РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 621.395
DOI https://doi.org/10.32838/2663-5941/2021.6/03

Кокіза С.В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

Щегельська Н.М.
Приватне акціонерне товариство «Український інститут із проектування
і розвитку інформаційно-комунікаційної інфраструктури «Діпрозв'язок»

БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ СПІЛЬНОКАНАЛЬНОЇ СИГНАЛІЗАЦІЇ № 7 В УКРАЇНІ

У статті розглянуто проблему вразливостей телекомунікаційних мереж спільноканальної сигналізації № 7 (СКС-7), які використовують зловмисники для атак на телекомунікаційні мережі та абонентів мереж мобільного зв'язку.

Наголошено на проблемі відсутності в нормативних документах України конкретних технічних вимог до телекомунікаційних мереж, що використовують СКС-7, із точки зору захисту від несанкціонованого втручання в роботу, що негативно впливає на безпеку мереж СКС-7.

Наведено аналіз сучасного стану та проблем захисту мереж мобільного зв'язку в Україні, з якого видно, що мережі СКС-7 України мають високий ризик витоку інформації щодо ідентифікаторів абонента, яка може бути використана для здійснення атак різних видів.

Проаналізовано рекомендації міжнародних нормативних документів щодо безпеки телекомунікаційних мереж СКС-7. Розглянуто методи протидії загрозам мережам СКС-7, а саме: моніторинг та фільтрація повідомлень відповідно до визначених категорій; застосування «SMS Home Routing». Також наведено вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку в телекомунікаційних мережах.

На основі проведеного аналізу сучасного стану проблем захисту мереж мобільного зв'язку в Україні та міжнародних нормативних документів щодо безпеки телекомунікаційних мереж СКС-7 надано рекомендації щодо змісту технічних вимог до захисту телекомунікаційних мереж СКС-7 України від несанкціонованого втручання в роботу, які будуть сприяти впровадженню ефективних засобів та методів захисту телекомунікаційних мереж СКС-7 України від несанкціонованого втручання в роботу.

Ключові слова: *безпека телекомунікаційної мережі, несанкціоноване втручання та/або використання телекомунікаційних мереж, атаки на телекомунікаційні мережі, підозріла/шкідлива активність, витік конфіденційних ідентифікаторів абонента, захист телекомунікаційної мережі, безпека взаємоз'єднань телекомунікаційних мереж, спільноканальна сигналізація № 7, СКС-7, моніторинг сигнального трафіку, фільтрація сигнального трафіку, SMS Home Routing.*

Постановка проблеми. Система спільноканальної сигналізації № 7 (СКС-7) наразі є основним типом міжстанційної сигналізації, що об'єднує мережі різних технологій зв'язку. СКС-7 була розроблена Міжнародним союзом електрозв'язку (далі – МСЕ) у кінці 1970-х років як набір протоколів сигналізації, що використовуються для обміну сигнальною інформацією між різними елементами однієї мережі та/або між різними телекомунікаційними мережами. СКС-7 за своєю концепцією розроблялась як закрита система міжстанційної сигналізації, доступ до якої на той час мала порівняно невелика кількість постачальників послуг зв'язку з чітко визначеними межами телекомунікаційних мереж. Для забезпечення безпеки мереж на основі СКС-7 було достатньо фізичного захисту вузлів та ліній зв'язку, оскільки доступ за допомогою якогось окремого несанкціонованого вузла був неможливий.

Із розвитком телекомунікаційних технологій, упровадженням рухомого (мобільного) зв'язку стандартів 2G/3G, а також появою великої

кількості операторів телекомунікацій різних рівнів мережа СКС-7 перестала бути ізольованою. Оскільки під час розробки СКС-7 не були закладені механізми захисту, стало можливим несанкціоноване втручання у сигнальний обмін для здійснення неправомірних дій. Вразливості телекомунікаційних мереж СКС-7 використовують не тільки шахраї, а й розвідувальні органи іноземних держав для здійснення діяльності з негласного спостереження, кібершпигунства, диверсій тощо. Оскільки оператори телекомунікацій повинні забезпечувати підтримку стандартів 2G/3G та взаємодію між мережами різних поколінь та технологій, проблеми безпеки СКС-7 будуть залишатись актуальними ще довгий час.

