

Література

1. Про внесення змін до п. 12 Правил застосування спеціальних засобів при охороні громадського порядку в Українській РСР : постанова Кабінету Міністрів України від 21 квіт. 1995 р. № 302 [Електронний ресурс]. – Режим доступу: <http://www.rada.gov.ua>.
2. Про внесення змін до Правил застосування спеціальних засобів при охороні громадського порядку в Україні : постанова Кабінету Міністрів України від 4 серп. 1997 р. № 829 [Електронний ресурс]. – Режим доступу: <http://www.rada.gov.ua>.
3. Трубаєв С. І. Електрошокери / С. І. Трубаєв, М. М. Колєда, О. В. Горелов // Сучасна спеціальна техніка. – 2004. – № 1. – С. 59–65.
4. Губарєв Г. Г. Методика вимірювання експлуатаційних електричних параметрів електрошокерів / Г. Г. Губарєв, С. І. Трубаєв // Сучасна спеціальна техніка. – 2005. – № 2 (7). – С. 72–88.
5. Сидоренко А. П. Электрошок – защита для всей семьи / А. П. Сидоренко // Радиоаматор. – 1997. – № 12. – С. 21.
6. [Електронний ресурс]. – Режим доступу: <http://bugpage.h1.ru/lab/stungun.html>.
7. [Електронний ресурс]. – Режим доступу: <http://FrikZona.org/zashita/megashock1.shtml>.
8. Электрошочковое устройство повышенной надежности : пат. 2222761 Рос. Федерация ; опубл. 27.01.04.
9. Электрошочковое устройство для самообороны : патент 2108526 Рос. Федерация ; опубл. 10.04.98.
10. ТУ У 30592147.001-2000. Искровой разрядник ИР-4. – Зареєстр. 2000–05–12. – Х. : Ін-т електродинамики», 2000. – 18 с.
11. Дистанционное электрошочковое устройство : пат. 2287757 Рос. Федерация ; опубл. 20.11.06.
12. United States Patent, US 6,999,295 B2. Dual operating mode electronic disabling device for generating a time sequenced, shaped voltage output waveform.
13. Пат. 60071 Україна. Високовольтний електрошочковий пристрій контактної і дистанційної дії / Губарєв Г. Г. ; заявл. 21.01.03 ; опубл. 15.07.05, Бюл. № 7.
14. Пат. 79487 Україна. Электрошочковий пристрій / Губарєв Г. Г., Трубаєв С. І. ; заявл. 09.03.05 ; опубл. 15.03.07, Бюл. № 3.

Надійшла до редколегії 17.05.2010

УДК 343.1(477):65.012.8+004

О. В. МАНЖАЙ,

*викладач кафедри інформаційної безпеки
навчально-наукового інституту психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ*

НОРМАТИВНО-ПРАВОВА БАЗА ЗДІЙСНЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ШЛЯХОМ ВИКОРИСТАННЯ КІБЕРПРОСТОРУ

Досліджено питання нормативно-правового забезпечення проведення оперативно-розшукових заходів шляхом використання кіберпростору.

МАНЖАЙ О. В. НОРМАТИВНО-ПРАВОВАЯ БАЗА ОБЕСПЕЧЕНИЯ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ ПУТЕМ ИСПОЛЬЗОВАНИЯ КИБЕРПРОСТРАНСТВА

Исследован вопрос нормативно-правового обеспечения проведения оперативно-розыскных мероприятий с использованием киберпространства.

MANJAY O. NORMATIVE AND LEGAL BASE FOR CONDUCTING OPERATIONAL AND SEARCH MEASURES THROUGH CYBERSPACE USAGE

Problem of normative and legal base for conducting operational and search measures through cyberspace usage is researched.

Найважливішим сучасним завданням правової науки, юридичної практики з попередження та розкриття злочинів є ефективне використання нових інформаційних технологій в оперативно-розшуковій діяльності (далі – ОРД) підрозділів кримінальної міліції, що сприяє підвищенню якості та своєчасності

прийнятих рішень, ефективності проведення оперативно-розшукових заходів.

