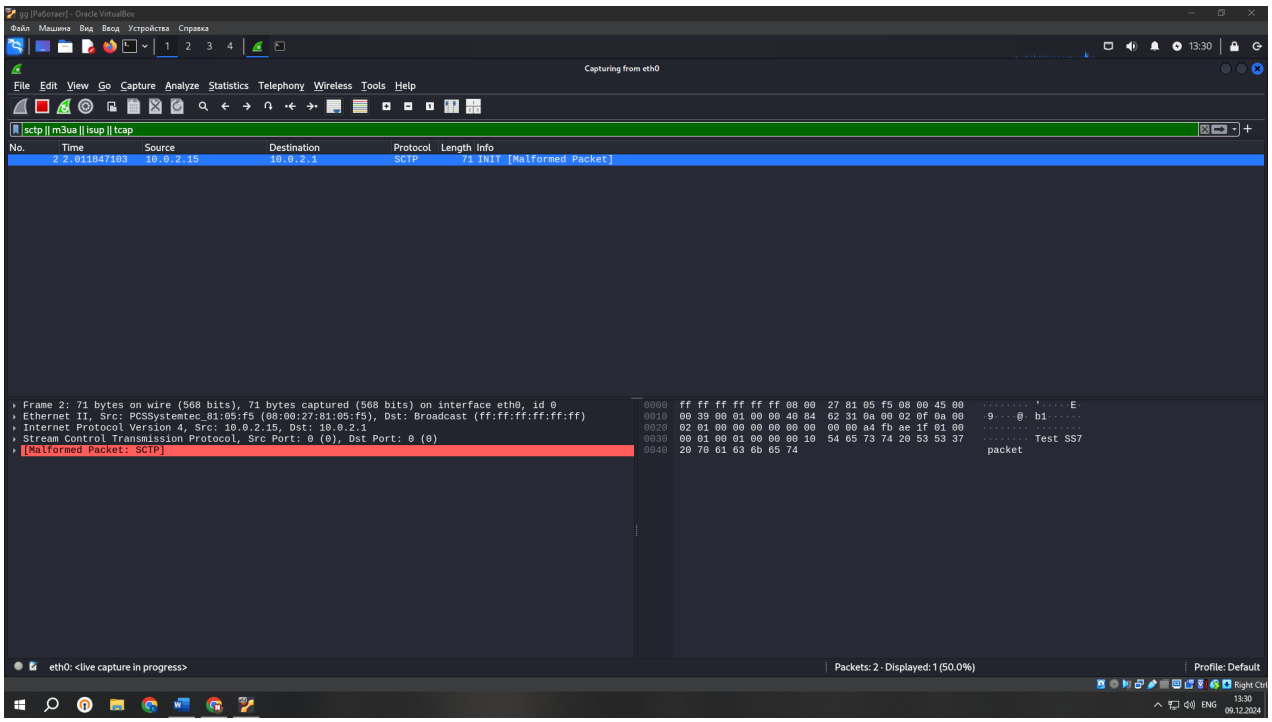

Рисунок 3.11 – Перехоплений тестовий пакет у wireshark

Це повідомлення свідчить про те, що пакет, який було створено та надіслано через Scapy, був захоплений Wireshark і відображений у вигляді протоколу SCTP (Stream Control Transmission Protocol).

Успішна передача: Пакет був надісланий, і Wireshark його захопив, що свідчить про правильну конфігурацію мережі та передачу даних.

Тестова природа пакета: Це не є реальним SS7-пакетом, а лише симуляція для навчальних цілей.

Під час тестування було створено кастомний сигнальний пакет SS7 та передано його через ізольовану віртуальну мережу. Його успішна фіксація у Wireshark підтвердила працездатність середовища та правильність виконаних налаштувань. Даний підхід забезпечує безпечну імітацію трафіку SS7 та дозволяє аналізувати структуру повідомлень протоколу.

3.3 Імітація складної сигналізації протоколу SS7 через Scapy

Складна сигналізація протоколу SS7 включає багаторівневу взаємодію між компонентами мережі, такими як HLR, VLR, MSC та інші вузли. Цей процес передбачає обмін повідомленнями, що забезпечують ключові функції телекомунікацій, включаючи автентифікацію, маршрутизацію дзвінків, переадресацію та доставку SMS. Використання Scapy дозволяє моделювати ці взаємодії, створюючи кастомні пакети для імітації реальних сценаріїв роботи мережі. Завдяки цьому можна відтворити такі складні ситуації, як перехоплення маршрутизаційних даних, модифікація параметрів передачі або тестування реакції системи на аномальний трафік. Це надає можливість аналізувати поведінку мережі, виявляти вразливості та розробляти ефективні контрзаходи.

Для детального вивчення роботи протоколу SS7 було використано Scapy для моделювання складних сигнальних повідомлень. Цей інструмент дозволяє створювати кастомні пакети, які можуть відображати специфічні сценарії роботи сигнальних систем, включаючи M3UA (Message Transfer Part 3 User Adaptation

Layer). Мета даного пункту — створити складний пакет сигналізації SS7 (див. рисунок 3.12), відправити його в тестове середовище (див. рисунок 3.13) та проаналізувати за допомогою Wireshark (див. рисунок 3.14).

```
from scapy.all import *

class M3UA(Packet):
    name = "M3UA"
    fields_desc = [
        ByteField("version", 1),
        ByteField("reserved", 0), [24]
        ShortField("message_class", 1),
        ShortField("message_type", 1),
        IntField("message_length", 16),
        StrField("data", "Complex SS7 message")
    ]

bind_layers(SCTP, M3UA)

pkt = IP(src="10.0.2.15",
dst="10.0.2.1")/SCTP()/M3UA(data="Complex SS7 message")
send(pkt)
```

