ІНФОРМАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

УДК 343.14
DOI: 10.31733/2078-3566-2021-4-280-284

Валерій СТЕПАНОВ©
кандидат технічних наук
Сергій ГРИЩЕНКО©
начальник центру

(Український науково-дослідний інститут спеціальної техніки та судових експертиз СБУ)

ТЕХНІЧНІ ЗАСОБИ ДЛЯ НЕГЛАСНОГО ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

У статті наведено повну інформацію, яку мають отримувати уповноважені органи під час зняття інформації з електронних комунікаційних мереж, відповідно до вимог технічного комітету законного перехоплення Європейського інституту телекомунікаційних стандартів. Узагальнено ознаки технічних засобів для негласного зняття інформації з електронних комунікаційних мереж, що викладені в нормативно-правових актах та нормативних документах України.

Визначено поняття «технічні засоби для негласного зняття інформації з електронних комунікаційних мереж» та наведено поділ зазначених засобів на типи. Встановлено, що засоби управління та обробки єдиної системи технічних засобів взаємодіють за стандартизованим інтерфейсам із технічними засобами електронних комунікаційних мереж.

Зазначено, що стаціонарні комплекси активної дії для зняття інформації з електронних комунікаційних мереж відокремлюють/сегрегують інформацію щодо обміну даними між елементами мережі. Зазначено, що стаціонарні системи пасивної дії для зняття інформації з електронних комунікаційних мереж перехоплюють обмін даними між елементами мережевої інфраструктури.

***Ключові слова**: технічні засоби, негласне зняття інформації, електронна комунікаційна мережа, поділ на типи.*

Постановка проблеми. У зв'язку з прийняттям законів України «Про електронні комунікації» [1] та «Про розвідку» [2] постає актуальність питання подальшого дослідження спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації (далі – СТЗ) у контексті заходів зі зняття інформації з електронних комунікаційних (телекомунікаційних) мереж. Зазначені заходи здійснюються уповноваженими органами під час проведення оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій. Відповідно до Постанови Кабінету Міністрів України [3] одним із різновидів СТЗ є технічні засоби для негласного зняття інформації з телекомунікаційних мереж.

Згідно із Законом України [1] з 01.01.2022 у сфері телекомунікаційної діяльності встановлюються зміни в термінології. Так, наприклад, замість понять «телекомунікація», «телекомунікаційна мережа», «оператор телекомунікацій» вводяться відповідні поняття «електронна комунікація», «електронна комунікаційна мережа», «постачальник послуг». Тому в подальшому викладі матеріалів статті будемо надавати в термінології, що прийнята Законом України [1].

На жаль, у законодавстві та в опублікованих результатах наукових і прикладних досліджень на даний час не визначено поняття «технічні засоби для негласного зняття

icte@ssu.gov.ua

інформації з електронних комунікаційних мереж» та не наведено поділ зазначених засобів на типи.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Технічні засоби для зняття інформації з телекомунікаційних мереж України досліджували Ю. Балтер [4], А. Манжай [5], Ю. Парасіч [6], С. Пеньков [5], І. Стішенко [7] та інші.

У більшості наукових праць та прикладних робіт досліджувались теоретичні та нормативні аспекти побудові наведених технічних засобів. Праці зазначених вище науковців прикладних установ та роботи фахівців уповноважених органів, безсумнівно, є вагомим внеском у дослідження вказаних проблемних питань. Однак, на думку авторів, вирішення зазначених проблемних питань на даний час не завершено. Отримані результати потребують усебічного осмислення, систематизації та подальшого удосконалення науковцями та фахівцями різних профілів знань в єдиному контексті із застосуванням як єдиної системи технічних засобів відповідно до Закону України [1], так і вузькопрофільних технічних засобів зняття інформації з електронних комунікаційних мереж.

Метою статті є визначення поняття «технічні засоби для негласного зняття інформації з електронних комунікаційних мереж» та наведення поділу зазначених засобів на типи.

Виклад основного матеріалу. З метою визначення поняття «технічні засоби для негласного зняття інформації з електронних комунікаційних мереж» спочатку розглянемо ознаки зазначених технічних засобів, що наведені у визначеннях, та порядку їх застосування. Сьогодні згадка про окрему негласну слідчу (розшукову) дію зі зняття інформації з транспортних телекомунікаційних мереж, пов'язану з втручанням у приватне спілкування, наведена у Кримінальному процесуальному кодексі України [8], у Коментарі до нього [9], у проекті Закону України «Про оперативно-розшукову діяльність» [10], в Інструкції [11], у Загальних технічних вимогах [4] та інших документах.