За допомогою засобів комп'ютерної техніки утворюється кіберпростір, який, безперечно, має бути об'єктом особливої уваги оперативних працівників. Така увага обумовлена високою криміногенністю даного середовища,

адже, використовуючи кіберпростір, злочинці розповсюджують порнографію, продають наркотичні та психотропні речовини; за його допомогою підтримують зв'язок організовані злочинні угруповання, вчиняються так звані комп'ютерні злочини тощо. Вказані злочини нерідко мають латентний характер, причому їх виявлення без використання кіберпростору інколи є неможливим. Таким чином, без належної уваги з боку правоохоронців до цього середовища з кожним роком дедалі складніше буде контролювати оперативну обстановку на місцях.

В Україні лише за останні п'ять років у сфері високих технологій було виявлено/розкрито 3252/2434 злочини, з них у 2005 р. – 615/362; у 2006 р. – 583/415; у 2007 р. – 656/475, у 2008 р. – 691/572, у 2009 р. – 707/610.

Загальною науково-теоретичною базою для дослідження у сфері здійснення оперативно-розшукових заходів шляхом використання кіберпростору є окремі праці вітчизняних та зарубіжних вчених з теоретичних і практичних проблем використання інформаційних технологій в оперативно-розшуковій діяльності.

Зазначені питання досліджували такі вітчизняні вчені, як О. Ю. Бусол, В. М. Бутузов, Н. Л. Волкова, І. О. Воронов, В. О. Голубєв, О. Ф. Долженков, В. Ю. Журавльов, Г. В. Загіка, В. П. Захаров, М. Ю. Литвинов, Ю. Ю. Орлов, В. Л. Ортинський, М. М. Перепелиця, Е. В. Рижков, С. М. Рогозін, М. В. Салтевський, Л. П. Скалозуб, О. П. Снігерьов, Ю. В. Степанов, І. Ф. Харабєрюш, В. Г. Хахановський, В. П. Шеломенцев тощо. Різні аспекти застосування інформаційних технологій в оперативно-розшуковій діяльності розглядали російські дослідники С. С. Овчинський, В. С. Овчинський, А. С. Овчинський, А. Л. Осипенко, американські дослідники Дж. Макнамара, С. Хейман, Д. Грін, В. Вайтлідж, білоруський дослідник В. Є. Козлов тощо.

Діяльність ОВС щодо проведення оперативно-розшукових заходів через кіберпростір базується на ряді нормативно-правових актів, основними серед яких є:

1. Закон України «Про оперативно-розшукову діяльність»;
2. Закон України «Про телекомунікації»;
3. Державна програма інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою зі злочинністю [1];
4. Нормативний документ. Технічні засоби для здійснення уповноваженими органами

оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги (далі – Технічні вимоги);

5. Окремі відомчі та міжвідомчі інструкції.

У Законі України «Про оперативно-розшукову діяльність» [2] окреслено основні положення щодо здійснення оперативно-розшукової діяльності, зокрема її організації. Ці положення, звичайно, мають застосовуватися і до діяльності, пов'язаної з провадженням оперативно-розшукових заходів шляхом використання кіберпростору.

Часто використання кіберпростору в оперативно-розшуковій діяльності пов'язано зі зняттям інформації з каналів зв'язку й застосуванням інших технічних засобів отримання інформації. Ми не поділяємо думок окремих науковців (див., наприклад, [3, с. 12]), які вважають за необхідне назвати даний оперативно-розшуковий захід «прослуховуванням телефонних і інших переговорів», а відповідну слідчу дію – «зняття інформації з каналів зв'язку», оскільки це значно звужує права оперативних підрозділів. Більше того, в умовах сучасного розвитку технологій було б корисним об'єднати вказаний захід із контролем за поштово-телеграфною кореспонденцією у «перехоплення комунікацій», як це зроблено, наприклад, у Великобританії. Відповідно до підрозділу 4 розділу 17 глави I першої частини Закону Великобританії «Про правове регулювання слідчих повноважень», перехоплення комунікацією вважається будь-яка комунікація, перехоплена в ході її передачі за допомогою поштового обслуговування або телекомунікаційної системи [4]. Причому особа перехоплює комунікацію в ході її передачі за допомогою телекомунікаційної системи тоді і тільки тоді, коли для цього вона:

- а) модифікує або втручається в систему або її операцію;
- б) контролює передачі, зроблені за допомогою системи;
- в) контролює передачі, зроблені за допомогою бездротового телеграфу до чи від апаратури, яка входить до складу системи, щоб зробити частину або весь зміст переданої комунікації доступним для особи, яка не є відправником або визначеним одержувачем комунікації [4].

Відповідно до п. 3 Постанови Пленуму Верховного Суду України «Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження

окремих конституційних прав громадян під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства» від 28 березня 2008 р. № 2 [5], зняття інформації з каналів зв'язку полягає в застосуванні технічного обладнання, яке дає змогу прослуховувати, фіксувати та відтворювати інформацію, що передавалася цим каналом зв'язку. Така інформація може включати дані як про взаємоз'єднання телекомунікаційних мереж, так і щодо змісту інформації, яка була передана каналом зв'язку.

З назви заходу – *зняття інформації з каналів зв'язку та застосування інших технічних засобів отримання інформації* – випливає, що під час його проведення можуть застосовуватися спеціальні технічні засоби негласного отримання інформації (далі – СТЗ), які належать до категорії майна, що не може перебувати у власності громадян, громадських об'єднань, міжнародних організацій та юридичних осіб інших держав на території України [6].

Замовниками розроблення, виготовлення та придбання СТЗ в Україні можуть бути центральні органи виконавчої влади, розвідувальні органи, підрозділи яких провадять оперативно-розшукову діяльність, міжнародні правоохоронні організації, спеціальні служби та правоохоронні органи іноземних держав [7].

Відповідно до п. 1.2 Ліцензійних умов провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації, затверджені наказом Державного комітету України з питань регуляторної політики та підприємництва і Служби безпеки України від 10 жовтня 2006 р. № 92/669 [8], СТЗ визначаються як технічні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, спеціально розроблені, виготовлені, пристосовані для негласного отримання інформації, або технічні засоби, запрограмовані з цією метою з використанням спеціального програмного забезпечення.

До таких засобів належать:

- спеціальні технічні засоби для негласного отримання та реєстрації аудіоінформації;
- спеціальні технічні засоби негласного візуального спостереження і фото-, теле- та

відеодокументування;

- спеціальні технічні засоби для негласного отримання, реєстрації інформації з телекомунікаційних мереж;
- спеціальні технічні засоби негласного контролю поштових повідомлень і відправлень;
- спеціальні технічні засоби негласного обстеження предметів і документів;
- спеціальні технічні засоби негласного проникнення у приміщення, транспортні засоби, інші об'єкти, а також негласного обстеження приміщень транспортних засобів та інших об'єктів;
- спеціальні технічні засоби негласного контролю за переміщенням транспортних засобів та інших об'єктів;
- спеціальні технічні засоби негласного отримання (зміни, знищення) інформації з технічних засобів її зберігання, обробки та передавання.

У контексті використання кіберпростору можна визначити:

- *СТЗ для негласного перехоплення та реєстрації інформації з технічних каналів зв'язку* – комплекс або окремі засоби моніторингу оптичних, кабельних і провідних ліній зв'язку: спеціалізовані пристрої зняття інформації з оптичних, кабельних і провідних ліній зв'язку, засоби демодуляції електро- та оптичних сигналів, спеціалізоване програмне забезпечення отримання негласного доступу до аудіо-, відео-, текстової інформації, а також даних, які передаються оптичними, кабельними та провідними лініями зв'язку.

