Метелев О. П.,
аспірант кафедри кримінального права
та кримінального процесу
Національної академії Служби безпеки України
ORCID ID:*0000–0003–2969–8388*

Науковий керівник:
М. Є. Шумило*, доктор юридичних наук, професор,*
професор кафедри правосуддя юридичного факультету
Київського національного університету імені Тараса Шевченка

DOI: *https://doi.org/10.17721/2413-5372.2019.4/161-173*

УДК:343.14

ТРАНСПОРТНІ ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ЯК ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ДЛЯ ОТРИМАННЯ ВІДОМОСТЕЙ ЗНАЧУЩИХ ДЛЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ: ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ

Анотація. *Науково-технічний прогрес, а також стрімкий розвиток інформаційних технологій, формування інформаційного суспільства, впровадження телекомунікаційних систем та мереж в усі життєво важливі процеси, доступність засобів цифрового зв'язку та передачі інформації обумовило необхідність застосування нових методів боротьби зі злочинами в новому інформаційному (кібернетичному) просторі, цьому штучно створеному середовищі, невід'ємною складовою якого є транспортні телекомунікаційні мережі (ТТМ). Екстериторіальний характер транспортних телекомунікаційних мереж та систем разом із глобальною мережею Інтернет в значній мірі ускладнює їх правове регулювання, оскільки іноді досить складно визначити, до юрисдикції якої держави відноситься кримінальне правопорушення. Отже, при проведенні негласних розшукових (слідчих) дій виникає закономірне питання щодо правомірності роботи в інформаційному середовищі транспортної телекомунікаційної мережі для отримання цифрових доказів в інтересах кримінального провадження.*

Мета статті: *дослідити проблемні питання правового регулювання при роботі в транспортних телекомунікаційних мережах для отримання відомостей значущих для кримінального провадження під час проведення негласних (слідчих) розшукових дій.*

У роботі звертається увага на недостатній рівень наукових досліджень у висвітленні проблемних питань вивчення транспортних телекомунікаційних мереж як інформаційного середовища для законного отримання цифрових доказів в інтересах кримінального судочин-

ства. Аналізуються норми вітчизняного законодавства, які регулюють суспільні відносини в цій сфері, а також наводиться практика Європейського Суду з прав людини, яка викриває деякі «білі плями» в національних законодавствах щодо забезпечення законності та захисту прав людини під час проведення негласних заходів по втручанню у приватне спілкування в інформаційному середовищі транспортних телекомунікаційних мереж.

З урахуванням екстериторіального характеру інформаційного (кібернетичного) простору робиться висновок щодо необхідності чіткого законодавчого регулювання процесуальної діяльності в транспортних телекомунікаційних мережах для забезпечення в цій сфері суспільних відносин безпеки особистості, суспільства і держави в цілому.

У статті також розглядаються різні підходи щодо юридичних розбіжностей під час розслідувань злочинів у кіберпросторі. Ставиться питання щодо визначення місця злочину в інформаційному (кібернетичному) просторі, робиться спроба дати дефініцію «місця вчинення злочину» та надаються пропозиції щодо удосконалення законодавства.

Ключові слова: *кримінальний процес, транспортна телекомунікаційна мережа, кібернетичний простір, місце вчинення злочину.*

Постановка проблеми. В сучасному світі глобальний інформаційний простір, який становить собою єдність двох складових: технічної (глобальна мережа Інтернет з телекомунікаційною інфраструктурою зв'язку і комунікаціями) і соціальної (глобальна спільнота інтернет-користувачів) став одним із ключових чинників, який суттєво впливає на стан і розвиток суспільства та світову економіку. Процес глобалізації, який сьогодні охопив кожну економіки світу, тісно пов'язаний з розвитком телекомунікаційних мереж і мережевих технологій. Тепер в Україні стрімко розвиваються напрями підвищення швидкостей передачі даних як в магістральних мережах (зі швидкістю передачі інформації до 100 Гбіт/с), так і в бездротових широкосмугових мережах (швидкими темпами йде перехід мобільних пристроїв на технології 4G, а згодом і на 5G, які забезпечують швидкість передачі даних до 20 Гбіт/с, із набагато більшим покриттям ніж у WiMAX і WiFi мережах), що, в свою чергу, позитивно позначиться на розвитку інтернету речей – перспективної концепції обчислювальної мережі фізичних предметів (речей).

Аналіз останніх досліджень і публікацій. Проведений аналіз наукової літератури свідчить, що наукові дослідження транспортних телекомунікаційних мереж як особливого інформаційного середовища для отримання відомостей значущих для кримінального провадження у юридичній літературі практично відсутні. Основна увага дослідників у переважній більшості зосереджувалась у процесуальній площині процедури зняття інформації з каналів зв'язку (транспортних телекомунікаційних мереж) як способу документування протиправних дій, а також діяльності правоохоронних органів та органів державної безпеки. У цій сфері процесуальної науки проводили дослідження М. В. Багрій, В. Д. Берназ, В. М. Биков, Р. І. Благута, С. М. Гриняєв, С. М. Гусаров, Є. А. Доля, С. В. Єськов, В. І. Зажицький, Г. С. Корж, М. В. Корнієнко, О. А. Коцюба, С. В. Лаврухин, О. В. Литвиненко, І. М. Лоскутов, Є. Д. Лук'янчиков, Д. О. Максимус, О. В. Манжай, Д. Й. Никифорчук, Ю. Ю. Орлов, М. М. Перепелиця, І. Л. Петрухин, В. С. Серьогін, А. В. Тарасюк, В. М. Тертишник, В. Г. Уваров, Д. М. Цехан, В. М. Шевченко С. П. Щерба і деякі інші науковці. До того ж такі науковці, як Л. І. Аркуша, О. А. Білічак, С. О. Гриненко, О. М. Дроздов, С. В. Єськов, В. А. Колеснік, С. С. Кудінов, М. А. Погорецький, Д. Б. Сергєєва, Є. Д. Скулиш, С. Р. Тагієв, Р. М. Шехавцов досліджували деякі аспекти втручання у приватне спілкування та їх використання у кримінальному провадженні.

