Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

10.11.2021 № 16/03/01-1766 На № _____ від _____

Державна регуляторна служба
України

вул. Арсенальна, 9/11,
м. Київ, 01011

Щодо погодження проєкту наказу
Адміністрації Держспецзв'язку

Адміністрація Державної служби спеціального зв'язку та захисту інформації України надсилає на погодження проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку» (далі – проєкт наказу).

Просимо погодити проєкт наказу у найкоротший термін.

Додатки:
1. Проєкт наказу на 15 арк.
2. Аналіз регуляторного впливу до проєкту наказу на 6 арк.
3. Копія оприлюдненого повідомлення про оприлюднення проєкту наказу на 1 арк.
4. Пояснювальна записка до проєкту наказу на 4 арк.
5. Інформаційно-аналітичні матеріали з публічного обговорення на 7 арк.

Голова Служби
підполковник Юрій ЩИГОЛЬ

ДЕРЖАВНА РЕГУЛЯТОРНА СЛУЖБА УКРАЇНИ
«12» 11 2021 р.
Вх. № 10148

Марина Кравченко 281-87-19
281-87-18

ПРОЄКТ
Прим. № ___

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

___ _____ 20___ року №_____

Про затвердження Технічних вимог
до мереж рухомого (мобільного) зв'язку
України і технічних засобів телекомунікацій
щодо моніторингу та фільтрації сигнального
трафіку

Відповідно до статті 15 Закону України «Про телекомунікації», пункту 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, на виконання доручення Першого віце-прем'єр-міністра України – Міністра економічного розвитку і торгівлі України від 15 лютого 2017 року № 45158/1/1-17 до листа заступника Секретаря Ради національної безпеки і оборони України від 10 лютого 2017 року № 2030/16-06/2-17, для запобігання несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж

НАКАЗУЮ:

1. Затвердити Технічні вимоги до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку, що додаються.

2. Департаменту розвитку електронних комунікацій Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова Служби
підполковник Юрій ЩИГОЛЬ

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 сигнального трафіку

I. 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 сигнального 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.

II. 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 MCC та MNC міжнародного ідентифікатора абонента рухомого (мобільного) зв'язку (IMSI);

сигнальний трафік – сукупність інформаційних сигналів службової інформації, що передаються телекомунікаційною мережею за визначений інтервал часу;

SMS-маршрутизатор – технічний засіб телекомунікацій, що здійснює доставку вхідних коротких повідомлень (SM) власним абонентам мережі;

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*);

SCTP – протокол передавання з керуванням потоком (*Stream Control Transmission Protocol*);

SendRoutingInfo_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;

SMS TCAP Handshake – підтвердження SMS TCAP;

STP – транзитний пункт сигналізації (*Signalling Transfer Point*);

TCAP – підсистема використання можливостей транзакцій (*Transaction Capabilities Application Part*);

TCAPsec – безпека користувачів TCAP – набір протоколів безпеки шлюзів безпеки СКС-7 (*TCAP user security – the SS7 security gateway security protocol suite*);

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 сигнального трафіку міжмережевого обміну.

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

системах виявлення та запобігання вторгненням (за наявності);

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

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

SMS-маршрутизаторі;

мережевих системах моніторингу;

інших елементах мережі, які отримують міжмережевий сигнальний трафік.

3. Для забезпечення можливості аналізу, встановлення походження (джерела) підозрілої/шкідливої активності та планування заходів реагування на виявлені атаки необхідно накопичувати та зберігати сигнальний трафік міжмережевого обміну за останні 7 діб.

4. 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 «SendRoutingInfo_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.

Для запобігання обходу «SMS Home Routing» повинні застосуватись такі механізми:

усі вхідні запити «SendRoutingInfo_for_SM» MAP, які стосуються

кінцевого обладнання власних абонентів телекомунікаційної мережі, повинні бути перенаправлені для оброблення до SMS-маршрутизатора, а всі «SendRoutingInfo_for_SM», в яких адресою призначення у GT SCCP вказаний HLR, повинні бути заблоковані;

усі прямі вхідні SM (MT_Forward_SM MAP), які стосуються кінцевого обладнання 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, повинні бути заблоковані, оскільки адресою призначення у GT SCCP повинен бути SMS-маршрутизатор;

вхідні SM, призначені для кінцевого обладнання абонентів інших телекомунікаційних мереж, що знаходяться у роумінгу, не повинні блокуватися.

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

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

мати змогу відстежувати весь сигнальний трафік, який необхідно моніторити та фільтрувати;

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

враховувати всі існуючі маршрути сигнального трафіку міжмережевого обміну;

виявляти підозрілу/шкідливу активність та перешкоджати несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж під час міжмережевого обміну сигнальним трафіком;

виконувати поглиблений аналіз стеку протоколів, які використовуються у мережі рухомого (мобільного) зв'язку, тобто аналіз визначених параметрів повідомлень (команд) протоколу.

