Проєкт

|  |  |
| --- | --- |
|  | ЗАТВЕРДЖЕНО  Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України  \_\_\_ \_\_\_\_\_\_\_\_\_\_20\_\_ року № \_\_\_\_\_ |

**ТЕХНІЧНІ ВИМОГИ**

**до мереж рухомого (мобільного) зв’язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку**

**І. Загальні положення**

1. Ці Технічні вимоги розроблені відповідно до Закону України «Про телекомунікації».

2. Дія цих Технічних вимог поширюється на мережі рухомого (мобільного) зв’язку України та на технічні засоби телекомунікацій, що здійснюють моніторинг та фільтрацію трафіку, зокрема повідомлень системи спільноканальної сигналізації № 7 та команд протоколу «Diameter», з метою підвищення безпеки телекомунікаційних мереж, а також для запобігання несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж.

3. Ці Технічні вимоги застосовують суб’єкти господарювання, які здійснюють проєктування, побудову, реконструкцію, розвиток та експлуатацію мереж рухомого (мобільного) зв’язку, а також орган державного нагляду (контролю) у сфері телекомунікацій.

**IІ. Терміни та визначення понять**

1. У цих Технічних вимогах застосовуються такі терміни та визначення понять:

агент протоколу «Diameter» – вузол протоколу «Diameter», який забезпечує ретрансляцію, проксі, перенаправлення або передавання;

візитний регістр місцезнаходження (VLR) – база даних мережі рухомого (мобільного) зв’язку, призначена для запису та зберігання інформації для забезпечення надання телекомунікаційних послуг абоненту, кінцеве обладнання якого перебуває в межах зони дії певного центру комутації рухомого (мобільного) зв’язку;

власний абонент телекомунікаційної мережі – абонент, для якого ця телекомунікційна мережа є домашньою;

домашній регістр місцезнаходження (HLR) – база даних мережі рухомого (мобільного) зв’язку, призначена для запису та зберігання інформації про власних абонентів цієї мережі;

домашня мережа (home network) – мережа рухомого (мобільного) зв’язку, в якій мобільний код країни (MCC) та код мережі рухомого (мобільного) зв’язку (MNC), збігаються з МСС та MNC міжнародного ідентифікатора абонента рухомого (мобільного) зв’язку (IMSI);

фільтрація – функція виявлення та блокування недопустимої сигнальної інформації.

2. Інші терміни, що використовуються у цих Технічних вимогах, вживаються у значеннях, наведених у Законі України «Про телекомунікації», Правилах надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11 квітня 2012 року № 295, нормативному документі «Спільноканальна сигналізація № 7. Національна версія України. Правила використання у телефонній мережі загального користування. Версія 3.0», затвердженому наказом Міністерства транспорту та зв’язку України від 13 грудня 2007 року № 1164, нормативному документі «Телекомунікаційна мережа загального користування. Телефонна мережа. Технічні вимоги (у трьох частинах)», затвердженому наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від   
07 травня 2015 року № 252.

3. У цих Технічних вимогах вживаються такі скорочення та позначення:

|  |
| --- |
| СКС-7 – система спільноканальної сигналізації № 7;  3GPP – проєкт партнерства третього покоління (*3rd Generation Partnership* *Project*);  AVP – пара атрибут-значення (*Attribute Value Pair*);  CAMEL – персоналізовані застосунки для мереж рухомого (мобільного) зв’язку з розширеною логікою (*Customised Applications for Mobile networks Enhanced Logic*);  CAP – підсистема використання CAMEL (*CAMEL Application Part*);  DEA – крайовий агент протоколу «Diameter» (*Diameter Edge Agent*);  DoS attack – відмова в обслуговуванні (*Denial Service*);  DRA – агент маршрутизації протоколу «Diameter» (*Diameter Routing Agent*);  GSM – глобальна система рухомого (мобільного) зв’язку (*Global System for Mobile Communications*);  GSMA – Асоціація GSM (*GSM Association*);  GT – глобальний заголовок (*Global Title*);  HLR – домашній регістр місцезнаходження (*Home Location Register*); |
| ID – ідентифікатор (*Identity*);  IP – інтернет-протокол (*Internet Protocol*);  IMSI – міжнародний ідентифікатор абонента рухомого (мобільного) зв’язку (International Mobile Subscriber Identity);  ISDN – цифрова мережа з інтеграцією послуг (*Integrated Services Digital Network*);  LTE – довгостроковий розвиток (*Long Term Evolution*);  MAP – підсистема використання рухомого (мобільного) зв’язку *(Mobile Application Part);*  MCC – мобільний код країни (*Mobile Country Code*);  MNC – код мережі рухомого (мобільного) зв’язку (*Mobile Network Code*);  MSC – центр комутації рухомого (мобільного) зв’язку (*Mobile Switching Centre*);  MSISDN – ISDN-номер абонента рухомого (мобільного) зв’язку (*Mobile Subscriber ISDN Number*);  SCCP – підсистема управління з’єднанням сигналізації (*Signalling Connection Control Part*);  Send Routing Info\_for\_SM – надсилання інформації маршрутування для SM;  SGSN – обслуговуючий вузол підтримки GPRS (*Serving GPRS Support Node*);  SM – коротке повідомлення (*Short Message*);  SMS – послуга коротких повідомлень (*Short Message Service*);  SMS Home Routing – домашнє маршрутування SMS;  SCTP – протокол передавання з керуванням потоком (*Stream Control Transmission Protocol*);  UMTS – універсальна система рухомого (мобільного) зв’язку (*Universal Mobile Telecommunications System*);  VLR – візитний регістр місцезнаходження (*Visitor Location Register*). |

**III. Технічні вимоги до мереж рухомого (мобільного) зв’язку України щодо запобігання несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж**

1. Для запобігання несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж необхідно застосовувати моніторинг та фільтрацію трафіку в точках взаємоз’єднання телекомунікаційних мереж.

2. Для запобігання несанкціонованому втручанню в роботу телекомунікаційних мереж з використанням SMS застосовується «SMS Home Routing» згідно з прийнятим консорціумом 3GPP документом 3GPP TR 23.840 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Study into routeing of MT-SMs via the HPLMN.

«SMS Home Routing» передбачає модифікацію оброблення вхідних SM таким чином, щоб доставкою SM до кінцевого обладнання абонента керувала його домашня мережа.

Усі вхідні запити «Send Routing Info\_for\_SM» MAP, які стосуються кінцевого обладнання власних абонентів телекомунікаційної мережі, перенаправляються для оброблення до SMS‑маршрутизатора. У відповідь SMS‑маршрутизатор надсилає підтвердження «sendRoutingInfo\_for\_SM ack», вказавши адресу SMS‑маршрутизатора замість адреси MSC/VLR, та спеціально згенероване (замість реального) значення IMSI. Таким чином, стороні, яка надіслала запит, не повідомляється реальне місцезнаходження кінцевого обладнання абонента та його IMSI.

Після отримання SM SMS‑маршрутизатор пересилає його до MSC/VLR, у зоні дії якого знаходиться кінцеве обладнання абонента.

**IV. Загальні технічні вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію** **трафіку**

1. Технічний засіб телекомунікацій, що здійснює моніторинг і фільтрацію трафіку, повинен відповідати таким технічним вимогам:

розміщуватися так, щоб мати змогу відстежувати весь трафік, який необхідно моніторити та фільтрувати (міжнародний, національний, на безпосередніх взаємоз’єднаннях з іншими телекомунікаційними мережами тощо);

бути типовим елементом телекомунікаційної мережі та забезпечувати надійне передавання та обробку трафіку;

враховувати всі існуючі маршрути трафіку та підтримувати його поточну маршрутизацію до мережі та з мережі;

виявляти підозрілу/шкідливу активність та перешкоджати несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж;

виконувати поглиблений аналіз стеку протоколів, які використовуються у мережі рухомого (мобільного) зв’язку;

мати можливість кореляції технічних параметрів на різних рівнях протоколів;

виконувати перехресний аналіз протоколів для запобігання несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж, якщо застосовуються одразу кілька протоколів.