Отже, **метою статті є:** дослідити проблемні питання правового регулювання при роботі в транспортних теле-

комунікаційних мережах для отримання відомостей значущих для кримінального провадження під час проведення негласних (слідчих) розшукових дій.

Виклад матеріалу дослідження. По-перше, визначимось з поняттями «інформаційний простір» (або інакше «кіберпростір») та «транспортна телекомунікаційна мережа», а також як ці поняття співвідносяться.

Поява поняття «інформаційний простір» було обумовлене зростаючою потребою суспільства в постійному безперервному інформаційному потоці.

Законодавець визначив, що інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді[1]. За філософським словником, «простір» – це філософська категорія, яка передає спосіб співіснування розмаїтих матеріальних утворень[2]. Таким чином, об'єднавши разом два поняття, отримаємо певну систему взаємодії суб'єктів і об'єктів оточуючого середовища, пов'язаних між собою завдяки процесам виробництва (створення) передачі та споживання (отримання) відомостей. Ця система і є «інформаційним простором». Цілком можливо погодитись з думкою В. Л. Гирича та В. Н. Чуприної, які дали наступне визначення: «Інформаційний простір – це сукупність інформаційних ресурсів і інфраструктур, які складають державні і міждержавні комп'ютерні мережі, телекомунікаційні системи і мережі загального користування, інші транскордонні канали передачі інформації»[3].

Інформаційні системи, такі як всесвітня інформаційна система загального доступу Інтернет, є складовими кіберпростору. Згідно з ст. 1 Закону України «Про телекомунікації» інформаційна система загального користування – це сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних[4]. Далі в ст. 1 Закону зазначається, що телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням. У свою чергу, транспортна телекомунікаційна мережа (ТТМ) – це мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу.

Таким чином, транспортна телекомунікаційна мережа – це невід'ємна частина глобального інформаційного простору, яка становить собою інформаційне середовище, що забезпечує передачу цифрової інформації (даних) у глобальному інформаційному (кібернетичному) просторі.

У транспортній телекомунікаційній мережі циркулюють цифрові відомості, які можуть бути значущими для кримінального провадження, тому під час проведення негласних слідчих (розшукових дій) виникає необхідність використання ТТМ для належного отримання цифрових доказів для їх подальшого використання в кримінальному процесі.

У цій статті розглянемо два найбільш значущих проблемних питання, які нерозривно пов'язані між собою – це законність роботи в ТТМ при отриманні цифрових відомостей та транскордонний (екстериторіальний) характер ТТМ, що значно ускладнює визначення

[1] Про інформацію: Закон України від 02.10.1992 № 2657-XII <https://zakon.rada.gov.ua/laws/show/2657–12> дата звернення 18.12.2019.

[2] В Шинкарук та ін, *Філософський енциклопедичний словник* (Київ 2002) 529.

[3] В Гирич, В Чуприна, '*Глобальное информационное пространство и проблема доступа к мировым информационным ресурсам*' <http://marc21.rsl.ru/upload/mba2007/mba2007_05.pdf> дата звернення 20.12.2019.

[4] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV <https://zakon.rada.gov.ua/laws/show/1280–15> дата звернення 18.12.2019.

просторової дії кримінально-процесуального законодавства.

При проведенні негласних розшукових (слідчих) дій перш за все необхідно передбачити та забезпечити законність роботи в інформаційному середовищі ТТМ, оскільки таке втручання, певним чином, обмежує права та свободи людини на таємницю спілкування.

У вітчизняному законодавстві забезпечення гарантії прав і свобод щодо таємниці спілкування законодавець передбачив у новелах Кримінального процесуального кодексу України. Так, відповідно до п. 7 ч. 1 ст. 7 КПК України таємниця спілкування є однією із загальних засад кримінального провадження[1]. Також у ст. 14 КПК України наголошується, що під час кримінального провадження кожному гарантується таємниця приватного листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Єдиною умовою втручання у таємницю спілкування є лише судове рішення, яке прийняте у випадках, передбачених КПК України, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети. До того ж інформація, отримана внаслідок втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального провадження.

Відповідно до положень Розділу II Рекомендацій Комітету міністрів Ради Європи «Про особливі методи розслідувань тяжких злочинів, в тому числі терористичних актів» від 20.04.2005 № Rec (2005) 10[2] та вимог Європейської Конвенції «Про захист прав і основних свобод людини» (ETS № 5)[3] у законодавстві України було необхідно вказати обставини та умови, за яких компетентні органи були б уповноважені застосувати особливі методи розслідування та прийняти належні законодавчі заходи, які б дозволяли надавати докази, отримані в результаті використання особливих методів розслідування, у суді. Також згідно з Рекомендаціями процесуальні норми, які регулюють надання та належність таких доказів, повинні були гарантувати право обвинуваченого на справедливе судове провадження.

Як наслідок, у Кримінальний процесуальний кодекс України 2012 року був включений Розділ 21 «Негласні слідчі розшукові дії».

Також з метою забезпечення належної організації проведення негласних заходів була розроблена відповідна Інструкція щодо організації проведення НСРД, яка регулює процеси втручання у приватне спілкування, у тому числі в транспортних телекомунікаційних мережах, а саме зняття інформації з ТТМ. Відповідно до Інструкції зняття інформації з транспортних телекомунікаційних мереж полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду)[4].