2. Технічний засіб телекомунікацій, що здійснює моніторинг і фільтрацію сигнального 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 сигнального 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 сигнального 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 міжмережевого сигнального трафіку та пошуку можливих нових атак.

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 сигнального 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 національному 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), що зберігається 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, за наявності технічної можливості, 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 та заходи безпеки SMS, зокрема:

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 механізму SMS TCAP Handshake згідно з прийнятим консорціумом 3GPP документом 3GPP TS 33.200 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; MAP application layer

security та/або SMS TCAPsec згідно з прийнятими консорціумом 3GPP документами 3GPP TS 29.204 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Signalling System No. 7 (SS7) security gateway; Architecture, functional description and protocol details та 3GPP TS 33.204 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security.

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

VI. Технічні вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального 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 сигнального 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»

Продовження таблиці 1

1	2	3
Вищий (поглиблений аналіз): 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
Вищий (поглиблений аналіз): 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 (поглиблений аналіз): 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 сигнального 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 сигнального трафіку, повинні-дозволяти 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 формат AVP «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 значенню AVP «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 сигнального 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

Продовження таблиці 2

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
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 сигнального 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, що стосуються власних абонентів телекомунікаційної мережі та надходять з телекомунікаційних мереж інших операторів, повинні бути заблоковані.

Отримання команд категорії 2 повинно бути дозволено лише по визначених інтерфейсах тільки для обслуговування кінцевого обладнання абонентів, що перебувають у роумінгу.

Отримання команд категорії 2, які стосуються кінцевого обладнання абонентів, що перебувають у національному роумінгу, повинно бути дозволено лише по визначених інтерфейсах і тільки якщо вони надіслані з їхньої домашньої мережі.

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.		

Фільтрація на основі аналізу IMSI та MSISDN може 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 сигнального 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 абонента[1]

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
Примітка[1]. 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

Технічні засоби телекомунікацій, що здійснюють моніторинг та фільтрацію сигнального трафіку, повинні моніторити та, за умови технічної можливості, блокувати 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 — Василь МЕКЕНЧЕНКО

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ

до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку»

І. Визначення проблеми

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку» (далі – проєкт Наказу) розроблено на виконання доручення Першого віце-прем'єр-міністра України – Міністра економічного розвитку і торгівлі України від 15 лютого 2017 року № 45158/1/1-17 до листа заступника Секретаря Ради національної безпеки і оборони України від 10 лютого 2017 року № 2030/16-06/2-17.

Необхідність розроблення проєкту Наказу виникла у зв'язку з тим, що недостатня нормативно-правова база у сфері телекомунікацій, особливо, що стосується технічних вимог до мереж рухомого (мобільного) зв'язку та технічних засобів телекомунікацій, які здійснюють моніторинг та фільтрацію сигнального трафіку в телекомунікаційних мережах, призвела до несанкціонованого втручання в роботу та/або використання телекомунікаційних мереж, наслідком якої став виток інформації про місцезнаходження кінцевого обладнання відповідних абонентів у мережах рухомого (мобільного) зв'язку і передачі цієї інформації до осіб, які використовували цю інформацію, для завдання шкоди таким абонентам.

Технічні вимоги до порядку та способів передачі даних про місцезнаходження кінцевого обладнання абонентів у мережах рухомого (мобільного) зв'язку визначаються у документах відповідних міжнародних організацій – Асоціації GSM (*GSM Association*), 3GPP проєкт партнерства третього покоління (*3rd Generation Partnership Project*).

Тобто затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку, які побудовані на основі відповідних технічних документів зазначених вище міжнародних організацій, дасть змогу підвищити безпеку мереж рухомого (мобільного) зв'язку та забезпечити збереження даних про місцезнаходження кінцевого обладнання абонентів мережі відповідно до чинного законодавства.

Основні групи (підгрупи), на які впливає проблема:

Групи (підгрупи)	Так	Ні
Громадяни	Так	-
Держава	-	-
Суб'єкти господарювання, у тому числі суб'єкти малого підприємництва	Так -	- -

Проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки на сьогодні немає технічних вимог до мереж рухомого (мобільного) зв'язку України та технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку, що унеможливлює збереження відповідної інформації в мережах рухомого (мобільного) зв'язку.

Проблема не може бути розв'язана за допомогою чинних регуляторних актів, оскільки на сьогодні таких нормативно-правових актів немає.

