УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2022-8/113

ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ: ФОКУС НОВЕЛ

REMOVAL OF INFORMATION FROM ELECTRONIC COMMUNICATION NETWORKS: FOCUS INNOVATION

Луцик В.В., к.ю.н., доцент,
заступник керівника департаменту запобігання і виявлення корупції
Національне агентство з питань запобігання корупції

У статті досліджуються питання правового регулювання зняття інформації з електронних комунікаційних мереж. Під час постановки проблеми зазначається, що прийняття Закону України «Про електронні комунікації» призвело до низки змін у кримінальне процесуальне законодавство. Закріплення нових підходів до роботи з електронними комунікаційними мережами викликає потребу переосмислення підходів щодо проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних комунікаційних мереж, її співвідношення із аналогічними розвідувальними заходами.

У перебігу розкриття стану опрацювання відповідної проблематики підкреслюється, що на сьогоднішній день ці питання у доктрині ще не досліджувалися, крім розгляду у аспекті інших змін та доповнень до законодавства.

У процесі викладу основного матеріалу аналізується процесуальний порядок зняття інформації з електронних комунікаційних мереж, виокремлюються її види та особливості отримання доказової інформації. Наголошується на необхідності розмежування зняття інформації з електронних комунікаційних мереж, як негласної слідчої (розшукової) дії та як розвідувального заходу.

Робиться загальний висновок, що трансформація негласної слідчої (розшукової) дії – зняття інформації з електронних комунікаційних мереж зумовлено розвитком інформаційних технологій, приведенням у відповідність українського кримінального процесуального законодавства до міжнародних стандартів. Обґрунтовується, що недооціненим є потенціал розвідувальної діяльності, як способу отримання доказів у кримінальному провадженні. В зв'язку з цим виникає нагальна необхідність розроблення процедури легалізації інформації отриманої в ході розвідувальної діяльності у кримінальному провадженні, що дозволить використовувати у доказуванні перехоплення телефонних розмов окупантів, дані радіотехнічної розвідки, інформацію щодо ідентифікації осіб, які вчинили злочини на території України, отриману в ході проведення розвідувальних заходів.

Ключові слова: негласні слідчі (розшукові) дії, зняття інформації, електронні комунікаційні мережі, розвідувальні заходи, електронні комунікації, розвідка.

The article examines the issues of legal regulation of the removal of information from electronic communication networks. In setting the problem it is noted that the adoption of the Law of Ukraine "On electronic communications" has led to a number of changes in the criminal procedural legislation. Consolidation of new approaches to work with electronic communication networks causes the need to rethink approaches to the conduct of such covert investigative action as the removal of information from electronic communication networks, its correlation with similar intelligence activities.

While analyzing the state of relevant issues studying it is emphasized that for today, these issues have not yet been studied in the doctrine, except in the aspect of other changes and additions to the legislation.

In the process of presentation of the main material the procedure of information removal from electronic communication networks is analyzed, its types and peculiarities of obtaining evidentiary information are highlighted. The need to distinguish between the removal of information from electronic communication networks as a covert investigative action and as an intelligence activity is emphasized.

The general conclusion is made that the transformation of covert investigative action – information removal from electronic communication networks due to the development of information technology, harmonization of Ukrainian criminal procedural legislation with international standards.

It is substantiated that the potential of intelligence activities as a method of obtaining evidence in criminal proceedings was underestimated. In this regard, there is an urgent need to develop a procedure for legalization of information obtained during the intelligence activities in the criminal proceedings, which will allow to use in evidencing the interception of telephone conversations of the occupants, the data of radio intelligence, information about the identification of persons who committed crimes on the territory of Ukraine, obtained during the intelligence activities.

Key words: covert investigative actions, information removal, electronic communication networks, intelligence activities, electronic communications, intelligence.

