УДК 343.96 **DOI:** https://doi.org/10.32631/v.2021.3.10

Валентин Миколайович Лазебний,
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України (старший науковий співробітник), м. Київ;
https://orcid.org/0000-0002-2597-8203,
e-mail: 25_valentin_27@ukr.net

Актуальні аспекти правового регулювання моніторингу електронних комунікацій та зняття інформації з електронних комунікаційних мереж в Україні

Розглянуто актуальні аспекти нормативно-правового регулювання моніторингу електронних комунікацій в іноземних державах та в Україні, особливості проведення розшукових і слідчих дій в електронних комунікаційних мережах. Констатовано потребу оновлення порядку здійснення таких заходів, зумовлену динамічним розвитком законодавства. Запропоновано перспективні заходи, реалізація яких поліпшить можливості уповноважених правоохоронних органів із протидії злочинності у сфері інформаційно-комунікаційних технологій.

Ключові слова: електронні комунікації, мережі, моніторинг, перехоплення, зняття інформації, правове регулювання.

Оглядова стаття

Постановка проблеми

Стрімкий розвиток новітніх інформаційних технологій суттєво змінив світову спільноту. Стійка тенденція проникнення цих технологій у всі сфери життєдіяльності та суспільних відносин супроводжується розширенням кола загроз безпеці держави і громадян.

Засоби електронної комунікації та інші новітні технології дедалі активніше застосовуються у протиправній діяльності. Це потребує як організації системної протидії протиправним проявам із використанням оперативних і технічних можливостей правоохоронних органів, так і належного унормування підстав їх застосування з дотриманням прав і свобод людини та громадянина. Тому для забезпечення ефективного проведення пошукових і слідчих (розшукових) заходів в електронних комунікаційних мережах необхідно завершити процес формування в Україні правових засад перехоплення даних у таких мережах, узгоджених з нормами законодавства ЄС.

Стан дослідження проблеми

Вивченням проблем моніторингу комунікацій, зняття інформації з каналів зв'язку як напряму діяльності правоохоронних органів і

спецслужб у цій сфері, а також різновиду документування протиправних дій займалися С. Баранов, С. Гриняєв, С. Грищенко, О. Ковальов, О. Коцюба, О. Манжай, М. Перепелиця, В. Серьогін, В. Степанов, О. Литвиненко, А. Тарасюк, О. Ходич та ін. Однак більшість їхніх досліджень стосується технічних і процесуальних складових цього питання.

Разом з тим окремі вчені (С. Єськов, О. Климчук, О. Манжай, Д. Мельник, М. Перепелиця) у своїх працях все ж розглядали особливості правового регулювання зняття інформації з електронних комунікаційних мереж. Однак стан регулювання цього питання в українському законодавстві не було досліджено з необхідною повнотою через оновлення його норм, що триває.

Мета і завдання дослідження

Відповідно, *метою* дослідження є висвітлення чинного в Україні порядку моніторингу електронних комунікацій та зняття інформації з електронних комунікаційних мереж, а його *завданнями* – з'ясування наявних проблемних аспектів та надання пропозицій з удосконалення його правового регулювання.

Новизна дослідження полягає в тому, що комплексно досліджено особливості моніторингу електронних комунікацій та зняття інформації з електронних комунікаційних мереж, з'ясовано наявні проблеми та запропоновано шляхи їх вирішення.

Виклад основного матеріалу

Наукове дослідження проблем запобігання, своєчасного виявлення, документування та доказування злочинів, які вчиняються з використанням новітніх інформаційних технологій та зумовлюють необхідність удосконалення правового регулювання перехоплення електронних комунікацій для отримання даних про правопорушення в електронних мережах, наразі набуває надзвичайної актуальності в умовах зростання протиправної активності в кібернетичній сфері держави.