II. Цілі державного регулювання

Основною ціллю регуляторного акта є нормативне визначення технічних вимог до мереж рухомого (мобільного) зв'язку та технічних засобів телекомунікацій, які забезпечують моніторинг та фільтрацію сигнального трафіку, з метою підвищення безпеки телекомунікаційних мереж та забезпечення неможливості передачі інформації про місцезнаходження кінцевого обладнання абонентів у мережі рухомого (мобільного) зв'язку для не передбачених до цього інших мереж і технічних засобів телекомунікацій.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива1	Збереження існуючої нормативно-правової бази унеможливить досягнення поставленої цілі та не створить відповідних умов для підвищення безпеки телекомунікаційних мереж і визначення місцезнаходження кінцевого обладнання абонентів без порушення порядку маршрутизації трафіку. Такий спосіб не сприятиме досягненню цілей державного регулювання.
Альтернатива 2	Затвердження технічних вимог сприятиме підвищенню безпеки телекомунікаційних мереж і забезпеченню збереження інформації про місцезнаходження абонентів мережі відповідно до встановлених технічних вимог стосовно проходження трафіку.

Інші способи є неприйнятними, оскільки розв'язання порушеної проблеми лежить передусім у правовій площині.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає	Немає
Альтернатива 2	Немає	Немає

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Немає	Немає
Альтернатива 2	Збереження інформації про місцезнаходження кінцевого обладнання абонентів мережі не дозволить представникам інших мереж отримати інформацію про їх місцезнаходження з порушенням вимог чинного законодавства України.	Немає

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	3	3	-	-	6
Питома вага групи у загальній кількості, відсотків	50	50	-	-	X

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Вигод не передбачається, оскільки відсутність затверджених технічних вимог залишає ситуацію на сьогоднішньому рівні.	Немає
Альтернатива 2	Затвердження технічних вимог забезпечить цілі державного регулювання, а саме – підвищення безпеки мереж рухомого (мобільного) зв'язку щодо моніторингу та фільтрації сигнального трафіку.	Немає

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	–
Альтернатива 2	–

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Найменш ефективний при розв'язанні існуючої проблеми.
Альтернатива 2	4	Найбільш ефективний при розв'язанні існуючої проблеми.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Вигод немає	Немає	Найменш ефективний у розв'язанні існуючої проблеми.
Альтернатива 2	Обраний спосіб забезпечує досягнення мети державного регулювання, а саме: нормативно врегулювати питання щодо проходження трафіку в мережах з метою підвищення безпеки мереж і збереження інформації про місцезнаходження кінцевого обладнання абонентів мережі.	Немає	Найбільш ефективний у розв'язанні існуючої проблеми.

Рейтинг	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1	Зазначений спосіб є неприйнятним, оскільки відсутність затверджених технічних вимог ускладнює питання забезпечення безпеки мереж рухомого (мобільного) зв'язку та збереження інформації про місцезнаходження кінцевого обладнання абонентів мережі.	X
Альтернатива 2	Обраний спосіб забезпечує досягнення цілі державного регулювання, а саме: підвищення захисту мереж рухомого (мобільного) зв'язку щодо моніторингу та фільтрації сигнального трафіку та збереження інформації про місцезнаходження кінцевого обладнання абонентів мережі.	Ризику впливу зовнішніх чинників на дію запропонованого регуляторного акта немає

V. Механізми та заходи, які забезпечать розв'язання визначеної проблеми

Механізмом, який забезпечить розв'язання проблеми, є прийняття регуляторного акта.

Затвердження технічних вимог надасть можливість підвищити безпеку мереж рухомого (мобільного) зв'язку та забезпечить збереження інформації про місцезнаходження кінцевого обладнання абонентів мережі.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація наказу не потребує додаткових матеріальних, фінансових та інших ресурсів державного та місцевих бюджетів.

За результатами введення в дію запропонованого регуляторного акта не передбачається нанесення шкоди суб'єктам господарювання, тому механізм повної або часткової компенсації можливої шкоди у разі настання очікуваних наслідків дії акта не розроблявся.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта не обмежується у часі.

Регуляторний акт набирає чинності з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Показниками результативності запропонованого регуляторного акта є:

підвищення безпеки мереж рухомого (мобільного) зв'язку та забезпечення збереження інформації про місцезнаходження кінцевого обладнання абонента мережі;

кількість суб'єктів господарювання, на які поширюватиметься дія акта – оператори телекомунікацій, які надають послуги рухомого (мобільного) зв'язку.

Надходження до державного і місцевих бюджетів та державних цільових фондів, пов'язаних з дією акта, не передбачаються, оскільки цей акт не регулює цих надходжень і не має впливу на них.

Рівень поінформованості суб'єктів господарювання – достатній: проєкт регуляторного акта оприлюднено на офіційному вебсайті Держспецзв'язку з метою одержання зауважень і пропозицій від фізичних та юридичних осіб.

Норми проєкту Наказу попередньо були обговорені з учасниками ринку телекомунікацій під час виконання науково-дослідної роботи.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відстеження результативності цього регуляторного акта буде здійснюватися Адміністрацією Державної служби спеціального зв'язку та захисту інформації України шляхом проведення:

базового відстеження – після опрацювання статистичної звітності, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта;

повторного відстеження – через рік з дня набрання чинності;

періодичного відстеження – раз на кожні три роки, починаючи з дня закінчення заходів із повторного відстеження.