Постановка проблеми. Прийняття Закону України «Про електронні комунікації» призвело до низки змін у кримінальне процесуальне законодавство. Закріплення нових підходів до роботи з електронними комунікаційними мережами викликає потребу переосмислення підходів щодо проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних комунікаційних мереж, її співвідношення із аналогічними розвідувальними заходами.

Ці питання у доктрині ще не досліджувалися, крім розгляду у аспекті інших змін та доповнень до законодавства у працях О. Бабікова, В. Завтура, І. Гловюк та ін.

Метою статті є визначення мети та порядку проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних комунікаційних мереж, виокремлення її видів та співвідношення із аналогічними розвідувальними заходами.

Виклад основного матеріалу. Відповідно до ч. 1 ст. 263 КПК зняття інформації з електронних комунікаційних мереж є різновидом втручання у приватне спілкування, що проводиться без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можливо встановити обставини, які мають значення для кримінального провадження.). Варто погодитися з думкою, що зняття інформації з електронних комунікаційних мереж з огляду на бурхливий розвиток засобів зв'язку та інформаційних технологій є одним із найбільш перспективних засобів розкриття і розслідування злочинів, здобуття і перевірки доказів [1, с. 160].

У зв'язку з прийняттям ЗУ «Про електроні комунікації» замість терміну «транспортна телекомунікаційна мережа» запроваджено термін «електронна комунікаційна мережа». Згідно п. 25 ч. 1 ст. 2 вказаного Закону електронна комунікаційна мережа це комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг, що є ширшим поняттям ніж транспортна телекомунікаційна мережа, під якою розумілася мережа, що забезпечує пере-

давання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу, оскільки включає в себе як технічні засоби передачі так і забезпечувальні споруди [2].

Водночас, таке визначення не повністю узгоджується із європейськими стандартами у сфері електронних комунікацій. Зокрема, згідно п. 1. ч. 1 ст. 2 Директиви «Про запровадження Європейського кодексу електронних комунікацій» «електронна комунікаційна мережа» означає системи передачі, незалежно від того, чи вони базуються на постійній інфраструктурі або централізованому адмініструванні потужностей, і, якщо застосовно, обладнання для комутації або маршрутизації та інші ресурси, включаючи неактивні елементи мережі, які дозволяють передавати сигнали через дротові, радіо-, оптичні або інші електромагнітні засоби, включаючи супутникові мережі, мережі фіксованого (з комутацією каналів та з комутацією пакетів, включаючи Інтернет) та мобільного зв'язку, електросилові кабельні системи, в тій мірі, в якій вони використовуються для передачі сигналів, мережі радіота телевізійного мовлення та мережі кабельного телебачення, незалежно від типу переданої інформації [3].

Доступ до інформації про споживача, факти надання електронних комунікаційних послуг, у тому числі до даних, що обробляються з метою передачі такої інформації в електронних комунікаційних мережах, здійснюється виключно на підставі рішення прокурора, суду, слідчого судді у випадках та порядку, передбачених законом (ч. 1 ст. 121 ЗУ «Про електроні комунікації»).

Незважаючи на те, що законодавець змінив назву НСРД у ст. 263, відповідні зміни у Інструкцію про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні внесені не були. Однак, за своєю правовою природою зняття інформації з електронних комунікаційних мереж можна розподілити на два види:

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

– зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на електронних комунікаційних мереж, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

Таким чином, об'єктом першого виду зняття інформації з електронних комунікаційних мереж будуть: телефонні лінії загального користування; відомчі мережі, що мають вихід на телефоні лінії загального користування; виділені мережі зв'язку невиробничого призначення; мережі пересувного радіотелефонного зв'язку; системи пересувного супутникового зв'язку.

Зняття інформації з електронних комунікаційних мереж цього виду завжди повинно передбачати контроль розмов обидвох абонентів, шляхом використання безпосереднього підключення до телефонного каналу або сканування радіоканалу. Прослуховування телефонної розмови тільки одного з абонентів, в тому числі і з використанням технічних засобів, без підключення до мережі зв'язку не вважається зняттям інформації з електронних комунікаційних мереж, як інша НСРД пов'язана із втручанням у приватне спілкування (наприклад, аудіо-, відеоконтроль особи).