Рисунок 3.12 – Код для створення пакета M3UA

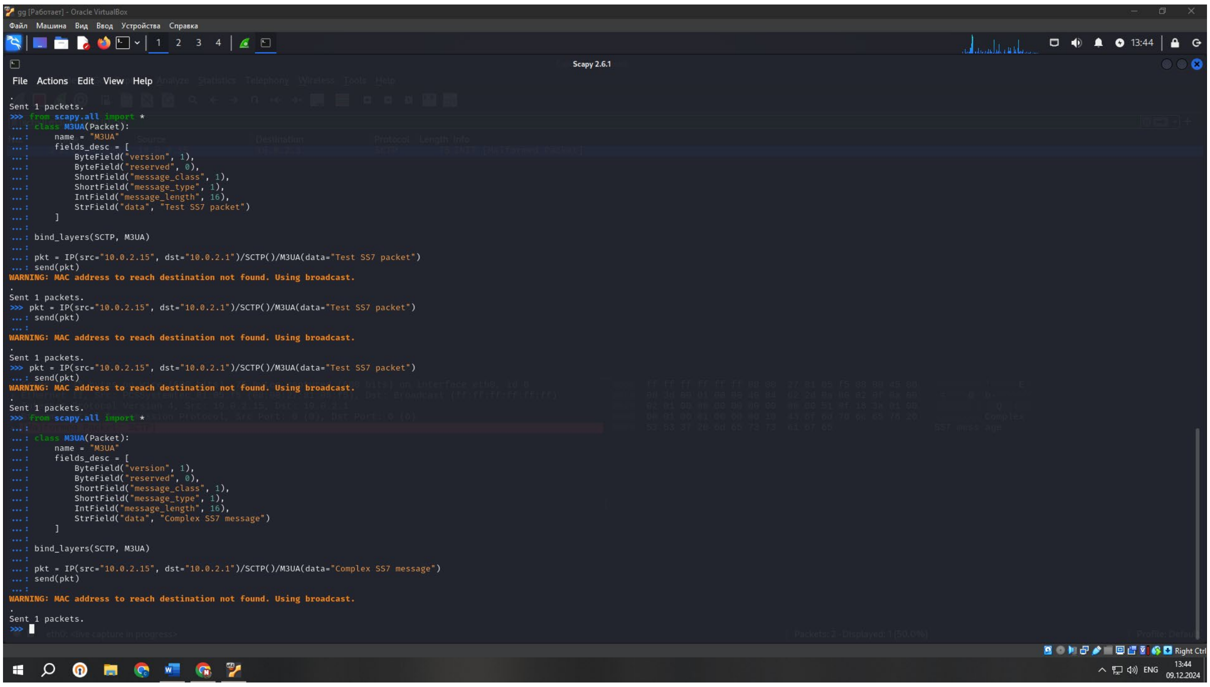

Рисунок 3.13 – Відправлення складного пакету сигналізації ss7 через scapy

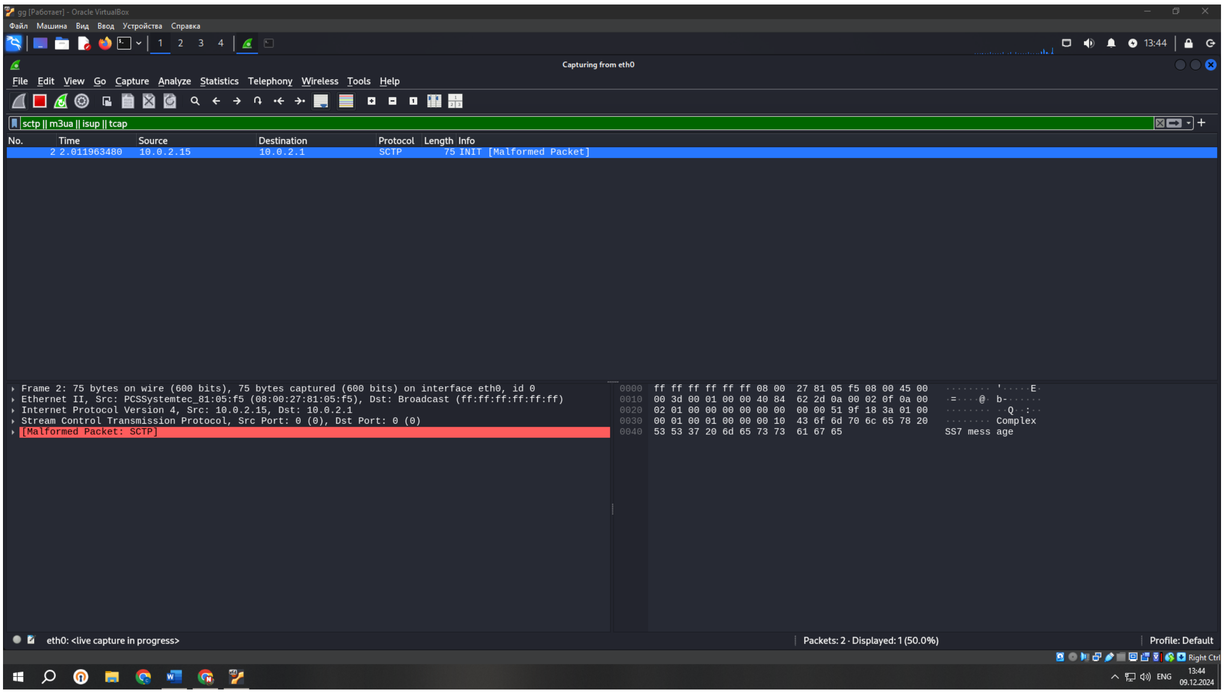

Рисунок 3.14 – Перехоплення пакету через wireshark

Захоплені пакети демонструють передачу даних із зазначеними параметрами (джерело, призначення, тип повідомлення). Якщо Wireshark відображає повідомлення як "Malformed Packet", це може бути не тільки через

помилки у структурі пакета, але й через те, що пакет був сформований для тестових цілей, а не відповідає повністю стандартам реального протоколу SS7.

3.4 Симуляція телекомунікаційної інфраструктури та аналіз сигнального трафіку з використанням Mininet

Для розширення дослідження, пов’язаного з протоколом SS7, було використано Mininet для симуляції телекомунікаційної інфраструктури, яка дозволяє виявляти потенційні проблеми маршрутизації трафіку. Було створено топологію з кількома вузлами, яка імітує роботу реальної мережі.

У Mininet була побудована складніша мережа (див. рисунок 3.15). з трьома вузлами (h1, h2, h3) та двома комутаторами (s1, s2) [25], підключеними до одного контролера. (див. рисунок 3.16).

h1 – ініціатор атаки, який виконує атаки (перехоплення SMS, локаційне відстеження тощо).

h2 – абонент-ціль, кого атакують (наприклад, абонент, чий SMS або місцезнаходження намагаються отримати).

h3 – вузол (або сервер), який обслуговує запити, або абонент, на якого здійснюється перенаправлення запиту чи SMS.

```
from mininet.topo import Topo
class CustomTopo(Topo):
    def build(self):
        # Створення вузлів
        h1 = self.addHost('h1')
        h2 = self.addHost('h2')
        h3 = self.addHost('h3')
        s1 = self.addSwitch('s1')
        # Створення з'єднань між хостами та комутатором
        self.addLink(h1, s1)
        self.addLink(h2, s1)
        self.addLink(h3, s1)
topos = {'custom': (lambda: CustomTopo())}
```

Рисунок 3.15 – Код для створення топології в mininet

Рисунок 3.16 – Побудова топології з кількома вузлами за допомогою mininet

На вузлі h1 було створено та надіслано тестовий трафік, який симулює сигнальні пакети SS7.