Досвід провідних держав світу, які системно протидіють кіберзлочинності та тероризму, свідчить про те, що впровадження у практику роботи правоохоронних органів систем моніторингу електронних комунікацій суттєво поліпшило здобування випереджувальних даних про терористичні прояви та інші протиправні дії, що готуються і вчиняються з використанням новітніх інформаційних технологій. Така практика була сформована відповідно до положень Конвенції про кіберзлочинність 2001 р., ратифікованої зокрема й нашою країною[1], де зазначається, що необхідною передумовою ефективної

[1] Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV // База даних (БД) «Законодавство України» / Верховна

протидії терористам та організованим злочинним угрупованням є моніторинг даних у мережах електронних комунікацій.

Також у керівних настановах Ради Європи зазначено, що ефективною протидія злочинності у сфері новітніх інформаційних технологій може бути за умови узгодження законодавств країн ЄС з урахуванням рекомендацій, зазначених у Директиві Європарламенту і Ради ЄС від 12 липня 2002 р. № 2002/58/ЄС, щодо обробки персональних даних та захисту права на приватність у сфері електронних комунікацій[1]. Ця Директива допускає зберігання персональних даних упродовж визначеного періоду, якщо це необхідно для здійснення захисту національної і громадської безпеки, оборони та запобігання, виявлення і розслідування злочинів та несанкціонованого використання систем електронного зв'язку. Також Директива зобов'язала уряди держав ЄС ухвалити закони про збереження інформації щодо передання даних в електронних мережах для потреб правоохоронних органів.

Крім того, упровадження систем негласного спостереження та зняття даних з мереж електронних комунікацій визначено основним механізмом моніторингу стану національної безпеки у керівних документах Великобританії, Ізраїлю, США, ФРН та інших провідних держав світу.

Зокрема, здобуття інформації про підготовку злочинів Стратегією кібернетичної безпеки США та керівною настановою «Перехоплення комунікацій Великобританії» названо головним методом контролю електронних комунікаційних мереж та отримання з них інформації. Також у вказаних керівних документах зазначено, що без застосування одночасного моніторингу всіх загальнодоступних електронних мереж забезпечити комплексне проведення операцій проти міжнародних терористичних та інших злочинних організацій неможливо. Тому виправдовує себе практика створення окремих спецслужб або спецпідрозділів для проведення заходів оперативного пошуку на пріоритетних напрямах роботи (наприклад АНБ у США або «GTAC» MI-5 у Великобританії).

Резолюції Ради ЄС «Про законне перехоплення телекомунікацій» від 17 січня 1995 р. № 96/С329/01[2] та «Про оперативні запити

Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 15.09.2021).

[1] Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканність особистого життя в сфері електронних комунікацій : від 12.07.2002 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_b34 (дата звернення: 15.09.2021).

[2] Резолюція Ради ЄС «Про законне перехоплення телекомунікацій» : від 17.01.1995 № 96/С329/01 // БД «Законодавство України» / ВР України.

правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг» від 20 червня 2001 р.[1], Директиви Європейського Парламенту й Ради ЄС «Про універсальні послуги» від 7 березня 2002 р. № 2002/22/ЄС[2] і «Про обробку персональних даних і захист права на недоторканність особистого життя у сфері електронних комунікацій» від 12 липня 2002 р. № 2002/58/ЄС, а також національні законодавчі акти Великобританії, ФРН та США нормативно зафіксували процедури створення і використання систем перехоплення на всіх загальнодоступних електронних комунікаційних мережах. Крім того, законодавчі акти провідних країн передбачають ідентифікацію відправника й одержувача електронних поштових повідомлень [1, с. 198].

Проведення оперативно-розшукових заходів у Великобританії регламентує Закон «Про правове регулювання слідчих повноважень» 2000 р.[3], що встановлює чіткі підстави, порядок та умови санкціонування та здійснення оперативно-розшукових заходів, серед іншого фактично наділяє слідчі органи повноваженнями щодо перехоплення, зберігання і відстеження комунікацій.