Об'єктом другого виду зняття інформації з електронних комунікаційних мереж будуть: телексні, факсимільні, селекторні, радіорелейні, пейджингові канали обміну інформації між абонентами, комп'ютерні мережі різного рівня.

Фіксація повідомлень, переданих в комп'ютерних мережах, має певні особливості. Загальним правилом є те, що інтернет-провайдер, укладаючи договір з користувачем про підключення до глобальної мережі Інтернет, з'ясовує і фіксує в договорі анкетні дані і точну адресу користувача. Це дає можливість «прив'язати» MAC-адресу та IP-адресу комп'ютера до конкретної особи. Однак при реєстрації в чатах, на форумах, в блогах, соціальних мережах користувач може не вказувати свої анкетні дані, а використовувати нікнейм, який становить собою умовне ім'я, яке не містить ніяких реальних відомостей про певну фізичну особу.

Всі повідомлення користувача надходять на центральний пристрій – сервер, потім за допомогою інших пристроїв (комутатора, маршрутизатора) направляються абонентам. При цьому відомості про відправника фіксуються і зберігаються на сервері провайдера.

Таким чином, повідомлення в комп'ютерних мережах можна відстежити за:

а) MAC-адресою, тобто ідентифікаційною адресою комп'ютерного обладнання;

б) IP-адресою, присвоєною комп'ютеру у відповідній комп'ютерній мережі;

в) адресою електронної поштової скриньки;

г) ідентифікаційному номеру UIN, наявного у користувачів ICQ;

д) даними, що містяться в облікового запису відвідувачів чатів, форумів, блогів, соціальних мереж.

В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікальне ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання, на якому може здійснюватися втручання у приватне спілкування.

До таких ідентифікаційних ознак можна віднести:

– електронний код (ідентифікатор) кінцевого (термінального) обладнання – код, який присвоюється виробником технічних засобів телекомунікацій для унікальної ідентифікації кінцевого обладнання (міжнародні серійні коди IMEI, ESN, MEID тощо) [4]. Це зумовлено визначенням кінцевого (термінального) обладнання, під яким законодавець розуміє, обладнання, призначене для з'єднання з кінцевим пунктом електронної комунікаційної мережі з метою забезпечення доступу до електронних комунікаційних послуг (п. 41 ч. 1 ст. 2 ЗУ «Про електроні комунікації»);

− ідентифікаційна телекомунікаційна картка – засіб, який використовується для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо);

− мережевий ідентифікатор споживача – індивідуальний набір цифр та/або символів, присвоєний кінцевому обладнанню абонента та/або споживачеві в телекомунікаційній мережі чи Інтернеті. Під ним потрібно розуміти або номер абонента в мережах GSM, CDMA або IP-адресу електронної інформаційної системи (ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад, Інтернет));

− MAC-адреса (*Media Access Control* – управління доступом до носія) – унікальний ідентифікатор, що зіставляється з різними типами обладнання для комп'ютерних мереж (мережевими картами, Wi-Fi роутерами тощо). Усі комп'ютери, підключені до локальної мережі з виходом в Інтернет, як правило, мають дві адреси: логічну адресу мережевого рівня (IP-адресу) і фізичну адресу мережевої інтерфейсної карти (MAC-адресу).