У терміналі відкрито h1 за допомогою команди: `mininet> xterm h1`, і створено тестовий пакет (див. рисунок 3.17). з використанням scapy(див. рисунок 3.18) [26].

```
from scapy.all import *
pkt = IP(src="10.0.0.1",
dst="10.0.0.3")/UDP(dport=2905)/Raw(load="SS7 Test Message")
send(pkt)
```

Рисунок 3.17 – Код для створення тестового пакету в scapy

Рисунок 3.18 – Відправлення тестовго пакету за допомогою scapy

На вузлі h3 було виконано моніторинг трафіку за допомогою Wireshark або іншого інструменту (див. рисунок 3.19). Трафік було перевірено на доступність, а також на можливість його модифікації.

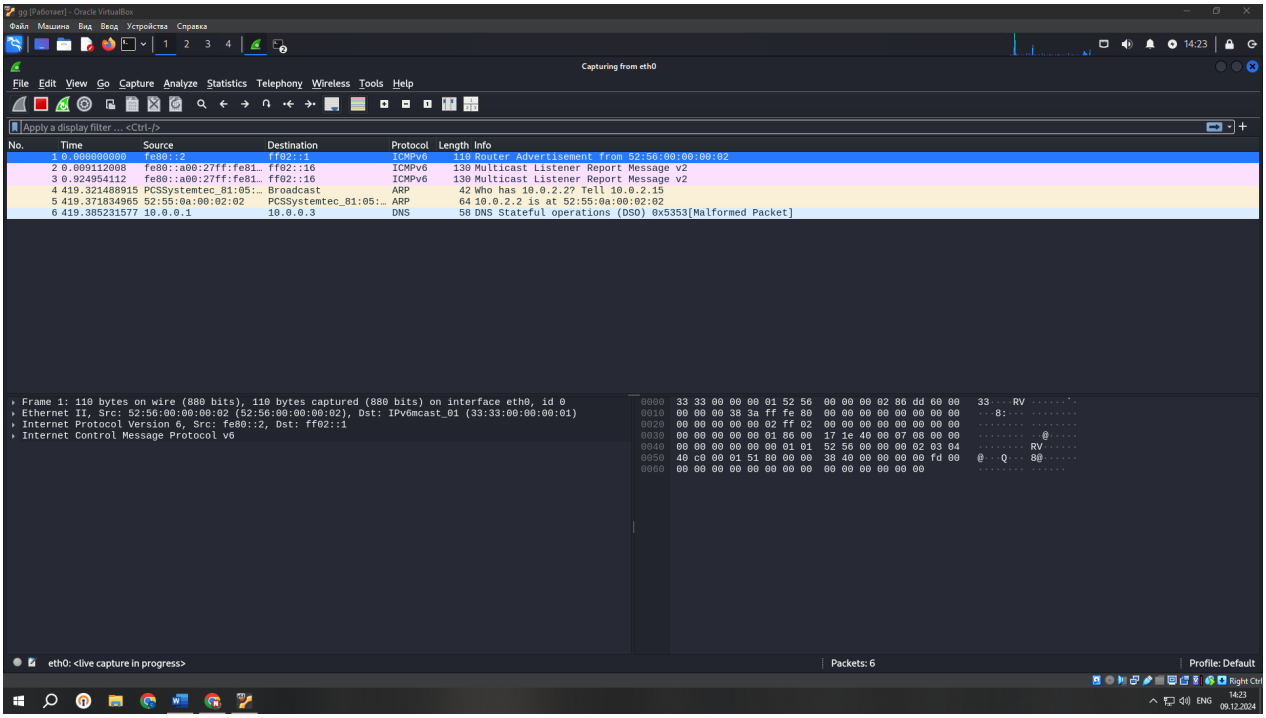

Рисунок 3.19 – Моніторинг трафіку за допомогою wireshark

Цей підхід дозволяє дослідити поведінку трафіку в розподіленій мережі, а також демонструє можливі сценарії атак, пов’язаних із SS7. Якщо такий підхід цікавий, можна залишити його. Якщо ні – обговоримо, що ще можна додати або залишити пункт без змін.

3.5 Моделювання атак на основі вразливостей SS7

У цьому розділі досліджено моделювання атак на основі протоколу SS7 з метою практичного розуміння його вразливостей. Проведено тестування двох основних типів атак: перехоплення SMS і локаційного відстеження. Всі експерименти були виконані виключно в ізольованому тестовому середовищі з використанням інструментів Kali Linux та Scapy.

Для симуляції цих атак використовувалися запити Mobile Application Part (MAP), що є частиною функціоналу SS7.

Атака на перехоплення SMS.

Для реалізації атаки на перехоплення SMS, включаючи одноразові паролі (OTP), виконується модифікований запит SendRoutingInfoForSM. Це дозволяє перенаправляти SMS на підроблений вузол, симулюючи атаку.

Відкриємо термінал для вузла ініціатора атаки (h1). У терміналі h1 запустимо Python та створимо запит, що імітує перехоплення SMS (див. рисунок 3.20). Для цього використовується код для моделювання запиту (див. рисунок 3.21), який дозволяє відтворити сценарій атаки та протестувати реакцію системи [27].

```
    from scapy.all import *

    class MAP_SendRoutingInfoForSM(Packet):
        name = "MAP_SendRoutingInfoForSM"
        fields_desc = [
            ByteField("version", 1),
            StrField("imsi", "123456789012345"),  # Ідентифікатор
абонента
            StrField("smsc", "0352 524 181"),     # Номер SMSC
            StrField("sms_content", "Diploma 2024 Novosad")  #
Ваше SMS
        ]
    bind_layers(UDP, MAP_SendRoutingInfoForSM, dport=2905) #
Створення пакета
    sms_request = IP(src="10.0.0.1", dst="10.0.0.3") /
UDP(dport=2905) / MAP_SendRouting
```