2. Технічний засіб телекомунікацій, що здійснює моніторинг і фільтрацію трафіку, не повинен:

створювати технічний ризик для телекомунікаційної мережі або для її безпеки (не повинен призводити до технічних збоїв у роботі телекомунікаційної мережі, переривання надання телекомунікаційних послуг, не бути вразливим до несанкціонованого втручання в роботу та/або використання телекомунікаційних мереж тощо). Надійність передавання трафіку повинна бути збережена. Безпека технічного засобу телекомунікацій, що здійснює моніторинг та фільтрацію трафіку, повинна бути перевірена в установленому порядку;

впливати на дозволений трафік;

впливати на роботу технічних засобів, необхідних для забезпечення проведення оперативно-розшукових заходів.

3. Технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію трафіку, повинні мати можливість накопичувати та зберігати статистичні дані для отримання інформації про якість роботи мережі, аналізу проблем, виявлення та аналізу підозрілої/шкідливої активності, для можливості з’ясування причин і походження підозрілого трафіку та пошуку можливих нових атак.

Повинна бути забезпечена можливість накопичення та зберігання трафіку за останні 7 діб.

У разі виявлення несанкціонованого втручання в роботу та/або використання телекомунікаційної мережі повинна бути забезпечена можливість зберігання пов’язаного з подією трафіку до 30 діб. Також для узагальнення даних про такі події має формуватися файл з інформацією про час та вид події, ініціатора (джерело) несанкціонованого втручання, про ідентифікатори абонентів, які були ціллю атаки/інциденту.

**V. Технічні вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію трафіку, щодо повідомлень СКС‑7**

1. Моніторинг та фільтрація повідомлень СКС‑7 технічними засобами телекомунікацій виконуються відповідно до категорій, визначених згідно з прийнятими GSMA документами: GSMA PRD FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines (далі – FS.11) та GSMA PRD IR.82 SS7 Security Network Implementation Guidelines.

2. Категорія 1 містить усі повідомлення СКС‑7, які отримуються тільки в межах однієї мережі. Повідомлення СКС‑7 категорії 1, отримані у точках взаємоз’єднання з іншими мережами та призначені вузлам всередині мережі, повинні блокуватися, якщо інше не передбачено угодами між операторами цих мереж про взаємодію телекомунікаційних мереж.

Ідентифікація повідомлень СКС‑7 категорії 1 проводиться лише на основі типу повідомлення (за значенням поля «OperationCode» (код операції) для повідомлень MAP та CAP).

Перелік повідомлень СКС‑7 категорії 1 наведено у FS. 11.

3. Категорія 2 складається з повідомлень СКС‑7, що стосуються кінцевого обладнання абонента, який знаходиться у роумінгу, та надходять з його домашньої мережі. Такі повідомлення, отримані у точках взаємоз’єднання з іншими телекомунікаційними мережами, не повинні призначатися кінцевому обладнанню власного абонента телекомунікаційної мережі.

Категорія 2 передбачає перевірку достовірності повідомлень СКС‑7, зокрема повідомлень SCCP та MAP, на основі аналізу походження (джерела) повідомлення.

Повинні блокуватися повідомлення MAP категорії 2, які надійшли від інших телекомунікаційних мереж, якщо вони призначені кінцевому обладнанню власного абонента мережі. Також повинні блокуватися повідомлення MAP категорії 2, якщо вони отримані для кінцевого обладнання абонента, який знаходиться в роумінгу, але мережа, визначена на основі MSISDN або IMSI (тобто MCC + MNC) на рівні MAP, не відповідає мережі, вказаній у GT параметра «Calling party address» (адреса сторони, що викликає) на рівні SCCP.

Повідомлення MAP категорії 2 можна додатково розділити на дві категорії:

категорія 2.1: повідомлення MAP, які потребують відповіді;

категорія 2.2: повідомлення MAP, які не потребують відповіді.

Перелік повідомлень MAP категорії 2 наведено у FS.11.

4. Категорія 3: повідомлення з достовірної мережі. Повідомлення СКС‑7 категорії 3 стосуються кінцевого обладнання власних абонентів мережі, які перебувають у роумінгу, та надсилаються з телекомнікаційної мережі поточного або можливого (відносно поточного) місцезнаходження кінцевого обладнання абонента. Категорія 3 передбачає перевірку достовірності повідомлень СКС‑7 на основі аналізу місцезнаходження кінцевого обладнання абонента та часу (швидкості) зміни місцезнаходження.