Проведення відстеження результативності цього регуляторного акта здійснюватиметься шляхом збирання статистичних даних та аналізу звернень заінтересованих осіб щодо необхідності перегляду нормативно-правового акта з метою внесення до нього змін.

Голова Державної служби спеціального
зв'язку та захисту інформації України
підполковник
«___»_____ 2021 р.

Юрій ЩИГОЛЬ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Повідомлення про оприлюднення проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку»

Оприлюднення проектів актів Регуляторна діяльність

04.06.2021 09:26

1. Стислий виклад змісту проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку» (далі – проєкт наказу) розроблено на виконання доручення Першого віце-прем'єр-міністра України – Міністра економічного розвитку і торгівлі України від 15 лютого 2017 року N° 45158/1/1-17 до листа заступника Секретаря Ради національної безпеки і оборони України від 10 лютого 2017 року N° 2030/16-06/2-17 з метою запобігання несанкціонованому втручанню
в роботу та/або використанню телекомунікаційних мереж.

Проєкт наказу підготовлено за результатами виконання науково-дослідної роботи із залученням учасників ринку телекомунікацій.

Керуючись статтями 9 та 13 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», Адміністрація Держспецзв'язку повідомляє про оприлюднення проєкту цього регуляторного акта.

2. Адреси для зауважень та пропозицій до проєкту акта:

Адміністрації Державної служби спеціального зв'язку та захисту інформації України:

поштова: вул. Солом'янська, 13, м. Київ, 03680;
електронна: info@dsszzi.gov.ua;

Державної регуляторної служби України:

поштова: вул. Арсенальна, 9/11, м. Київ, 01011;
електронна: inform@dkrp.gov.ua.

3. Обраний спосіб оприлюднення проєкту акта

Проєкт наказу та аналіз його регуляторного впливу розміщено на вебсайті Держспецзв'язку.

4. Строк, протягом якого приймаються зауваження та пропозиції

Пропозиції та зауваження до проєкту наказу просимо надсилати протягом місяця з дати його оприлюднення.

5. Спосіб надання зауважень та пропозицій

Зауваження та пропозиції до проєкту акта надсилати на адреси, зазначені у пункті 2.

Прим. №__

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку»

1. Мета

Проєкт наказу Адміністрації Держспецзв'язку «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку» (далі – проєкт наказу) розроблено з метою підвищення безпеки телекомунікаційних мереж операторів телекомунікацій та захисту інформації про споживачів послуг рухомого (мобільного) зв'язку.

2. Обґрунтування необхідності прийняття акта

Проєкт наказу розроблено на виконання доручення Першого віце-прем'єр-міністра України – Міністра економічного розвитку і торгівлі України від 15.11.2017 № 45158/1/1-17 до листа заступника Секретаря Ради національної безпеки і оборони України від 10.11.2017 № 2030/16-06/2-17, з метою повного та всебічного опрацювання пропозицій Генеральної прокуратури України, наданих листом від 04.08.2017 № 10/4/1-21869-17, щодо вжиття заходів, спрямованих на підвищення безпеки телекомунікаційних мереж операторів телекомунікацій та захисту інформації про споживачів послуг рухомого (мобільного) зв'язку. Для визначення шляхів вирішення зазначених питань наказом Адміністрації Держспецзв'язку від 31.01.2018 № 51 було створено робочу (далі – Робоча група).

За результатами діяльності Робочої групи було, зокрема, визнано за необхідне розробити технічні вимоги до маршрутизації, оброблення та фільтрації сигнального обміну в мережах рухомого (мобільного) зв'язку України.

Необхідність розроблення проєкту наказу виникла у зв'язку з тим, що недостатня нормативно-правова база у сфері телекомунікацій, особливо, що стосується технічних вимог до мереж рухомого (мобільного) зв'язку та технічних засобів телекомунікацій, які здійснюють моніторинг та фільтрацію сигнального трафіку в телекомунікаційних мережах, призвела до несанкціонованого втручання в роботу та/або використанню телекомунікаційних мереж, наслідком якої став виток інформації про місцезнаходження кінцевого обладнання відповідних абонентів у мережах

рухомого (мобільного) зв'язку і передачі цієї інформації до осіб, які використовували цю інформацію для завдання шкоди таким абонентам.

Технічні вимоги до порядку та способів передачі даних про місцезнаходження кінцевого обладнання абонентів у мережах рухомого (мобільного) зв'язку визначаються у документах відповідних міжнародних організацій – Асоціації GSM (GSM Association), проєкті партнерства третього покоління 3GPP (3rd Generation Partnership Project).

За результатом виконання науково-дослідної роботи розроблено проєкт Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку, який побудовано на основі відповідних технічних документів зазначених вище міжнародних організацій.

3. Основні положення проєкту акта

Проєктом наказу передбачається затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації сигнального трафіку.