---

[1] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI <http://zakon5.rada.gov.ua/laws/show/4651–17> дата звернення 19.12.2019.

[2] Об особых методах расследования» тяжких преступлений, в том числе террористических актов: Рекомендация Комитета министров Совета Европы государствам-членам от 20.05.2005 N Rec (2005) 10 <https://zakon.rada.gov.ua/laws/show/994_670?lang=uk> дата звернення 18.12.2019.

[3] Конвенція про захист прав і основних свобод людини, Рим, 4.XI.1950: Конвенцію ратифіковано Законом № 475/97-ВР від 17.07.97 <https://zakon.rada.gov.ua/laws/show/995_004> дата звернення 20.12.2019.

[4] Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Інструкція затверджена наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5 <https://zakon.rada.gov.ua/laws/show/v0114900–12> дата звернення 18.12.2019.

Таким чином, транспортна телекомунікаційна мережа є тим інформаційним середовищем, де правоохоронними органами, які мають такі повноваження, за умови отримання відповідного судового рішення здійснюється:

– 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), 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 транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

Зазначимо, що в побудові та організації функціонування транспортних телекомунікаційних мереж все визначається міжнародними стандартами, які визначені міжнародною організацією зі стандартизації (ISO – International Standards Organization). Найбільш відомий стандарт ISO в сфері телекомунікації – це багаторівнева модель взаємодії відкритих систем, так звана «модель OSI» (OSI – Open Systems Interconnection), яка була розроблена для сполучення різних видів обчислювального та телекомунікаційного обладнання сторонніх виробників.

Ці стандарти виключають двояке тлумачення, проте юридичне розуміння використання ТТМ як інформаційного середовища для отримання цифрових доказів в інтересах кримінального провадження досить неоднозначне.

Практика Європейського Суду з прав людини свідчить про те, що у національних законодавствах ще багато «білих плям», які необхідно динамічно заповнювати і є нагальна потреба в правильному правовому тлумаченні правових приписів для захисту прав людини під час проведення негласних заходів у транспортних телекомунікаційних мережах, які стосуються втручання у приватне спілкування, у тому числі це стосується і зняття інформації з ТТМ.

Так, Європейський Суд з прав людини, розглядаючи справу «Биков проти Росії» (Bykov v. Russia) від 10 березня 2009 року № 4378/02, не визнав логічними доводи обвинувачення про те, що чинні національні правила РФ стосовно прослуховування телефонних розмов не повинні за аналогією поширюватись щодо радіопередавачів, а отже для здійснення радіоперехоплення розмов (так званого «вільного пошуку в радіоефірі») отримання дозволу суду не потрібно. В рішенні Європейського Суду з прав людини, зокрема, зазначалось: «Суд неодноразово заявляв, що коли йдеться про перехоплення повідомлень з метою поліційного розслідування, «закон має бути достатньо чітким у своїх формулюваннях, щоб давати громадянам належне розуміння того, за яких обставин та на яких умовах органи держави уповноважені вдаватися до таких таємних і потенційно небезпечних способів посягання на їхнє право на повагу до особистого життя і кореспонденції»… На думку Суду, ці принципи так само застосовні до використання і радіопередавачів, які за своєю природою та рівнем втручання практично тотожні телефонам, які прослуховують. За відсутності конкретних і детальних правил застосування цього способу спостереження в рамках «оперативного експерименту» не супроводжувалося достатніми заходами захисту від різних можливих зловживань. Отже, його застосування уможливлювало свавілля і не відповідало вимогам законності». Суд дійшов висновку про порушення пункту 2 статті 8 Конвенції про захист прав людини і основоположних свобод[1].

[1] Д Макбрайд, *Європейська конвенція з прав людини та кримінальний процес. Практика Європейського*

Дійсно, з інженерно-технічного погляду немає різниці між бездротовим радіоканалом і проводовим каналом передачі інформації – це лише різні види середовища (канали) передачі даних. Транспортні телекомунікаційні мережі використовують чотири основні середовища передачі інформації з одного пункту в інший:

Мідні кабелі, які використовують у локальних обчислювальних мережа і телефонних абонентських лініях.

Оптоволоконні кабелі, які використовують для високошвидкісної передачі даних у телекомунікаційних мережах.

Радіодіапазон вільного простору, який використовується для радіозв'язку, мобільного і супутникового зв'язку.

Оптичний діапазон вільного простору, який використовується для контролю інфрачервоних віддалених випромінювань (ІЧ-порти).

Протягом багатьох років у середовищі процесуалістів точилися дискусії щодо законності проведення «вільного пошуку» на радіоканалах (у тому числі транкінгового і GSM зв'язку), каналах пейджингового, факсимільного та супутникового зв'язку. Звичайно, в умовах нормативної невизначеності на початку XXI століття мали місце і зловживання. Цілком закономірно з погляду захисту прав і свобод людини Європейський суд з прав людини ще в 2009 році прийняв обґрунтоване рішення, а в 2012 році з прийняттям Кримінального процесуального кодексу України в питанні законності «вільного пошуку» в радіоефірі теж була поставлена крапка: такі заходи проводяться тільки з санкції слідчого судді.