Законодавство України, зокрема частина третя статті 9 Закону України «Про телекомунікації» [1], містить вимоги до операторів, провайдерів телекомунікацій «вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами». Вимоги щодо забезпечення безпеки електронних комунікаційних мереж містить також Закон України «Про електронні комунікації» [2], який набирає чинності з 01 січня 2022 року. Зокрема, частина друга статті 31 зобов'язує постачальників електронних комунікаційних мереж та/або послуг «вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг із метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж».

Але нормативних документів щодо конкретних технічних вимог до телекомунікаційних мереж та обладнання з точки зору захисту від несанкціонованого втручання в їх роботу наразі в Україні недостатньо.

Взаємодія мереж операторів рухомого (мобільного) зв'язку України між собою та з телекомунікаційною мережею загального користування здійснюється відповідно до чинних нормативних документів в сфері телекомунікацій. Ці документи також не передбачають конкретних технічних вимог до захисту від несанкціонованого втручання в роботу та/або використання телекомунікаційних мереж.

Виходячи з вищезазначеного, існує необхідність впровадження в Україні нормативних документів, які мають регламентувати технічні вимоги щодо захисту телекомунікаційних мереж СКС-7, зокрема мереж рухомого (мобільного) зв'язку, від несанкціонованого втручання в їх роботу. Застосування таких нормативних документів сприятиме підвищенню безпеки телекомунікаційних мереж та захисту інформації про споживачів послуг рухомого (мобільного) зв'язку.

Аналіз останніх досліджень і публікацій. Вимоги до системи СКС-7 викладені в Рекомендаціях Сектора стандартизації електрозв'язку МСЕ (МСЕ-Т) серії Q.7XX. МСЕ також займається дослідженням питань безпеки СКС-7.

29 червня 2016 року в Женеві, Швейцарія, був проведений Семінар МСЕ на тему «Безпека SS7» [3]. Як документи щодо технічної реалізації захисту телекомунікаційних мереж Семінаром МСЕ «Безпека SS7» рекомендовано використовувати документи GSM Association (GSMA).

Різні аспекти захисту мереж СКС-7 розглядаються, зокрема, у документах GSMA [4-8].

У документі GSMA FS.07 [4] наданий огляд СКС-7 та SIGTRAN, а також обробки повідомлень СКС-7 на межі мережі. Документ містить аналіз атак, які здійснюються у мережі СКС-7, безпеки СКС-7 та SIGTRAN, та надає набір контрзаходів, які можна розгорнути. Зокрема, надається класифікація повідомлень СКС-7 за категоріями, правила фільтрації та інші підходи до підвищення безпеки.

У документі GSMA FS.11 [5] описано, як контролювати трафік СКС-7, включно з методами запобігання атакам та виявлення підозрілої/шкідливої активності. Додаток А містить оцінку ризику для всіх типів пакетів GSM-MAP (GSM-Global System for Mobile Communications; MAP-Mobile Application Part) та CAMEL (Customised Applications for Mobile networks Enhanced Logic). У Додатку до цього документа наведено описи рекомендованих правил мережевого екрана СКС-7 для захисту від вразливостей MAP та CAMEL та рекомендації щодо впровадження мережевого екрана в мережі СКС-7. Рекомендовані правила мережевого екрану СКС-7 визначають набір, яким оператори мереж мобільного зв'язку можуть забезпечити захист своєї мережі.

Документ GSMA IR.70 [6] розглядає проблеми, пов'язані з послугою передання коротких повідомлень (SMS) (спам, шахрайство, незаконне використання адрес SMS-центрів). Документ визначає кожен випадок шахрайства із SMS та описує технічні аспекти для кожного випадку.