Варто зауважити, що закон вимагає від слідчого, прокурора вказати ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання, на якому може здійснюватися втручання у приватне спілкування. Тобто, у клопотання мають бути зазначені, як мінімум три цих елементи для ідентифікації абонента та відповідного обладнання. В зв'язку з цим, варто погодитися з думкою, що у конкретному випадку зняття інформації з транспортних телекомунікаційних мереж необхідно забезпечити повну ідентифікацію особи. Проте зробити це лише за допомогою ідентифікації певного телекомунікаційного обладнання неможливо. У такій ситуації завжди залишається імовірність того, що телекомунікаційне обладнання використовував не особисто підозрюваний, обвинувачений, навіть якщо на належність йому такого обладнання вказують матеріали справи, а інша особа. Інформація, що в такому разі була предметом зняття, може не належати до особи підозрюваного, обвинуваченого та/або не входити до предмета доказування. Тобто отримані в такий спосіб докази не можуть визнаватися належними і допустимими [5, с. 73].

Певну складність у розмежуванні зняття інформації з електронних комунікаційних мереж та електронних інформаційних систем під час здійснення онлайн-трансляцій вніс Верховний Суд, який зазначає, що оскільки зображення через веб-камеру одного комп`ютера транслюється на монітор іншого комп`ютера в системі загальної для них мережі, за час проходження через останню має місце запізнення сигналу з тимчасовим збереженням зображення на серверах та у пам`яті електронних пристроїв для здійснення безперервного потоку інформації шляхом буферизації та створення тимчасових файлів, то фактично має місце форма його матеріальної фіксації в комп`ютерній мережі, в якій відбувається трансляція, хоча і на дуже незначний час [6]. Однак, вважаємо, що цей підхід все одно свідчить про те, що навіть створення тимчасових файлів у мережі не спростовує факту зняття інформації, яка циркулює у електронній комунікаційній мережі, а отже така інформація має отримуватися в ході проведення такої НСРД, як зняття інформації з електронних комунікаційних мереж.

Згідно ч. 3 ст. 262 КПК України проведення зняття інформації з електронних комунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки. Керівники та працівники операторів електронних комунікацій зобов'язані сприяти виконанню дій із зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді. Цьому положенню кримінального процесуального законодавства кореспондує п. 2 до ч. 8 ст. 105 ЗУ «Про електроні комунікації», відповідно до якого постачальники електронних комунікаційних послуг повинні зберігати записи про надані електронні комунікаційні послуги протягом строку позовної давності, визначеного законом. Постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість підключення технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації, в точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг.

У ст. 265 КПК визначено, що зміст інформації, що передається особами через електронні комунікаційні мережі, з яких здійснюється зняття інформації, зазначається у протоколі про проведення зазначених негласних слідчих (розшукових) дій. При виявленні в інформації відомостей, що мають значення для конкретного досудового розслідування, в протоколі відтворюється відповідна частина такої інформації, після чого прокурор вживає заходів для збереження знятої інформації. В свою чергу зміст інформації, одержаної внаслідок здійснення зняття відомостей з електронних інформаційних систем або їх частин, фіксується на відповідному носієві особою, яка здійснювала зняття у спосіб, що забезпечує обробку, збереження або передання інформації.

Отримана у такий спосіб звукова інформація має бути розшифрована уповноваженою службовою особою із залученням, у необхідних випадках, відповідного спеціаліста. До протоколу даної НСРД вносяться лише ті фрагменти, які мають значення для кримінального провадження. Як спеціалісти, у даному випадку, можуть залучатися фахівці у галузі економіки, кредитування, аграрного сектору, природних ресурсів тощо, у залежності від виду розслідуваного кримінального правопорушення. Якщо особи, чия звукова інформація знята з електронних комунікаційних мереж спілкувалися іноземною мовою для розшифровування (перекладу) інформації залучається перекладач. Носії інформації, на яких міститься звукозапис розмов, можуть бути досліджені на предмет ототожнення особи за фізичними параметрами голосу та встановлення технічних умов і технології отримання відео-, звукозапису [7, с. 210].

