УДК 004.056:004.775 **DOI:** 10.31673/2412-9070.2026.0245317

В. А. СТЕПАНОВ, канд. техн. наук, науковий співробітник;
ORCID: 0000-0002-5249-6883
Ю. В. ЧЕЛПАН, провідний науковий співробітник,
ORCID: 0009-0007-3540-6421
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, Київ

ОСОБЛИВОСТІ РОБОТИ ШЛЮЗОВОГО ПРИСТРОЮ МЕРЕЖНОГО КОМПЛЕКТУ В СУЧАСНИХ УМОВАХ

Стаття присвячена аналізу особливостей роботи шлюзового пристрою мережного комплекту під час автономного доступу всіх уповноважених органів до інформації в електронній комунікаційній мережі. Розроблено вимоги до його практичної реалізації в сучасних умовах. Отримані результати відповідають концептуальним наративам ETSI, мають бути враховані під час розбудови єдиної системи технічних засобів та підготовки порядку щодо перехоплення інформації в електронних комунікаційних мережах.

Ключові слова: законне перехоплення інформації, ідентифікаційна ознака, мережний комплект, об'єкт перехоплення, умовна ознака, шлюзовий пристрій.

Постановка проблеми

Заходи з перехоплення інформації в електронних комунікаційних мережах стають адекватним механізмом попередження та розслідування тяжких або особливо тяжких злочинів, а також запобігання вчиненню і припинення терористичних актів та інших посягань спеціальних служб іноземних держав, організацій. Уряди провідних країн світу та суспільство розуміють необхідність застосування цього механізму.

Зазначені заходи відбуваються у кожній окремій країні відповідно до національного законодавства та мають назву "wiretapping", "phone-tapping", "interception of information", "interception d'informations", "intercettazione di informazioni" тощо. В Україні в правовому полі перехоплення інформації (interception of information) в електронних комунікаційних мережах здійснюється уповноваженими органами під час проведення оперативно-розшукових, контррозвідувальних, розвідувальних заходів, боротьби з тероризмом та негласних слідчих (розшукових) дій.

Згідно з пунктами 2 та 3 статті 121 Закону України "Про електронні комунікації" [1] постачальник електронних комунікаційних послуг та/або мереж повинен визначити точку в електронній комунікаційній мережі та забезпечити можливість підключення до неї технічних засобів єдиної системи, що використовується всіма уповноваженими законом органами для автономного доступу до інформації у порядку, визначеному законодавством.

У статті [2] єдиною системою технічних засобів, структурна схема якої наведена на рис. 1, вважають функціональне поєднання технічних засобів управління та обробки уповноважених органів, засобів захищених електронних комунікаційних мереж та мережного комплекту (МК).

Наведена на рис. 1 структурна схема єдиної системи технічних засобів відповідає концептуальним наративам Європейського інституту телекомунікаційних стандартів (European telecommunications standards institute, ETSI) та підходу до побудови системи перехоплення інформації, визначеному у нормативному документі [3].

В єдиній системі технічних засобів МК призначений для забезпечення відбору об'єктів перехоплення інформації та передавання даних до засобів управління та обробки (LEMF) кож-

