

УДК 343.14

КОКІЗА С.В., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.

ORCID: <https://orcid.org/0000-0001-8111-9203>.

СТЕПАНОВ В.А., кандидат технічних наук, провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.

ORCID: <https://orcid.org/0000-0002-5249-6883>.

ВИМОГИ ПРАВООХОРОННИХ ОРГАНІВ ЄС ЩОДО ЗАКОННОГО ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Анотація. Стаття присвячена аналізу нормативно-правових актів та нормативних документів ЄС щодо перехоплення інформації в електронних комунікаційних мережах в контексті підготовки технічного регламенту єдиної системи технічних засобів.

Ключові слова: перехоплення інформації, об'єкт перехоплення, суб'єкт перехоплення, правоохоронний орган, електронна комунікаційна мережа.

Summary. The article is devoted to the analysis of regulatory and legal acts and normative documents of the EU on information interception in electronic communication networks in the context of preparation of technical regulations of the united system of technical means.

Keywords: interception of information, object of interception, subject of interception, law enforcement agency, electronic communications network.

Аннотация. Статья посвящена анализу нормативно-правовых актов и нормативных документов ЕС относительно перехвата информации в электронных коммуникационных сетях в контексте подготовки технического регламента единой системы технических средств.

Ключевые слова: перехват информации, объект перехвата, субъект перехвата, правоохранительный орган, электронная коммуникационная сеть.

Постановка проблеми. В концептуальних документах з національної безпеки провідних країн світу особливе місце займають заходи з перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах. Зазначені заходи відбуваються в кожній окремій країні відповідно до національного законодавства та мають назву “*wiretapping*”, “*phone-tapping*”, “*lawful interception*” та інші. В Україні перехоплення інформації у телекомунікаційних мережах здійснюється уповноваженими органами під час проведення оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій.

Особливе значення під час здійснення перехоплення інформації в електронних комунікаційних мережах надається забезпеченню додержання конституційних прав громадян. З цією метою в Службі безпеки України здійснюється нормативне забезпечення вказаного заходу відповідно до європейських норм з врахуванням національних особливостей його організації та проведення. Враховуючи викладене, потребують аналізу та систематизації згідно з реаліями сьогодення вимоги правоохоронних органів щодо перехоплення інформації в електронних комунікаційних мережах, наведені в актах законодавства та нормативних документах Європейського Союзу (далі – ЄС), в контексті підготовки технічного регламенту єдиної системи технічних засобів.

Результати аналізу наукових публікацій. Питання перехоплення інформації у телекомунікаційних мережах досліджували Б. Гольдштейн [1], С. Грищенко [2], В. Елагин [1], Дж. Макнамара [3], О. Манжай [4], І. Стішенко [5] та інші. В більшості наукових робіт досліджувались системні аспекти вказаного питання. В статтях Б. Гольдштейна та В. Елагина [1], Дж. Макнамара [3], В. Степанова та І. Стешенка [5] проведено порівняльний аналіз підходів щодо законного перехоплення інформації з телекомунікаційних мереж, відображених в існуючих нормативних документах провідних країн світового суспільства. В статтях В. Степанова, С. Грищенко [2] та О. Манжая [4] здійснено порівняння підходу, на якому базується український нормативний документ [6], з підходами, що визначені у стандартах, рекомендаціях, специфікаціях та інших нормативних документах ETSI, CALEA та COPM.

Праці зазначених науковців, безсумнівно, є вагомим внеском в дослідження цього питання. Проте, аналіз та систематизація вимог правоохоронних органів ЄС, що пов'язані з перехопленням інформації в електронних комунікаційних мережах, в контексті підготовки технічного регламенту технічних засобів залишаються не повною мірою висвітленими, а тому потребують додаткового дослідження.

Метою статті є систематизація вимог правоохоронних органів щодо перехоплення інформації в електронних комунікаційних мережах на основі аналізу актів законодавства та нормативних документів ЄС та в межах підготовки технічного регламенту єдиної системи технічних засобів

