УДК 343.14

СТЕПАНОВ В.А., *кандидат технічних наук,* науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0002-5249-6883.
ГРИЩЕНКО С.М., начальник підрозділу Українського науково- дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0002-5922-280X.

ТОЧКА ДЛЯ АВТОНОМНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В ЕЛЕКТРОННІЙ КОМУНІКАЦІЙНІЙ МЕРЕЖІ

DOI...

Анотація. *Стаття присвячена проблемі визначення поняття "точка для автономного доступу до інформації в електронній комунікаційній мережі", введеного вжиток Законом України "Про електронні комунікації". Зазначену точку визначає постачальник електронних комунікаційних послуг та/або мереж і забезпечує можливість підключення до неї технічних засобів єдиної системи, що використовується всіма уповноваженими законодавством органами для перехоплення/зняття інформації з електронних комунікаційних мереж.*

Ключові слова: *зняття інформації, точка для автономного доступу, електронна комунікаційна мережа, єдина система технічних засобів.*

Summary. *The article is devoted to the problem of determination of concept of "point for autonomous access to information in the electronic communications network", introduced in everyday life by the Law of Ukraine "On electronic communications". The specified point for such access is determined by the provider of electronic communications services and/or networks. It provides the possibility at the point for autonomous access to information to connect the technical means of a united system that is used by all statutory authorities to intercept/obtain information from electronic communications networks.*

Keywords: *interception of information, point for autonomous access, electronic communication network, united system of technical means.*

Постановка проблеми. У зв'язку з прийняттям Закону України "Про електронні комунікації" [1] актуальним стає вирішення низки питань, пов'язаних з доступом уповноважених законом органів до інформації в електронній комунікаційній мережі. В пунктах 2 та 3 статті 121 зазначеного Закону [1] зазнчено, що 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. На даний час законодавцями та науковцями не визначено поняття "точка для автономного доступу до інформації в електронній комунікаційній мережі" та не розроблено вимог до її практичної реалізації з врахуванням потреб всіх уповноважених органів на зняття інформації з електронних комунікаційних мереж.

Результати аналізу наукових публікацій. Аспекти доступу (зняття/ перехоплення) до інформації в телекомунікаційних мережах загального користування України досліджували Ю.Б. Балтер та О.М. Мошков [2], С.В. Кокіза [3], А.В. Манжай

та С.В. Пеньков [4], І.К. Стішенко [5], інші науковці профільних установ та фахівці уповноважених органів. У більшості наукових робіт досліджувались теоретичні та прикладні проблеми побудови систем технічних засобів. Однак результати зазначених досліджень не дають відповіді на питання щодо визначення введеного у вжиток поняття "точка для автономного доступу до інформації в електронній комунікаційній мережі" та наявності вимог до зазначеної точки відповідно до положень Закону [1]. В іншій статті викладено умови для автономного доступу уповноважених законодавством органів до інформації в електронній комунікаційній мережі [7].

Метою статті є визначення поняття "точка для автономного доступу до інформації в електронній комунікаційній мережі" та розробка вимог до її практичної реалізації з метою підключення до неї технічних засобів єдиної системи, що використовується всіма уповноваженими законом органами для зняття інформації з електронних комунікаційних мереж під час проведення оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій.

Виклад основного матеріалу. В технічній специфікації Європейського інституту телекомунікаційних стандартів ETSI TS 101 158 [6], що розроблена його технічним комітетом з законного перехоплення телекомунікацій (TC LI), викладено механізм перехоплення інформації в телекомунікаційних мережах. Згідно з зазначеним механізмом технічні засоби уповноважених законодавством органів(LEMF) взаємодіють з електронним комунікаційним (телекомунікаційним) обладнанням постачальників електронних комунікаційних послуг та/або мереж (операторів мережі NWOs, провайдерів послуг SvPs та провайдерів доступу APs) за допомогою функцій управління (administration function) та посередництва (mediation function) через інтерфейс передавання (handover interface) та внутрішній мережевій інтерфейс (internal network interface). Місце перетворення інтерфейсу передавання в внутрішній мережний інтерфейс та навпаки, а також виконання функцій управління та посередництва, знаходиться в домені телекомунікаційного обладнання постачальників електронних комунікаційних послуг та/або мереж. Тому фізична реалізація вказаного місця перетворення інтерфейсів та виконання зазначених функцій здійснюється в телекомунікаційному обладнанні (наприклад, шлюзовому пристрої, спеціалізованому сервері тощо).

Виходячи з цього, на думку авторів, саме згадане місце перетворення інтерфейсів та виконання відповідних функцій і є точкою доступу (access point) до інформації в електронній комунікаційній мережі.

Розглянемо вимоги до зазначеної вище точки доступу.