У статті 263 Кримінального процесуального кодексу України [8] наведені такі ознаки зазначеного заходу:

1) зняття інформації з транспортних телекомунікаційних мереж проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації;

2) в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування мають бути зазначені ідентифікаційні ознаки, що дозволять унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування;

3) зняття інформації з транспортних телекомунікаційних мереж полягає у проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, що передається особою та має значення для досудового розслідування, а також одержанні, перетворенні та фіксації різних видів сигналів, що передаються каналами зв'язку.

В. Тертишник у Коментарі [9], аналізуючи поняття «зняття інформації з транспортних телекомунікаційних мереж», виділяє встановлені слідчим під час досудового розслідування такі ідентифікаційні ознаки, що дозволяють унікально ідентифікувати:

1) абонента спостереження (споживача телекомунікаційних послуг), тобто його абонентський номер (сукупність цифрових знаків для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі);

2) транспортну телекомунікаційну мережу, тобто який оператор телекомунікацій має право на технічне обслуговування та експлуатацію телекомунікаційної мережі, до якої належить номер абонента спостереження;

3) кінцеве обладнання – його ідентифікатор для розпізнання в телекомунікаційній мережі, що надав цьому кінцевому обладнанню виробник (наприклад, код IMEI мобільного телефону, USB-модему) або адресу точки підключення кінцевого обладнання для публічних фіксованих проводових мереж телекомунікацій.

У проекті Закону [10] зазначено, що зняття інформації з каналів зв'язку (транспортних телекомунікаційних мереж) – «оперативно-розшуковий захід, що полягає в негласному одержанні, фіксації із застосуванням відповідних технічних засобів, зокрема встановлених на транспортних телекомунікаційних мережах, обробці та відтворенні, у тому числі придатних для автоматизованої обробки засобами обчислювальної техніки, різних

видів сигналів, що передаються через будь-яку контрольовану мережу передачі даних».

Дещо інший підхід закладено в Інструкції [11], де під зняттям інформації з транспортних телекомунікаційних мереж розуміють захід, що полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, що передається особою, а також одержанні, перетворенні та фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду). Зазначене зняття інформації поділяється на:

1) контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), що передаються телефонним каналом зв'язку, що контролюється;

2) зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні та фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, що передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

Тобто до дій з одержання, фіксації, обробки та відтворення додаються дії зі спостереження, відбору та перетворення, але не названими залишаються дії з розпізнавання та відгалуження.

Автори розглянутих документів не зазначають у них повного обсягу інформації, яку мають отримувати уповноважені органи під час зняття інформації з електронних комунікаційних (телекомунікаційних, у тому числі транспортних телекомунікаційних мереж). Окрім різних видів сигналів, що передаються через будь-яку мережу передачі даних, у тому числі мережу Інтернет, різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду), змісту телефонних розмов, сигналів SMS, MMS, факсимільного та модемного зв'язку, як зазначено вище, уповноважені органи мають отримувати відповідно до Загальних технічних вимог [4] також дані щодо місцезнаходження абонентів спостереження та профіль послуг, що їм надаються. Ці аспекти відображені в концептуальних вимогах технічного комітету «Законне перехоплення телекомунікацій» (TC LI) Європейського інституту телекомунікаційних стандартів (ETSI).

Звернемо увагу на типи СТЗ, що застосовують уповноважені органи під час негласного зняття інформації з електронних комунікаційних мереж.

По-перше, *засоби управління та обробки* єдиної системи технічних засобів, що згадана в пункті 2 статті 121 Закону України [1], системи технічних засобів, що використовується всіма розвідувальними органами та яка згадується в пункті 3 статті 15 Закону України [2], стаціонарної системи перехоплення інформації, що наведена в Загальних технічних вимогах [4], для зняття інформації з електронних комунікаційних мереж фіксованого, мобільного (рухомого) зв'язку та передачі даних. Зазначені засоби взаємодіють за стандартизованими інтерфейсами з технічними засобами електронних комунікаційних мереж (як правило, зі шлюзами мережних комплектів [4] та/або серверами, що виконують посередницькі функції під час взаємодії з комутаційним обладнанням, вузловими шлюзами мережі, регістрами місцезнаходження, серверами абонентських даних, тощо).