У США закони, що стосуються здійснення оперативно-розшукової діяльності, об'єднано у «Звід законів Сполучених Штатів» [2, с. 14]. Основними слідчими методами в законах США визначено серед іншого неконсенсуальне електронне спостереження (перехоплення без відома сторін), консенсуальне електронне спостереження (перехоплення за згодою однієї зі сторін), доступ до збережених повідомлень і записів тощо [2, с. 26].

Спецслужби та правоохоронні органи США отримали повноваження з перехоплення електронних комунікацій після подій 11 вересня 2001 р. у цій країні, зокрема право здійснювати постійний моніторинг мережевих ресурсів для отримання даних щодо діяльності

URL: https://zakon.rada.gov.ua/laws/show/994_235 (дата звернення: 15.09.2021).

[1] Резолюція Ради ЄС «Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг» : від 20.06.2001 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_234 (дата звернення: 15.09.2021).

[2] Директива № 2002/22/ЄС Європарламенту та Ради Європи про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг : від 07.03.2002 // Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації : офіц. сайт. URL: https://nkrzi.gov.ua/images/upload/58/19/6ad521f49a3af8c4642834474a790eac.pdf (дата звернення: 15.09.2021).

[3] Regulation of Investigatory Powers Act 2000 // Legislation.gov.uk : сайт. URL: https://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf (дата звернення: 15.09.2021).

політичних, громадських і релігійних організацій та зняття з них інформації у межах оперативної діяльності, а не лише під час розслідування.

Також слід зазначити, що у керівному документі Комітету НАТО з цивільного зв'язку щодо захисту уразливої інформаційної інфраструктури 2002 р. подано рекомендації з формування норм законодавства, які б стимулювали постачальників електронних комунікацій створювати умови для безпечного комунікаційного середовища, зокрема шляхом упровадження систем моніторингу, в умовах розвитку ринкових відносин і зменшення контролю держави [3, с. 102].

У нашій країні питання впровадження системи перехоплення електронних комунікацій свого часу набуло значного суспільного розголосу через побоювання, що правоохоронці зможуть здійснювати системний моніторинг електронних інформаційних мереж, чим безпідставно обмежувати основоположні права і свободи людини, закріплені в Конституції України, Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р.[1] та інших міжнародних актах, ратифікованих Україною.

Варто зважати на те, що інформаційна безпека держави передбачає не лише захист інформаційних ресурсів від негативних впливів, але й недопущення протиправного використання електронних комунікацій. Водночас забезпечення захисту прав і свобод людини передбачає як захист особистої безпеки від протиправних посягань, так і гарантію невтручання держави у приватне життя.

Разом із тим методи і засоби скоєння злочинів постійно вдосконалюються, що потребує відповідного реагування правоохоронних органів за допомогою створення і впровадження нових алгоритмів протидії протиправній діяльності. Відповідно, це може призводити до обмеження конституційних прав і свобод громадян (права на інформацію, на повагу до таємниці кореспонденції, на недоторканність особистого життя, свободу самовираження тощо).

Український законодавець визначає зняття інформації з каналів електронних комунікацій за наявності передбачених законом підстав одним із повноважень суб'єктів оперативно-розшукової діяльності. Однак наразі відсутні правові акти, які б надали можливість правоохоронним органам і спецслужбам упроваджувати і застосовувати системи перехоплення електронних комунікацій під час проведення оперативно-розшукових та контррозвідувальних заходів.

[1] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : від 28.01.1981 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 15.09.2021).

Зважаючи на викладене, доречно зауважити, що СБУ підготувала законопроєкт «Про моніторинг телекомунікацій» від 7 серпня 2003 р. № 4042, який зазнав критики експертного товариства та не був ухвалений. Також на розгляд Верховної Ради України раніше неодноразово виносилися законопроєкти (від 26 березня 2004 р. № 4042-1, від 21 березня 2005 р. № 4042-2, від 2 вересня 2010 р. № 7023-1, від 3 грудня 2010 р. № 7023/П) про перехоплення електронних комунікацій, які були зняті з розгляду Верховної Ради України через необхідність суттєвого коригування з урахуванням зауважень, зроблених державними органами та громадськістю.

