УДК 343.96+343.326+343.341

ПЕРСПЕКТИВИ НОРМАТИВНО-ПРАВОВОГО ВРЕГУЛЮВАННЯ ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ У НОВОМУ КПК УКРАЇНИ

Дмитро Мельник
Служба безпеки України

Анотація: **Розглядаються актуальні аспекти нормативно-правового врегулювання проведення розшукових та слідчих дій у телекомунікаційних мережах та електронних інформаційних системах.**
Summary: **The article is devoted to the problems of law regulation the interception of telecommunications in Ukraine.**
Ключові слова: **Зняття інформації, перехоплення телекомунікацій, правове регулювання, телекомунікаційні мережі, інформаційні системи.**

І Вступ

Інформаційна безпека держави передбачає захист якісних і кількісних параметрів інформаційних потоків у самій державі та за її межами від будь-яких негативних випливів, а також недопущення використання інформаційно-телекомунікаційних ресурсів і технологій з протиправною метою.

Новітні технології, засоби телекомунікації активно використовуються й у протиправній діяльності, що потребує налагодження ефективної системи протидії на рівні як відповідних оперативних та технічних можливостей правоохоронних органів, так і нормативно-правового забезпечення їх застосування.

Тому на сучасному етапі особливої актуальності в рамках забезпечення інформаційної безпеки держави набуває наукова розробка проблеми протидії транснаціональній кіберзлочинності та екстремістським і терористичним організаціям, які у своїй діяльності широко застосовують новітні інформаційні технології. Не менш актуальними є й практичні проблеми у сфері виявлення, документування та доказування комп'ютерних злочинів, які також підтверджують необхідність вирішення як проблем законодавчого регулювання, протидії комп'ютерній злочинності та комп'ютерному тероризму, перехоплення телекомунікацій з метою своєчасного отримання інформації про злочини в електронних системах та мережах.

У концептуальних документах щодо забезпечення національної безпеки

провідних країн світу (США, Великобританії, ФРН) як один із важливих механізмів моніторингу її стану визначається негласний збір, пошук та фіксація інформації з використанням систем перехоплення телекомунікацій [1, с.100].

Наявний досвід провідних країн світу, які активно протидіють тероризму та злочинності, свідчить про те, що впровадження систем перехоплення телекомунікацій суттєво підвищило ефективність збору упереджувальної інформації про терористичні акти та інші протиправні дії, що плануються. У ратифікованій Україною «Конвенції про кіберзлочинність» від 23. 11. 2001 р. зазначається, що здійснення перехоплення інформації у міжнародних телекомунікаційних мережах є необхідною умовою боротьби проти найбільш небезпечних злочинних угрупувань та міжнародних терористів [2].

Разом з тим, проведення пошукових та оперативно-технічних заходів в автоматизованих інформаційних системах та у мережах телекомунікацій потребує створення у нашій державі необхідних нормативно-правових засад перехоплення інформації у таких системах і мережах, адаптованих до норм європейського законодавства.

І Результати досліджень

Окремі питання нормативного врегулювання протидії комп'ютерній злочинності розглядаються у роботах вітчизняних та іноземних фахівців – Ю. В. Гавріліної, А. Л. Осипенко, М. Н. Скріпіна, Н. М. Ахтирської, П. Д. Біленчука, В. М. Вєртузаєва, В. Д. Гавловського, В. О. Голубєва, М. В. Гуцалюка, І. Г. Поплавського, В. М. Поповича, В. Б. Хлевицького, В. С. Цимбалюка та інших.

Науковими дослідженнями перехоплення телекомунікацій, зняття інформації з каналів зв'язку як документування протиправних дій, а також діяльності спецслужб та правоохоронних органів у цій сфері займалися С. М. Гриняєв, О. А. Коцюба, М. М. Перепелиця, О. В. Манжай, В. С. Серьогін,

О. В. Литвиненко, Г. С. Корж, І. М. Лоскутов, А. В. Тарасюк та ін. Однак більшість їх публікацій стосуються процесуальних та технічних аспектів цього питання.

Разом з тим, деякі дослідники (М. М. Перепелиця, О. В. Манжай, В. С. Серьогін) все ж торкалися у своїх роботах такого важливого аспекту зняття інформації з телекомунікаційних мереж та електронних інформаційних систем, як його належне правове врегулювання. Однак нормативне врегулювання цього питання у новому КПК України від 13. 04. 2012 р. поки що не було досліджено з необхідною повнотою вітчизняними дослідниками в силу новизни його норм.

Тому ***метою*** статті є висвітлення питання зняття інформації з телекомунікаційних мереж та електронних інформаційних систем та надання пропозицій щодо його нормативно-правового врегулювання у національному законодавстві.