Документ GSMA IR.71 [7] визначає методи, за допомогою яких оператори мереж мобільного

зв'язку можуть ідентифікувати атаки на свої мережі з використанням SMS та надає рекомендації як окремим операторам, так й індустрії мобільного зв'язку, яким може знадобитися короткострокове вирішення цих питань.

Документ GSMA IR.82 [8] окреслює загальні заходи безпеки СКС-7 (зокрема, MAP та CAP-CAMEL Application Part), включно із заходами, характерними для безпеки SMS, та можливими точками примусового виконання для кожного заходу.

Згідно з вищенаведеними документами одним із методів, який рекомендовано використовувати для запобігання несанкціонованому втручанню з використанням SMS, є «SMS Home Routing» (домашнє маршрутування SMS). Детальний опис «SMS Home Routing» та його впровадження у мережах мобільного зв'язку наведений у документі 3GPP TR 23.840 [9].

Документ 3GPP TR 23.840 [9] пропонує дослідження архітектури базової мережі для доставки коротких повідомлень між PLMN (Public Land Mobile Network) та дослідження щодо вдосконалення цієї архітектури.

Дослідженнями безпеки СКС-7 займається також компанія P1 Security, яка (за даними GSMA [10]) є незалежною від постачальника нейтральною компанією та має визнане лідерство в галузі телекомунікацій та мобільної безпеки, засноване на інноваційних продуктах та передових знаннях. У [11] компанією P1 Security були запропоновані показники безпеки телекомунікаційних мереж СКС-7 та за результатами досліджень було складено рейтинг 164 країн світу за декількома категоріями.

Постановка завдання. Метою дослідження є надання рекомендацій щодо змісту нормативного документа, який регламентуватиме основні технічні вимоги до захисту телекомунікаційних мереж СКС-7 в Україні від несанкціонованого втручання в їх роботу.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз досліджень безпеки системи СКС-7 в Україні;

– провести аналіз рекомендацій міжнародних нормативних документів щодо безпеки телекомунікаційних мереж СКС-7;

– на основі аналізу міжнародних нормативних документів надати рекомендації щодо змісту основних технічних вимог до захисту телекомунікаційних мереж СКС-7 в Україні від несанкціонованого втручання в їх роботу.

Виклад основного матеріалу дослідження.

1. Дослідження безпеки телекомунікаційних мереж СКС-7 в Україні.

Як уже було зазначено раніше, телекомунікаційні мережі СКС-7 мають вразливості, які використовують зловмисники для атак на мережі та абонентів телекомунікаційних мереж.

Основні напрями атак такі:

– отримання конфіденційних ідентифікаторів абонента;

– визначення / відстеження місцезнаходження абонента;

– маніпулювання даними профілю абонента;

– порушення доступності абонента / мережі;

– перехоплення / перенаправлення викликів;

– перехоплення / перенаправлення SMS-повідомлень;

– DoS-атаки;

– фальсифікація номера абонента, який викликає;

– SMS-спам.

Важливим етапом підготовки до багатьох атак є отримання конфіденційних ідентифікаторів абонента, як-от міжнародний ідентифікатор мобільного абонента (IMSI). У разі успішної атаки зловмисник отримує IMSI абонента, а також дані про MSC/VLR та HLR, у якому зареєстрований абонент. Ці дані можуть бути використанні в подальшому для здійснення багатьох інших атак, як-от визначення та/або відстеження місцезнаходження, перехоплення та/або перенаправлення викликів і SMS-повідомлень та порушення доступності абонентів/мереж.

Такі атаки, як визначення та/або відстеження місцезнаходження, перехоплення та/або перенаправлення викликів і SMS-повідомлень та порушення доступності абонентів/мереж, зокрема співробітників правоохоронних та інших державних органів, а також DoS-атаки на абонентів, на державні органи та об'єкти критичної інфраструктури, несуть загрозу національній безпеці України.