Наразі здійснення оперативно-технічних заходів у мережах електронних комунікацій регламентовано в Законі України «Про оперативно-розшукову діяльність» та Кримінальному процесуальному кодексі (далі – КПК) України.

Відповідно до п. 9 ч. 1 ст. 8 Закону України «Про оперативно-розшукову діяльність» оперативним підрозділам для виконання завдань оперативно-розшукової діяльності за наявності підстав надається право здійснювати зняття інформації з транспортних телекомунікаційних мереж згідно з положеннями статей 260, 263, 265 КПК України.

Згідно з ч. 1 ст. 263 КПК України зняття інформації з транспортних телекомунікаційних мереж (далі – ТТМ)[1] є різновидом втручання у приватне спілкування, передбачене ч. 4 ст. 258 КПК України, яке проводиться без відома осіб, що користуються засобами електронних комунікацій для передачі інформації (так зване неконсенсуальне спостереження), якщо можна з'ясувати обставини, що мають значення для досудового розслідування. Цей захід здійснюється у кримінальному провадженні виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, попередження і припинення терористичних актів та інших посягань спецслужб іноземних держав та організацій, якщо в інший спосіб одержати інформацію неможливо.

Відповідно до ч. 3 ст. 263 КПК України *зняття інформації з ТТМ* полягає у проведенні спостереження, відбору та фіксації змісту інформації, яка передається із застосуванням технічних засобів та має значення для досудового розслідування, а також одержанні, перетворенні та фіксації різних видів сигналів, що передаються мережами комунікацій. Згідно з ч. 4 ст. 263 КПК України зняття інформації з ТТМ покладено на уповноважені підрозділи Нацполіції, НАБУ, ДБР та СБУ.

[1] ТТМ – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та будь-яких звуків або повідомлень між підключеними до неї мережами доступу (ст. 1 Закону України «Про телекомунікації»).

Указана негласна слідча (розшукова) дія здійснюється за клопотанням слідчого або керівника оперативного підрозділу, погодженим із прокурором на підставі ухвали слідчого судді про дозвіл на втручання в приватне спілкування. Відповідно до ч. 2 ст. 263 КПК України в ухвалі слідчого судді мають бути зазначені *ідентифікуючі ознаки*, які дадуть змогу унікально визначити об'єкта спостереження, ТТМ і кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування.

До складу таких унікальних ознак можна віднести номер абонента в мобільній телефонній мережі загального користування, міжнародний ідентифікаційний номер мобільного терміналу (IMEI) або абонента (IMBI). У разі передання інформації через мережу Інтернет або інші мережі передачі даних такими ознаками можуть бути адреса електронної пошти, адреса в мережі передачі даних із комутацією пакетів, зокрема IP-адреса для Інтернет, або MAC-адреса пристрою, приєднаного до мережевого середовища [4, с. 80]

Відповідно до положень ст. 263 КПК України керівники та працівники операторів електронних комунікацій зобов'язані сприяти виконанню заходів зі зняття інформації з ТТМ, вживати заходів щодо нерозголошення факту їх проведення та отриманої інформації і зберігати її у незмінному вигляді з метою використання в інтересах кримінального судочинства.

Указані норми КПК України наразі узгоджуються з ч. 4 ст. 39 Закону України «Про телекомунікації», відповідно до положень якої оператори телекомунікацій зобов'язані власним коштом установлювати на ТТМ технічні засоби для проведення оперативно-розшукових заходів і забезпечувати їх функціонування, сприяти проведенню таких заходів та не допускати розголошення прийомів проведення. Також на операторів покладено обов'язок організовувати захист таких засобів від несанкціонованого доступу.