Рисунок 3.20 – Запит імітації перехоплення SMS

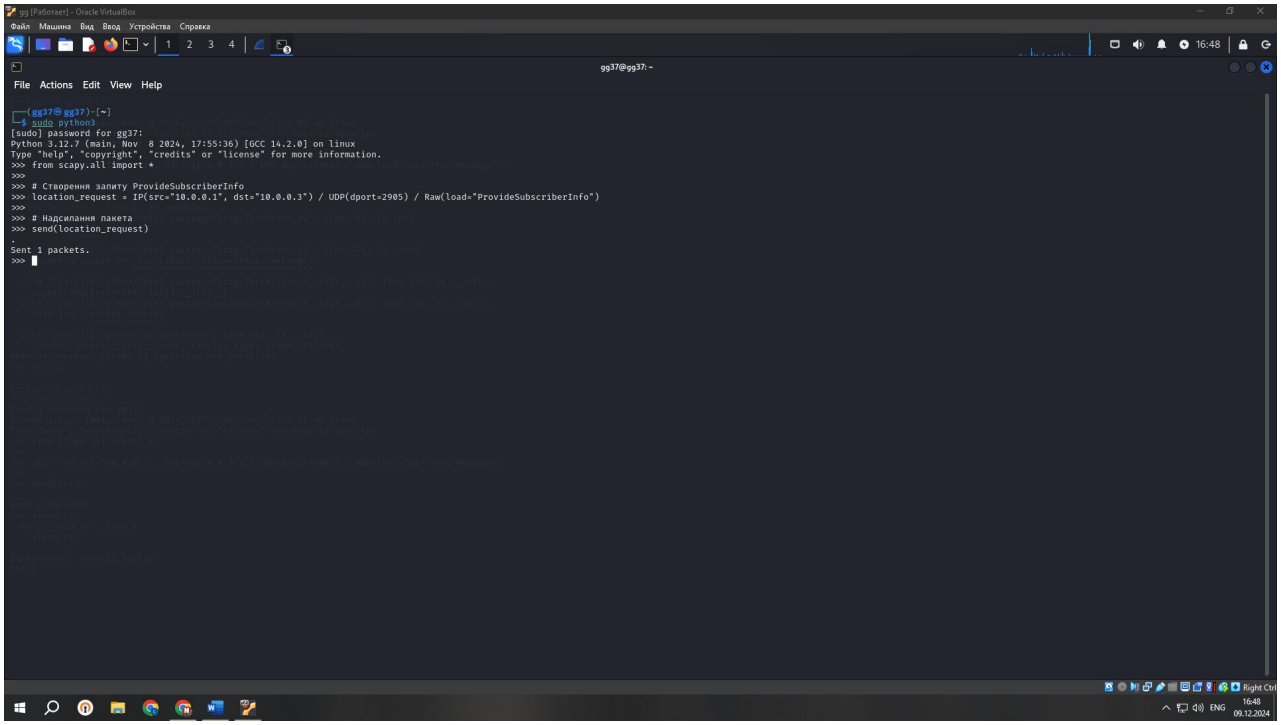

Рисунок 3.21 – Моніторинг трафіку за допомогою wireshark

В Wireshark ми бачимо що було успішно отримано пакети (див. рисунок 3.22; 3.23).

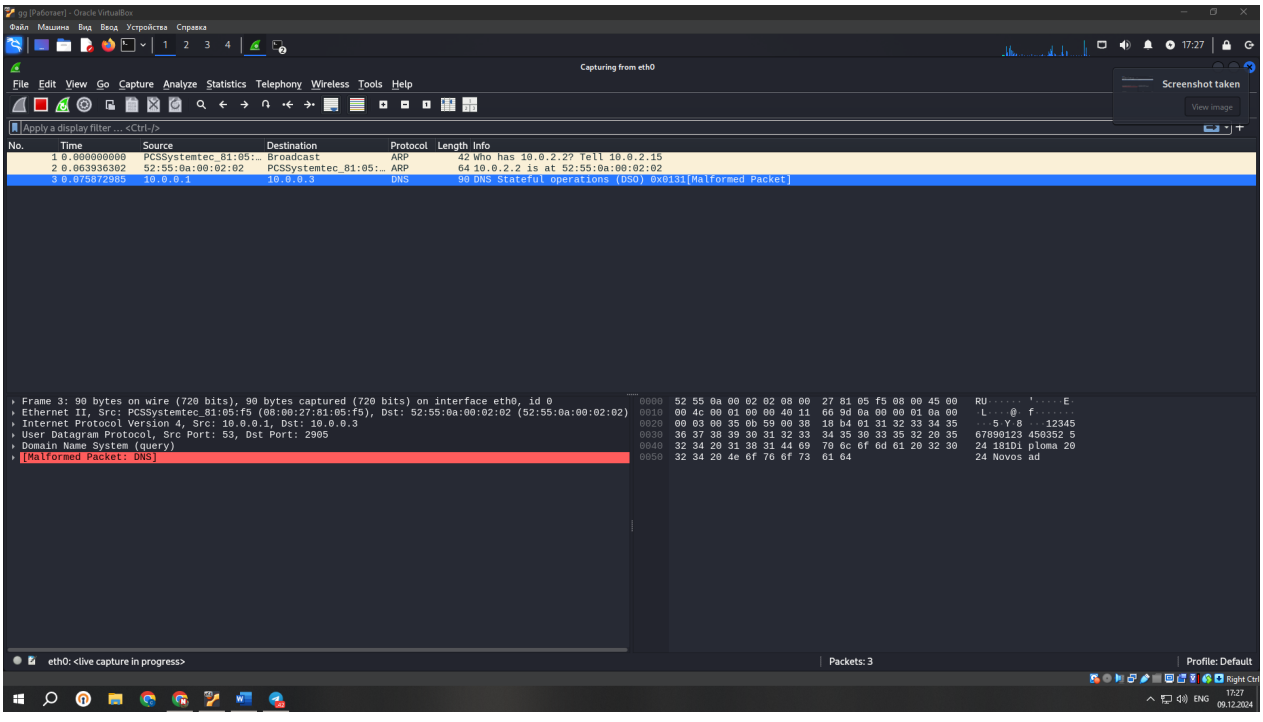

Рисунок 3.22 – Перехопленні пакети

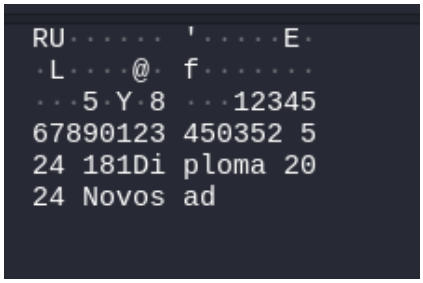

Рисунок 3.23 – Інформація яка містилась в перехопленому смс

Симуляція перехоплення інформації про абонента за допомогою ProvideSubscriberInfo.

Атака на основі запиту ProvideSubscriberInfo дозволяє зловмиснику отримати інформацію про номер та для отримання інших даних про абонента, включаючи місцезнаходження. Ця техніка демонструє вразливості протоколу SS7 у контексті конфіденційності даних користувачів. Нижче представлено кроки для моделювання атаки та аналізу результатів.

Створення та надсилання пакету зловмисником (h1).

Відкриємо термінал на вузлі h1 і запустимо інтерпретатор Python. Виконаємо код для створення запиту ProvideSubscriberInfo (див. рисунок 3.24) [28].

```
    from scapy.all import *

    class MAP_ProvideSubscriberInfo(Packet):
        name = "MAP_ProvideSubscriberInfo"
        fields_desc = [
            ByteField("version", 1),
            StrField("imsi", "123456789012345"),  # Ідентифікатор
абонента
            StrField("location", "Novovolynsk, Ukraine")  #
Локація абонента
        ]

    bind_layers(UDP, MAP_ProvideSubscriberInfo, dport=2905)

    # Створення пакета
    location_request = IP(src="10.0.0.1", dst="10.0.0.3") /
UDP(dport=2905) / MAP_ProvideSubscriberInfo()

    # Надсилання пакета
    send(location_request)
```

Рисунок 3.24 – Код для створення запиту ProvideSubscriberInfo.

Ми бачимо успішне перехоплення вмісту (див. рисунок 3.25; 3.26).