Застосування цього нормативно-правового акта дасть змогу підвищити безпеку мереж рухомого (мобільного) зв'язку та забезпечити збереження даних про місцезнаходження кінцевого обладнання абонентів мережі відповідно до чинного законодавства.

4. Правові аспекти

У зазначеній сфері суспільних відносин діють такі нормативно-правові акти:

Закон України «Про телекомунікації»;

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 03.09.2014 р. № 411;

Правила надання та отримання телекомунікаційних послуг, затверджені постановою Кабінету Міністрів України від 11 квітня 2012 року № 295;

Також у цій сфері діють документи міжнародних організацій – Асоціації GSM (GSM Association), проєкт партнерства третього покоління 3GPP (3rd Generation Partnership Project).

5. Фінансово-економічне обґрунтування

Реалізація наказу не потребує додаткових матеріальних, фінансових та інших ресурсів державного та місцевих бюджетів.

6. Позиція заінтересованих сторін

Проєкт наказу не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної.

Проєкт наказу не стосується сфери наукової та науково-технічної діяльності.

Проєкт наказу згідно із статтями 9 і 13 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» 04.06.2021 оприлюднено на вебсайті Держспецзв'язку.

До проєкту наказу надійшли зауваження та пропозиції від Української асоціації операторів зв'язку «Телас» (лист від 02.07.2021 № 73/21).

З метою обговорення пропозицій і зауважень, наданих під час громадського обговорення проєкту наказу, Адміністрацією Держспецзв'язку 29.07.2021 та 06.10.2021 проведені узгоджувальні наради за участі представників ПрАТ «Діпрозв'язок» (виконавця науково-дослідної роботи), Української асоціації операторів зв'язку «Телас» та СБУ (протоколи узгоджувальних нарад від 30.07.2021 № 16/03/01-1202, від 08.10.2021 № 16/03/01-1581).

7. Оцінка відповідності

Проєкт наказу не містить положень, що: стосуються зобов'язань у сфері європейської інтеграції, прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод; впливають на забезпечення рівних прав та можливостей жінок і чоловіків; містять ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією; створюють підстави для дискримінації.

Громадська антикорупційна, громадська антидискримінаційна та громадська гендерно-правова експертизи не проводилися.

8. Прогноз результатів

Упровадження наказу дасть змогу підвищити безпеку мереж рухомого (мобільного) зв'язку і забезпечити збереження даних про місцезнаходження кінцевого обладнання абонентів мереж рухомого (мобільного) зв'язку відповідно до чинного законодавства.

Проєкт наказу за предметом правового регулювання не матиме впливу на розвиток регіонів, територіальних громад, ринок праці, громадське здоров'я, екологію та навколишнє природне середовище, інші сфери суспільних відносин.

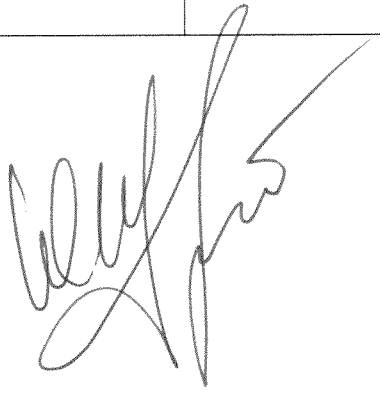
Проєкт наказу матиме вплив на ринкове середовище, забезпечення прав та інтересів суб'єктів господарювання.

Вплив на інтереси заінтересованих сторін:

Заінтересована сторона	Вплив реалізації акта на заінтересовану сторону	Пояснення очікуваного впливу
Споживачі телекомунікаційних послуг	Позитивний. Збереження інформації про місцезнаходження кінцевого обладнання абонентів у телекомунікаційній мережі не дасть змогу небажаним особам отримати інформацію про їхне місцезнаходження з порушенням вимог чинного законодавства України.	Наявність нормативно-правового акта забезпечить безпеку споживачів послуг рухомого (мобільного) зв'язку щодо визначення їхнього місцезнаходження, що не дасть змогу використання цій інформації особами, що мають намір застосовувати її для завдання шкоди таким споживачам
Держава	Позитивний. Безпека мереж рухомого (мобільного) зв'язку від небажаного втручання у їхню роботу та захист споживачів послуг від витоку інформації з даними про них є обов'язком держави.	Забезпечується захист телекомунікаційних ресурсів і споживачів послуг рухомого (мобільного) зв'язку від завдання матеріальних та моральних збитків.
Оператори, провайдери телекомунікацій	Позитивний. Затвердження Технічних вимог забезпечить цілі державного регулювання, а саме – підвищення безпеки мереж рухомого (мобільного) зв'язку щодо небажаного втручання у їхню роботу	З впровадженням нормативно-правового акта буде підвищена безпека мереж рухомого (мобільного) зв'язку щодо фільтрації сигнального трафіку відповідно до умов, передбачених чинним законодавством.

Голова Державної служби
спеціального зв'язку
та захисту інформації України
підполковник

«___» _____ 2021 р.