- *СТЗ для негласного отримання (зміни, знищення) інформації з технічних засобів її зберігання, обробки та передавання* – радіоелектронне обладнання (комплекси) для прийому та декодування побічного електромагнітного випромінювання електронно-обчислювальної техніки, іншого радіоелектронного обладнання (для зняття інформації з джерел побічних електромагнітних випромінювань та наведень) [9].

Ознаками приналежності виробів до СТЗ, спільними для усіх груп, є:

- мініатюрність виробу в цілому або окремого модуля (наприклад модуля датчика);
- конструктивне виконання виробів у вигляді безкорпусних мініатюрних модулів;
- використання при проектуванні радіоелектронних виробів схемотехнічних або конструкторських рішень, що направлені на протидію пошуковим радіоелектронним засобам.

Ознакою належності виробів до СТЗ також

є їх конструктивне виконання у закамуюльованому вигляді або у вигляді, який передбачає їх камуюльовання.

Спiрнi питання щодо приналежностi до СТЗ конкретного технiчного засобу, який розробляється, виготовляється й реалiзується суб'єктом господарювання, вирiшуються Службою безпеки України.

Перелiк ознак СТЗ та орієнтовний перелiк кодiв УКТЗЕД, якi призначенi для визначення належностi товарiв до СТЗ, мiстяться в контрольному списку товарiв, наведеному в частинi АЗ роздiлу 5 «Спецiальнi технiчнi засоби» Списку товарiв подвійного використання, що можуть бути використанi у створеннi звичайних видiв озброєнь, вiйськової чи спецiальної технiки, який додається до Порядку здійснення державного контролю за мiжнародними передачами товарiв подвійного використання, затвердженого постановою Кабiнету Міністрiв України вiд 28 сiчня 2004 р. № 86 [10]. Бiльш докладно питання нормативного регулювання СТЗ розглянуто в нашiй статтi [11].

Важливою нормою, що стосується проведення оперативно-розшукових заходiв через кiберпростiр, є положення, викладенi в п. 4 ст. 39 Закону України «Про телекомунiкацiї» вiд 18 листопада 2003 р. [12]. Так, оператори телекомунiкацiй зобов'язанi за власнi кошти *встановлювати* (курсив наш – О. М.) на своїх телекомунiкацiйних мережах технiчнi засоби, необхіднi для здійснення уповноваженими органами оперативно-розшукових заходiв, i *забезпечувати* функцiонування цих технiчних засобiв, а також у межах своїх повноважень *сприяти* проведенню оперативно-розшукових заходiв та недопущенню розголошення органiзацiйних i тактичних прийомiв їх проведення. Оператори телекомунiкацiй зобов'язанi забезпечувати захист зазначених технiчних засобiв вiд несанкцiонованого доступу.

Крiм того, у 2010 р. в рамках боротьби з дитячою порнографiєю ст. 39 Закону України «Про телекомунiкацiї» було доповнено важливою нормою, згiдно з якою оператори, провайдери телекомунiкацiй зберiгають та надають iнформацiю про з'єднання свого абонента в порядку, встановленому законом. Таким чином, на законодавчому рiвнi було закрiплено обов'язок оператора (провайдера телекомунiкацiй) не тiльки щодо реєстрацiї мережної активностi своїх клiєнтiв, але й щодо збереження такої iнформацiї протягом певного перiоду часу.

Згiдно з п. 4.1.1 Технiчних вимог [13] до

складу технiчних засобiв для здійснення уповноваженими органами оперативно-розшукових заходiв у телекомунiкацiйних мережах загального користування України належать:

- 1) мережний комплект (далi – МК) для здійснення перехоплення телекомунiкацiй;
- 2) засоби управлiння системою перехоплення телекомунiкацiї (сервери, станцiї, термiнали тощо – ЗУСП);
- 3) засоби захищеної телекомунiкацiйної мережi спецiального призначення;
- 4) програмне забезпечення технiчних засобiв;
- 5) експлуатацiйна та програмна документацiя технiчних засобiв;
- 6) комплект запасних iнструментiв та приладiв.