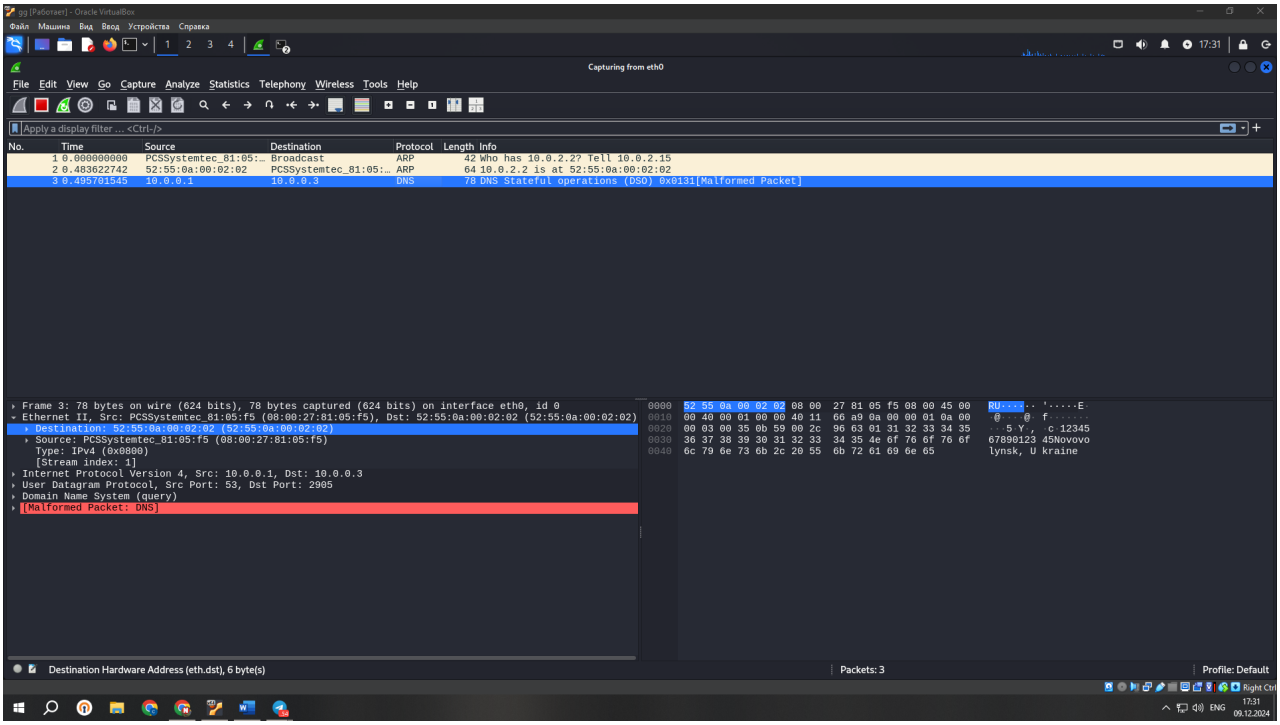

Рисунок 3.25 – Перехопленні пакети

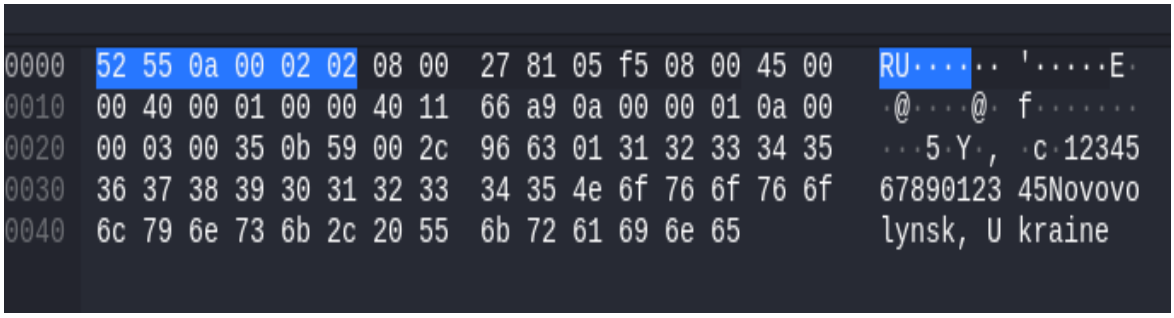

Рисунок 3.26 – Інформація про місцезнаходження

Усі пункти вище працюють в режимі моніторингу, тобто h1 та h3 бачать повідомлення

3.6 Моделювання захисту

Фільтрація трафіку за допомогою IPTables є одним із базових методів захисту мережевої інфраструктури, який широко використовується в реальних телекомунікаційних системах для блокування небажаного або небезпечного трафіку. Основна перевага IPTables полягає в його можливості фільтрувати

пакети за різними критеріями, такими як IP-адреса, порт, протокол або вміст. У контексті захисту протоколу SS7, IPTables дозволяє налаштувати правила для обмеження доступу до портів, які використовуються для сигнального трафіку, таких як UDP порт 2905

Встановимо правила фільтрації на вузлі, який виконує роль серверної частини (наприклад, h3) (див. рисунок 3.27). Це правило заблокує всі вхідні пакети, спрямовані на UDP-порт 2905, який зазвичай використовується для сигнальних повідомлень SS7.

```
from scapy.all import *
def handle_packet(packet):
    if Raw in packet and b"MySecureToken2024" in
packet[Raw].load:
        print("Valid request received:", packet.summary())
[29]
    else:
        print("Blocked packet: Invalid or missing token.")

sniff(filter="udp and port 2905", prn=handle_packet)
```

Рисунок 3.27 – Код для встановлення правил фільтрацій

Далі перейдемо на h3 та надішлемо тестовий пакет (див. рисунок 3.28).

```
from scapy.all import *
pkt = IP(src="10.0.0.1", dst="10.0.0.3") / UDP(dport=2905) /
Raw(load="InvalidToken")
send(pkt)
```

Рисунок 3.28 – Код для надсилання тестового пакета

При надсиланні тестового пакета з вузла h1, що не містив валідного токена, у терміналі на вузлі h3 з’явилося повідомлення:

Blocked packet: Invalid or missing token (див. рисунок 3.29)

Це підтверджує працездатність розробленого механізму фільтрації, який ефективно ідентифікує пакети з відсутнім або некоректним токеном, блокуючи їх обробку. Даний підхід може бути використаний для підвищення безпеки в тестових та реальних мережах, запобігаючи несанкціонованому доступу до сигнального трафіку.