Виклад основного матеріалу. На даний час в Україні продовжуються процеси з унормування та законодавчого закріплення заходів з перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах. В пункті 2 статті 121 Закону України “Про електронні комунікації” [7] наведено, що зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством. В статті [8, с. 124] під єдиною системою технічних засобів розуміють функціональне поєднання засобів управління та обробки органів, уповноважених на зняття інформації з електронних комунікаційних мереж, засобів захищених транспортних мереж та мережного комплексу, що відноситься до категорії електронного комунікаційного обладнання. Визначення вимог до характеристик зазначеної єдиної системи технічних засобів та законодавче встановлення процедурних положень та норм її розробки, впровадження та експлуатування, додержання яких є обов'язковим, є вельми актуальним. Вирішення цього питання можливо через підготовку та прийняття відповідного технічного регламенту. В статті 1 Закону України “Про технічні регламенти та оцінку відповідності” [9] визначено, що технічний регламент є нормативно-правовим актом, в якому визначено характеристики продукції або пов'язані з ними процеси та методи виробництва, включаючи відповідні процедурні положення, додержання яких є обов'язковим. В пункті 3 статті 9 цього Закону України також наведено, що технічні регламенти України розробляються на основі міжнародних стандартів та актів законодавства ЄС. Тому для підготовки підґрунтя технічного регламенту єдиної системи технічних засобів проведемо систематизацію вимог правоохоронних органів ЄС щодо перехоплення інформації в електронних комунікаційних мережах на основі аналізу актів законодавства та нормативних документів (стандартів).

З цією метою розглянемо зміст нормативних документів Європейського інституту телекомунікаційних стандартів ETSI (European Telecommunication Standards Institute) технічних специфікацій [10] та [11], а також актів законодавства ЄС ENFOPOL [12], Директиви [13] та Резолюції [14].

Умовно усі вимоги правоохоронних органів, що наведені в зазначених документах, систематизуємо в наступних блоках:

- загальні вимоги;
- вимоги щодо місцезнаходження кінцевих терміналів споживачів послуг (абонентів електронних комунікаційних мереж);
- вимоги до заходів з одночасного перехоплення інформації;
- вимоги до інтерфейсу передачі та управління (в термінології нормативного документа [6]);
- вимоги про додержання принципів конфіденційності під час перехоплення інформації.

По-перше, в *загальних вимогах* відображені наступні аспекти:

- національне законодавство визначає зобов'язання постачальників електронних комунікаційних послуг (оператора мережі, провайдера доступу, провайдера послуг) щодо перехоплення трафіку (пункт 4.2.a технічної специфікації [10]);
- повний зміст інформації, пов'язаної з ідентифікаційною ознакою об'єкта перехоплення, має бути перехоплений протягом повного проміжку часу дії дозволів (пункт 4.2.b технічної специфікації [10], пункт 1 ENFOPOL [12], ст. 3 Директиви [13], пункт 1 Резолюції [14]);
- будь-який зміст зв'язку, пов'язаний з ідентифікаційною ознакою об'єкта перехоплення, котрий передається до технічних засобів зберігання інформації або надходить від них, має бути перехоплений протягом повного проміжку часу дії дозволів (пункт 4.2.2 технічної специфікації [10], пункт 5.2 ENFOPOL [12], ст. 3 Директиви [13], пункт 5.2 Резолюції [14]);
- доставка інформації, пов'язаної з перехопленням, має бути надійною; інформація, яка не може бути доставлена негайно, має буферизуватись (зберігатись) до того часу, поки не стане можливим її доставка (пункт 4.2.4 технічної специфікації [10], пункти 2 та 10 ENFOPOL [12], ст. 8 Директиви [13], пункти 2 та 10 Резолюції [14]);
- має забезпечуватись можливість перехоплення електронних комунікацій (телекомунікацій) споживачів послуг – суб'єктів перехоплення, які працюють в межах електронної комунікаційної (телекомунікаційної) системи постійно, наприклад, абонентів або власників облікового запису (пункт 4.2.c технічної специфікації [10], пункт 1.1 ENFOPOL [12], пункт 1.1 Резолюції [14]);
- має забезпечуватись можливість перехоплення електронних комунікацій (телекомунікацій) споживачів послуг, які працюють в електронній комунікаційній (телекомунікаційній) системі тимчасово, наприклад, гостьових мобільних абонентів або гостьових абонентів, що використовують мережу доступу для отримання послуг, що надаються в домашній мережі (пункт 4.2.d технічної специфікації [10], пункт 1.1 ENFOPOL [12], пункт 1.1 Резолюції [14]);
- усі результати перехоплення мають отримувати унікальні ідентифікаційні ознаки (пункт 4.2.f технічної специфікації [10]).