Разом із тим наразі ані КПК України, ані Закон України «Про оперативно-розшукову діяльність», що надає оперативним підрозділам право здійснювати зняття інформації з ТТМ, не передбачають норм, які розкривали б зміст таких дій. Приписи деяких норм цього Закону роз'яснює Постанова Пленуму Верховного Суду України «Про деякі питання застосування судами законодавства при наданні дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства» від 28 березня 2008 р. № 2. Зокрема, у ній (п. 3) ідеться про те, що зняття інформації з каналів комунікацій полягає в застосуванні технічних засобів, що дають змогу відстежувати, фіксувати і відтворювати інформацію, яка передавалася цими каналами. Загальний порядок установлення таких

засобів визначено Правилами здійснення діяльності у сфері телекомунікацій, затвердженими рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, від 19 листопада 2019 р. № 541.

Під час зняття інформації з ТТМ можна здобути інформацію, що вказує на ознаки кримінального правопорушення в діях контрольованої особи (осіб), а також дані про злочинну діяльність інших осіб, що комунікували з ними в мережі до та під час проведення негласної слідчої (розшукової) дії. Зміст відомостей з електронних мереж, що мають значення для досудового розслідування, фіксується на відповідному носієві особою, яка здійснювала зняття і зобов'язана забезпечити обробку, збереження або передання інформації, та зазначається у відповідному протоколі про зняття інформації з ТТМ [4, с. 80].

До винесення ухвали слідчого судді зняття інформації з ТТМ може бути розпочато на підставі постанови слідчого, прокурора лише у випадку, передбаченому ч. 1 ст. 250 КПК України. У такому разі слідчий за погодженням із прокурором або прокурор зобов'язані невідкладно звернутися з клопотанням до слідчого судді, який розглядає таке клопотання згідно з вимогами ст. 248 КПК України. Якщо ж слідчий суддя винесе ухвалу про відмову в дозволі на зняття інформації з ТТМ, його проведення негайно припиняється, а інформація, отримана внаслідок такої негласної розшукової дії, підлягає знищенню відповідно до ст. 255 КПК України, за винятком випадків, коли такі відомості свідчать про інше кримінальне правопорушення, а тому підлягають збереженню.

Наразі українське законодавство не передбачає правил збереження та подальшого використання отриманих персональних даних, обсягів таких даних, тривалості їх зберігання та як саме вони використовуватимуться в майбутньому.

В Україні, на відміну від європейських країн, не існує окремого закону про збереження даних, отриманих під час зняття інформації з ТТМ. Однак це негативно впливає на тривалість збереження даних трафіку, визначену вимогами законодавства до постачальників комунікаційних послуг, і суттєво збільшує їх фінансовий тягар у зв'язку з цими вимогами[1].

Заходи зі зняття інформації з ТТМ здійснюються з метою пошуку і фіксації даних, що можуть бути використані під час розкриття і розслідування злочинів. Також такі дані можуть бути використані для планування і проведення слідчих дій у кримінальному провадженні та

[1] Захаров Є. Захист персональних даних та діяльність органів розслідування. Проблемні питання // Право на приватність : сайт. 06.04.2021. URL: http://privacy.khpg.org/1604922616 (дата звернення: 15.09.2021).

для попередження і припинення інших кримінальних правопорушень. Водночас під час зняття інформації з ТТМ можна зібрати інформацію, що може свідчити про вчинення злочину певними особами, місцезнаходження предметів і документів, що можуть бути доказами [4, с. 87].