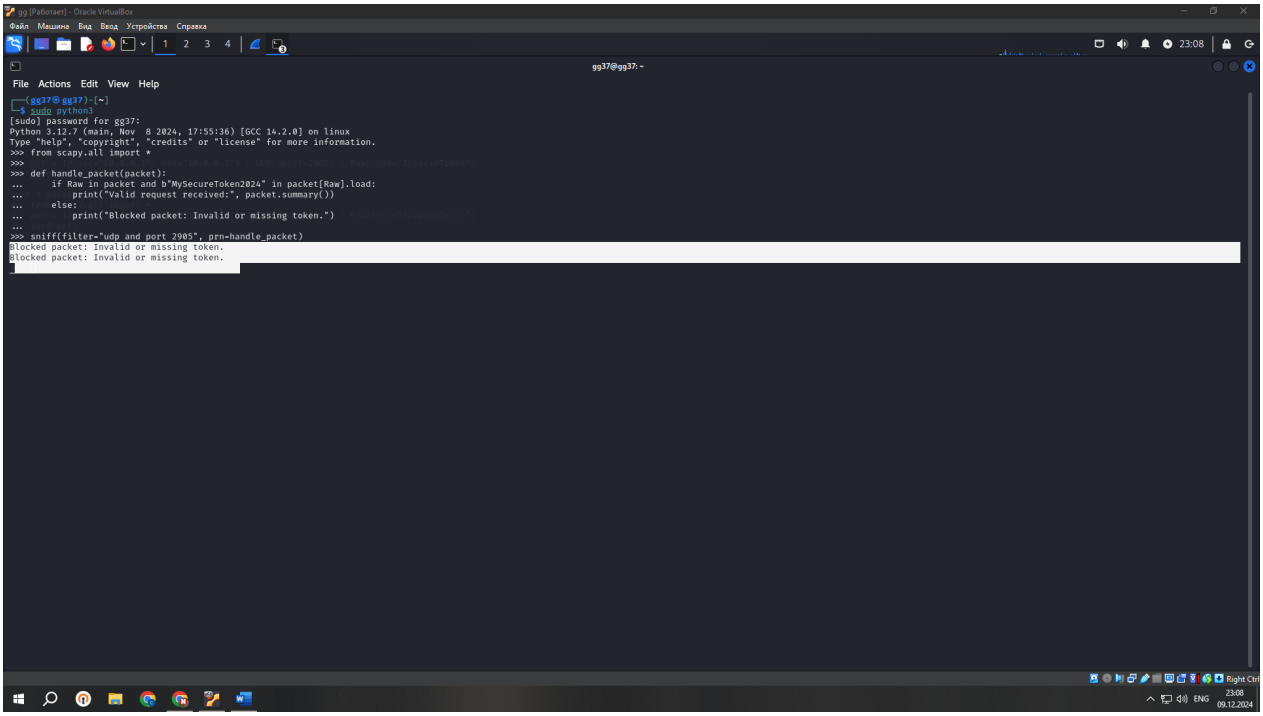

Рисунок 3.29 – Результат розробленого механізму фільтрації

Розроблений механізм фільтрації, що базується на перевірці валідності токенів у сигнальному трафіку, демонструє високу ефективність у запобіганні несанкціонованому доступу. Блокування пакетів із некоректними або відсутніми токенами підтверджує працездатність запропонованого підходу. Застосування такого механізму в реальних та тестових мережах дозволяє значно підвищити рівень безпеки, забезпечуючи захист критичних компонентів телекомунікаційної інфраструктури від потенційних загроз.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Під час виконання магістерської кваліфікаційної роботи було дотримано всіх норм і вимог до організації робочого місця для роботи з комп'ютерною технікою, забезпечуючи безпечні й комфортні умови праці. Особлива увага приділялася гігієнічним вимогам до параметрів мікроклімату, освітлення, шуму та ергономіки.

Вимоги до виробничих приміщень включають достатню площу (не менше ніж 6 м² на одне робоче місце) та об'єм приміщення (мінімум 20 м³). Приміщення мають бути забезпечені природним і штучним освітленням, яке відповідає санітарним нормам, а також обладнані системами опалення, вентиляції або кондиціонування для підтримки комфортних параметрів мікроклімату. Для зниження шуму передбачена звукоізоляція, а щоденне вологе прибирання забезпечує гігієнічність приміщення.

Параметри мікроклімату передбачають підтримання температури повітря в межах 20-24 °С із відносною вологістю 40-60% і швидкістю руху повітря не більше 0,1 м/с.

Освітлення забезпечує рівень освітленості на робочій поверхні в межах 300-500 лк за допомогою світлодіодних або люмінесцентних ламп. Для запобігання відблискам використовуються регульовані світильники.

Шум і вібрація обмежуються допустимими рівнями. Шум на робочих місцях не перевищує 50 дБ завдяки застосуванню звукопоглинаючих матеріалів, а вібрація обладнання мінімізується за допомогою амортизаторів.

Ергономіка робочих місць враховує зручність і комфорт працівників. Стіл забезпечує достатній простір для обладнання, а крісло має регулювання висоти й нахилу. Монітор розташовується на відстані 60-70 см від очей, причому його верхній край знаходиться на рівні або трохи нижче рівня очей.

Організація перерв і відпочинку передбачає регулярні перерви кожні 45-60 хвилин для зменшення зорового та фізичного навантаження. Приміщення обладнані зонами відпочинку з місцями для сидіння, доступом до питної води та можливістю виконання вправ.

Забезпечення першої медичної допомоги реалізується через оснащення приміщень аптечками з необхідним набором медикаментів і інструкцією для їх використання.

Дотримання цих вимог сприяє створенню безпечного й комфортного середовища, що знижує ризики для здоров’я та підвищує ефективність роботи.

4.2 Безпека в надзвичайних ситуаціях

Оцінка стійкості роботи об’єкту економіки до впливу вражаючих факторів ядерної зброї є критично важливим завданням, що передбачає детальний аналіз ризиків, вразливостей і можливостей відновлення. У даній роботі розглянуто основні аспекти стійкості об’єктів економіки, вплив вражаючих факторів ядерної зброї та рекомендації щодо підвищення рівня їх захищеності.

Об'єкти економіки, такі як промислові підприємства, енергетична інфраструктура та транспортні вузли, відіграють ключову роль у забезпеченні функціонування держави. Наприклад, електростанції є критично важливими для підтримки енергозабезпечення регіону, а їх вихід з ладу може спричинити масові перебої у життєзабезпеченні населення та промисловості. У разі ядерного нападу, ці об'єкти стають вразливими до низки руйнівних факторів. Це створює значні ризики для економічної стабільності країни, оскільки руйнування таких об'єктів може призвести до довготривалих наслідків. Важливо розглянути як короткострокові, так і довгострокові впливи, що можуть значно ускладнити відновлення роботи об'єктів економіки.