По-друге, до правоохоронних органів має надходити інформація про поточне *географічне, фізичне та логічне місцезнаходження кінцевого обладнання (терміналу) споживачів послуг* в визначених формах (пункт 4.4 технічної специфікації [10], пункт 1.5 ENFOPOL [12], ст. 1 пункту 2 та ст. 2 пункту 2 Директиви [13], пункт 1.5 Резолюції [14]):

- під час здійснення електронної комунікаційної (телекомунікаційної) діяльності, включаючи сеанси зв'язку або послуги;

- незалежно від того, чи має місце електронна комунікаційна (телекомунікаційна) діяльність одночасно із сеансами зв'язку або послугами;
- під час тимчасового надання послуг щодо об'єкта перехоплення;
- під час успішної або ні спроби встановлення сеансу зв'язку;
- під час надання послуг, постійно пов'язаних з об'єктом перехоплення.

По-третє, *вимоги до заходів з одночасного перехоплення інформації* (пункт 4.14 технічної специфікації [10], пункт А.3 технічної специфікації [11], пункт 8 ENFOPOL [12], пункт 8 Резолюції [14]) враховують наступне:

- можливість одночасного застосування більше ніж одного заходу перехоплення для одного і того ж об'єкта перехоплення;
- можливість одночасного перехоплення однієї послуги, пов'язаної з об'єктом перехоплення, більше ніж одним правоохоронним органом;
- можливість одночасного перехоплення різних послуг, пов'язаних з об'єктом перехоплення, одним і тим же правоохоронним органом;
- максимальна кількість одночасних перехоплень відносно одного і того ж споживача послуг залежить від специфіки мережі та має бути визначена за національною згодою;
- якщо активовано одночасне перехоплення, повинні вживатись запобіжні заходи для захисту ідентифікаційних ознак правоохоронних органів та забезпечення конфіденційності розслідувань;
- заходи одночасного перехоплення можуть відбуватись відповідно до різних дозволів;
- при здійсненні заходів одночасного перехоплення в мережі мають бути створені та налаштовані механізми для забезпечення своєчасного усунення затримок в потенційно вузьких місцях.

По-четверте, *інтерфейс управління та передачі* (в термінології нормативного документа [6]) має відповідати наступному (пункт 4.10 технічної специфікації [10], пункт 5 технічної специфікації [11], пункт 3 ENFOPOL [12], пункт 3 Резолюції [14]):

- забезпечувати перехоплення інформації протягом всього заходу;
- використанню його в тих електронних комунікаційних (телекомунікаційних) мережах, в яких національне законодавство передбачає проведення перехоплення інформації;
- конфігурація має забезпечити передачу результатів перехоплення інформації;
- конфігурація має гарантувати якість електронного комунікаційного (телекомунікаційного) трафіку не гіршу за якість, що пропонується послугами щодо об'єкта перехоплення для кожного конкретного сеансу зв'язку;
- передача до правоохоронних органів результатів перехоплення інформації має відбуватись загальнодоступними шляхами зі стандартними протоколами та принципами кодування;
- кожний об'єкт перехоплення має бути однозначно пов'язаним з окремим каналом або ідентифікатором;
- між інформаційними повідомленнями та службовою інформацією сеансів зв'язку (в термінології нормативного документа [6]) має визначатись однозначна кореляція;
- формат передачі перехопленої інформації має бути загальнодоступним;
- якщо постачальник послуг використовує кодування, стиснення або шифрування електронного комунікаційного (телекомунікаційного) трафіку, то перехоплення має забезпечуватись у вигляді, придатному до застосування правоохоронними органами.

По-п'яте, вимоги *про додержання принципів конфіденційності* під час перехоплення інформації визначають наступне (пункт 4.9 технічної специфікації [10], пункти 7.3 та 8.6 технічної специфікації [11], пункт 4 ENFOPOL [12], ст. 7 Директиви [13], пункт 4 Резолюції [14]):

- перехоплення має здійснюватись та управлятись таким чином, щоб жодна неуповноважена особа не могла помітити різницю із звичайним режимом;
- перехоплення має здійснюватись таким чином, щоб ніхто із сторін, які використовують електронну комунікацію (телекомунікацію), не зміг помітити різницю із звичайним режимом;
- функції управління послугами щодо об'єкта перехоплення та будь-яких інших послуг не мають змінюватись за результатами будь-яких заходів перехоплення;
- якість обслуговування послуг щодо об'єкта перехоплення та будь-яких інших послуг не має змінюватись за результатами будь-яких заходів перехоплення.

Висновки.

Результати систематизації вимог правоохоронних органів ЄС до перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах спрямовані на підготовку в подальшому технічного регламенту єдиної системи технічних засобів та на гармонізацію політики перехоплення інформації в Україні з державами-членами Європейського Союзу з метою включення її до національного законодавства.