Повідомлення СКС‑7 категорії 3 можна додатково розділити на три категорії:

категорія 3.1: повідомлення, в яких місцезнаходження кінцевого обладнання абонента може бути підтверджено попередньою/поточною інформацією про VLR за допомогою перевірки SGSN/VLR. Повинні блокуватися всі повідомлення, отримані в точках взаємоз’єднання з іншими мережами, що стосуються кінцевого обладнання власних абонентів мережі, які перебувають у роумінгу, якщо адреса VLR (VLR Id), щозберігається у HLR, не відповідає мережі, вказаній у параметрі «Calling party address» (адреса сторони, що викликає) на рівні SCCP;

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

категорія 3.3: повідомлення, які стосуються SMS і до яких потрібно застосувати специфічні перевірки безпеки SMS згідно з прийнятим GSMA документом GSMA PRD IR.71 SMS SS7 Fraud Prevention.

Перелік повідомлень СКС‑7 категорії 3 наведено у FS.11.

**VI. Технічні вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію трафіку, щодо команд протоколу «Diameter»**

1. Загальні технічні вимоги

DEA та DRA повинні забезпечувати встановлення тільки тих з’єднань та пересилання тільки тих команд протоколу «Diameter», які використовуються для забезпечення роумінгу і взаємодії та надходять від телекомунікаційних мереж, з операторами телекомунікацій яких є відповідні угоди. Для цього у DEA/DRA визначають, які команди відповідають безпечному обміну інформацією та які команди і на яких інтерфейсах можуть бути прийняті у випадках взаємоз’єднань. Інтерфейси для взаємоз’єднання з іншими телекомунікаційними мережами також повинні бути обмежені лише інтерфейсами, необхідними для цього використання.

Технічними засобами телекомунікацій команди протоколу «Diameter» необхідно фільтрувати на рівні AVP та прапорців, залежно від угод про роумінг та відповідно до категорій. Команди протоколу «Diameter» згідно з прийнятими GSMA документами: GSMA PRD FS.19 Diameter Interconnect Security (далі – FS.19) та GSMA PRD IR.88 LTE and EPC Roaming Guidelines, можуть бути розподілені на кілька категорій та методів фільтрації, залежно від того, який тип фільтрації може бути для них застосований.

Таблиця 1. Категорії та методи фільтрації протоколу «Diameter»

|  |  |  |  |
| --- | --- | --- | --- |
| Шар/рівень, який оцінюється фільтром | Категорії фільтрації та методи фільтрації | Мета фільтрації | |
| 1 | 2 | 3 | |
| Нижній (перевірка трафіку на мережевому рівні): IP, SCTP, базовий рівень протоколу «Diameter» | Фільтрація за форматом нижнього шару (IP, host (вузол), realms (область адрес)) | Захист від підробки, перевірка базового рівня протоколу «Diameter» | |
| Вищий (поглиблена перевірка): перевірка відповідності коду команди протоколу «Diameter» визначеному інтерфейсу | Категорія 1. Фільтрація несанкціонованих пакетів по визначеному інтерфейсу за полями «Application ID» (ідентифікатор застосунка) та «Command Code» (код команди) | Повинні бути лише команди, які дозволені від телекомунікаційних мереж інших операторів телекомунікацій по визначених інтерфейсах | |
| Продовження таблиці 1 | | |
| 1 | 2 | 3 |
| Вищий (поглиблена перевірка): перевірка команди протоколу «Diameter», що надсилається з домашньої мережі або з телекомунікаційної мережі, за якою закріплено кінцеве обладнання абонента | Категорія 2. Фільтрація пакетів домашньої мережі за змістом AVP | Повинні бути лише команди, які стосуються кінцевого обладнання абонентів телекомунікаційних мереж інших операторів телекомунікацій, що перебувають у роумінгу, та надходять з їхніх домашніх мереж |
| Вищий (поглиблена перевірка): перевірка команди протоколу «Diameter», що надсилається з телекомнікаційної мережі поточного або можливого (відносно поточного) місцезнаходження кінцевого обладнання абонента | Категорія 3. Фільтрація пакетів за достовірністю мережі:  перевірка попереднього місцезнаходження кінцевого обладнання абонента;  перевірка часу (швидкості) зміни місцезнаходження кінцевого обладнання абонента | Повинні бути лише команди, які стосуються кінцевого обладнання власних абонентів телекомунікаційної мережі, що перебувають у роумінгу, та надсилаються лише з телекомунікаційної мережі, в якій наразі перебуває кінцеве обладнання абонента |