Основними вражаючими факторами ядерної зброї є вибухова хвиля, теплове випромінювання, радіоактивне забруднення та електромагнітний імпульс (EMI). Вибухова хвиля здатна зруйнувати будівлі, пошкодити транспортні шляхи та

інфраструктуру зв’язку. Вона також є основною причиною фізичного пошкодження об’єктів, які знаходяться у зоні ураження. Теплове випромінювання може викликати масштабні пожежі, що знищують матеріальні цінності, порушують логістичні ланцюги постачання та призводять до втрати життів. Радіоактивне забруднення створює тривалу загрозу для здоров’я людей, що перебувають поблизу об’єкта, а також для екосистем, які оточують цей об'єкт. ЕМІ може пошкодити електронні системи управління і зв'язку, що особливо небезпечно для сучасних технологічно залежних структур. Крім цього, ефекти взаємодії цих факторів посилюють руйнівний вплив і ускладнюють ліквідацію наслідків.

Для оцінки стійкості об’єкту до цих факторів використовується комплексний підхід, що включає аналіз технічних характеристик інфраструктури, моделювання можливих сценаріїв атак та розробку планів відновлення. Наприклад, об’єкти з міцними залізобетонними конструкціями мають вищу стійкість до вибухової хвилі. Дослідження показують, що правильно розроблені будівлі можуть витримати значний тиск вибуху, що мінімізує ризики для критичних елементів інфраструктури. Водночас, системи, що використовують захищене електроживлення і дублювання каналів зв’язку, здатні функціонувати навіть за умов впливу ЕМІ. Особлива увага приділяється технологіям резервування електроживлення, які дозволяють запобігти катастрофічним збоям у роботі обладнання. Крім цього, необхідно впроваджувати сучасні системи раннього попередження про можливі загрози.

Значну увагу слід приділяти питанням радіаційного захисту. Будівництво захищених сховищ, впровадження систем вентиляції з фільтрацією повітря та забезпечення засобів індивідуального захисту дозволяють знизити вплив радіоактивного забруднення на персонал і технологічне обладнання. Важливим етапом є розробка кризових планів, що включають евакуацію, організацію першочергових відновлювальних робіт та забезпечення резервних ресурсів. Такі заходи сприяють підвищенню готовності до надзвичайних ситуацій, а також мінімізації шкоди у разі реалізації найгірших сценаріїв. Слід також розглянути

використання інтегрованих систем моніторингу радіаційного фону, які забезпечують оперативне виявлення підвищеного рівня радіації.

Прикладом комплексного підходу до підвищення стійкості може слугувати моделювання захисту промислового підприємства. Уявімо, що підприємство з виробництва електроенергії розташоване в зоні можливого впливу ядерної зброї. Проведено аналіз стійкості його будівель, зокрема генераторних цехів, до вибухової хвилі, а також оцінено вразливість електронних систем управління до ЕМІ. На основі моделювання запропоновано додаткові заходи захисту: встановлення екрануючих пристроїв для обладнання, створення пожежних резервуарів для води та забезпечення персоналу засобами радіаційного захисту. Крім того, рекомендується впроваджувати системи швидкого реагування на пожежі, що дозволяють оперативно знижувати ризики подальших пошкоджень. Для зниження ризиків також варто використовувати сучасні матеріали з підвищеною стійкістю до впливу високих температур і радіації.

Крім того, слід звернути увагу на важливість навчання персоналу та населення. Регулярні тренування з евакуації, використання засобів індивідуального захисту та ліквідації наслідків надзвичайних ситуацій підвищують рівень готовності до кризових умов. Інформаційні кампанії сприяють формуванню культури безпеки, що є необхідним елементом стійкості. Досягнення високого рівня підготовки персоналу дозволяє суттєво знизити час реагування у разі кризових ситуацій, а також зменшити втрати серед співробітників і матеріальних активів.

Навчання персоналу та населення є ключовим аспектом стійкості. Регулярні тренування з евакуації, використання засобів захисту та ліквідації наслідків знижують час реагування на кризи й мінімізують втрати. Інформаційні кампанії та тренінги з кризового менеджменту допомагають підготуватися до надзвичайних ситуацій.

Оцінка стійкості роботи об’єктів економіки базується на технічних, організаційних і освітніх заходах. Захищеність мінімізує наслідки атак і дозволяє швидко відновити інфраструктуру.

ВИСНОВКИ

У ході дослідження було проведено детальний аналіз протоколу SS7, включаючи його архітектуру, функціональні особливості, основні вразливості та методи захисту.

Вразливості протоколу SS7. Створений у 1970-х роках, SS7 не відповідає сучасним вимогам кібербезпеки через відсутність шифрування, автентифікації вузлів та механізмів фільтрації запитів. Ці недоліки відкривають можливості для атак, таких як перехоплення SMS, локаційне відстеження, шахрайство у роумінгу та маніпуляції маршрутизацією викликів.

Аналіз сучасних загроз. Найпоширенішими сценаріями атак є використання команд SendRoutingInfo для перехоплення SMS, ProvideSubscriberInfo для локаційного відстеження та UpdateLocation для переадресації викликів. Реальні випадки атак демонструють значні фінансові та репутаційні втрати як для операторів зв’язку, так і для їхніх клієнтів.

Методи захисту. Базові заходи, такі як сегментування мережі та фільтрація запитів, забезпечують початковий рівень безпеки, проте не усувають всі ризики. Сучасні рішення, включаючи SS7 Firewall, моніторинг трафіку та поступовий перехід на протокол Diameter, значно підвищують захищеність телекомунікаційної інфраструктури.

Перехід на сучасні протоколи. Альтернативи, такі як Diameter та IPX-мережі, інтегрують вбудоване шифрування та автентифікацію вузлів. Попри високу вартість модернізації та необхідність сумісності з наявними системами, ці протоколи вважаються перспективними для забезпечення безпеки.

Практичні рекомендації. Для зниження ризиків оператори повинні регулярно проводити аудит конфігурацій вузлів SS7, використовувати SS7 Firewall для фільтрації нелегітимних запитів, організовувати тренінги для персоналу з виявлення кіберзагроз і планувати поступовий перехід на сучасні протоколи.

Результати дослідження допомагають глибше зрозуміти проблематику SS7, а запропоновані рекомендації можуть бути впроваджені операторами для покращення безпеки їхніх мереж. Подальші дослідження можуть бути спрямовані на моделювання атак у тестових середовищах та розробку нових технологій захисту, адаптованих до потреб мереж наступного покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адамович, І.І. (2020). Основи телекомунікаційних мереж. Київ: Техніка.

2. Звіт компанії Positive Technologies: Аналіз вразливостей протоколу SS7. URL: https://www.positive.com/ (дата доступу: 15.12.2024).

3. Lupenko, S., Orobchuk, O., Pasichnyk, V., Kunanets, N., & Xu, M. (2018). The axiomatic-deductive strategy of knowledge organization in onto-based e-learning systems for Chinese Image Medicine. In CEUR Workshop Proceedings (pp. 126-134).

4. Lupenko, S., Orobchuk, O., & Xu, M. (2020). The ontology as the core of integrated information environment of Chinese Image Medicine. In Advances in Computer Science for Engineering and Education II (pp. 471-481).

5. GSM Association. (2024). SS7 Security Best Practices. Retrieved from https://www.gsma.com/security/ (Accessed on 15 December 2024).