Також уповноважені правоохоронні органи під час моніторингу електронних комунікацій можуть здійснювати цілеспрямований пошук інформації з відкритих джерел з метою виявлення даних, необхідних для виконання завдань контррозвідувальної та оперативно-розшукової діяльності. Зокрема, може проводитися пошук відомостей стосовно осіб, підозрюваних у розвідувально-підривній та іншій протиправній діяльності, підготовці та вчиненні конкретних злочинів, їх зв'язків та іншої інформації. При цьому не потрібен дозвіл суду на пошук і фіксацію загальнодоступних даних, оскільки обмеження приватності спілкування окремих осіб не відбувається.

Однак з ухваленням 16 грудня 2020 р. Закону України «Про електронні комунікації» вказані положення перестануть діяти у зв'язку з втратою чинності Законом України «Про телекомунікації» вже у найближчій перспективі[1]. Відповідно, виникне потреба змінити положення КПК України, тож, зміниться підхід до перехоплення інформації в електронних комунікаційних мережах (наразі – ТТМ).

Разом із тим ст. 121 Закону України «Про електронні комунікації» визначає умови надання доступу до інформації у передбачених законом випадках. Зокрема, доступ до інформації про споживача, факти надання електронних комунікаційних послуг, зокрема до даних, що обробляються з метою передання такої інформації в електронних комунікаційних мережах, здійснюється виключно на підставі рішення суду, слідчого судді у випадках та порядку, передбачених законом. Відповідно до положень вказаної статті Закону зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів (далі – ЄСТЗ), що використовується всіма уповноваженими органами на умовах автономного доступу до інформації у порядку, визначеному законодавством. Фахівці пропонують визначати ЄСТЗ як функціональне поєднання засобів управління та обробки, що належать уповноваженим органам, а також засобів захищених транспортних мереж і мережевого комплекту для здійснення зняття інформації з електронної комунікаційної мережі постачальника послуг [5, с. 227].

Однак наразі порядок створення та впровадження вказаної системи для перехоплення електронних комунікацій не передбачено ані

[1] З 1 січня 2022 р. – відповідно до п. 2 Розділу XIX «Прикінцеві та перехідні положення» Закону України «Про електронні комунікації» від 16.12.2020 № 1089-IX.

в Законі України «Про електронні комунікації», ані в підзаконних нормативно-правових актах. Це ставить під сумнів можливість практичної реалізації положень ст. 121 Закону України «Про електронні комунікації» та ст. 263 КПК України.

Закон передбачає обов'язок постачальника електронних комунікаційних послуг та/або мереж забезпечити можливість підключення технічних засобів, що входять до складу ЄСТЗ, у точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг. Однак, на переконання експертів, надання такого доступу на практиці створює можливості для обходу наявних вимог щодо судового нагляду за зняттям інформації. На це звертав увагу і Європейський суд з прав людини у справі щодо перехоплення спецслужбами РФ телефонних комунікацій[1].

Також відповідно до ст. 119 Закону України «Про електронні комунікації» постачальники електронних комунікаційних послуг мають забезпечувати і нести відповідальність за схоронність даних про кінцевого користувача, отриманих під час надання таких послуг, включно зі змістом переданої інформації, даних про місцезнаходження особи, а також маршрутів передачі даних. Інформація про електронні комунікаційні послуги, отримані кінцевим користувачем, може надаватися лише за наявності його попередньої згоди.

Окрім того, низку новацій щодо здійснення перехоплення електронних комунікацій містить проєкт Закону України «Про внесення змін до Закону України «Про Службу безпеки України» щодо вдосконалення організаційно-правових засад діяльності Служби безпеки України» від 26 жовтня 2020 р. № 3196-д. Відповідно до цього проєкту СБУ отримує повний контроль над визначенням технічних характеристик та застосуванням засобів для зняття інформації з електронних комунікаційних мереж.

Водночас, на переконання правозахисників, у законопроєкті відсутні достатні запобіжники від зловживань під час перехоплення електронних комунікацій. Натомість запобіжники, встановлені ще у 2012 р. у КПК України, у цьому разі ігноруються. Також законопроєкт не містить гарантій захисту професійної таємниці (адвокатської, лікарської, журналістської тощо) у разі застосування перехоплення, на відміну від стандартів, що застосовуються для досудового розслідування[2].