В інших випадах в національних законодавствах недостатньо чітко визначені обставини, за яких здійснюється втручання в середовище транспортної телекомунікаційної системи для отримання цифрових доказів. Так, у справі «Роман Захаров проти Росії» (Roman Zakharov v. Russia) від 4 грудня 2015 року № 47143/06 Європейський Суд з прав людини дійшов висновку: «…що положення законодавства Російської Федерації, якими регламентується прослуховування засобів зв'язку, не забезпечують достатніх та ефективних гарантій від свавілля та ризику перевищення повноважень, властивого будь-якій системі негласного спостереження, і особливо високого в такій системі, де таємні служби і правоохоронні органи мають безпосередній доступ до прослуховування мобільних телефонів за допомогою технічних засобів. Зокрема обставини, за яких органи державної влади уповноважені вдаватися до заходів негласного спостереження, не визначені достатньо чітко. Положення про припинення заходів негласного спостереження не забезпечують достатніх гарантій від свавільного втручання. Національне законодавство дозволяє автоматично зберігати неактуальні дані і недостатньо виразно визначає обставини, за яких матеріал прослуховування зберігається і знищується після завершення судового розгляду. Дозвільні процедури не здатні забезпечити призначення заходів негласного спостереження лише в разі «необхідності в демократичному суспільстві». Нагляд над прослуховуванням, як він організований на сьогодні, не відповідає вимогам незалежності, повноважень і компетенції, достатнім для здійснення ефективного і постійного контролю, громадського нагляду та ефективності на практиці. Ефективність засобів юридичного захисту зменшується через відсутність повідомлення в будь-який момент про прослуховування або належного доступу до документів, пов'язаних із прослуховуванням… Показово, що наведені вище упущення в правовій базі імовірно впливають на саме функціонування системи негласного спостереження, яка існує в Росії. Суд не переконали доводи влади стосовно того, що всі прослуховування в Росії здійснюються законно з відповідного дозволу суду. Приклади, наведені заяв-

суду з прав людини. Рада Європи (друге видання) (Київ, К.І.С. 2018) 154–155.

ником у ході провадження в національних судах… і під час розгляду в цьому Суді… свідчать про існування свавільної та надмірної практики внаслідок недостатніх гарантій, передбачених законодавством… З огляду на названі вище упущення Суд вважає, що російське законодавство не відповідає вимозі про «якість закону» і не здатне утримувати «втручання» в межах «необхідного в демократичному суспільстві». Відповідно, на думку Європейського Суду з прав людини, мало місце порушення статті 8 Конвенції[1]. Крім того, має місце незаконне застосування технічних засобів для отримання інформації з середовища ТТМ. Так, у своєму рішенні по справі «Ван Вондель проти Нідерландів» (Van Vondel v. Netherlands) від 25 жовтня 2007 року № 38258/03 Європейській Суд зазначає: «Заявник скаржився на порушення його права на недоторканність приватного життя, бо низка його (телефонних) розмов із паном Р. була записана останнім за допомогою пристроїв, які Департамент внутрішніх розслідувань Національної поліції надав панові Р., також давши вказівки щодо суті розмови, яку слід вести із заявником… Хоча Суд і розуміє практичні труднощі, на які наражається особа, котрій органи слідства не довіряють, або котра побоюється, що вони їй не довіряють, при підтвердженні інформації, яку вона повідомляє таким органам, а також, що з цієї причини такій особі може знадобитися технічна допомога з боку цих органів, проте він не може погодитися з тим, що надання такої допомоги з боку органів влади не регулюються нормами, спрямованими на забезпечення правових гарантій проти свавільних дій. Через це Суд вважає, що в тому, що стосується оскаржуваного втручання, заявник був позбавлений мінімального ступеня захисту, на який він мав право відповідно до принципу верховенства права в демократичному суспільстві»[2]. Європейський Суд з прав людини дійшов висновку, що втручання в особисте життя було здійснене не «згідно із законом», а цього досить, щоб визнати порушення статті 8 Конвенції.

Разом із тим, міжнародна правознавча спільнота постійно досліджує питання та удосконалює підходи, пов'язані з проведенням особливих методів розслідувань тяжких та особливо тяжких злочинів, де важлива роль у боротьбі зі злочинністю відведена використанню середовища транспортних телекомунікаційних мереж для отримання значущої для кримінального слідства інформації. Так, у концептуальних документах з питань забезпечення національної безпеки провідних демократичних держав (зокрема – США, Великої Британії, ФРН тощо) одним із важливих механізмів моніторингу стану національної безпеки визначений негласний збір, пошук та фіксація інформації з використанням систем перехоплення інформації в телекомунікаційних мережах[3].

Багаторічний досвід провідних країн у боротьбі зі злочинністю та тероризмом однозначно свідчить про високу ефективність впровадження систем перехоплення в інформаційному просторі транспортних телекомунікаційних мереж для збору превентивної інформації щодо терористичних актів та інші протиправні дії, що плануються. В «Конвенції про кіберзлочинність» від 23.11.2001 (або Будапештській конвенції), яка ратифікована Верховною Радою України 07.09.2005, зазначається, що здійснення перехоплення інформації у міжнародних телекомунікаційних мережах є необхідною умовою боротьби проти найбільш небезпечних злочинних угруповань та міжнародних терористів[4]. Згодом був

[1] Там само 152–153.

[2] Там само 154–155.

[3] В Серьогін, 'Проблеми створення системи моніторингу інформаційного простору України' *Інформаційна безпека держави у світлі розвитку сучасних інформаційних технологій: Матеріали наук.-практ. конф.* (м. Київ, 30 червня 2006р.) (Київ 2007) 100.

[4] Конвенція про кіберзлочинність від 23.11.2001. Ратифіковано із застереженнями і заявами Законом

прийнятий «Додатковий протокол про криміналізацію дій расистського й ксенофобського характеру, вчинених через комп'ютерні системи» від 28.01.2003, який був ратифікований Верховною Радою України 21.07.2006 [1]. Діяння, які передбачені Конвенцією та Додатковим протоколом, підлягають обов'язковій криміналізації державою, що їх ратифікувала, поділяються на чотири групи: 1) правопорушення проти конфіденційності, цілісності й доступності комп'ютерних даних і систем; 2) правопорушення, які пов'язані з комп'ютерами; 3) правопорушення, які пов'язані зі зберіганням інформації; 4) правопорушення, які пов'язані з порушенням авторських і суміжних прав.