Аналіз досліджень безпеки системи СКС-7 в Україні був проведений на основі дослідження компанії P1 Security [11].

За результатами досліджень безпеки системи СКС-7 P1 Security складено рейтинг 164 країн світу за трьома категоріями:

– витоки конфіденційності;

– вплив мережі;

– глобальний ризик.

Витоки конфіденційності: наскільки з мереж операторів певної країни витікають такі конфіденційні дані їхніх абонентів:

– місцезнаходження абонента;

– приватна інформація про абонента (ідентифікатори, криптографічні ключі, статус післяплати/передплати);

– конфіденційність абонентських комунікацій (розшифровка SMS/дзвінків за допомогою відомих атак).

У межах дослідження впливу мережі фокус на магістральних мережах операторів у країні:

– поверхня атаки мереж операторів (топологія мережі, ідентифікація вузлів мережі (тобто мережеві елементи);

– неправильна конфігурація мережі, що дозволяє зловмисникам змінювати дані;

– обхід механізмів мережевої безпеки.

Глобальний ризик поєднує показники витоків конфіденційності та вплив мережі, надаючи більше значення витокам конфіденційності.

Згідно з даними P1 Security за результатами тестування двох операторів телекомунікацій Україна посідає 29 місце за безпекою СКС-7 в рейтингу зі 164 країн світу.

Рівень глобального ризику – 1059,8 (29 місце).

Рівень ризику конфіденційності – 494,6 (25 місце):

– повідомлень СКС-7, що розкривають місто місцезнаходження абонента – 3 (Україна дозволяє витік інформації про місто місцезнаходження абонента через три повідомлення MAP СКС-7);

– повідомлень СКС-7, що розкривають вулицю місцезнаходження абонента – 1 (Україна дозволяє витік інформації про точне місцезнаходження абонента до рівня вулиці (200 м) через одне повідомлення MAP СКС-7);

– повідомлень СКС-7, що розкривають приватну інформацію – 3 (Україна дозволяє витік інформації про IMSI абонента через три повідомлення MAP СКС-7);

– витік абонентських ключів – 1 (в Україні є 1 оператор, який дозволяє витік абонентських ключів. Витік абонентських ключів дозволяє зловмиснику розшифровувати сеанси зв'язку та SMS абонента, видаючи себе за мережу за допомогою підробленої базової станції);

– витік статусу передоплати/післяплати – 0 (в Україні немає операторів, які дозволяють витік статусу передоплати/післяплати. Витік статусу передплати/післяплати дозволяє зловмиснику збирати інформацію про статус абонента з баз даних операторів для підготовки шахрайства).

Рівень впливу мережі – 1766,7 (155 місце):

– поверхня атаки виявлення SCCP – 188 (Україна має 188 елементів магістральної мережі, ідентифікованих за допомогою SCCP СКС-7. Чим більше елементів базової магістральної (базової) мережі доступно (можливий доступ до них безпосередньо з міжнародної мережі СКС-7), тим більше точок входу має зловмисник до магістральної (базової) мережі СКС-7);

– ідентифікація елементів мережі – 188 (Україна має 188 елементів магістральної (базової) мережі, які успішно пройшли ідентифікацію через SCCP СКС-7. Точна ідентифікація елементів магістральної (базової) мережі дозволяє зловмисникам краще зрозуміти внутрішню структуру мереж операторів, що спрощує подальші атаки);

– потенційна зміна статусу передоплати/післяплати (шахрайство) – 0 (в Україні немає операторів, схильних до шахрайства через зміну статусу передплати/ післяплати);

– «SMS Home Routing» (домашнє маршрутування SMS) – 2 (в Україні є 2 оператори, які впровадили «SMS Home Routing». «SMS Home Routing» – це здатність мережі приховувати MSC (місто місцезнаходження) та IMSI абонента в деяких повідомленнях MAP СКС-7).