В нормативному документі [2] наведені вимоги до шлюзів мережного комплекту системи перехоплення електронних комунікацій. В умовах автономного доступу до інформації в електронній комунікаційній мережі та з врахуванням термінології, прийнятої Законом України [1], в точці доступу мають здійснюватися в автоматичному режимі наступні події:

1) взаємодія з технічними засобами кожного уповноваженого законодавством органу та обладнанням відбору об'єктів перехоплення інформації;

2) автентифікація технічних засобів кожного уповноваженого законодавством органу під час з'єднання з нею;

3) перетворення команд управління перехопленням в інтерфейсі передавання в команди взаємодії з електронною комунікаційною мережею в внутрішньому мережевому інтерфейсі;

4) прийняття від зазначеного обладнання відбору за парадигмами (правилами) внутрішнього мережевого інтерфейсу відгалужених об'єктів перехоплення та повідомлень про стан мережі, їх перетворення відповідно до парадигм інтерфейсу передавання;

5) формування відповідей про виконання команд управління перехопленням;

6) передавання відгалужених об'єктів перехоплення, повідомлень про стан мережі та відповідей про виконання команд управління перехопленням до технічних засобів кожного уповноваженого законодавством органу за допомогою інтерфейсу передавання;

7) зберігання ознак (ідентифікаторів) об'єктів перехоплення в окремій таблиці кожного уповноваженого органу в незмінному вигляді протягом терміну, необхідного для здійснення перехоплення (при цьому технологічно зміст зазначеної таблиці не повинен бути доступним іншим уповноваженим органам);

8) захист від несанкціонованого доступу до інформації, яка містить ознаки об'єктів перехоплення, інформацію щодо взаємодії з електронною комунікаційною мережею та відгалужені об'єкти перехоплення;

9) буферизацію (тимчасове зберігання інформації для запобігання її втраті) об'єктів перехоплення у випадку пошкодження каналів захищених електронних комунікаційних мереж між нею (точкою доступу) та технічними засобами кожного уповноваженого законодавством органу.

Слід зазначити, що під об'єктами перехоплення автори розуміють вміст сеансів зв'язку абонентів спостереження (суб'єктів перехоплення), інформацію про їх місцезнаходження та профілі послуг, що їм надаються.

Взаємодія технічних засобів відбору електронного комунікаційного обладнання постачальників електронних комунікаційних послуг та/або мереж з зазначеною точкою доступу здійснюється з використанням внутрішнього мережного інтерфейсу, який у кожного виробника обладнання електронних комунікаційних мереж унікальний, та інтерфейсів на основі стандартизованих протоколів СКС-7, DIAMETER, SIP тощо. Взаємодія точки доступу з технічними засобами кожного уповноваженого законодавством органу здійснюється з використанням стандартизованого інтерфейсу передавання [7].

Для обміну командами, повідомленнями та відповідями між технічними засобами кожного уповноваженого законодавством органу та точкою доступу пропонується використовувати стек протоколів TCP/IP. При цьому під час обміну даними функції серверу виконує точка доступу, а клієнта – зазначені технічні засоби. Обмін даними має здійснюватися наступним чином. На кожну команду від технічних засобів, що забезпечена міткою приналежності засобів до конкретного уповноваженого органу, має бути надіслана відповідна відповідь від точки доступу. Наступну команду від технічних засобів надсилають тільки після отримання відповіді на попередню команду. Якщо протягом встановленого часу технічні засоби не отримали відповіді від точки доступу, ситуація визначається аварійною. Для передавання повідомлень, що не пов'язані з дію команд, від точки доступу до технічних засобів повинно використовуватись окреме TCP- з'єднання, яке створюється після проходження автентифікації технічних засобів та припиняється після розриву з'єднання. У вказаному випадку сервером також має бути точка доступу, а клієнтом – технічні засоби. Схожа ситуація виникає під час взаємодії точки доступу з технічними засобами відбору електронного комунікаційного обладнання. Точка доступу виконує функції конвертору інтерфейсів з можливістю у разі необхідності буферизації інформації.

До того ж, відповідно до Директиви Ради Європейського Союзу від 20 червня 2001 року про оперативні запити правоохоронних органів стосовно громадських

телекомунікаційних мереж та послуг (ENFOPOL) [8] та Резолюції Ради Європейського Союзу від 17 січня 1995 року № 96/C329/01 про законне перехоплення телекомунікацій [9] уповноважені законодавством органі потребують, а постачальники електронних комунікаційних послуг та/або мереж шляхом їх конфігурування та налаштування забезпечують в точці доступу в електронній комунікаційній мережі наявність наступної інформації:

1) про усіх суб'єктів перехоплення, які постійно чи тимчасово користуються послугами електронної комунікаційної (телекомунікаційної) мережі;