На сьогодні Конвенція про кіберзлочинність залишається найбільш актуальним міжнародним документом відносно кіберзлочинності і електронних (цифрових) доказів. При цьому вона постійно оновлюється в протоколах та керівних вказівках. Також активно ведуться перемовини стосовно Другого Додаткового протоколу щодо розширення міжнародного співробітництва і доступу до доказів в «хмарних сховищах», що в перспективі значно збільшить кількість інструментів та засобів для забезпечення верховенства права в кіберпросторі.

Інший проблемний аспект ТТМ як середовища для отримання відомостей значущих для кримінального провадження – це екстериторіальний характер транспортних телекомунікаційних мереж цього штучно створеного інформаційного простору. Ця обставина ставить під сумнів традиційне поняття територіальної юрисдикції, а також основні норми міжнародного права в частині, що стосуються визначення місця злочину в кібернетичному просторі. Поява кіберпростору як особливого середовища існування людини вже призвело до корінних змін у соціумі архетипів, ритмах функціонування, естетичних образах, моделях економічної діяльності та формах соціальних взаємодій[2]. Отже, виникнення нового середовища для взаємодії суб'єктів правових відносин зумовило виникнення набагато ширшого кола юридичних питань, на які до цього часу ще не знайдено відповідей.

Ці правозастосовні проблеми закономірно привернули увагу злочинної спільноти до використання транспортних телекомунікаційних мереж у своїх цілях, оскільки кіберпростір дозволяє:

– здійснювати віддалений зв'язок між злочинними угрупованнями;

– здійснювати анонімний пошук співучасників та знарядь злочинів;

– здійснювати пошук і вивчення (через соціальні мережі) потенційних жертв і об'єктів злочинів;

– використовувати глобальну мережу Інтернет для готування, здійснення злочину, а також знищення слідів та ознак злочину тощо.

Вказані обставини лише підтверджують нагальну необхідність чіткого законодавчого регулювання процесуальної діяльності в транспортних телекомунікаційних мережах для забезпечення в цій сфері суспільних відносин безпеки особистості, суспільства і держави в цілому.

Таким чином, одним із актуальних проблемних питань у сучасній теорії доказів є визначення місця злочину в інформаційному просторі транспортних телекомунікаційних мереж. На сьогодні існує кілька підходів при розгляді юридичних розбіжностей під час розслідувань злочинів у кіберпросторі. В першо-

від 07.09.2005 N2824-IV (2824–15) <https://zakon.rada.gov.ua/laws/show/994_575> дата звернення 18.12.2019.

[1] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003, Протокол ратифіковано із застереженням Законом N23-V (23–16) від 21.07.2006 <https://zakon.rada.gov.ua/laws/show/994_687> дата звернення 18.12.2019.

[2] И Дзялошинский, 'Особенности коммуникативного поведения в киберпространстве' *Материалы 85 Всероссийской научной школы для молодежи* («Проблемы взаимодействия языка и мышления»), (Москва, сентябрь 2010) (Москва 2010) 17.

му підході за основу береться принцип громадянства (національний принцип), згідно з яким громадяни України та особи без громадянства, що постійно проживають в Україні, які вчинили злочин за її межами, підлягають кримінальній відповідальності за Кримінальним кодексом України, якщо інше не передбачено міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України (ч. 1 ст. 7 КК України)[1]. Якщо громадянин України або особа без громадянства, яка постійно проживає в Україні, за вчинений за кордоном злочин зазнали кримінального покарання за межами України, то вони не можуть бути притягнені до кримінальної відповідальності за ці злочини (ч. 2 ст. 7 КК). Це випливає із ст. 61 Конституції України, де зазначено, що ніхто не може бути двічі притягнений до юридичної відповідальності одного виду за одне й те саме порушення[2]. В другому підході, вважається, що злочин підпадає під юрисдикцію держави, на території якого він був здійснений, тобто перш за все враховується місце вчинення злочину.

На сьогодні саме поняття місця вчинення злочину в українському законодавстві чітко досі не визначено, тому думки науковців з цього приводу наводяться різні. Так, Кримінальний кодекс України визначає місце вчинення злочину в одних випадках як територію України (ст. ст. 268, 334 КК), економічну зону України (ст. 243 КК); повітряний простір України (ст. 282 КК); в інших випадках воно використовується як географічне поняття, наприклад, у ст. 240 КК України – це надра, в ст. 241 КК України – це атмосферне повітря, в ст. 242 КК України – водні об'єкти, в ст. 243 КК України – море, внутрішні морські і територіальні води, в ст. 244 КК України – це континентальний шельф; у третіх випадках під місцем вчинення злочину розуміється певна територія, на якій людина проживає чи займається виробничою або іншою діяльністю, наприклад, житло, інше приміщення чи сховище (ст.ст. 185, 186, 187 КК України), річкове, морське або повітряне судно (ст. 278 КК України), транспортні комунікації (ст. 279 КК України), вибухонебезпечні підприємства, вибухонебезпечні цехи (ст. 273 КК України).

Як зазначає В. Г. Мороз, аналіз переліку місця вчинення злочину свідчить, що він є різнобічним, але не повним, крім того, він не має належної класифікації. Науковець уважає, що місце вчинення злочину можна класифікувати за такими критеріями: 1) місце вчинення злочину як фізичний простір; 2) місце вчинення злочину як соціальне (суспільне утворення); 3) місце вчинення злочину як утворення, що має правовий статус[3]. Вона сформулювала поняття «місце вчинення злочину» таким чином: «Під місцем вчинення злочину потрібно розуміти територію, інше місце, яке характеризується фізичними, соціальними і правовими критеріями, де було розпочато, продовжено чи припинено злочинне діяння»[4].