За результатами дослідження можна зробити висновок, що мережі СКС-7 України мають високий ризик витоку інформації IMSI абонента, яка, як було зазначено вище, може бути використана в подальшому для здійснення багатьох інших атак.

За рівнем впливу мережі Україна перебуває в останній десятці рейтингу, що відображає погану захищеність телекомунікаційних мереж в Україні.

2. Рекомендації щодо безпеки телекомунікаційних мереж СКС-7.

За результатами аналізу документів GSMA визначено вимоги, що є необхідними для підвищення безпеки телекомунікаційних мереж СКС-7 в Україні. Зокрема, для запобігання несанкціонованому втручанню у сигнальний обмін обов'язково має застосовуватись моніторинг та фільтрація сигнального трафіку.

Моніторинг та фільтрація сигнального трафіку повинні виконуватись у вузлах, які отримують міжмережевий сигнальний трафік, зокрема:

– системах виявлення та запобігання вторгненням;

– транзитних та шлюзових вузлах обробки сигналізації (STP та шлюзові STP);

– вузлах, які надсилають/отримують міжмережевий сигнальний трафік (MSC, SGSN, HLR, VLR тощо);

– SMS-маршрутизаторі;

– мережевих системах моніторингу;

– інших елементах мережі, які отримують міжмережевий сигнальний трафік.

2.1. Вимоги щодо моніторингу та фільтрації сигнального трафіку.

Документи GSMA FS.11 [8], IR.82 [9] рекомендують для моніторингу та фільтрації повідомлень СКС-7, а саме повідомлень SCCP, MAP та CAP, застосовувати механізми так званих чорних або білих списків повідомлень СКС-7. Оскільки перелік повідомлень СКС-7 наразі є доволі сталим і його оновлення не передбачається, то для фільтрації повідомлень СКС-7 рекомендується використовувати саме механізм чорних списків, тобто мережевий екран має блокувати всі повідомлення, які входять до відповідного списку.

Фільтрація повідомлень СКС-7 має виконуватись відповідно до категорій згідно з документом GSMA FS.11 [8].

Категорія 1 містить усі повідомлення СКС-7, які повинні отримуватись тільки в межах однієї мережі. Повідомлення СКС-7 категорії 1 призначені для передавання між вузлами всередині мережі оператора та не повинні надходити у пункти взаємоз'єднання з мережами інших операторів. Повідомлення СКС-7 категорії 1, що надходять у пункти взаємоз'єднання з іншими мережами та призначені вузлам всередині мережі, повинні блокуватись, якщо між операторами телекомунікацій немає угод про обмін такими повідомленнями. Ідентифікація повідомлень СКС-7 категорії 1 проводиться лише на основі типу повідомлення.

Категорія 2 складається з повідомлень СКС-7, що стосуються зовнішнього абонента, який перебуває в роумінгу, та надходять із його домашньої мережі. Такі повідомлення, що надходять у пункти взаємоз'єднання з іншими мережами, не повинні призначатись власним абонентам мережі. Категорія 2 передбачає перевірку повідомлень СКС-7, зокрема повідомлень MAP, на основі аналізу походження (джерела) повідомлення.

Повинні блокуватись повідомлення MAP категорії 2, які надійшли від мереж інших операторів, якщо вони призначені власним абонентам цих мереж. Також повинні блокуватись повідомлення MAP категорії 2, якщо вони призначені для абонента, який перебуває в роумінгу, але мережа, визначена на основі номера цього абонента мобільного зв'язку (MSISDN) або IMSI (тобто MCC + MNC) на рівні MAP, не відповідає мережі, вказаній у глобальному заголовку на рівні SCCP.

Повідомлення MAP категорії 2 можна додатково розділити на 2 категорії:

– категорія 2.1: MAP-повідомлення, які потребують відповіді;

– категорія 2.2: MAP-повідомлення, які не потребують відповіді.

Повідомлення категорії 2.1 легше відстежувати, порівнюючи адреси SCCP та MAP, оскільки відповідь повинна повертатися до вказаної адреси. Несанкціоновані повідомлення категорії 2.2 важче виявити, оскільки адреса походження може бути підробленою.