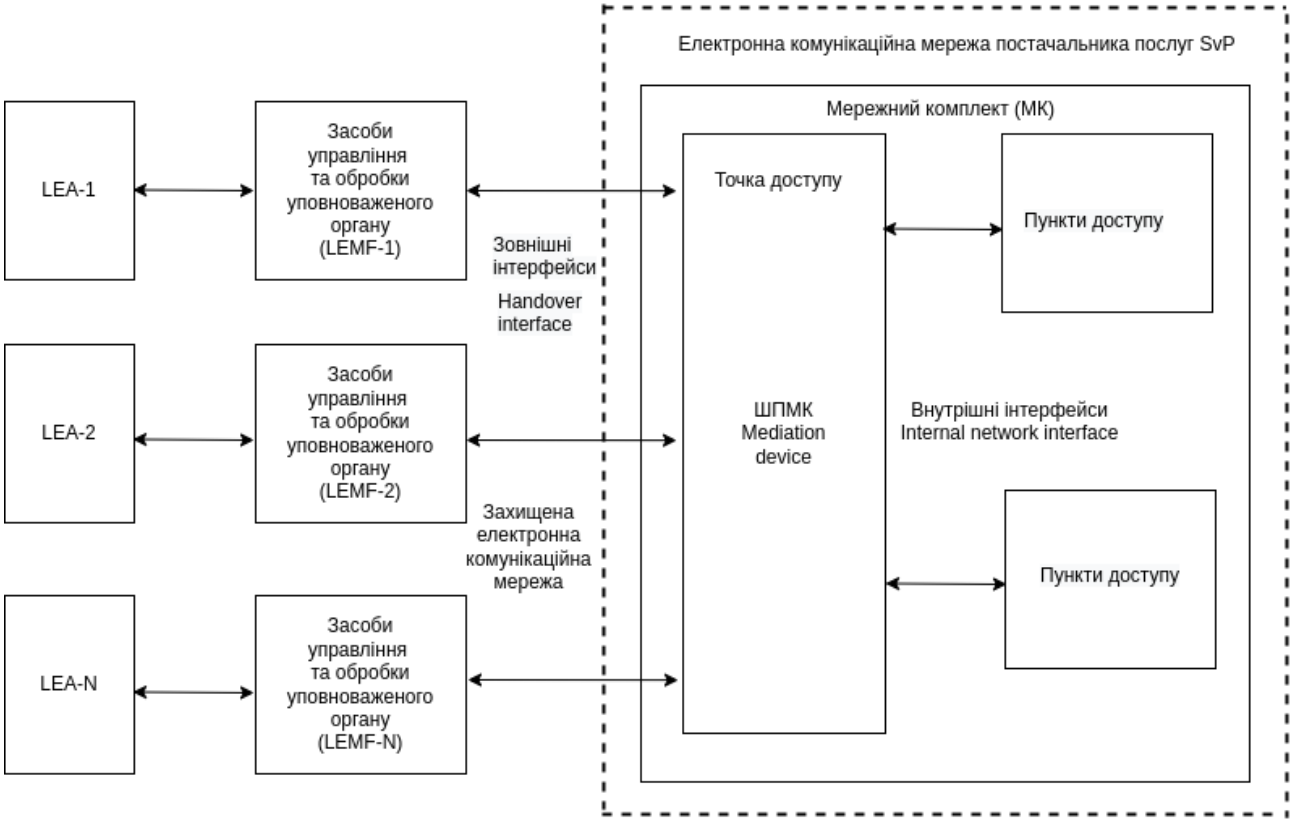

Рис. 1. Схема структурна єдиної системи технічних засобів

ного уповноваженого органу (LEA) шляхом реалізації автономного доступу до інформації цих органів. До складу МК входять пункти доступу та шлюзовий пристрій мережного комплекту (ШПМК). Пункти доступу знаходиться на сегменті електронної комунікаційної мережі постачальника послуг (SvP). Під час активного методу доступу до інформації зазначене обладнання інтегроване у пунктах доступу – засобах електронної комунікаційної мережі (комутаційному обладнанні, шлюзових вузлах, регістрах та інших). Зі свого боку, під час пасивного методу доступу до інформації пунктами доступу є мережні зонди (network probes) з оптичними відгалужувачами, що розташовані між пунктами доступу інформації на каналах електронної комунікаційної мережі постачальника послуг. На практиці часто задіюють гібридний метод доступу до інформації, як з'єднання зазначених активного та пасивного методів одночасно. Взаємодія обладнання пунктів доступу з ШПМК здійснюється з використанням "внутрішніх" інтерфейсів (internal network interface), які у кожного виробника обладнання електронних комунікаційних мереж унікальні.

У той же час взаємодія ШПМК з засобами управління та обробки кожного уповноваженого органу здійснюється з використанням "зовнішнього" стандартизованого інтерфейсу (handover interface).

На даний час фахівцями у сфері перехоплення інформації в електронних комунікаційних мережах не наведено особливості роботи ШПМК у сучасних умовах, обумовлених введенням в дію положень пунктів 2 та 3 статті 121 Закону України "Про електронні комунікації" [1] та не розроблено вимог до його практичної реалізації з врахуванням потреб всіх уповноважених органів на автономний доступ до інформації.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Аспекти зняття/перехоплення інформації (доступу до інформації) в електронних комунікаційних (телекомунікаційних) мережах загального користування України досліджували С. М. Грищенко [2], Ю. Б. Балтер [3], С. В. Кокіза [4], І. К. Стішенко [5] та інші науковці у сфері перехоплення електронних комунікацій. У більшості наукових робіт досліджувалися загальні питання перехоплення інформації у сфері електронних комунікацій (телекомунікацій). Однак, результати зазначених досліджень не дають відповіді на питання про особливості роботи ШПМК під час

автономного доступу до інформації всіх або декількох уповноважених органів та наявності вимог до практичної реалізації ШПМК у сучасних умовах.