Зазвичай, під місцем злочину в вузькому сенсі вважають територію, де безпосередньо було скоєне протиправне діяння і на якій можливо передбачити зміни в оточуючому середовищі, обумовлені цим явищем. У широку сенсі місце злочину – це шляхи підходу і втечі з місця події, а також прилягаючі ділянки. Такі ознаки, як безпосередність, наявність змін в оточуючому середовищі, не підпадають під визначення інформаційного простору, який створений та існує як екстериторіальне штучне утворення.

---

[1] Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. <https://zakon.rada.gov.ua/laws/show/2341–14> дата звернення 18.12.2019.

[2] Конституція України: Закон України від 28.06.1996 № 254к/96-ВР <https://zakon.rada.gov.ua/laws/show/254k/96-вр> дата звернення 18.12.2019.

[3] В Мороз, 'Поняття місця вчинення злочину як ознаки об'єктивної сторони злочину' (2014) 5 *Юридична наука* 132.

[4] Там само 133.

При цьому у кримінальному законодавстві не існує такого поняття, як злочин, скоєний у кібернетичному просторі, однак у деяких статтях Кримінального кодексу України глобальна мережа Інтернет (окремий випадок інформаційного простору) виділяється як кваліфікуюча ознака, але залишається відкритим питання щодо конкретизації місця злочину в кібернетичному просторі. Проведений аналіз ст.ст. 361–363 Розділу XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» дозволяє дійти висновку, що злочини, скоєні в мережі Інтернет, можливо віднести до комп'ютерних злочинів. Так, у ст. 361 КК України визначається відповідальність за несанкціоноване втручання в роботу комп'ютерних мереж; у ст. 361–1 КК України – встановлена відповідальність за створення з метою використання, розповсюдження або збуту шкідливих (вірусних) програмних чи технічних засобів для несанкціонованого втручання в роботу комп'ютерних мереж; у ст. 362 КК України – відповідальність за несанкціоновані дії з інформацією, яка обробляється в комп'ютерних мережах; у ст. 363 КК України – означена відповідальність за порушення правил експлуатації комп'ютерних мереж; у ст. 363–1 КК України – встановлена відповідальність за перешкоджання роботі комп'ютерних мереж шляхом масового розповсюдження повідомлень електрозв'язку. Мають-ся на увазі DoS-атаки (від англ. Denial of Service «відмова в обслуговуванні»), а якщо атака проводиться одночасно з великої кількості комп'ютерів, кажуть про DDoS-атаку (від англ. Distributed Denial of Service. розгалужена атака типу «відмова в обслуговуванні»).

Сучасна криміналістична методика розслідування злочинів у сфері комп'ютерної інформації вказує на огляд місця злочину, а саме робочого місця підозрюваного, а також виїмку технічних засобів і документів, відомостей, що зберігаються на машинних носіях інформації [1]. Проте, якщо брати до уваги, що інформаційний (кібернетичний) простір (у тому числі – транспортна телекомунікаційна мережа) – це штучно створене екстериторіальне цифрове середовище, яке функціонує за принципами та правилами, відмінними від звичних для нас фізичних явищ, то зазначена дефініція потребує уточнення. В цьому разі можливо погодитись з думкою І. С. Іскевич, що «…місцем злочину може бути частина інформаційного простору (домен, сайт), в якому фактично був здійснений злочин активним користувачем. У цьому визначенні поставлені в пряму залежність два фактори: фактичне місце злочину – сайт, який зареєстрований на сервері, який має фізичне розташування на певній території, і особа, активний користувач мережі Інтернет у момент здійснення злочину. Такий підхід може полегшити ідентифікацію злочинця, оскільки сучасні методи не дають високої точності окремо, а запропоноване формулювання дозволяє правоохоронним органам застосовувати їх сукупність залежно від технічних можливостей»[2].

Отже, враховуючи означене вище, можливо вважати «місцем вчинення злочину» передбачену диспозицією кримінально-правової норми ознаку об'єктивної сторони складу злочину, яка характеризує певну територію, інше місце, у тому числі частину інформаційного простору (сайт, домен), які характеризуються фізичними, соціальними і правовими критеріями, де суб'єкт вчинив передбачену кримінальним законом дію або бездіяльність.

Велика суспільна небезпека злочинів, учинених в інформаційному середовищі

[1] М Гребенюк, В Гавловський, М Гуцалюк В Хахановський та ін, *Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації* (Київ 2017) 24

[2] И Искевич, М Кочеткова, 'Особенности определения места преступления при нарушении авторских прав в глобальном информационном пространстве: международно-правовой и уголовно-правовой аспекты'(2017) 1 *Проблемы правоохранительной деятельности* 56

транспортних телекомунікаційних мереж (кіберпросторі), значна кількість потерпілих, встановлений, а також більш значний прихований матеріальний збиток роблять боротьбу із цим негативним явищем актуальним, як і те, що злочинність у сфері інформаційних технологій все ширше використовується в контексті організованої злочинної діяльності, особливо діяльності терористичних організацій, які усе активніше починають використовувати новітні інформаційні технології й комп'ютерну техніку. Проте на сьогодні у правоохоронних органів західних країн (у вітчизняних також) існує проблема ефективності засобів, які забезпечують належність цифрових (електронних) доказів. Переважна більшість компаній, які надають послуги хостингів, «хмарних» сховищ та серверів, знаходяться в США. Процедура отримання цифрових доказів складна і на практиці цей механізм працює дуже жваво (причини – складні бюрократичні і процесуальні процедури), що нівелює іноді цінність отриманих відомостей. І розвиток міжнародного співробітництва в цьому напрямі – єдиний можливий шлях відновлення рівня довіри суспільства до верховенства права в інформаційному просторі.