Повідомлення СКС-7 *категорії 3* стосуються власних абонентів мережі, які перебувають у роумінгу, та надсилаються з поточної або передбачуваної мережі, в якій перебуває абонент. Зазвичай перевірки цих повідомлень базуються на кореляції між повідомленнями та можуть містити перевірку повідомлень із точки зору місцезнаходження абонента, швидкості та часу зміни місцезнаходження.

Повідомлення СКС-7 категорії 3 можна додатково розділити на 3 категорії:

– категорія 3.1 – повідомлення, в яких місцезнаходження абонента може бути підтверджено попередньою / поточною інформацією про VLR за допомогою перевірки SGSN/VLR. Повинні блокуватися всі повідомлення, отримані в пунктах взаємоз'єднання з іншими мережами, що стосуються власного абонента мережі, який перебуває в роумінгу, якщо адреса VLR (VLR ID), яка зберігається у HLR, не відповідає мережі, вказаній на рівні SCCP;

– категорія 3.2 – повідомлення, в яких місцезнаходження абонента не може бути підтверджене за допомогою попередньої / поточної інформації VLR. Для визначення достовірності таких повідомлень використовують перевірку місцезнаходження абонента, часу та швидкості зміни місцезнаходження;

– категорія 3.3 – повідомлення, які стосуються SMS і до яких потрібно застосувати специфічні засоби безпеки SMS, а саме: перевірка кореляції адрес на рівнях SCCP, MAP, MTP (або іншого протоколу транспортного рівня), а також їх кореляції з топологією мережі; застосування «SMS Home Routing» та заходів щодо запобігання його обходу; за умови технічної можливості застосування механізмів «SMS TCAP Handshake» та/або «SMS TCAPsec».

2.2. Вимоги щодо впровадження «SMS Home Routing».

Згідно з документом 3GPP TR 23.840 [9] «SMS Home Routing» передбачає модифікацію оброблення вхідних коротких повідомлень (SM) так, щоб доставкою SM абоненту керувала його домашня мережа мобільного зв'язку.

Усі вхідні запити MAP_sendRoutingInfo_for_SM, які стосуються власних абонентів

мережі, перенаправляються для оброблення до SMS-маршрутизатора. У відповідь SMS-маршрутизатор надсилає повідомлення MAP_sendRoutingInfo_for_SM_ack, яке містить адресу SMS-маршрутизатора замість адреси MSC/VLR та спеціально згенерований (так званий «фейковий IMSI») замість реального IMSI. Таким чином, стороні, яка надіслала запит, не повідомляється реальне місцезнаходження абонента та його IMSI. Після отримання SM SMS-маршрутизатор пересилає його до MSC/VLR, в зоні дії якого наразі перебуває абонент.

«SMS Home Routing» є, на перший погляд, дуже ефективним засобом захисту від витоку ідентифікаторів абонента мережі мобільного зв'язку (як було зазначено вище, отримання ідентифікаторів абонента дає змогу зловмисникам здійснити більш серйозні атаки).

Однак це рішення не дозволяє оператору телекомунікацій на сто відсотків приховати конфіденційні дані про мережі й абонентів. Цьому сприяють:

– помилки конфігурації «SMS Home Routing»;

– помилки конфігурації STP;

– можливість отримання даних через використання інших повідомлень SS7.

Усе це робить застосування «SMS Home Routing» необхідним, але недостатнім методом захисту мережі оператора телекомунікацій. Застосування «SMS Home Routing» має бути обов'язковим доповненням до моніторингу та фільтрації сигнального трафіку.