2. Фільтрація за форматом нижнього шару

Метою фільтрації за форматом нижнього шару є виявлення технічними засобами телекомунікацій, що здійснюють моніторинг та фільтрацію трафіку, спроб підроблення повідомлень у мережі.

Фільтрація за форматом нижнього шару відповідає перевірці нижнього (базового) рівня протоколу «Diameter» без потреби повного розуміння застосунків вищого рівня або декодування певних AVP. Зазвичай вона базується на перевірці всієї інформації нижнього рівня (IP, SCTP, host (вузол), realms (область адрес)), а також перевірці формату команди протоколу «Diameter».

Можливі такі варіанти неправильного формування команди протоколу «Diameter»:

команда протоколу «Diameter» сформована так, що не може бути декодована відповідно до формату протоколу «Diameter» (наприклад, пошкоджена двійкова структура);

базова частина команди протоколу «Diameter» містить AVP, тип або довжина яких відрізняється від визначеного у словнику протоколу «Diameter» (наприклад, словник визначає тип AVP як ціле число, а в отриманій команді протоколу «Diameter» – рядок);

наявність повторювань AVP, які мають бути наявні тільки одноразово або їх взагалі не має бути, що робить команду протоколу «Diameter» невідповідною специфікації (наприклад, у команді «Update‑Location‑Request» (запит оновлення місцезнаходження) повторення дозволено лише для AVP «Route‑Record» (запис маршруту), Proxy‑Info (інформація проксі), Supported‑Features (підтримувані функції). Інші AVP не повинні повторюватися);

команда протоколу «Diameter» містить AVP, несумісні з її характеристиками, що може бути використано для обходу фільтрації або зміни обробки у вузлі, який отримує команду (наприклад, команда «Answer» (відповідь) містить AVP «Destination-Host» (вузол призначення));

команда протоколу «Diameter» містить одну або більше AVP перед AVP «Session‑Id» (ідентифікатор сесії). AVP «Session‑Id» завжди повинна декодуватися першою у команді протоколу «Diameter».

Під час обробки вхідного трафіку протоколу «Diameter» технічні засоби телекомунікацій, що здійснюють моніторинг та фільтрацію трафіку, повиннідозволяти тільки:

команди протоколу «Diameter», у яких AVP «Session‑Id» є першою AVP;

команди протоколу «Diameter», у яких AVP «Origin‑Host» (вихідний вузол) та «Origin‑Realm» (вихідна область) наявні тільки по одному разу. Команди протоколу «Diameter», у яких AVP «Origin‑Host» та/або «Origin‑Realm» немає або наявні більше одного разу, повинні блокуватися;

вхідні команди-відповіді протоколу «Diameter», що відповідають вихідному запиту;

команди протоколу «Diameter», які містять AVP, сумісні з характеристиками самої команди;

команди протоколу «Diameter», які містять очікувані AVP (набір очікуваних AVP визначається технічною специфікацією та може змінюватися залежно від конфігурації конкретної точки взаємоз’єднання);

команди протоколу «Diameter», що містять AVP, кодування даних у яких відповідають специфікаціям за типом та довжиною;

команди протоколу «Diameter», що містять AVP, значення яких відповідають специфікаціям застосунку;

команди протоколу «Diameter», у яких форматAVP «Origin‑Realm» відповідає прийнятому консорціумом 3GPP документу 3GPP TS 23.003 Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (далі – 3GPP TS 23.003);

команди протоколу «Diameter», у яких формат AVP «Origin‑Host» відповідає документу 3GPP TS 23.003;

команди протоколу «Diameter», у яких значення AVP «Origin‑Host» відповідає значеннюAVP «Origin‑Realm».