У протоколі даної НСРД вказуються дата складення, посада, прізвище та ініціали особи, що веде кримінальне провадження, номер кримінального провадження згідно з ЄРДР, номер ухвали (постанови), а також дата прийняття та найменування суду, яким видано дозвіл на здійснення зняття інформації з електронних комунікаційних мереж та строки здійснення. Окрім того, у протоколі зазначається найменування підрозділу, працівники якого залучалися до здійснення зняття інформації з електронних комунікаційних мереж, дані про особу, стосовно якої здійснювалася НСРД, її результати, відомості про МНІ (матеріали аудіо чи відеозапису, фото- і кінозйомки, магнітні накопичувачі тощо) [8, с. 668].

Потрібно враховувати, що МНІ на яких зафіксовано телефонні розмови осіб, є речовими доказами особливого виду – похідними від усного спілкування. Тому, враховуючи принцип безпосередності дослідження доказів і для перевірки обставин отримання звукозапису необхідно отримати також показання хоча б однієї з осіб, яка брала участь в телефонній розмові, якщо це можливо. В іншому випадку для перевірки достовірності звукозапису та ідентифікації осіб, які спілкувалися між собою може бути призначена фоноскопічна (фонографічна) експертиза, яка може дати відповіді на наступні питання: кому з числа перелічених осіб належать окремі вислови, що містяться на фонограмі; чи є голос, зафіксований на фонограмі, голосом конкретної особи; чи зазнавала змін дана фонограма; чи мають місце ознаки монтажу фонограми; які є ознаки механічного та електронного монтажу фонограми; чи велась зафіксована на фонограмі розмова по телефону тощо.

Згідно ч 2 ст. 266 КПК України носії інформації, на яких зафіксовані відомості, отримані в результаті проведення зазначених негласних слідчих (розшукових) дій, повинні зберігатися у стані, придатному для їх дослідження, до набрання законної сили вироком суду. Як вірно зазначають І. Головюк, В. Завтур після внесення змін в КПК України вже нема вимоги, що мають зберігатися технічні засоби, що застосовувалися під час проведення зазначених негласних слідчих (розшукових) дій, а також первинні носії отриманої інформації, а також нема вимоги, що технічні засоби, за допомогою яких отримано інформацію, можуть бути предметом дослідження відповідних спеціалістів або експертів у порядку, передбаченому цим КПК України [9].

В зв'язку з цією нормою виникає питання чи можуть додатками до протоколу цієї НСРД бути дублікати МНІ чи

повинні додаватися саме оригінали МНІ на яких зафіксовано зміст інформації отриманої в результаті НСРД.

У ч .4 ст. 99 КПК України законодавець під дублікатом документа, який визнається судом як оригінал документа, розуміє також копію інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста. Перелік об'єктів з яких дозволяється копіювання інформації, для використання її в якості оригіналу в доказуванні дозволяє зробити висновок, що законодавець мав на увазі фактично різновиди електронних інформаційних систем у кримінально процесуальному розумінні цього поняття. Таким чином, як випливає з переліку цих об'єктів інформація яка міститься в електронних комунікаційних мереж не належить до видів інформації з якої можна зробити дублікат, а отже до протоколів НСРД зняття інформації з електронних комунікаційних мереж мають додаватися саме оригінали МНІ зі змістом інформації отриманої в ході її проведення.

У пам'яті обладнання операторів і провайдерів електронних комунікаційних мереж часто залишаються дані (SMS, MMS, *e-mail* та інші повідомлення) з текстовою, а також фото- відеоінформацією, що передається як кореспонденція між особами. Проте слід врахувати, що повідомлення, які надійшли на пошту електронної адреси, SMS, MMS та ін., у тому числі й голосова пошта, повідомлення на автовідповідач, але не відкриті для прочитування (прослуховування, перегляду), належать до категорії кореспонденції, що підпадає під захист ст. 8 ЄКПЛ, і доступ до них може бути здійснено лише на підставі статей 261, 263 КПК. Але якщо буде встановлено, що отримувач ознайомлений з їхнім змістом, то вони можуть бути доступними для вилучення в порядку норм глави 15 КПК [10, с. 105].