Крім того, для запобігання обходу «SMS Home Routing» повинні застосуватись такі механізми:

– усі вхідні запити MAP_sendRoutingInfo_for_SM, які стосуються власних абонентів телекомунікаційної мережі, повинні бути перенаправлені для оброблення до SMS маршрутизатора, а всі MAP_sendRoutingInfo_for_SM, у яких адресою призначення у GT SCCP указаний HLR, повинні бути заблоковані;

– усі прямі вхідні SM (MAP_MT_Forward_SM), які стосуються власних абонентів телекомунікаційної мережі, повинні бути перенаправлені до SMS-маршрутизатора. Загалом, після впровадження «SMS Home Routing» вхідні повідомлення, в яких адресою призначення у GT SCCP вказаний MSC/VLR, мають бути заблоковані, оскільки адресою призначення у GT SCCP має бути SMS-маршрутизатор;

– вхідні SM, призначені абонентам інших телекомунікаційних мереж, що перебувають у роумінгу, не повинні блокуватися.

2.3. Вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку.

Для ефективного захисту від несанкціонованого втручання та/або використання телекомунікаційних мереж технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку повинні відповідати викладеним нижче вимогам.

Технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку, потрібно розміщувати так, щоб мати змогу відстежувати весь сигнальний трафік, який необхідно моніторити та фільтрувати (міжнародний трафік, національний трафік, трафік на безпосередніх взаємоз'єднаннях з іншими телекомунікаційними мережами тощо), враховувати всі маршрути сигнального трафіку та охоплювати всі точки входу в мережу чи виходу з неї, а також вузли всередині мережі, які беруть участь в обміні повідомленнями сигналізації. Такі засоби повинні виконувати поглиблений аналіз стеку протоколів, які використовуються у мережі мобільного зв'язку, мати можливість кореляції параметрів на різних рівнях протоколу, а також виконувати перехресний аналіз протоколів для запобігання несанкціонованим втручанням, які використовують одразу кілька протоколів. При цьому технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку, не повинні впливати на легальний трафік та створювати додаткові ризики для телекомунікаційної мережі або для її безпеки (не повинні призводити до технічних збоїв у роботі телекомунікаційної мережі, переривання надання телекомунікаційних послуг, не повинні бути вразливими до несанкціонованого втручання тощо). Безпека технічного засобу, що здійснює моніторинг і фільтрацію сигнального трафіку, має бути перевірена і доведена.

Крім того, технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку, повинні мати можливість накопичення статистичних даних для отримання інформації про якість роботи мережі, аналізу проблем, виявлення та аналізу підозрілої/шкідливої активності, з'ясування причин і походження підозрілого трафіку, пошуку можливих нових кібератак.

Для більшої ефективності бажано, щоб технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку, складали окремий комплекс або систему, яка має змогу акумулювати дані з усіх точок, у яких виконується моніторинг сигнального трафіку, тобто

контролювати мережу оператора загалом. Комплексний засіб моніторингу та фільтрації сигнального трафіку дозволить:

– оперативно виявляти те, на якій ділянці влаштована атака;

– відстежувати атаки, які використовують декілька протоколів одночасно, забезпечуючи комплексний багаторівневий захист мережі та абонентів;

– органам з оцінки відповідності та наглядовим органам перевіряти виконання вимог нормативних документів, що має призвести до збільшення ефективності захисту телекомунікаційних мереж;

– забезпечити більш ефективний захист конфіденційної інформації абонентів (MSISDN, IMSI тощо), внесених до списку захисту.

Висновки. На основі аналізу міжнародних нормативних документів сформовано необхідні рекомендації щодо вмісту нормативного документа, який має регламентувати технічні вимоги до захисту телекомунікаційних мереж СКС-7 України від несанкціонованого втручання в їх роботу.

1. Для запобігання несанкціонованому втручанню та/або використанню телекомукаційних мереж СКС-7 необхідно застосовувати моніторинг та фільтрацію сигнального трафіку у вузлах, які отримують міжмережевий сигнальний трафік.

2. Фільтрація повідомлень СКС-7 повинна здійснюватись відповідно до категорій згідно з документом GSMA FS.11 [8].