6. Національний центр кібербезпеки України. (2023). Рекомендації щодо захисту SS7. Київ.

7. ITU-T Recommendation. (2020). Specifications of Signaling System No. 7 (Q.700 Series). Geneva: International Telecommunication Union.

8. SANS Institute. (2024). SS7: Understanding and Mitigating Security Risks. Retrieved from https://www.sans.org (Accessed on 15 December 2024).

9. Cisco. (2024). Protecting the Critical Infrastructure of Telecommunication Networks. Retrieved from https://www.cisco.com (Accessed on 15 December 2024).

10. Palamar, A., Stadnyk, M., & Palamar, M. (2022). Adaptive pid regulation method of uninterruptible power supply battery charge current based on artificial neural network. Вісник Тернопільського національного технічного університету, 107(3), 5-13.

11. Erlang, B. (2019). Switching Systems and Telecommunication Infrastructure. Wiley.

12. ITU-T Recommendation. (2021). Signaling System No. 7 Protocol Performance Standards (Q.750 Series). Geneva: International Telecommunication Union.

13. Gollmann, D. (2020). Computer Security (4th ed.). Wiley.

14. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

15. Lupenko, O., & Pasichnyk, V. (2019). Ontologies in Information Systems. Lviv: Publishing House of Lviv Polytechnic.

16. Lupenko, S. A., Orobchuk, O. R., & Zahorodna, N. V. (2017, December). Formation of the onto-oriented electronic educational environment as a direction the formation of integrated medicine using the example of CIM. In Actual scientific research in the modern world: Collection of scientific papers of the XXIII International scientific conference (Vol. 12, No. 32, pp. 56-61).

17. NIST. (2024). Special Publication 800-187: Guide to LTE and SS7 Security. Retrieved from https://www.nist.gov (Accessed on 15 December 2024).

18. Розробка мережевих фаєрволів для захисту SS7. (2022). Вісник Київського національного університету, №8, 78-92.

19. Positive Technologies. (2023). Telecom Security: Threat Landscape 2023. Retrieved from https://positive-tech.com (Accessed on 15 December 2024).

20. Lupenko, S., Kunanets, N., & Orobchuk, O. (2021). Ontological Models in Secure Communication Systems. Kyiv: Scientific Research Publishing.

21. Telecom Security Alliance. (2024). Modern Approaches to SS7 Security. Retrieved from https://www.telecomsecurity.org (Accessed on 15 December 2024).

22. Kreibich, C. (2018). Protecting Mobile Networks: Standards and Protocols. Springer.

23. Wang, X. (2020). Advances in Mobile Telecommunication Security. Beijing: Tsinghua University Press.

24. Практичні аспекти впровадження SS7 Firewall. (2023). Журнал "Кібербезпека і технології", №5, 34-50.

25. Dworkin, M. (2022). Advanced Encryption in Telecommunication Networks. CRC Press.

26. Протокол SS7: Аналіз і виклики. (2022). Збірник наукових праць "Інформаційна безпека", №3, 90-105.

27. Lupenko, S., & Xu, M. (2021). Enhancing security through ontological frameworks. In Proceedings of the International Symposium on Secure Systems (pp. 150-167).

28. Hackett, J. (2020). Mobile Systems Security: Protocols and Threats. Elsevier.

29. Li, W., & Zhen, Y. (2021). Emerging Technologies in Telecom Security. Shenzhen: Guangdong Science Publishing.

30. CEPT ECC Report 293. (2024). Guidance on Secure Communication Standards. Retrieved from https://www.cept.org (Accessed on 15 December 2024).

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ

2024

УДК 001

М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професо**р.**

Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.

Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.

Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.

Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,

тел. (0352) 52-41-33, факс (0352) 25-49-83.

E-mail: conffis2024@gmail.com

Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп’ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп’ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 621.391.7:004.056.5
В.Д. Новосад, студент, Ph.D Олександра Оробчук
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ SS7, ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ

V. Novosad, student, Ph.D Oleksandra Orobchuk

ANALYSIS OF SS7 PROTOCOL VULNERABILITIES, THREATS, AND PROTECTION METHODS

Протокол SS7 (Signaling System No. 7) є фундаментальною технологією для телекомунікаційних мереж другого і третього поколінь (2G та 3G), та взаємодії між різними мережами, особливо між 4G і попередніми поколіннями. Він забезпечує передачу сигналів для маршрутизації викликів, передачі SMS та підтримки роумінгу.

Однак, архітектура SS7 побудована на принципі довіри між вузлами мережі, що створює значні ризики безпеки. Вразливості цього протоколу вже неодноразово використовувалися для таких атак, як перехоплення повідомлень, визначення місцезнаходження користувачів, шахрайство у роумінгу та перенаправлення викликів.

Актуальність даної теми обумовлена тим, що попри впровадження сучасніших протоколів, таких як LTE та 5G, SS7 залишається у використанні. Його широке застосування у мобільних мережах створює загрози для конфіденційності мільйонів користувачів, фінансової стабільності операторів та національної безпеки. У роботі проведено дослідження ключових вразливостей SS7, оцінка їх впливу на телекомунікаційні мережі та розробка рекомендацій щодо їх мінімізації. У ході дослідження систематизовано основні вразливості, зокрема відсутність шифрування даних між вузлами мережі, недостатня автентифікація запитів, а також відсутність ефективної фільтрації трафіку. Серед можливих заходів захисту розглянуто впровадження SS7 Firewall, який блокує небезпечні запити, систем моніторингу для аналізу мережевого трафіку та попередження атак у реальному часі, а також впровадження автентифікації вузлів. Крім того, важливим рішенням є перехід до сучасного протоколу Diameter, що забезпечує вищий рівень безпеки завдяки вбудованому шифруванню та автентифікації.

Ці результати можуть бути використані операторами мобільного зв'язку для забезпечення комплексного підходу до захисту їхніх мереж, включаючи впровадження сучасних технологій моніторингу, шифрування даних та багаторівневої автентифікації. Завдяки цьому оператори зможуть ефективніше виявляти та запобігати атакам, знижувати ризики витоку конфіденційної інформації та мінімізувати фінансові втрати, спричинені шахрайством у роумінгу чи іншими видами атак.

Література

1. 3GPP TS 29.002. Mobile Application Part (MAP) Specification. Version 15.6.0. Sophia Antipolis: 3GPP, 2020. 250 с.
2. Engel T. SS7: Locate. Track. Manipulate. Presentation at 31st Chaos Communication Congress (31C3). 2014. 58 с.
3. GSM Association. SS7 Interconnect Security Monitoring and Firewall Guidelines. London: GSM Association, 2017. 45 с.
4. Positive Technologies. SS7 Security: Threats and Vulnerabilities. [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ (дата звернення: 04.12.2024). 25 с.
5. RFC 6733. Diameter Base Protocol. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc6733 (дата звернення: 04.12.2024). 160 с.