Висновки. Таким чином, на сьогоднішній день інформаційне середовище (кіберпростір) і його основна функціональна складова – транспортні телекомунікаційні мережі стають все більш привабливими як платформи для здійснення злочинів як окремими особами, так і організованими злочинними угрупованнями з огляду на їх транснаціональних характер, анонімність і віртуальність. Загальновизнана суспільна небезпека протиправних дій у цифровому середовищі виражається в тому, що вони можуть викликати порушення в роботі автоматизованих систем керування та контролю різних (зокрема, життєзабезпечуючих об'єктів), серйозне порушення роботи ЕОМ та їх систем. Несанкціоновані дії по знищенню, модифікації, викривленню, копіюванню інформації та інформаційних ресурсів, інші форми незаконного втручання в транспортні телекомунікаційні мережі здатні викликати тяжкі й невідворотні наслідки, які пов'язані не тільки з майновими збитками, але й з фізичною шкодою людям. Небезпека злочинів у кіберпросторі багаторазово зростає, коли вони здійснюються стосовно функціонування об'єктів життєзабезпечення, транспортних і оборонних систем, атомної енергетики. А отже, інформаційне середовище транспортних телекомунікаційних мереж та законність роботи в ньому стають вагомим чинником при здійсненні діяльності органами досудового розслідування з отримання відомостей, які мають доказове значення для кримінального провадження. В свою чергу, розуміння всіма учасниками досудового розслідування основ і принципів їх функціонування та організації, їх навички роботи з цифровою технікою суттєво впливають на якість проведення кримінального провадження на всіх його етапах.

Крім того, з урахуванням екстериторіального характеру інформаційного (кібернетичного) простору необхідне чітке законодавче регулювання процесуальної діяльності в транспортних телекомунікаційних мережах для забезпечення в цій сфері суспільних відносин безпеки особистості, суспільства і держави в цілому. Тому питання щодо визначення місця злочину в інформаційному (кібернетичному) просторі та законодавче закріплення поняття «місця вчинення злочину» (можливо, у вигляді запропонованому у статті) є нагальним та потребує нормативного врегулювання.

REFERENCES
LIST OF LEGAL DOCUMENTS

LEGISLATION

1. Konstytutsiia Ukrainy: Zakon Ukrainy [Constitution of Ukraine: Law of Ukraine] vid 28.06.1996 № 254k/96-VR <https://zakon.rada.gov.ua/laws/show/254k/96-вр> data zvernennia 18.12.2019 [in Ukrainian].

2. Kryminalnyi kodeks Ukrainy: Zakon Ukrainy [Criminal Code of Ukraine: Law of Ukraine] vid 05.04.2001 № 2341-III <https://zakon.rada.gov.ua/laws/show/2341–14> data zvernennia 18.12.2019 [in Ukrainian].

3. Kryminalnyi protsesualnyi kodeks Ukrainy: Zakon Ukrainy [Criminal Procedural Code of Ukraine: Law of Ukraine] vid 13.04.2012 № 4651-VI <http://zakon5.rada.gov.ua/laws/show/4651–17> data zvernennia 06.12.2019 [in Ukrainian].

4. Konventsiia pro zakhyst prav i osnovnykh svobod liudyny [Europian Court of Human Right], Rym, 4.XI.1950: Konventsiiu ratyfikovano Zakonom № 475/97-VR vid 17.07.97 <https://zakon.rada.gov.ua/laws/show/995_004> data zvernennia 18.12.2019 [in Ukrainian].

5. Konventsiia pro kiberzlochynnist vid 23.11.2001 [Convention on Cybercrime] Ratyfikovano iz zasterezhenniamy i zaiavamy Zakonom vid 07.09.2005 N2824-IV (2824–15) <https://zakon.rada.gov.ua/laws/show/994_575> data zvernennia 18.12.2019 [in Ukrainian].

6. Dodatkovyi protokol do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy vid 28.01.2003 [The Additional Protocol to the Convention on Cybercrime? Concerning the criminalization of acts of a rasist and xenophobic nature committed through computer systems]: Protokol ratyfikovano iz zasterezhenniam Zakonom N23-V (23–16) vid 21.07.2006 <https://zakon.rada.gov.ua/laws/show/994_687> data zvernennia: 18.12.2019 [in Ukrainian].

7. Rekomendacija Komiteta ministrov Soveta Evropy gosudarstvam-chlenam «Ob «osobyh metodah rassledovanija» tjazhkih prestuplenij, v tom chisle terroristicheskih aktov» ot 20.05.2005 N Rec (2005) 10 <https://zakon.rada.gov.ua/laws/show/994_670?> data zvernennja 18.12.2019 [in Russian].

8. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 № 2657-XII [On Information: The Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/2657–12> data zvernennia 18.12.2019 [in Ukranian].

9. Pro telekomunikatsii: Zakon Ukrainy vid 18.11.2003 № 1280-IV [On telecommunications: Law of Ukraine] <https://zakon.rada.gov.ua/laws/show/1280–15> data zvernennia 18.12.2019 [in Ukranian].