Варто також розмежувати зняття інформації з електронних комунікаційних мереж, як негласну слідчу (розшукову) дію та як розвідувальний захід. Так, згідно п. 2 ч. 1 ст. 15 Закону України «Про розвідку» одним з розвідувальних заходів є зняття інформації з транспортних телекомунікаційних мереж шляхом відбору та фіксації змісту відповідних відомостей або даних, що передаються або отримуються особою. Як випливає з цієї законодавчої норми Закон України «Про розвідку» не зазнав змін в частині приведення у відповідність назви розвідувального заходу до термінології ЗУ «Про електронні комунікації», що зумовлено недоліками законодавчої техніки.

Першою відмінністю є суб'єкти проведення. Так, суб'єктами проведення зняття інформації з електронних комунікаційних мереж, як НСРД є органи визначені у ч. 3 ст. 262 КПК України, а суб'єктами проведення зняття інформації з електронних комунікаційних мереж, як розвідувального заходу виступають розвідувальні органи в особі: Служби зовнішньої розвідки України; розвідувального органу Міністерства оборони України (станом на сьогодні ним виступає Головне управління розвідки МОУ, яке координує діяльність суб'єктів воєнної розвідки, зокрема органів військового управління розвідки і військових частин розвідки Збройних Сил України та Сил спеціальних операцій Збройних Сил України); розвідувального орган центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону (станом на сьогодні ним виступає розвідувальний орган Адміністрації Державної прикордонної служби України), а також оперативні підрозділи Центрального управління Служби безпеки України, що здійснюють контррозвідувальну діяльність.

Друга відмінність полягає у тому як розвідувальний захід дана дія проводиться за умови, якщо він безпосередньо пов'язаний із здійсненням розвідувальної діяльності за межами України або спрямований на здобування розвідувальної інформації, що має джерело походження за межами України, та виключно на підставі рішення суду (ч. 1 ст. 15 ЗУ «Про розвідку») [11]. Метою ж цієї дії як НСРД є встановлення обставин, які мають значення для кримінального провадження.

Третя відмінність полягає у суб'єкті звернення з клопотанням про надання дозволу на проведення зняття інформації з електронних комунікаційних мереж. У випадку розвідувального заходу таким суб'єктом виступає виключно керівник розвідувального органу або уповноважений ним заступник керівника розвідувального органу, у випадку негласної слідчої (розшукової) дії суб'єктом є прокурор або слідчий за погодженням з прокурором. Потрібно звернути увагу, що розвідувальний захід – зняття інформації з електронних комунікаційних мереж, на відміну від аналогічної негласної слідчої (розшукової) дії чи оперативно-розшукового заходу не потребує погодження клопотання прокурором, що зумовлено відсутністю прокурорського нагляду за розвідувальною діяльністю.

Закон України «Про розвідку» визначає, що клопотання про надання дозволу на проведення розвідувального заходу розглядається уповноваженим суддею суду, у межах територіальної юрисдикції якого перебуває розвідувальний орган. Таким, суддею відповідно до п. 9-1 ч. 1 ст. 29 Закону України «Про судоустрій та статус суддів» є голова апеляційного суду та/або призначений ним суддя (судді) з числа суддів апеляційного суду, у межах територіальної юрисдикції якого перебуває розвідувальний орган [12].

Одним з проблемним питань під час проведення даного розвідувального заходу є використання отриманої інформації у кримінальному провадженні. Так, відповідно до ч. 3 ст. 24 ЗУ «Про розвідку » у разі виявлення під час проведення розвідувальних заходів ознак злочину розвідувальні органи повідомляють про це відповідний орган досудового розслідування. Постає запитання, чи мова йде виключно про інформування органу про виявлені ознаки злочину чи про передання матеріалів отриманих в ході проведення розвідувального заходу. В даному випадку вважаємо, що мова йде саме про інформування органу досудового розслідування шляхом надсилання розвідувальним органом рапорту, довідки тощо, у якому викладені виявлені під час проведення розвідувального заходу ознаки злочину. Така позиція, випливає також із положень ч. 3 ст. 14 Закону України «Про розвідку», згідно якої, розвідувальні заходи не можуть організовуватися і проводитися для вирішення завдань кримінального провадження.