Метою статті є аналіз особливостей роботи ШПМК під час автономного доступу до інформації всіх або декількох уповноважених органів та розробка вимог до практичної реалізації ШПМК у сучасних умовах.

Виклад основного матеріалу

У технічній специфікації ETSI TS 101 158 [6], що розроблена його технічним комітетом із законного перехоплення телекомунікацій (Technical committee lawful interception, TC LI), викладено механізм перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах. Згідно із зазначеним механізмом місце перетворення "зовнішнього" інтерфейсу (handover interface) у "внутрішні" мережні інтерфейси (internal network interface) та навпаки, а також виконання функцій управління (administration function) та посередництва (mediation function), знаходиться у домені мережного обладнання постачальників електронних комунікаційних послуг (service provider) та/або мереж (network operator). Фізична реалізація вказаного місця перетворення інтерфейсів та виконання зазначених функцій здійснюється в ШПМК (mediation device).

Виходячи з цього, у статті [7] згадане місце перетворення інтерфейсів та виконання відповідних функцій, а саме ШПМК, визначено точкою доступу (access point) до інформації в електронній комунікаційній мережі.

Умови для автономного доступу до інформації в електронній комунікаційній мережі уповноважених законодавством органів викладені у статті [8].

У нормативному документі [3] наведені загальні вимоги до ШПМК єдиної системи технічних засобів. У сучасних умовах автономного доступу до інформації в електронній комунікаційній мережі загальні вимоги потребують часткової зміни та доповнення окремими положеннями. З врахуванням термінології, прийнятої Законом України [1], в ШПМК відповідно до нормативного документа [3] мають здійснюватися в автоматичному режимі наступні події:

1) Автентифікація LEMF кожного LEA під час з'єднання з ними.
2) Взаємодія із зазначеними LEMF та обладнанням пунктів доступу.
3) Прийняття від LEMF команд управління перехопленням з ідентифікаційними ознаками об'єктів перехоплення та термінами дії перехоплення інформації, отриманими за відповідними дозволами.
4) Формування та ведення узагальненої таблиці кореляції умовних ознак LEMF з наданими у командах управління перехопленням ідентифікаційними ознаками об'єктів перехоплення та термінами дії перехоплення інформації.
5) Формування узагальненої таблиці спостереження з ідентифікаційними ознаками об'єктів перехоплення, зберігання її в незмінному вигляді протягом терміну, необхідного для здійснення перехоплення інформації (при цьому технологічно зміст зазначеної таблиці має бути доступним LEA тільки у частині, що їх стосується), передавання зазначеної таблиці до обладнання пунктів доступу.
6) Перетворення команд управління перехопленням handover interface у команди взаємодії з електронною комунікаційною мережею internal network interface.
7) Підготовка відповідей про виконання команд управління перехопленням відповідно до парадигм handover interface.
8) Прийняття від обладнання пунктів доступу за парадигмами (правилами) internal network interface відгалужених об'єктів перехоплення та повідомлень про стан мережі, їх перетворення відповідно до парадигм handover interface.
9) Передавання до LEMF через засоби їх захищених електронних комунікаційних мереж за допомогою handover interface відгалужених об'єктів перехоплення, повідомлень про стан мережі та відповідей про виконання команд управління перехопленням.
10) Формування команд зі зняття з відбору інформації за ідентифікаційними ознаками об'єктів перехоплення, термін дії яких за дозволами закінчився, та передавання їх до обладнання пунктів доступу.

11) Буферизацію об'єктів перехоплення у випадку пошкодження каналів захищених електронних комунікаційних мереж між ними та LEMF.

12) Захист від несанкціонованого доступу до інформації, яка містить ідентифікаційні ознаки об'єктів перехоплення, дані щодо взаємодії з електронною комунікаційною мережею та відгалужені об'єкти перехоплення.

Слід зазначити, що під об'єктами перехоплення розуміємо вміст сеансів зв'язку суб'єктів перехоплення (interception subject), інформацію про їх місцезнаходження та профілі послуг, що їм надаються.