Юрій ЩИГОЛЬ

Прим. №__

ЗАТВЕРДЖУЮ
Заступник директора Департаменту
розвитку електронних комунікацій
Адміністрації Держспецзв'язку

Сергій СТАРОСТЕНКО
«30» липня 2021 року

Протокол

узгоджувальної наради щодо розгляду пропозицій та зауважень до проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку»

м. Київ **29.07.2021**

Присутні:

Грідасов О.М.	-	начальник 3 управління ДЕК Адміністрації Держспецзв'язку
Міхньов А.В.	-	заступник начальника управління – начальник 1 відділу 3 управління ДЕК Адміністрації Держспецзв'язку
Кравченко М.О.	-	головний спеціаліст 1 відділу 3 управління ДЕК Адміністрації Держспецзв'язку
Ляш Т.Г.	-	начальник науково-технічного відділу ПрАТ «Діпрозв'язок»
Щегельська Н.М.	-	старший науковий співробітник групи наукових робіт науково-технічного відділу ПрАТ «Діпрозв'язок»
Майстров О.О.	-	представник СБУ
Мартусенко Ю.О.	-	представник СБУ
Ошеров Л.М.	-	Голова Ради Української асоціації операторів зв'язку «Телас»
Нікітенко В.В.	-	помічник Голови Ради Української асоціації операторів зв'язку «Телас»
Воронцов С.Б.	-	начальник департаменту ПрАТ «ВФ Україна»
Куприков А. В.	-	інженер 2 категорії ПрАТ «ВФ Україна»
Зуєв М.О.	-	юрисконсульт ПрАТ «ВФ Україна»
Сегеда А.О.	-	провідний фахівець ПрАТ «ВФ Україна»
Бойко О.В.	-	директор ТОВ «ТриМоб»
Лоза О.В.	-	провідний радник з регуляторних питань та цифрових технологій ПрАТ «Київстар»
Охрущак А.В.	-	начальник відділу управління трафіком та сервісами ПрАТ «Київстар»

Булавін А.Г. - професіонал із організації інформаційної безпеки ПрАТ «Київстар»

Порядок денний:

Розгляд та обговорення пропозицій та зауважень до проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України і технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку» (далі – проєкт наказу), які надійшли від Української асоціації операторів зв'язку «Телас» (лист від 02.07.2021 № 73/21).

Відкрив **Грідасов О.М.,** повідомив, що до Адміністрації Держспецзв'язку від Української асоціації операторів зв'язку «Телас» надійшли пропозиції та зауваження до проєкту наказу. Представники ДЕК Адміністрації Держспецзв'язку спільно з фахівцями ПрАТ «Діпрозв'язок» та співробітниками СБУ опрацювали надані пропозиції та склали порівняльну таблицю з коментарями до цих пропозицій. Зазначена таблиця була надіслана учасникам наради заздалегідь. Запропонував з метою усунення розбіжностей розглянути позиції сторін та обговорити суперечливі моменти.

У процесі тривалого обговорення учасники наради погодили зняття низки пропозицій та зауважень, а саме:

- до п. 3 розділу II – щодо скорочень та позначень GSM, HLR і SM;
- до п. 2 розділу III – щодо коригування змісту та розташування положень абзаців 1 та 2 (щодо «SMS Home Routing»);
- до п. 2 розділу IV – щодо виключення абзацу 4;
- до п. 1 розділу V – щодо необхідності зазначення версій документів GSMA;

Учасниками наради було погоджено врахування низки пропозицій і зауважень, а саме:

- до п. 1 розділу II – щодо визначення терміну SMS-маршрутизатор;
- до п. 1 розділу III – щодо виключення словосполучення «в точках взаємоз'єднання телекомунікаційних мереж»;
- до п. 2 розділу III – щодо коригування змісту положень абзаців 3 та 4 (щодо відсутності терміну SMS-маршрутизатор);
- до п. 1 розділу IV – щодо коригування змісту положень абзацу 3 (щодо сигнального трафіку);
- до п. 3 розділу IV – щодо коригування змісту положень абзацу 1 (щодо виключення словосполучення «отримання інформації про якість роботи мережі,») та редакційна правка абзацу 3 («файл» замінено на «звіт»)

У ході наради було визначено, що потребують додаткового опрацювання положення:

- абзаців 2, 4, 5, 6, 7 і 8 пункту 1 розділу IV;
- абзацу 2 пункту 3 розділу IV;
- абзацу 3 пункту 3 розділу V;
- абзацу 5 пункту 4 розділу V;
- абзацу 4 пункту 4 розділу VI;

- останнього абзацу пункту 4 розділу VI;
- останнього абзацу пункту 5 розділу VI.

Детальні матеріали за результатами наради через їх значний обсяг передані учасникам наради в електронному вигляді.