У разі безпосереднього взаємоз’єднання з мережею, з якої надійшла команда, необхідно перевірити, що значення AVP «Origin‑Host» та «Origin‑Realm» відповідають узгодженій IP‑адресі вузла, з якого надсилаються команди.

3. Категорія 1: фільтрація команд протоколу «Diameter» за полями «Application ID» (ідентифікатор застосунка) та «Command Code» (код команди)

Категорія 1 передбачає перевірку технічними засобами телекомунікацій, що здійснюють моніторинг і фільтрацію трафіку, полів «Application ID» (ідентифікатор застосунка) та «Command Code» (код команди) без потреби декодування конкретних AVP.

Дозволяються лише команди, визначені відповідними документами, для кожного з інтерфейсів, які використовуються для взаємоз’єднання з телекомунікаційними мережами інших операторів.

Для взаємоз’єднання з телекомунікаційними мережами інших операторів інтерфейси також повинні бути обмежені лише інтерфейсами, необхідними для цього використання.

Для роумінгу в мережах LTE найчастіше використовують інтерфейс S6a/S6d.

У таблиці 2 наведені команди згідно з FS.19 зазвичай потрібні для роумінгу і тому дозволені на інтерфейсі S6a/S6d (Application‑ID=«16777251»).

Усі інші команди протоколу «Diameter» на інтерфейсі S6a/S6d слід або заблокувати, або перевірити чи дійсно вони потрібні.

Таблиця 2. Команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d

|  |  |  |
| --- | --- | --- |
| Назва команди | Скорочення | Значення поля «Command Code» (код команди) |
| 1 | 2 | 3 |
| Update‑Location-Request/Answer (запит/відповідь оновлення місцезнаходження) | ULR/ULA | 316 |
| Cancel‑Location-Request/Answer (запит/відповідь видалення місцезнаходження) | CLR/CLA | 317 |
| Authentication‑Information-Request/Answer (запит/відповідь інформації аутентифікації) | AIR/AIA | 318 |
| Insert‑Subscriber-Data-Request/Answer (запит/відповідь внесення змін до даних абонента) | IDR/IDA | 319 |
| Delete‑Subscriber-Data-Request/Answer (запит/відповідь видалення даних абонента) | DSR/DSA | 320 |

Продовження таблиці 2

|  |  |  |
| --- | --- | --- |
| 1 | 2 | 3 |
| Purge‑UE-Request/Answer (запит/відповідь видалення інформації про UE) | PUR/PUA | 321 |
| Reset‑Request/Answer (запит/відповідь скидання) | RSR/RSA | 322 |
| Notify-Request/Answer (запит/відповідь сповіщення) | NOR/NOA | 323 |

Фільтрація також може враховувати походження (джерело) команди.

Крім того, необхідно перевірити, щоб в командах протоколу «Diameter» не були наявні більше одного разу такі AVP:

«Vendor‑Specific‑Application‑ID» (постачальник визначеного ID застосунка);

«Visited‑PLMN‑ID» (ID візитної наземної телекомунікаційної мережі рухомого (мобільного) зв’язку).

4. Категорія 2: фільтрація команд протоколу «Diameter» на рівні AVP

Категорія 2 передбачає виконання технічними засобами телекомунікацій, що здійснюють моніторинг та фільтрацію трафіку, фільтрації команд протоколу «Diameter» на основі аналізу AVP «User‑Name» (ім’я користувача) за IMSI та MSISDN, але яка також може бути поширена на інші AVP. AVP «User‑Name» (ім’я користувача) повинна бути наявна лише один раз для уникнення обходу фільтрації.

Команди категорії 2 не повинні призначатися кінцевому обладнанню власних абонентів телекомунікаційної мережі, що надходять з телекомунікаційних мереж інших операторів телекомунікацій.

Отримання команд категорії 2 повинно бути дозволено лише по визначених інтерфейсах тільки для обслуговування кінцевого обладнання абонентів, що перебувають у роумінгу, та тільки якщо вони надіслані з домашньої мережі таких абонентів.

Для роумінгу в мережах LTE найбільш широко використовують інтерфейс S6a/S6d.