Для обміну командами, повідомленнями та відповідями між LEMF та ШПМК використовують стек протоколів TCP/IP [3]. При цьому під час обміну даними функції серверу виконує ШПМК, а клієнта – зазначені технічні засоби. Обмін даними має здійснюватися наступним чином. На кожну команду від LEMF, що забезпечена умовною ознакою приналежності засобів до конкретного LEA, має бути надіслана відповідна відповідь від ШПМК. Наступну команду від LEMF надсилають тільки після отримання відповіді на попередню команду. Якщо протягом встановленого часу LEMF не отримали відповіді від ШПМК, ситуація визначається аварійною. Для передавання повідомлень, що не пов'язані з дією команд, ШПМК до LEMF повинно використовуватись окреме TCP з'єднання, яке створюється після проходження автентифікації зазначених LEMF та припиняється після розриву з'єднання. У вказаному випадку сервером також має бути ШПМК, а клієнтом – LEMF. Схожа ситуація виникає під час взаємодії ШПМК з обладнанням пунктів доступу.

У технічних засобах управління та обробки кожного уповноваженого законодавством органу формується окрема таблиця спостереження, що містить перелік ідентифікаційних ознак об'єктів перехоплення та терміни дії перехоплення за ними, що отримані за відповідними дозволами, а також режими та категорії спостереження. ШПМК виконує агрегацію інформації з команд управління перехопленням, формуючи узагальнену таблицю кореляції та відповідно до неї узагальнену таблицю спостереження з ідентифікаційними ознаками об'єктів перехоплення та термінами дії перехоплення. На обладнання пунктів доступу передаються лише актуальні записи з узагальненої таблиці спостереження. Перехоплення інформації за ідентифікаційними ознаками зберігається до завершення останнього активного терміну дії перехоплення незалежно від кількості джерел (технічних засобів управління та обробки), що його ініціювали.

Доступ до узагальненої таблиці кореляції ШПМК з технічних засобів управління та обробки кожного уповноваженого законодавством органу повинен бути строго розмежований — зміст зазначеної таблиці має бути доступним вказаним технічним засобам тільки у частині, що їх стосується. Адміністративний доступ до змісту таблиці забезпечується лише через інтерфейс управління ШПМК із багаторівневою авторизацією.

У разі, коли до ШПМК надходить одна і та сама ідентифікаційна ознака об'єкта перехоплення від декількох технічних засобів управління та обробки із різними термінами дії перехоплення, то він здійснює узгодження таких процедур. Ідентифікаційна ознака об'єкта перехоплення залишається під спостереженням до завершення останнього активного терміну, наданого будь-яким із технічних засобів управління та обробки. Зняття ідентифікаційної ознаки об'єкта перехоплення з відбору виконується лише після закінчення всіх термінів дії перехоплення або після отримання команд із зняття з відбору інформації з усіх технічних засобів управління та обробки, що ініціювали перехоплення цього об'єкта.

Трафік, що надходить до ШПМК з обладнання пунктів доступу, маркується відповідно до узагальненої таблиці спостереження. Кожному об'єкту перехоплення в ШПМК ставляться у відповідність технічні засоби управління та обробки, які ініціювали його постановку на перехоплення, та виконується маркування трафіку у вигляді службових атрибутів. У разі, коли декілька уповноважених законодавством органів мають дозволи на перехоплення одних і тих же об'єктів, ШПМК здійснює копіювання отриманих об'єктів перехоплення та направляє їх до технічних засобів управління та обробки кожного із уповноважених законодавством органів через транспортні канали окремих захищених електронних комунікаційних мереж.

Слід зазначити, якщо постачальники електронних комунікаційних послуг та/або мереж використовують кодування/шифрування трафіку електронних комунікацій та якщо кодування/шифрування не може бути знято/видалено за допомогою засобів, що є загальнодоступними у мережі під час надання послуг комунікацій, то уповноважені законодавством органи відповідно до ДСТУ ETSI TS 101 331:2021 [9] мають бути забезпечені ключами та необхідними технічними засобами, що дадуть змогу отримати з ШПМК необхідну інформацію під час здійснення пасивного методу доступу.

Висновки

Наведені вимоги до ШПМК доцільно враховувати під час розбудови єдиної системи технічних засобів, проведення його оцінки відповідності та підготовки відповідного порядку щодо перехоплення інформації в електронних комунікаційних мережах, який має бути затвердженим спільним наказом відповідних уповноважених законодавством органів (або уповноваженого законодавством органу, який в сфері перехоплення інформації координує діяльність інших уповноважених органів) та державного органу виконавчої влади, що виконує функції технічного регулювання у сфері електронних комунікацій.