В обговоренні взяли участь: Грідасов О.М., Ошеров Л.М., Ляш Т.Г., Щегельська Н.М., Бойко О.В., Воронцов С.Б., Охрущак А.В., Булавін А.Г., Мартусенко Ю.О., Майстров О.О., Міхньов А.В., Нікітенко В.В., Куприков А.В., Зуєв М.О., Сегеда А.О., Лоза О.В.

За результатами наради вирішено запропонувати:

1. Фахівцям ПрАТ «Діпрозв'язок», які виконували науково-дослідну роботу «Розроблення проєкту Технічних вимог до маршрутизації, оброблення та фільтрації сигнального обміну в мережах рухомого (мобільного) зв'язку України», разом із представниками СБУ, з урахуванням висловлених учасниками наради додаткових зауважень, доопрацювати питання, які не були узгоджені, та передати пропозиції до Адміністрації Держспецзв'язку.
2. Адміністрації Держспецзв'язку:
- узагальнити пропозиції та надіслати до Асоціації «Телас» для остаточного узгодження;
- у разі необхідності організувати проведення додаткової узгоджувальної наради.

Протокол вела Кравченко М.О.

16/03/01-1202

30.01.2024

Прим. № 1

ЗАТВЕРДЖУЮ
Директор Департаменту
розвитку електронних комунікацій
Адміністрації Держспецзв'язку

Василь МЕКЕНЧЕНКО

«08» жовтня 2021 року

Протокол

узгоджувальної наради щодо розгляду пропозицій та зауважень до проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України та технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку».

м. Київ **06.10.2021**

Присутні:

Мекенченко В.В.	-	директор ДЕК Адміністрації Держспецзв'язку
Старостенко С.О.	-	заступник директора ДЕК Адміністрації Держспецзв'язку
Грідасов О.М.	-	начальник 3 управління ДЕК Адміністрації Держспецзв'язку
Міхньов А.В.	-	заступник начальника управління – начальник 1 відділу 3 управління ДЕК Адміністрації Держспецзв'язку
Кравченко М.О.	-	головний спеціаліст 1 відділу 3 управління ДЕК Адміністрації Держспецзв'язку
Русінов С.Ю.	-	провідний консультант 1 відділу 3 управління ДЕК Адміністрації Держспецзв'язку
Щегельська Н.М.	-	старший науковий співробітник групи наукових робіт науково-технічного відділу ПрАТ «Діпрозв'язок»
Мартусенко Ю.О.	-	представник СБУ
Соболєв А.М.	-	представник СБУ
Ошеров Л.М.	-	Голова Ради Української асоціації операторів зв'язку «ТЕЛАС»
Нікітенко В.В.	-	помічник Голови Ради Української асоціації операторів зв'язку «ТЕЛАС»
Воронцов С.Б.	-	начальник департаменту ПрАТ «ВФ Україна»
Куроєдов Т.	-	експерт з питань безпеки ПрАТ «ВФ Україна»
Зуєв М.	-	юрисконсульт ПрАТ «ВФ Україна»
Сегеда А.	-	провідний фахівець ПрАТ «ВФ Україна»

Захаров Р.	-	начальник відділу ПрАТ «ВФ Україна»
Бойко О.В.	-	директор ТОВ «ТриМоб»
Дунаєвський К.В.	-	старший спеціаліст ТОВ «ТриМоб»
Лоза О.В.	-	провідний радник з регуляторних питань та цифрових технологій ПрАТ «Київстар»
Охрущак А.В.	-	начальник відділу управління трафіком та сервісами ПрАТ «Київстар»
Овчиннікова С.Г.	-	провідний юрисконсульт з регуляторних відносин ТОВ «лайфселл»

Порядок денний:

Розгляд та обговорення пропозицій до проєкту наказу Адміністрації Держспецзв'язку «Про затвердження Технічних вимог до мереж рухомого (мобільного) зв'язку України та технічних засобів телекомунікацій щодо моніторингу та фільтрації трафіку», опрацьованих за результатами узгоджувальної наради щодо розгляду пропозицій та зауважень до проєкту наказу Адміністрації Держспецзв'язку, яка відбувалась 29.07.2021.

Відкрив **Грідасов О.М.**, повідомив, що відповідно до рішення засідання узгоджувальної наради щодо розгляду пропозицій та зауважень до проєкту наказу, яка відбувалась 29.07.2021, фахівцями ПрАТ «Діпрозв'язок», які виконували науково-дослідну роботу «Розроблення проєкту Технічних вимог до маршрутизації, оброблення та фільтрації сигнального обміну в мережах рухомого (мобільного) зв'язку України» разом із представникам СБУ було доопрацьовано спірні питання та передані пропозиції до Адміністрації Держспецзв'язку. Фахівці Адміністрації Держспецзв'язку узагальнили пропозиції та ознайомили з результатами Асоціацію «Телас» у робочому порядку.