Однак, такий підхід законодавця потребує переосмислення в сучасних умовах в контексті можливості використання розвідувальної інформації у кримінальному процесуальному доказуванні. Агресія росії призвела до того, що велика частина доказової інформації отримується саме членами розвідувального співтовариства, а використання її у кримінальному провадженні фактично неможливе через відсутність процедури легалізації такої інформації та положення ч. 3 ст. 14 Закону України «Про розвідку».

Висновки.

Трансформація негласної слідчої (розшукової) дії – зняття інформації з електронних комунікаційних мереж зумовлено розвитком інформаційних технологій, приведенням у відповідність українського кримінального процесуального законодавства до міжнародних стандартів. Враховуючи що дана НСРД істотно втручається в права та свободи громадян, процесуальний порядок її проведення має забезпечувати гарантії від неправомірного втручання в приватне спілкування, а саме проведення негласної слідчої (розшукової) дії має відповідати завданням кримінального провадження, щоб не допустити необґрунтованого порушення прав громадян.

Водночас, недооціненим є потенціал розвідувальної діяльності, як способу отримання доказів у криміналь-

ному провадженні. В зв'язку з цим виникає нагальна необхідність розроблення процедури легалізації інформації отриманої в ході розвідувальної діяльності у кримінальному провадженні, що дозволить використовувати у доказуванні перехоплення телефонних розмов окупантів, дані радіотехнічної розвідки, інформацію щодо ідентифікації осіб, які вчинили злочини на території України, отриману в ході проведення розвідувальних заходів.

ЛІТЕРАТУРА

1. Щербаковський М. Г., Коршенко В. А. Тактичні та організаційні особливості зняття інформації з транспортних телекомунікаційних мереж. *Криміналістика і судова експертиза.* 2018. Вип. 63. С. 154-162.
2. Про електронні комунікації: Закон України від 16 грудня 2020 року №1089-IX. *Офіційний вісник України.* 2021. № 6. ст. 306.
3. Директива Європейського парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року «Про запровадження Європейського кодексу електронних комунікацій». URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972. (дата звернення: 21.06.2022).
4. Правила надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України №295 від 11 квітня 2012 р.: [із змінами і доповненнями на 05.06.2021]. *Офіційний вісник України.* 2012. №29. ст. 1074.
5. Бабкова В. С. Проблеми визнання результатів зняття інформації з транспортних телекомунікаційних мереж належними та допустимими доказами. *Юрист України.* 2018. № 2. С. 68-75.
6. Постанова Верховного Суду від 18.06.2020 року у справі № 711/7900/17. Єдиний державний реєстр судових рішень. https://reyestr.court.gov.ua/Review/89929158
7. Бараненко Б.І. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: [навч – практ. посіб.]. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2014. 414 с.
8. Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. / за заг. ред. В.Я. Тація, В.П. Пшонки, А.В. Портнова. Т. 1. Х.: Право, 2012. 767 с.
9. Главюк І., Завтур В. Від окремого до загального. Підвищення ефективності досудового розслідування: до питання пропорційності обмеження прав людини. Інтернет: https://zib.com.ua/ua/print/151120.html.
10. Тагієв С. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Часопис цивільного і кримінального судочинства*. 2013. №4. С. 98-110.
11. Про розвідку: Закон України від 17 вересня 2020 року № 912-IX [із змінами та доповненнями станом на 30.04.2022]. *Офіційний вісник України.* 2020. № 86. ст. 2761.
12. Про судоустрій і статус суддів: Закон України від 2 червня 2016 року №1402- [із змінами та доповненнями станом на 15.03.2022]. *Офіційний вісник України.* 2016. № 56. ст. 1935.