Внесок авторів

Валерій СТЕПАНОВ - аналіз особливостей роботи шлюзового пристрою мережного комплекту під час автономного доступу всіх уповноважених органів до інформації в електронній комунікаційній мережі; Юрій ЧЕЛПАН - розробка вимог до практичної реалізації шлюзового пристрою мережного комплекту у сучасних умовах.

Декларація про штучний інтелект

Автор не використовував штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. Офіційний вісник України. 2021. № 6. Ст. 306.

2. Степанов В.А., Грищенко С.М. Особливості побудови системи законного перехоплення інформації з телекомунікаційних мереж. Збірник наукових праць НА СБУ. 2018. №69. С. 199-204.

3. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України. Загальні технічні вимоги: наказ Служби безпеки України і Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 31.12.2021 року № 460/781. URL: ssu.gov.ua/ uploads/ documents/ 2022/01/24/ztv-31122021.pdf (дата звернення 29.12.2025).

4. Кокіза С.В., Степанов В.А. Вимоги правоохоронних органів ЄС щодо законного перехоплення інформації в електронних комунікаційних мережах. Інформація і право. 2021. № 3 (38). С. 115-120. URL: ippi.org.ua/kokiza-sv-stepanov-va-vimogi-pravookhoronnikh-organiv-ės-shchodo-zakonnogo-perekhoplennya-informatsii (дата звернення 29.12.2025).

5. Степанов В.А., Стішенко І.К. Особливості дозволеного законом перехоплення інформації з телекомунікаційних мереж. Спеціальні телекомунікаційні системи та захист інформації. 2005. № 10. С. 76-80.

6. ETSI TS 101 158 V1.3.1 (2014-02) Telecommunications security; Lawful interception (LI);

7. Requirements for network functions (Безпека телекомунікацій; Законне перехоплення (LI); Ви-моги до мережних функцій). URL: https://www.etsi.org/deliver/etsi_ts/101100_101199/ 101158/ 01.03.01_60/ts_101158v010301p.pdf (дата звернення 29.12.2025).

8. Степанов В.А., Грищенко С.М. Точка для автономного доступу до інформації в електронній комунікаційній мережі. Інформація і право. 2024. №3(50). С. 171-176. URL: il.ippi.org.ua/article/view/311724 (дата звернення 29.12.2025).

9. Грищенко С.М., Степанов В.А. Умови автономного доступу до інформації під час зня-ття інформації з електронних комунікаційних мереж. Інформація і право. 2021. № 1(36). С. 123-127. URL: ippi.org.ua/grishchenko-sm-stepanov-va-umovi-avtonomnogo-dostupu-do-informatsii-pid-chaz-znyattya-informatsii-z (дата звернення 29.12.2025).

10. ДСТУ ETSI TS 101 331:2021 Законне перехоплення. Вимоги правоохоронних органів. Тех-нічна специфікація: наказ ДП УкрНДНЦ від 29.12.2025 № 405.

V. Stepanov, Y. Chelpan

OPERATIONAL ASPECTS OF NETWORK KIT'S GATEWAY DEVICE IN MODERN CONDITIONS

The article is devoted to analyzing operational aspects of the network kit's gateway device during autonomous access of all authorized bodies to information in the electronic communications network. The network kit's gateway device is a technical means for converting an external standardized interface into internal network interfaces and vice versa, and for performing administration and mediation functions. It is located in the telecommunications equipment domain of the electronic communications service provider and/or networks. The network kit's gateway device interacts with the technical means of administrating and processing of each lawful authorized body, as well as with the equipment for selecting objects for information interception. It is used in operating modes with active, passive, and hybrid methods of access to information. Requirements for its practical implementation in modern conditions have been developed. The network kit's gateway device should create and correct a general correlation table of technical means of administrating and processing of each lawful authorized body, with the identifying features of the interception objects and the terms of the information interception, as well as store the identifying features of interception objects in a separate surveillance table in an unchanged form for the period necessary to carry out the interception of information. The results obtained are consistent with ETSI's conceptual narratives and should be taken into account when developing a unified system of technical means and preparing procedures for intercepting information in electronic communications networks.

Keywords: lawful interception of information, identifying feature, network kit, interception object, conditional feature, gateway device.

Надійшла до редакції: 18.02.2026
Прийнята до друку: 21.04.2026
Опубліковано: 27.04.2026