2) про зв'язок, коли суб'єкт перехоплення використовує функцію для його спрямування (переадресації) до інших електронних комунікаційних (телекомунікаційних) послуг чи терміналів, включаючи зв'язок, який до свого завершення перетинає більш ніж одну мережу або обробляється більш ніж одним постачальником електронних комунікаційних послуг та/або мереж;

3) про всі застосовані щодо суб'єкта перехоплення електронні комунікаційні (телекомунікаційні) процедури внаслідок перехоплення його зв'язку, якщо вони зберігаються постачальниками електронних комунікаційних послуг та/або мереж відповідно до вимог національного законодавства;

4) про якомога точніше географічне місцезнаходження, відоме для мережі мобільного зв'язку;

5) щодо особливих послуг, які використовуються суб'єктом перехоплення, та технічних параметрів задіяних видів зв'язку;

6) щодо зв'язку від цільової служби у спосіб, який передбачає точну кореляцію службової інформації, пов'язаної із зв'язком, із змістом самого зв'язку;

7) в узгодженому форматі та в відкритому вигляді щодо перехопленого зв'язку.

При цьому, якщо постачальники електронних комунікаційних послуг та/або мереж використовують код, скорочення чи шифрування трафіку електронних комунікацій та якщо кодування/шифрування не може бути знято/видалено за допомогою засобів, що є загальнодоступними в мережі під час надання послуг зв'язку, то уповноважені законодавством органи відповідно до ДСТУ ETSI TS 101 331:2021 [10] мають бути забезпечені ключами та необхідними технічними засобами, що дадуть змогу отримати доступ до інформації.

З метою надання визначення поняття "точка для автономного доступу до інформації в електронній комунікаційній мережі" розглянемо ознаки, що характерні його складовим частинам.

Відповідно до статті 2 Директиви Європейського Парламенту і Ради (ЄС) [11] під "*доступом*" слід вважати забезпечення доступності засобів або комунікаційних послуг іншим суб'єктам господарювання на визначених умовах на виключній або невиключній основі, яка серед іншого охоплює доступ до мереж фіксованого, мобільного зв'язку та послуг віртуальних мереж, а також доступ до елементів мережі та пов'язаних засобів. В статті [7] під "*доступом до інформації*" в контексті зняття інформації з електронних комунікаційних мереж вважають не тільки можливість отримання інформації, а також її фіксація та оброблення.

До того ж в п. 1.2 Правил взаємоз'єднання телекомунікаційних мереж загального користування, затверджених Рішенням Національної комісії України з питань регулювання зв'язку від 08.12.05 р. № 155 [12], під поняттям "*точка взаємоз'єднання*" розуміють місце безпосереднього з'єднання між технічними засобами ініціатора та постачальника, яке призначене для взаємного обміну трафіком, пропуску транзитного

трафіку від/до мереж інших операторів. Разом з цим в п. 4 розділу 1 Правил з пожежного спостерігання, затверджених наказом Міністерства внутрішніх справ України від 30.03.15 р. № 349 [13], та у розділі 2 Правил з пожежного спостерігання, затверджених наказом Міністерства надзвичайних ситуацій України від 07.04.11 р. № 351 [14], надається визначення поняття "*точка доступу*" відповідно, як IP-адреса обладнання, яке розташоване в оперативно-диспетчерській службі та забезпечує приймання сигналів…, та як устаткування приймання сигналів пожежної тривоги, яке розташоване в оперативно-диспетчерській службі та забезпечує з'єднання… .

Термін "*автономність*" відповідно до [15] має кілька значень. Одне із значень – незалежність від чого-небудь.

Виходячи із викладеного, за результатами дослідження різних систем законного перехоплення інформації іноземного виробництва та на основі досвіду з унормування вимог до технічних засобів для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій у електронних комунікаційних (телекомунікаційних) мережах загального користування України та з їх створення, пропонуємо вважати, що *точка для автономного доступу до інформації в електронній комунікаційній мережі* – електронне комунікаційне обладнання, в якому здійснюється приймання інформації від технічних засобів кожного уповноваженого законодавством органу і її передавання до технічних засобів відбору електронного комунікаційного обладнання постачальників електронних комунікаційних послуг та/або мереж та навпаки, а також перетворення команд управління перехоплення в інтерфейсі передавання в команди взаємодії з електронною комунікаційною мережею в внутрішньому мережевому інтерфейсі під час виконання функцій управління та посередництва, формування відповідей про виконання команд управління, перетворення відгалужених об'єктів перехоплення та повідомлень про стан мережі в внутрішньому мережевому інтерфейсі в відповідні дані інтерфейсу передавання під час виконання функцій посередництва.

Висновки.