3. Додатково до моніторингу та фільтрації сигнального трафіку для запобігання вторгненням з використанням SMS необхідно застосовувати «SMS Home Routing» та заходи для запобігання його обходу.

4. Нормативний документ також має містити вимоги до технічних засобів телекомунікацій, які здійснюють моніторинг та фільтрацію сигнального трафіку.

Затвердження такого нормативного документа буде сприяти прискоренню впровадження ефективних засобів та методів захисту телекомунікаційних мереж СКС-7 України від несанкціонованого втручання в їх роботу.

Після затвердження технічних вимог щодо моніторингу та фільтрації сигнального трафіку необхідні подальші дослідження для розроблення методики випробувань засобів захисту та телекомунікаційних мереж загалом на відповідність цим вимогам.

Список літератури:

1. Про телекомунікації : Закон України від 18 листопада 2003 р. № 1280-IV. https://zakon.rada.gov.ua/laws/show/1280-15#Text (дата звернення: 08.11.2021).

2. Про електронні комунікації : Закон України від 16 грудня 2020 р. № 1089-IX. https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 08.11.2021).

3. ITU Workshop on “SS7 Security". https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx (дата звернення: 08.11.2021).

4. GSM Association Official Document FS.07 – SS7 and SIGTRAN Network Security. Version 4.0. 08, December 2017.

5. GSM Association Official Document FS.11 – SS7 Interconnect Security Monitoring and Firewall Guidelines. Version 6.0. 17, May 2019.

6. GSM Association Official Document IR.70 – SMS SS7 Fraud. Version 4.0. 25, July 2013.

7. GSM Association Official Document IR.71 – SMS SS7 Fraud Prevention. Version 6.0. 26, September 2016.

8. GSM Association Official Document IR.82 – SS7 Security Network Implementation Guidelines. Version 5.0. 25, November 2016.

9. 3GPP TR 23.840 V7.1.0 (2007-03) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Study into routeing of MT-SMs via the HPLMN (Release 7).

10. Membership. P1 Security. https://www.gsma.com/membership/m/p1-security/ (дата звернення: 08.11.2021).

11. SS7map: SS7 country risk ratings. https://labs.p1sec.com/2014/12/28/ss7map-country-risk-ratings/ (дата звернення: 08.11.2021).

Kokiza S.V., Shchehelska N.M. SIGNALLING SYSTEM № 7 NETWORKS SECURITY IN UKRAINE

The article considers the problem of vulnerabilities of telecommunication networks of signalling system № 7 (SS7), which are used by attackers to attack telecommunication networks and subscribers of mobile communication networks.

The problem of absence in the normative documents of Ukraine of specific technical requirements to the telecommunication networks using SS7 from the point of view of protection against unauthorized interference in their work, which negatively affects the security of SS7 networks, is emphasized.

An analysis of the current state and existing problems of protection of mobile networks in Ukraine shows that the networks of SS7 Ukraine have a high risk of leakage of information about subscriber IDs, which can be used to carry out various kinds of attacks.

The analysis of recommendations of international normative documents on security of SS7 telecommunication networks is carried out. Methods of counteraction to threats of SS7networks are considered, namely: monitoring and filtering of messages according to certain categories; application of "SMS Home Routing". Also the requirements to the technical means of telecommunications which carry out monitoring and filtering of traffic in telecommunication networks are resulted.

Based on the analysis of the current state of protection of mobile networks in Ukraine and international regulations on the security of SS7 telecommunications networks provided recommendations on the content of technical requirements for protection of SS7 telecommunications networks of Ukraine from unauthorized interference in their work, which will promote effective means and methods of protection of SS7 telecommunication networks of Ukraine from unauthorized interference in their work.

Key words: *telecommunication network security, unauthorized interference and/or use of telecommunication networks, attacks on telecommunication networks, suspicious/harmful activity, telecommunication network protection, telecommunication network interconnect security, Signalling System № 7, monitoring signal traffic, signal traffic filtering, SMS Home Routing.*