10. Instruktsiia pro orhanizatsiiu provedennia nehlasnykh slidchykh (rozshukovykh) dii ta vykorystannia yikh rezultativ u kryminalnomu provadzhenni [Instruction on the organization of the holding of secret investigative (search) actions and the use of their results in criminal proceedings]: Nakaz Heneralnoi Prokuratury Ukrainy, Ministerstva Vnutrishnikh sprav Ukrainy, Sluzhby Bezpeky Ukrainy, Administratsii Derzhanoi prykordonnoi sluzhby Ukrainy, Ministerstva finansiv Ukrainy, Ministerstva yustytsii Ukrainy vid 16.11.2012 № 114/1042/516/1199/936/1687/5 <https://zakon.rada.gov.ua/laws/show/v0114900–12> data zverennia 18.12.2019 [in Ukrainian].

BIBLIOGRAPHY

AUTHORED BOOKS

11. Makbraid D, *Yevropeiska konventsiia z prav liudyny ta kryminalnyi protses. Praktyka Yevropeiskoho sudu z prav liudyny* [European Convention on Human Rights and Criminal Procedure. Case law of the European Court of Human Rights]. Rada Yevropy (druhe vydannia) (Kyiv «K.I.S.» 2018) 554 [in Ukrainian].

12. Hrebeniuk M V, Havlovskyi V D, Hutsaliuk M V, Khakhanovskyi V H ta in.., *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh. Metodychni rekomendatsii* [Use of electronic (digital) evidence in criminal proceedings. Methodological guidelines] (Kyiv 2017) 76 [in Ukrainian].

13. Shynkaruk V I ta in., *Filosofskyi entsyklopedychnyi slovnyk* [Philosophical Encyclopedic Dictionary] (Kyiv 2002) 742 [in Ukrainian].

ARTICLES

14. Girich V L, Chuprina V N, 'Globalnoe informatsionnoe prostranstvo i problema dostupa k mirovyim informatsionnyim resursam' [Global Information Space and access problem to World information resources] <http://marc21.rsl.ru/upload/mba2007/mba2007_05.pdf> data zverennia 18.12.2019 [in Russian].

15. Iskevich I S, Kochetkova M N, 'Osobennosti opredelenija mesta prestuplenija pri narushenii avtorskih prav v global'nom informacionnom prostranstve: mezhdunarodno-pravovoj i ugolovno-pravovoj aspekty'[Features of determining the place of crime in violation of copyright in the global information space: international legal and criminal law aspects] (2017) 1 Problemy pravoohranitel'noj dejatel'nosti 56 [in Russian].

16. Moroz V H, 'Poniattia mistsia vchynennia zlochynu yak oznaky obiektyvnoi storony zlochynu' [The concept of the crime scene as a sign of the objective side of the crime] (2014) 5 Yurydychna nauka 133 [in Ukrainian].

17. Dzjaloshinskij I M, 'Osobennosti kommunikativnogo povedenija v kiberprostranstve' [Features of communicative behavior in cyberspace] Materialy 85 Vserossijskoj nauchnoj shkoly dlja molodezhi [Problemy vzaimodejstvija jazyka i myshlenija], (Moskva, sentjabr' 2010) (Moskva 2010) 17 [in Russian].

18. Serohin V S, 'Problemy stvorennia systemy monitorynhu informatsiinoho prostoru Ukrainy Informatsiina bezpeka derzhavy u svitli rozvytku suchasnykh informatsiinykh tekhnolohii [Problems of monitoring system creation in information space of Ukraine]: Materialy nauk. – prakt. konf. (Kyiv, 30 chervnia 2006r.) (Kyiv 2007) 100 [in Ukrainian].

Metelev O.,
Postgraduate student on the Departtment of criminal ang criminal procedural law National academy of the Security service of Ukraine
ORCID ID: *0000–0003–2969–8388*

DOI: *https://doi.org/10.17721/2413-5372.2019.4/161-173*

TRANSPORT TELECOMMUNICATION NETWORKS AS AN INFORMATION MEDIUM FOR OBTAINING INFORMATION RELEVANT TO CRIMINAL PROCEEDINGS: PROBLEMATIC ISSUES OF LEGAL REGULATION

Annotation*. Scientific and technological progress, as well as the rapid development of information technologies, the formation of the information society, the introduction of telecommunications systems and networks into all vital processes, the availability of digital communications and information transmission have necessitated the use of new methods of combating crime in the new information (cybernetic) space, this artificially created environment, which is an integral part of transport telecommunications networks (TTN).*

The extraterritorial nature of transport telecommunication networks and systems, together with the global Internet, greatly complicates their legal regulation, as it is sometimes quite difficult to determine the jurisdiction of which state relates a criminal offense. Thus, when conducting silent investigative actions, a legitimate question arises as to the lawfulness of work in the information environment of the transport telecommunication network for obtaining digital evidence in the interests of criminal proceedings.

Purpose of the article: to investigate the problematic issues of legal regulation when working in transport telecommunication networks in order to obtain information relevant to criminal proceedings during the conduct of silent investigative actions.

The paper draws attention to the insufficient level of scientific research to cover the problematic issues of studying transport telecommunications networks as an information medium for legal obtaining digital evidence in the interests of criminal justice. The national legislation regulating public relations in this field is analyzed, as well as the case law of the European Court of Human Rights, which reveals some «white spots» in national legislation on ensuring the legitimacy and protection of human rights in the conduct of vague private communication interventions in the information environment of transport telecommunication networks.

Taking into account the extraterritorial nature of the information (cyber) space, it is concluded that there is a need for clear legislative regulation of procedural activity in the transport telecommunication networks in order to ensure the security of the individual, society and the state as a whole in this sphere.

The article also discusses different approaches to legal disparities in cyber crime investigations. The question of determining the crime scene in the information (cybernetic) space is raised, an attempt is made to define the «crime scene» and provides suggestions for improving legislation.

Keywords*: criminal process, transport telecommunication network, cyber space, crime scene.*

Стаття надійшла до редакції журналу 20.12.2019.