У таблиці 3 наведено команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d (Application‑ID=«16777251»), якщо вони стосуються кінцевого обладнання абонентів, які перебувають у роумінгу.

Таблиця 3. Команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d, якщо вони стосуються кінцевого обладнання абонентів, які перебувають у роумінгу 1, 2

| Назва команди | Скорочення | Значення поля «Command Code» (код команди) |
| --- | --- | --- |
| Cancel‑Location-Request/Answer (запит/відповідь видалення місцезнаходження) | CLR/CLA | 317 |
| Insert‑Subscriber-Data-Request/Answer (запит/відповідь внесення змін до даних абонента) | IDR/IDA | 319 |
| Delete‑Subscriber-Data-Request/Answer (запит/відповідь видалення даних абонента) | DSR/DSA | 320 |
| Reset-Request/Answer (запит/відповідь скидання) | RSR/RSA | 322 |
| Примітки:  1 Це орієнтовний перелік, який може уточнюватися відповідно до конкретних конфігурацій мережі рухомого (мобільного) зв’язку.  2 Навіть якщо код команди дозволений, не всі прапорці команди дозволяються, щоб запобігти DoS attack або відстеженню місцезнаходження кінцевого обладнання абонента. | | |

Для підвищення ефективності фільтрація на основі аналізу IMSI та MSISDN повинні поєднуватися з фільтрацією за форматом нижнього шару та з фільтрацією категорії 1.

5. Категорія 3: фільтрація команд протоколу «Diameter» на основі аналізу місцезнаходження кінцевого обладнання абонента

Категорія 3 передбачає виконання технічними засобами телекомунікацій, що здійснюють моніторинг і фільтрацію трафіку, фільтрації пакетів на основі перевірки попереднього місцезнаходження кінцевого обладнання абонента та перевірки часу (швидкості) зміни місцезнаходження. Отримання таких команд повинно відбуватися лише по визначених інтерфейсах.

У таблиці 4 наведено команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d (Application‑ID=«16777251»), якщо вони відповідають умові перевірки попереднього місцезнаходження кінцевого обладнання абонента.

Таблиця 4. Команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d, якщо вони відповідають умові перевірки попереднього місцезнаходження кінцевого обладнання абонента1

| Назва команди | Скорочення | Значення поля «Command Code» (код команди) |
| --- | --- | --- |
| Purge‑UE-Request/Answer (запит/відповідь видалення інформації про UE) | PUR/PUA | 321 |
| Notify‑Request/Answer (запит/відповідь сповіщення) | NOR/NOA | 323 |
| Примітка1. Отримання команд PURабо NOR дозволяється, якщо значення їхніх AVP «Origin‑Host» та «Origin‑Realm» відповідають значенням відповідних AVP в останній команді «Update‑Location» (оновлення місцезнаходження), яка стосується того самого абонента. | | |

У таблиці 5 наведено команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d (Application‑ID=«16777251»), якщо вони відповідають умові за часом (швидкістю) зміни місцезнаходження кінцевого обладнання абонента.

Таблиця 5. Команди протоколу «Diameter», дозволені на інтерфейсі S6a/S6d, якщо вони відповідають умові за часом (швидкістю) зміни місцезнаходження кінцевого обладнання абонента

| Назва команди | Скорочення | Значення поля «Command Code» (код команди) |
| --- | --- | --- |
| Update‑Location-Request/Answer (запит/відповідь оновлення місцезнаходження) | ULR/ULA | 316 |
| Authentication‑Information-Request/Answer (запит/відповідь інформації аутентифікації) | AIR/AIA | 318 |

Технічними засобами телекомунікацій, що здійснюють моніторинг та фільтрацію трафіку, повинні блокуватися команди ULR та AIR, які вказують на невластиво швидку зміну місцезнаходження кінцевого обладнання абонента (визначається за допомогою перевірки часу послідовних команд «Update‑Location» (оновлення місцезнаходження) з країн, що не мають спільного кордону, протягом короткого періоду).

Директор Департаменту  
розвитку електронних комунікацій  
Адміністрації Держспецзв’язку  Микола ТКАЧЕНКО