---

[1] Case of Roman Zakharov v. Russia (Application no. 47143/06) // HUDOC : сайт. URL: https://hudoc.echr.coe.int/eng#{"itemid":["001-159324"]} (дата звернення 11.11.2021).

[2] Заява Коаліції «За вільний інтернет» щодо загроз правам людини в новій редакції законопроєкту про СБУ // ZMINA : сайт. 10.11.2020.

Отже, підвищенню ефективності моніторингу електронних комунікаційних мереж та зняття з них інформації, безсумнівно, сприятиме узгодження положень КПК України про зняття інформації з електронних комунікаційних мереж з положеннями Закону України «Про електронні комунікації» (після набрання ним чинності), а також закріплення в законодавстві необхідних умов, які покращуватимуть можливості вітчизняних правоохоронних органів у протидії злочинності у сфері інформаційно-комунікаційних технологій.

1. Ухвалення Закону України «Про моніторинг електронних комунікацій» з урахуванням приписів Конвенції про кіберзлочинність та вимог технічного регламенту щодо законного перехоплення телекомунікацій (TL LI) Європейського інституту телекомунікаційних стандартів (ETSI). У законі необхідно передбачити механізм, який дасть змогу правоохоронним органам отримати необхідні можливості для ефективного моніторингу електронних комунікацій з метою запобігання, виявлення, припинення та розкриття злочинів з використанням новітніх інформаційних технологій, а також створити організаційно-технічні засади контролю за дотриманням законності під час такої діяльності. Водночас цей закон має забезпечити оптимальний баланс між потребами правоохоронних органів та громадськості, передбачити надійні гарантії проти зловживань і незаконного перехоплення електронних комунікацій.

2. Внесення необхідних змін до Закону України «Про електронні комунікації» щодо вдосконалення регулювання сфери надання і використання послуг у сфері електронних комунікацій за такими основними моментами:

– унормування відповідного порядку створення й упровадження ЄСТЗ як універсальної системи перехоплення електронних комунікацій, її використання уповноваженими державними органами на умовах автономного доступу до інформації у порядку, визначеному законодавством;

– поліпшення регулювання правових відносин між операторами і постачальниками електронних комунікаційних мереж та/або послуг, споживачами їх послуг та уповноваженими правоохоронними органами.

3. Приведення положень Кримінального кодексу України у відповідність до ст. 3 Конвенції про кіберзлочинність – слід передбачити відповідальність за навмисне незаконне перехоплення даних шляхом фіксації технічними засобами електромагнітних випромінювань електронної інформаційної системи / мережі.

URL: https://zmina.ua/statements/zayava-koalicziyi-za-vilnyj-internet-shhodo-zagroz-pravam-lyudyny-u-novij-redakcziyi-zakonoproyektu-pro-sbu/ (дата звернення: 15.09.2021).

4. Внесення необхідних змін і доповнень до КПК України та законів України «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про боротьбу з тероризмом» і «Про електронні комунікації» щодо закріплення процесуальних повноважень уповноважених суб'єктів та порядку фіксації доказів в електронній формі, проведення обшуків і вилучення електронних систем та мереж або їх складових, а також наявних даних [6, с. 39].

5. Налагодження належної співпраці з правоохоронними органами іноземних держав щодо протидії злочинності у сфері інформаційно-комунікаційних технологій відповідно до приписів ст. 34 Конвенції про кіберзлочинність щодо надання взаємної допомоги у перехопленні даних.