По-друге, *стаціонарні комплекси активної дії* для зняття інформації з електронних комунікаційних мереж мобільного (рухомого) та фіксованого зв'язку. Указані комплекси відгалужують інформацію щодо обміну даними між елементами мережі, в інтерфейсах взаємодії яких відсутні механізми шифрування даних. Відгалужується, як правило, «сигнальний» трафік із даними, що призначені для користування, та службовими даними. Можливий варіант, коли вони імітують роботу елементів мережі з метою отримання інформації про персональні ідентифікатори абонентів спостереження (споживачів послуг), наприклад, міжнародні номери абонентів рухомого (мобільного) зв'язку MSISDN, міжнародні ідентифікатори обладнання – IMEI, тощо. В подальшому, оперуючи отриманими даними, здійснюється відгалуження інформаційних повідомлень та/або службових даних сеансів зв'язку абонентів спостереження, інформація (у разі її наявності) щодо їх місцезнаходження та закріплений профіль послуг.

По-третє, *мобільні комплекси активної дії* для зняття інформації з електронних комунікаційних мереж мобільного (рухомого) зв'язку. Вони використовують підроблені (несправжні) базові станції для обслуговування абонентів спостереження (споживачів послуг) і, як наслідок, перехоплення їх сеансів зв'язку.

По-четверте, *мобільні комплекси пасивної дії* для зняття інформації з електронних комунікаційних мереж мобільного (рухомого) та супутникового зв'язку шляхом перехоплення та за необхідності дешифрування інформації, що циркулює в інтерфейсах обміну інформації між кінцевим (термінальним) обладнанням та базовими станціями та/або ретрансляторами сигналів, що входять до складу мережевої інфраструктури.

По-п'яте, *стаціонарні системи пасивної дії* для зняття інформації з електронних комунікаційних мереж мобільного (рухомого), фіксованого та супутникового зв'язку. Зазначені системи перехоплюють обмін даними між елементами мережевої інфраструктури.

По-шосте, *мобільні комплекси* для зняття інформації з проводових або волоконно-оптичних ліній зв'язку (каналів) електронних комунікаційних мереж шляхом безпосереднього підключення до них контактним або безконтактним способом.

Висновки. За результатами аналізу наведеного матеріалу вважаємо за доцільне запропонувати визначення технічних засобів для негласного зняття інформації з електронних комунікаційних мереж різновидом спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, що під час проведення оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій придатні для отримання інформації (спостереженні, розпізнаванні, відгалуження та відбору за визначеними ознаками, фіксації, відтворення та обробки) стосовно/щодо змісту інформаційних повідомлень та/або службових даних сеансів зв'язку абонентів спостереження, стосовно/щодо даних (у разі наявності) їх місцезнаходження та з питання профілів послуг, що закріплені за ними.

Запропоновану класифікацію зазначених технічних засобів рекомендуємо використовувати під час підготовки нормативно-правових актів та нормативних документів у сфері СТЗ, а також плануванні оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах.

Список використаних джерел

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

2. Про розвідку : Закон України від 17.09.2020. *Урядовий кур'єр* від 04.11.2020. № 214.

3. Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації : постанова Кабінету Міністрів України від 22.09.2016 № 669. *Офіційний Вісник України*. 2016. № 79. Ст. 2640.

4. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги : наказ Служби безпеки України і Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 04.09.2018 № 1559/533. URL : https://zakononline.com.ua/ documents/show/399084_399149.

5. Манжай А. В., Пеньков С. В. Стандартизация в сфере законного перехвата телекомуникаций. *Legia si Viata*. 2017. № 5/2. С. 86-89.

6. Парасіч Ю. М. Використання можливостей DPI-систем для організації законного перехоплення на магістральних каналах зв'язку. *Збірник наукових праць НА СБУ*. 2017. № 65. С. 239-244.

7. 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.

8. Кримінальний процесуальний кодекс України 13.04.2012. *Відомості Верховної Ради України.* 2013. № 9-10, № 11-12, № 13. Ст. 88.

9. Тертишник В. М. Коментар до Кримінального процесуального кодексу України. Вид. 16-е, доп. і перероб. Київ : Правова Єдність, 2020. 1070 с.

10. Про оперативно-розшукову діяльність : проєкт Закону України від 04.04.2017. № 6284. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/ JH4UK00A. html.

11. Про затвердження Інструкції «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» : наказ Генеральної прокуратури України, МВС, СБУ, Адміністрації ДПС, Мінфіну, Мінюсту України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL : https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.

Надійшла до редакції 19.11.2021

References

1. Pro elektronni komunikatsiyi [On electronic communications] : Zakon Ukrayiny vid 16.12.2020. *Ofitsiynyy visnyk Ukrayiny.* 2021. № 6, art. 306.