Функцiональне поєднання цих засобiв утворює систему перехоплення телекомунiкацiй.

Основною складовою частиною технiчних засобiв для здійснення уповноваженими органами оперативно-розшукових заходiв у телекомунiкацiйних мережах загального користування України є МК.

МК для здійснення перехоплення телекомунiкацiй призначенi для розпiзнавання i вiдгалуження об'єктiв перехоплення, вiдбору та передавання даних до ЗУСП (див. схему).

На сьогодні бiльшiсть опитаних автором оперативних працівникiв (62,4 %) ¹ вважають, що проведення оперативно-розшукових заходiв шляхом використання кiберпростору мають регламентуватися як окремий захiд ОРД, тодi як решта опитаних схиляються до думки про можливiсть застосування кiберпростору в рамках iснуючих оперативно-розшукових заходiв. На нашу думку, другий пiдхiд є бiльш рацiональним, оскiльки, по-перше, узгоджується з чинними нормами, якi регламентують оперативно-розшукову дiяльнiсть, а, по-друге, кiберпростiр у даному випадку є допомiжним iнструментом, який дозволяє здiйснювати оперативно-розшуковi заходи.

Слiд вiдрiзняти органiзацiю боротьби з кiберзлочинами та органiзацiю здійснення оперативно-розшукових заходiв шляхом використання кiберпростору, оскiльки останнi можуть проводитися як у справах про кiберзлочини, так i у справах про злочини, вчиненi у звичайному фiзичному середовищi.

¹ Всього було опитано 304 оперативних працівника рiзних служб iз 24 рiвонiв України

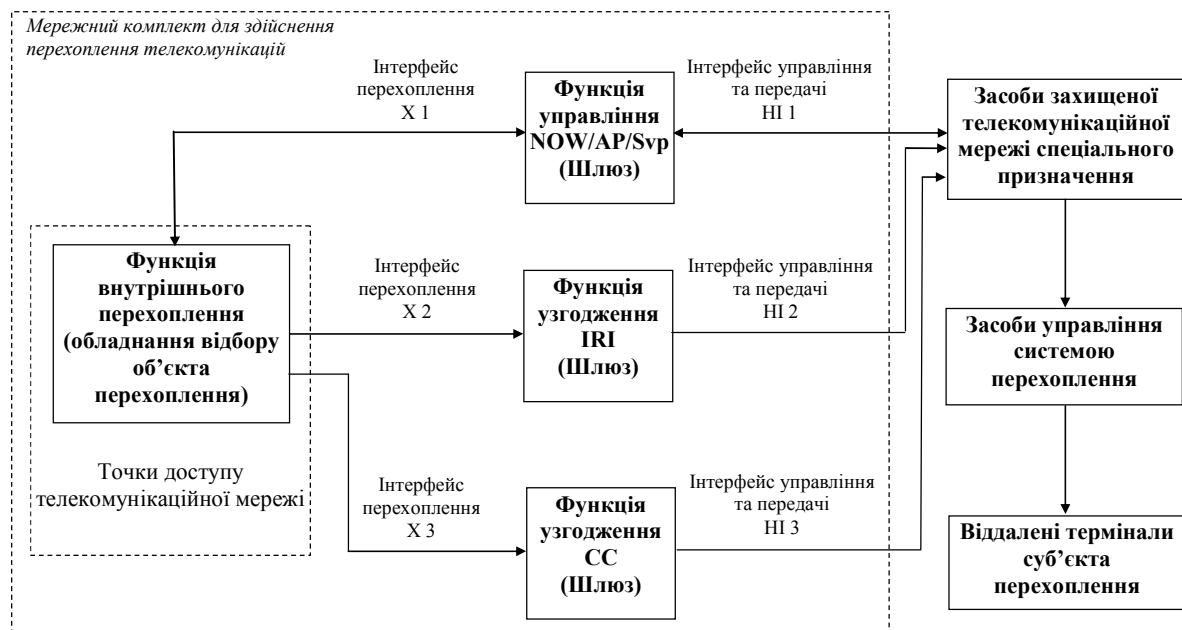


Схема функціонування інтерфейсів

За результатами опитування на сьогодні при необхідності використання кіберпростору в оперативно-розшуковій діяльності оперативні працівники найчастіше стикаються з такими проблемами:

- 1) відсутність відповідних методик проведення оперативно-розшукових заходів з урахуванням специфіки діяльності оперативного підрозділу – 49,4 %;
- 2) недостатність правових механізмів регламентації такої діяльності (особливо щодо легалізації отриманих матеріалів) – 43,7 %;
- 3) незнання можливостей сучасної техніки та програмного забезпечення – 40,6 %;
- 4) нерозуміння професійних проблем з боку керівництва – 18,0 %;
- 5) невміння користуватися сучасною технікою – 15,3 %.

Одним із напрямів використання кіберпростору в оперативно-розшуковій діяльності є утворення сприятливої обстановки для проведення слідчих дій. Ефективність цього напрямку досягається завдяки конструктивній взаємодії оперативних працівників та осіб, які провадять досудове слідство.

Серед основних відомих нормативних актів, які регулюють питання взаємодії оперативних апаратів зі слідчими підрозділами, можна виділити такі:

- 1) Інструкція з організації взаємодії органів досудового слідства з оперативними підрозділами органів внутрішніх справ України у виявленні, документуванні та розслідуванні

злочинів у сфері економіки [14];

- 2) Інструкція з організації взаємодії органів досудового слідства з оперативними підрозділами органів внутрішніх справ України на стадіях документування злочинних дій, реалізації оперативних матеріалів, розслідування кримінальної справи та її розгляді в суді [15].

Зазвичай така взаємодія реалізується за схемою, відповідно до якої на основі наявної оперативно-розшукової інформації або даних кримінальної справи плануються як стандартні оперативно-розшукові заходи, так і застосування в ході їх проведення кіберпростору. Це дозволяє отримати первинну орієнтуючу інформацію, на підставі якої ретельно обирається тактика та методика проведення слідчих дій з метою виявлення нових доказів та осіб, причетних до злочину.

Ефективна взаємодія слідчих та оперативних працівників по лінії використання кіберпростору дозволяє суттєво покращити ефективність боротьби зі злочинами, особливо з такими, де використовуються знання сучасних технологій для вчинення протиправних діянь.

Важливу роль під час використання кіберпростору в правоохоронній діяльності відіграє міжнародна взаємодія, зокрема в рамках СНД (див., наприклад, дослідження О. П. Снігерьова [16, с. 31–33]).

Базовими нормативно-правовими актами, що регламентують міжнародну взаємодію компетентних органів у боротьбі зі злочинністю, є багатосторонні договори (конвенції),

наприклад, Мінська конвенція 1993 р.

З урахуванням вимог цих конвенцій розроблено ряд відомчих та міжвідомчих документів, зокрема:

– Інструкція про порядок виконання європейських конвенцій з питань кримінального судочинства, затверджена спільним наказом Міністерства юстиції України, Генеральної прокуратури України, Служби безпеки України, МВС України, Верховного суду України, Державної податкової адміністрації України, Державного департаменту України з питань виконання покарань від 29 червня 1999 р. № 34/5/22/103/512/326/73 [17];

– Інструкція про порядок організації співробітництва органів внутрішніх справ України з правоохоронними органами іноземних держав з питань попередження, розкриття та розслідування злочинів, затверджена наказом МВС України «Про організацію міжнародної діяльності органів внутрішніх справ України» від 15 травня 2007 р. № 158 [18];

– Інструкція про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні в попередженні, розкритті та розслідуванні злочинів, затверджена спільним наказом МВС України, Генеральної прокуратури України, Служби безпеки України, Державного комітету у справах охорони державного кордону України, Державної митної служби України, Державної податкової адміністрації України від 9 січня 1997 р. № 3/1/2/5/2/2 [19];

– наказ МВС України «Про порядок відносин органів внутрішніх справ України з компетентними правоохоронними органами іноземних держав по питаннях попередження, розкриття і розслідування злочинів» від 6 вересня 1995 р. № 600 [20];

– Положення про Департамент зв'язків із громадськістю та міжнародної діяльності Міністерства внутрішніх справ України, затверджене наказом МВС України від 8 лютого 2008 р. [21].