Визначене поняття "точка для автономного доступу до інформації в електронній комунікаційній мережі" відповідає основним концептуальним вимогам технічного комітету з законного перехоплення телекомунікацій (TC LI) Європейського інституту телекомунікаційних стандартів (ETSI) та може бути рекомендовано для врахування в роботі фахівцям та науковцям, задіяним у заходах з перехоплення/зняття інформації з електронних комунікаційних мереж, а також у діях з оцінки відповідності зазначеної точки доступу.

Наведені вимоги до точки для автономного доступу до інформації доцільно враховувати під час розбудови єдиної системи технічних засобів, проведенні оцінки відповідності зазначеної точки доступу та підготовки відповідного порядку щодо зняття інформації з електронних комунікаційних мереж, який має бути затверджено спільним наказом відповідних уповноважених законодавством органів та державного органу виконавчої влади, що виконує функції технічного регулювання у сфері електронних комунікацій.

Використана література

1. Про електронні комунікації: Закон України від 16.12.20 р. № 1089-IX. *Офіційний вісник України*. 2021. № 6. Ст. 306. – (20.08.2024).

2. 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 31.12.21 р. № 460/781.

3. Кокіза С.В., Степанов В.А. Вимоги правоохоронних органів ЄС щодо законного перехоплення інформації в електронних комунікаційних мережах. *Інформація і право*. № 3 (38)/ 2021. С. 115-120. URL: ippi.org.ua/kokiza-sv-stepanov-va-vimogi-pravookhoronnikh-organiv-єs-shch odo-zakonnogo-perekhoplennya-informatsii (дата звернення: 20.08.2024).

4. Манжай А.В., Пеньков С.В. Стандартизация в сфере законного перехвата телекомуникаций. *Legia si Vista*. 2017. № 5/2. С. 86-89. URL: https://www.researchgate.net/profile/ Oleksandr_Manzhai/publication/337991533_Standartizatsiia_v_Sfere_Zakonnogo_Perekhvata_Telekomu nikatsii_Standardization_in_the_Field_of_Lawful_Interception_of_Telecommunications/links/5df921109 2851c8364854202/Standartizatsiia-v-Sfere-Zakonnogo-Perekhvata-Telekommunikatsii-Standardization- in-the-Field-of-Lawful-Interception-of-Telecommunications.pdf (дата звернення: 20.08.2024).

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); Requirements for network functions (Безпека телекомунікацій; Законне перехоплення (LI); Вимоги до мережних функцій). URL: https://www.etsi.org/deliver/etsi_ts/101100_101199/101158/ 01.03.01_60/ts_101158v010301p.pdf (дата звернення: 20.08.2024).

7. Грищенко С.М., Степанов В.А. Умови автономного доступу до інформації під час зняття інформації з електронних комунікаційних мереж. *Інформація і право*. № 1(36)/2021. С. 123-127. URL: ippi.org.ua/grishchenko-sm-stepanov-va-umovi-avtonomnogo-dostupu-do-informatsii- pid-chaz-znyattya-informatsii-z (дата звернення: 13.08.2024).

8. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL): Директива Ради Європейського Союзу від 20 червня 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_234#Text (дата звернення: 20.08.2024).

9. Про законне перехоплення телекомунікацій : Резолюції Ради Європейського Союзу від 17 січня 1995 року № 96/С329/01. URL: https://zakon.rada.gov.ua/laws/show/994_235#Text (дата звернення: 20.08.2024).

10. ДСТУ ETSI TS 101 331:2021 Законне перехоплення. Вимоги правоохоронних органів. Технічна специфікація: наказ ДП УкрНДНЦ від 05.11.21 р. № 405. URL: https://zakon.rada.gov. ua/rada/show/v0405774-21#Text (дата звернення: 20.08.2024).

11. Про запровадження Європейського кодексу електронних комунікацій: Директива Європейського Парламенту і Ради ЄС від 11 грудня 2018 року № 2018/1972. URL: https://zakon. rada.gov.ua/laws/show/984_013-18#Text (дата звернення: 20.08.2024).

12. Правила взаємоз'єднання телекомунікаційних мереж загального користування: рішення Національної комісії України з питань регулювання зв'язку від 08.12.05 р. № 155. URL: https://zakononline.com.ua/documents/show/274175_564459 (дата звернення: 20.08.2024).

13. Правила з пожежного спостерігання: наказ Міністерства внутрішніх справ України від 30.03.15 р. № 349. URL: https://zakon.rada.gov.ua/laws/show/z0920-15#Text (дата звернення: 20.08.2024).

14. Правила з пожежного спостерігання: наказ Міністерства надзвичайних ситуацій України від 07.04.11 р. № 351. URL: https://zakon.rada.gov.ua/laws/show/z0744-11#Text (дата звернення: 20.08.2024).

15. Автономність. URL: https://uk.wikipedia.org/wiki/Автономність (дата звернення: 20.08.2024).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~