У процесі тривалого обговорення учасники наради погодили:

- доповнення пункту 1 розділу II таким терміном і визначенням поняття: «сигнальний трафік – сукупність інформаційних сигналів службової інформації, що передаються телекомунікаційною мережею за визначений інтервал часу»;

- коригування формулювання пункту 1 розділу III, виклавши його в редакції: «1. Для запобігання несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж необхідно застосовувати моніторинг та фільтрацію сигнального трафіку міжмережевого обміну.»;

- коригування формулювання пункту 2 розділу III, виклавши його в редакції: «2. Для забезпечення можливості аналізу, встановлення походження (джерела) підозрілої/шкідливої активності та планування заходів реагування на виявлені атаки необхідно накопичувати та зберігати сигнальний трафік міжмережевого обміну за останні 7 діб.»;

- коригування назви розділу IV, виклавши її в редакції: «IV. Загальні технічні вимоги до технічних засобів телекомунікацій, що здійснюють моніторинг і фільтрацію сигнального трафіку»;

- коригування формулювання абзацу 4 пункту 1 розділу IV, виклавши його в редакції: «враховувати всі існуючі маршрути сигнального трафіку міжмережевого обміну;»;

- коригування формулювання абзацу 5 пункту 1 розділу IV, виклавши його в редакції: «виявляти підозрілу/шкідливу активність та перешкоджати несанкціонованому втручанню в роботу та/або використанню телекомунікаційних мереж під час міжмережевого обміну сигнальним трафіком;»;

- коригування формулювання абзацу 1 пункту 3 розділу IV, виклавши його в редакції: «3. Технічні засоби телекомунікацій, що здійснюють моніторинг і фільтрацію трафіку, повинні мати можливість накопичувати та зберігати статистичні дані для аналізу проблем, виявлення та аналізу підозрілої/шкідливої активності, для можливості з'ясування причин і походження підозрілого міжмережевого сигнального трафіку та пошуку можливих нових атак.»;

- коригування формулювання абзацу 3 пункту 3 розділу V, виклавши його в редакції: «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 у національному 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.»;

- виключення абзацу 4 пункту 4 розділу VI;

- коригування формулювання останнього абзацу пункту 4 розділу VI, виклавши його в редакції: «Фільтрація на основі аналізу IMSI та MSISDN може поєднуватися з фільтрацією за форматом нижнього шару та з фільтрацією категорії 1.»;

- коригування формулювання останнього абзацу пункту 5 розділу VI, виклавши його в редакції: «Технічні засоби телекомунікацій, мають здійснювати моніторинг та, за умови технічної можливості, блокування 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).».

У ході наради було визначено, що потребують додаткового опрацювання положення:

- абзацу 2 пункту 1 розділу IV, зокрема в формулюванні абзацу «мати змогу відстежувати весь сигнальний трафік, який необхідно моніторити та фільтрувати, а саме міжнародний та національний міжмережевий обмін, ***в тому числі у точках взаємоз'єднання з іншими телекомунікаційними мережами***».

де виділена частина тексту має бути замінена на інформацію про 7 джерел отримання даних щодо моніторингу трафіку – виконавець ***Асоціація «ТЕЛАС»***;

- абзаців 6–8 пункту 1 розділу IV про надання додаткових коментарів щодо доцільності їх застосування – виконавець ***Служба безпеки України***;

- абзацу 4 пункту 4 розділу V щодо доопрацювання абзацу з урахуванням пропозицій до розділу VI стосовно протоколу «Diameter» – виконавці ***Асоціація «ТЕЛАС»***, ***ПрАТ «Діпрозв'язок»***;

- абзацу 5 пункту 4 розділу V щодо узгодження форми викладення абзацу з двома попередніми абзацами та розкриття за текстом або у пункті 3 розділу 2 скорочення OTA SM і Silent SM – виконавці ***Асоціація «ТЕЛАС»***, ***ПрАТ «Діпрозв'язок»***;

- абзацу 3 пункту 4 розділу VI щодо узгодження формулювання абзацу з абзацом 6 і назвою таблиці 3 – виконавець ***ПрАТ «Діпрозв'язок»***.

Також необхідно визначитися з доцільністю заміни за текстом всього документа словосполучення «сигнальний трафік» на «міжмережевий сигнальний трафік» або редагування визначення цього терміну у пункті 1 розділу II – виконавець ***ПрАТ «Діпрозв'язок»***.

В обговоренні взяли участь: Грідасов О.М., Ошеров Л.М., Старостенко С.О., Щегельська Н.М., Бойко О.В., Воронцов С.Б., Охрущак А.В., Мартусенко Ю.О.

За результатами наради учасники засідання **вирішили:**

Запропонувати фахівцям Асоціація «ТЕЛАС», ПрАТ «Діпрозв'язок», Служби безпеки України до 09.10.2021 надати до ДЕК Адміністрації Держспецзв'язку пропозиції із наведених питань, які потребують доопрацювання, для формування Адміністрацією Держспецзв'язку остаточної редакції документа.

Протокол вела Марина КРАВЧЕНКО

16/03/01-1581
08.10.2021