2. Pro rozvidku [On Intelligence] : Zakon Ukrayiny vid 17.09.2020. *Uryadovyy kur'yer* vid 04.11.2020. № 214.

3. Deyaki pytannya shchodo spetsial'nykh tekhnichnykh zasobiv dlya znyattya informatsiyi z kanaliv zv'yazku ta inshykh tekhnichnykh zasobiv nehlasnoho otrymannya informatsiyi [Some matters concerning special technical means for removing information from communication channels and other technical means of secretly receiving information] : postanova Kabinetu Ministriv Ukrayiny vid 22.09.2016 № 669. *Ofitsiynyy Visnyk Ukrayiny*. 2016. № 79, art. 2640.

4. Tekhnichni zasoby dlya zdiysnennya upovnovazhenymy orhanamy operatyvno-rozshukovykh zakhodiv ta nehlasnykh slidchykh (rozshukovykh) diy u telekomunikatsiynykh merezhakh zahal'noho korystuvannya Ukrayiny. Zahal'ni tekhnichni vymohy [Technical means for carrying out operative-search measures and covert investigative (search) actions by authorized bodies in public telecommunication networks of Ukraine. General technical requirements] : nakaz Sluzhby bezpeky Ukrayiny i Administratsiyi Derzhavnoyi sluzhby spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny vid 04.09.2018 № 1559/533. URL : https://zakononline.com.ua/ documents/show/399084_399149.

5. Manzhay, A. V., Pen'kov, S. V. (2017). Standartizatsyya v sfere zakonnoho perekhvata telekomunykatsyy [Standardization in the field of legal interception of telecommunications]. *Legia si Viata*. № 5/2, pp. 86-89.

6. Parasich, Yu. M. (2017). Vykorystannya mozhlyvostey DPI-system dlya orhanizatsiyi zakonnoho perekhoplennya na mahistral'nykh kanalakh zv'yazku [Using the capabilities of DPI-systems to organize legal interception on trunk communication channels]. *Zbirnyk naukovykh prats' NA SBU*. № 65, pp. 239-244.

7. Stepanov, V. A., Stishenko, I. K. (2005). Osoblyvosti dozvolenoho zakonom perekhoplennya informatsiyi z telekomunikatsiynykh merezh [Features of the law of interception of information from telecommunications networks]. *Spetsial'ni telekomunikatsiyni systemy ta zakhyst informatsiy*i. № 10, pp. 76-80.

8. Kryminal'nyy protsesual'nyy kodeks Ukrayiny 13.04.2012 [Criminal Procedure Code of Ukraine 13.04.2012]. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2013. № 9-10, № 11-12, № 13, art. 88.

9. Tertyshnyk, V. M. (2020). Komentar do Kryminal'noho protsesual'noho kodeksu Ukrayiny [Commentary to the Criminal Procedure Code of Ukraine]. Vyd. 16-e, dop. i pererob. Kyiv : Pravova Yednist', 1070 p.

10. Pro operatyvno-rozshukovu diyal'nist' [On operational-search activities] : proyekt Zakonu Ukrayiny vid 04.04.2017. № 6284. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/JH4UK00A.html.

11. Pro zatverdzhennya Instruktsiyi «Pro orhanizatsiyu provedennya nehlasnykh slidchykh (rozshukovykh) diy ta vykorystannya yikh rezul'tativ u kryminal'nomu provadzhenni» [On approval of the Instruction «On organization of covert investigative (search) actions and use of their results in criminal proceedings»] : nakaz Heneral'+

3.noyi prokuratury Ukrayiny, MVS, SBU, Administratsiyi DPS, Minfinu, Minyustu Ukrayiny vid 16.11.2012 № 114/1042/516/1199/936/1687/5. URL : https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.

ABSTRACT

Valeriy Stepanov, Serhiy Hryshchenko. Technical means for covert interception of information from electronic communication networks. The article is provides the full information to be the authorized agencies, when intercepting of information from electronic communication networks, in accordance with the requirements of the technical committee lawful interception of the European telecommunication standards institute. The features of technical means for covert interception of information from electronic communication networks, which are set out in regulations and normative documents of Ukraine, are generalized.

The concept of «technical means for interception of information from electronic communication networks» is defined and division of these means into types is given. It is established, that the means of control and processing of united system of technical means cooperate on standardized interfaces with technical means of electronic communication networks.

It has been indicated, that stationary active complexes for intercepting information from electronic communication networks branch information on date exchange between network elements.It is given, that stationary passive systems for removing information from electronic communication networks intercept information data exchange between elements of network infrastructure.

The authors recommend using the proposed classification of these technical means in the preparation of regulations and normative documents in the field of special technical means, as well as planning operational search, counterintelligence, intelligence activities and covert investigative (search) actions in electronic communications networks.

Keywords*: technical means, covert interception of information, electronic communication network, division into types.*