Висновок

Отже, законодавче регулювання моніторингу електронних комунікацій та зняття інформації з електронних комунікаційних мереж потребує вдосконалення, насамперед у вигляді остаточного приведення у відповідність до положень Конвенції про кіберзлочинність норм вітчизняного законодавства, ухвалення Закону України «Про моніторинг електронних комунікацій», узгодження норм КПК України з положеннями Закону України «Про електронні комунікації» (після набрання ним чинності), а також законодавчого закріплення умов, які покращуватимуть можливості уповноважених правоохоронних органів з протидії злочинності у сфері інформаційно-комунікаційних технологій, і налагодження належної співпраці з іноземними правоохоронними органами.

Список бібліографічних посилань: 1. Коцюба О. А. Щодо оптимізації законодавчого регулювання окремих напрямів протидії розвідувальній діяльності // Проблеми законодавчого регулювання діяльності Служби безпеки України у контексті положень Конституції України та побудови демократичного суспільства : матеріали наук.-практ. конф. (м. Київ, 9 лют. 2006 р.). Київ : НКЦ «Інститут оперативної діяльності та державної безпеки», 2006. С. 196–199. **2.** Перепелиця М. М., Манжай О. В. Провадження оперативно-розшукових заходів у Великій Британії, Росії, США та Україні : монографія. Харків : Друкарня № 13, 2008. 248 с. **3.** Серьогін В. С. Проблеми створення системи моніторингу інформаційного простору України // Інформаційна безпека держави у світлі розвитку сучасних інформаційних технологій : матеріали наук.-практ. конф. (м. Київ, 30 черв. 2006 р.). Київ : НВВ НА СБУ, 2007. С. 99–103. **4.** Негласні слідчі (розшукові) дії. Коментар до глави 21 Кримінального процесуального кодексу України / за заг. ред. Є. Д. Скулиша. Київ : НВЦ НА СБУ, 2012. 132 с. **5.** Степанов В., Грищенко С. Єдина система технічних засобів зняття інформації з електронних комунікаційних мереж. *Збірник наукових праць Національної академії Служби безпеки України.* 2020.

№ 78. С. 226–230. **6.** Мельник Д. С. Перспективи нормативно-правового врегулювання зняття інформації з телекомунікаційних мереж та електронних інформаційних систем у новому КПК України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2012. № 2 (24). С. 34–40.

Надійшла до редколегії 17.09.2021

Lazebnyi V. M. Current Aspects of Legal Regulation for Monitoring Electronic Communications and Removal of Information from Electronic Communication Networks in Ukraine

The article is focused on studying current aspects of normative and legal regulation for monitoring electronic communications in foreign countries and in Ukraine; on the features of conducting search and investigative actions on the removal of information from electronic communication networks.

The legislation of Ukraine does not currently provide the procedure for creation and implementation of interception systems for electronic communications, does not define organizational and technical requirements that should guarantee conditions for monitoring such activities, despite the relevance of modern legal regulation of conducting search, operative and technical measures in communication networks. rapid development of electronic information technology.

The legislator made an attempt to legally regulate the implementation of operative and technical measures in electronic communication networks in the Criminal Procedural Code of Ukraine dated from April 13, 2012, which provided the removal of information from transport telecommunication networks. Relevant norms were also provided in the Law of Ukraine "On Operative and Search Activities". Regarding the dynamic development of legislation, which is primarily due to the adoption of the Law of Ukraine "On Electronic Communications" dated from December 16, 2020, the author of the article has stated the need to update the existing procedure for such activities.

The author has suggested measures, the realization of which should improve the capacity of authorized law enforcement agencies to combat crime in the field of information and communication technologies: adoption of the Law of Ukraine "On Interception of Electronic Communications", amendments to the Laws of Ukraine "On Electronic Communications", "On Operative and Search Activities", "On Counterintelligence Activities", "On Combating Terrorism"; bringing the norms of domestic legislation in line with the provisions of the Convention on Cybercrime; creation of conditions necessary to improve the capacity of authorized state agencies to remove information from electronic communication networks; establishing proper cooperation with foreign law enforcement agencies.

Key words: electronic communications, networks, monitoring, interception, removal of information, legal regulation.