Крім того, в ході міжнародної правоохоронної діяльності нерідко застосовуються норми ст. 10 Кримінального кодексу України [22] та ст. 31 Кримінально-процесуального кодексу України [23].

Слід констатувати, що на сьогодні в законодавстві відсутня пряма вказівка на можливість використання кіберпростору в правоохоронній діяльності. Тож, на нашу думку, зважаючи на необхідність покращення стану здійснення даного напрямку оперативно-розшукової діяльності, доцільно доповнити ст. 8 (Права підрозділів, які здійснюють оперативно-розшукову діяльність) Закону України «Про оперативно-розшукову діяльність» від 18 лютого 1992 р. пунктом 19, який викласти у такій редакції:

«19) реалізовувати права, передбачені пп. 1–18 цієї статті шляхом використання кіберпростору.

Під кіберпростором необхідно розуміти інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами».

Внесення таких змін надасть можливість чітко легітимізувати оперативно-розшукові заходи, які реалізуються шляхом використання кіберпростору, та створить умови для їх розвитку як самостійного виду оперативно-розшукових заходів, що безперечно призведе до покращення стану боротьби з кіберзлочинністю.

Література

1. Державна програма інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою зі злочинністю : затв. постановою Кабінету Міністрів України від 8 квіт. 2009 р. № 321 // Офіційний вісник України. – 2009. – № 27. – Ст. 896.
2. Про оперативно-розшукову діяльність : закон України від 18 лют. 1992 р. // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303. – Зі змінами і доповненнями на 15 груд. 2005 р.
3. Сергєєва Д. Б. Зняття інформації з каналів зв'язку: кримінально-процесуальні і криміналістичні засади : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза» / Д. Б. Сергєєва. – К., 2008. – 16 с.
4. Regulation of Investigatory Powers Act. – London, 2000.
5. Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав громадян під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства : постанова Пленуму Верховного Суду України від 28 берез. 2008 р. № 2 // Юридичний вісник України. – 2008. – № 5. – Ст. 20.
6. Про право власності на окремі види майна : постанова Верховної Ради України від 17 черв. 1992 р. № 2471-ХІІ // Відомості Верховної Ради України. – 1992. – № 35. – Ст. 517. – Зі змінами і доповненнями на 24 січ. 1995 р.

7. Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації : затв. постановою Кабінету Міністрів України від 27 жовт. 2001 р. № 1450 // Офіційний вісник України. – 2004. – № 28. – Ст. 1870. – Зі змінами і доповненнями на 25 трав. 2006 р.

8. Ліцензійні умови провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації : затв. наказом Державного комітету України з питань регуляторної політики та підприємництва і Служби безпеки України від 10 жовт. 2006 р. № 92/669 // Офіційний вісник України. – 2006. – № 44. – Ст. 2967.

9. Про надання додаткової інформації [щодо переліку спеціальних технічних засобів] [Електронний ресурс] : лист Державної митної служби № 25/7-09-18/13158 від 2 листоп. 2004 р. – Режим доступу: Ліга : Еліт : комп'ютер.-прав. система / Всеукр. мережа розповсюдж. прав. інформ. [Електр. прогр.]. – Версія 7.4. – Зі змінами і доповненнями на 11 трав. 2006 р.

10. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затв. Постановою Кабінету Міністрів України від 28 січ. 2004 р. № 86 // Офіційний вісник України. – 2004. – № 4. – Ст. 167. – Зі змінами і доповненнями на 17 жовт. 2007 р.