Автори не претендують на те, що всі вимоги, наведені в статті, обов'язково мають бути застосовані в Україні. Вони можуть бути використані під час доповнення та уточнення мережних вимог і вимог до інтерфейсів управління та передачі, що розроблені.

Викладені в статті матеріали можуть бути враховані під час підготовки Технічним комітетом стандартизації ТК 196 “Спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації” відповідного стандарту України.

Використана література

1. Гольдштейн Б.С., Елагин В.С. Законный перехват сообщений: подходы ETSI, CALEA и COPM. *Вестник связи*. 2007. № 3. С. 1-11. URL: <http://iks.sut.ru/publications/zakonnyu-perehvat-soobsheniya-podhody-etsi-calea-i-sorm> (дата звернення: 29.04.2021).
2. Степанов В.А., Грищенко С.М. Особливості побудови системи законного перехоплення інформації з телекомунікаційних мереж. *Збірник наукових праць Нац. акад. СБУ*. 2019. № 69. С. 199-204.
3. Макнамара Дж. Секреты компьютерного шпионажа: тактика и контрмеры/ пер. с англ. под. ред. М. Молявко. *БИНОМ. Лаборатория знаний*. 2004. 536 с. URL: <http://padaread.com/?book=36641&pg=20> (дата звернення: 29.04.2021).
4. Манжай А.В., Пеньков С.В. Стандартизация в сфере законного перехвата телекоммуникаций. *Legia si Vista*. 2017. № 5/2. С. 86-89. URL: https://www.researchgate.net/profile/Oleksandr_Manzhai/publication/337991533_Standartizatsiia_v_Sfere_Zakonnogo_Perekhvata_Telekommunikatsii_Standardization_in_the_Field_of_Lawful_Interception_of_Telecommunications/links/5df9211092851c8364854202/Standartizatsiia-v-Sfere-Zakonnogo-Perekhvata-Telekommunikatsii-Standardization-in-the-Field-of-Lawful-Interception-of-Telecommunications.pdf (дата звернення: 11.03.2021).
5. Степанов В.А., Стіщенко І.К. Особливості дозволеного законом перехоплення інформації з телекомунікаційних мереж. *Спеціальні телекомунікаційні системи та захист інформації*. 2005. № 10. С. 76-80.

6. 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 04.09.18 р. № 1559/533. URL: https://zakononline.com.ua/documents/show/399084_399149 (дата звернення: 11.03.2021).

7. Про електронні комунікації: Закон України від 16.12.20 р. № 1089-IX. *Офіційний вісник України*. 2021. № 6. Ст. 306. – (26.01.2021 р.).

8. 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: <http://repository.vsau.org/getfile.php/28071.pdf> (дата звернення: 29.04.2021).

9. Про регламенти та оцінку відповідності: Закон України від 15.01.15 р. № 124-VIII. *Відомості Верховної Ради України*. 2015. № 14. Ст. 96. URL: <https://zakon.rada.gov.ua/laws/show/124-19#Text> (дата звернення: 29.04.2021).

10. Telecommunications security. Lawful Interception. Requirements of Law Enforcement Agencies (Безпека систем зв'язку. Законне перехоплення. Вимоги правоохоронних органів): технічна специфікація ETSI TS 101 331 V1.7.1. URL: https://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.07.01_60/ts_101331v010701p.pdf (дата звернення: 29.04.2021).

11. Telecommunications security. Lawful Interception. Requirements for network functions (Безпека систем зв'язку. Законне перехоплення. Вимоги до мережних функцій): технічна специфікація ETSI TS 101 158 V1.3.1. URL: https://www.etsi.org/deliver/etsi_ts/101100_101199/101158/01.03.01_60/ts_101158v010301p.pdf (дата звернення: 29.04.2021).

12. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL): Директива Ради ЄС від 20.06.01 р. URL: https://zakon.rada.gov.ua/laws/show/994_234#Text (дата звернення: 29.04.2021).

13. On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку, та внесення поправок в Директиву 2002/58/ЄС): Директива Європейського Парламенту та Ради 2006/24/ЄС від 15.03.06 р. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024> (дата звернення: 29.04.2021).

14. Про законне перехоплення телекомунікацій: Резолюція Ради ЄС 96/C329/01 від 17.01.95 р. URL: https://zakon.rada.gov.ua/laws/show/994_235#Text (дата звернення: 29.04.2021).

~~~~~ \* \* \* ~~~~~