11. Манжай О. В. Щодо особливостей використання в Україні спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації / О. В. Манжай // Інформатизація вищих навчальних закладів МВС України : матеріали наук.-практ. конф. (м. Харків, 15–16 травня 2008 р.). – Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2008. – С. 130–133.

12. Про телекомунікації : закон України від 18 листоп. 2003 р. // Офіційний вісник України. – 2003. – № 51. – Ст. 2644. – Зі змінами і доповненнями на 20 січ. 2010 р.

13. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги : затв. спільним наказом Служби безпеки України, Мінтрансзв'язку України від 31 лип. 2008 р. № 645/962 [Електронний ресурс]. – Режим доступу: Ліга : Еліт : комп'ютер.-прав. система / Всеукр. мережа розповсюдж. прав. інформ. [Електр. прогр.]. – Версія 7.4.

14. Інструкція з організації взаємодії органів досудового слідства з оперативними підрозділами органів внутрішніх справ України у виявленні, документуванні та розслідуванні злочинів у сфері економіки : затв. наказом МВС України від 8 верес. 2005 р. № 760 // Слідча практика : збірник. – К. : ГСУ МВС України, 2007. – С. 132–141.

15. Інструкція з організації взаємодії органів досудового слідства з оперативними підрозділами органів внутрішніх справ України на стадіях документування злочинних дій, реалізації оперативних матеріалів, розслідування кримінальної справи та її розгляді в суді : затв. наказом МВС України від 7 верес. 2005 р. № 777 // Слідча практика : збірник. – К. : ГСУ МВС України, 2007. – С. 113–131.

16. Снігирев А. П. Основания для проведения оперативно-розыскных мероприятий / А. П. Снігирев // Вісник ЛАВС. Методологічні проблеми теорії і практики ОРД в сучасних умовах. Ч. 1. – 2004. – Спецвипуск № 3 – С. 22–34.

17. Інструкція про порядок виконання європейських конвенцій з питань кримінального судочинства : затв. спільним наказом Міністерства юстиції України, Генеральної прокуратури України, Служби безпеки України, МВС України, Верховного суду України, Державної податкової адміністрації України, Державного департаменту України з питань виконання покарань від 29 черв. 1999 р. № 34/5/22/103/512/326/73.

18. Інструкція про порядок організації співробітництва органів внутрішніх справ України з правоохоронними органами іноземних держав з питань попередження, розкриття та розслідування злочинів : затв. наказом МВС України від 15 трав. 2007 р. № 158.

19. Інструкція про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні в попередженні, розкритті та розслідуванні злочинів : затв. спільним наказом МВС України, Генеральної прокуратури України, Служби безпеки України, Державного комітету у справах охорони державного кордону України, Державної митної служби України, Державної податкової адміністрації України від 9 січ. 1997 р. № 3/1/2/5/2/2.

20. Про порядок відносин органів внутрішніх справ України з компетентними правоохоронними органами іноземних держав по питаннях попередження, розкриття і розслідування злочинів : наказ МВС України від 6 верес. 1995 р. № 600.

21. Положення про Департамент зв'язків із громадськістю та міжнародної діяльності Міністерства внутрішніх справ України : затв. наказом МВС України від 8 лют. 2008 р.

22. Кримінальний кодекс України : станом на 21 січ. 2010 р. [Електронний ресурс]. – Режим доступу: Ліга : Еліт : комп'ютер.-прав. система / Всеукр. мережа розповсюдж. прав. інформ. [Електр. прогр.]. – Версія 7.4.

23. Кримінально-процесуальний кодекс України : станом на 23 груд. 2009 р. [Електронний ресурс]. – Режим доступу: Ліга : Еліт : комп'ютер.-прав. система / Всеукр. мережа розповсюдж. прав. інформ. [Електр. прогр.]. – Версія 7.4.

Надійшла до редколегії 21.04.2010