ІІ Основна частина

У документах Ради Європи визначено, що вирішення проблеми боротьби зі злочинністю в сфері інформаційно-телекомунікаційних технологій можливе за умови створення ефективної системи міжнародного співробітництва шляхом гармонізації законодавств країн ЄС відповідно до рекомендацій щодо здійснення правоохоронними органами країн ЄС перехоплення телекомунікацій, викладених у Директиві від 12. 07. 2002 р. №2002/58/ЄС. Цією Директивою Європарламент зобов'язав уряди країн ЄС до жовтня 2003 р. прийняти закони щодо збереження даних трафіку телекомунікаційних послуг в інтересах правоохоронних органів. На виконання вказаної директиви у більшості держав-членів ЄС вже прийнято правові акти, що регламентують відносини, які виникають при перехопленні інформації у телекомунікаційних мережах і системах, збереженні даних трафіку.

Так, зокрема, створення та впровадження сучасних систем моніторингу та зняття інформації з каналів телекомунікацій визначається як головний механізм захисту національної безпеки у концептуальних документах США, Великобританії та інших західних держав з цього питання. При цьому, Концепцією інформаційної безпеки США та документом «Перехоплення комунікацій Великобританії» як основний метод законного моніторингу телекомунікацій та зняття з них інформації визначається збирання інформації про злочини, що плануються або готуються, а також про злочинні наміри. Окрім того, у документах зазначено, що без використання одночасного моніторингу всіх мереж загального користування неможливо повноцінно забезпечити операції проти транснаціональних терористичних та злочинних організацій. Тому цілком виправданою є практика створення спецпідрозділів, як проводять пошукову роботу на виділених напрямах (наприклад, Government Technical Assistance Centre – GTAC британської MI-5).

Рекомендації Ради ЄС «ENFOPOL 98» та «ENFOPOL 99» від 30. 03. 2001 р., а також прийняті законодавчі акти США, Великобританії та Німеччини закріпили порядок упровадження та функціонування систем законного моніторингу на всіх телекомунікаційних мережах загального користування. Окрім того, законодавчі норми більшості розвинутих країн світу вимагають чіткої ідентифікації відправника та одержувача повідомлення електронної пошти [3, с. 198].

Слід зауважити, що у документі Комітету НАТО з планування цивільного зв'язку «Захист вразливої інформаційної інфраструктури» 2002 р. наведено рекомендації щодо підготовки нормативно-правової бази, яка б стимулювала провайдерів телекомунікаційних мереж створювати умови для убезпечення телекомунікаційного середовища (у т. ч. впровадження систем перехоплення) в умовах розвитку ринкових відносин та послаблення контролю держави [1, с. 102].

Після подій 11 вересня 2001 р. в США спецслужби цієї держави отримали нові додаткові повноваження з перехоплення телекомунікацій – право здійснювати моніторинг веб-сайтів, форумів та інших Інтернет-ресурсів щодо діяльності громадських, релігійних і політичних організацій та зняття з них інформації не лише у рамках розслідування.

В Україні питання впровадження системи перехоплення телекомунікацій та його законодавчого забезпечення набуло широкого суспільного резонансу. Вагомою підставою для нього стало застереження, що правоохоронні органи можуть здійснювати тотальний контроль змісту інформаційних потоків, чим порушувати права і свободи людини, визначені Конституцією України та міжнародними актами, у першу чергу Конвенцією про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28. 01. 1981 р. [4].

Забезпечення захисту прав і свобод людини передбачає, з одного боку, захист особистої безпеки від загрози терористичних посягань, а з іншого – гарантування невтручання держави у приватне життя особи. З часом виконання цих завдань поступово ускладнюється: постійно змінюються у бік вдосконалення методи та засоби вчинення злочинів, що зумовлює адекватне реагування правоохоронних органів, яке проявляється у пошуку й упровадженні нових механізмів протидії злочинній діяльності. Це на певному етапі призводить до

часткового обмеження низки прав і свобод громадян (право на недоторканість приватного життя, таємницю переговорів тощо).

В Україні національне законодавство визначає право суб'єктів оперативно-розшукової діяльності на застосування зняття інформації з каналів зв'язку як одного з оперативно-технічних заходів за наявності відповідних підстав. Однак, не зважаючи на актуальність правового забезпечення проведення оперативно-технічних заходів на каналах зв'язку для правоохоронних органів в умовах стрімкого розвитку інформаційного середовища, на законодавчому рівні не регламентовано прозорий порядок створення та впровадження систем перехоплення телекомунікацій, не визначені організаційно-технічні вимоги, які повинні забезпечувати парламентський та інші види контролю.

Доречно зазначити, що на розгляд ВР України свого часу було внесено два законопроекти щодо перехоплення телекомунікацій: від 26. 03. 2004 р. №4042-1 та від 21. 03. 2005 р. №4042-2, однак які так і не були прийняті через потребу суттєвого доопрацювання з урахуванням зауважень, висловлених центральними органами виконавчої влади України. З метою забезпечення реалізації правоохоронної функції держави під час проведення оперативно-технічних заходів у мережах телекомунікацій з додержанням прав людини, імплементації норм законодавства ЄС, у СБ України було підготовлено законопроект «Про перехоплення телекомунікацій», який також не було прийнято.

На сучасному етапі проведення оперативно-технічних заходів у мережах телекомунікацій та електронних інформаційних системах зроблено у новому Кримінальному процесуальному кодексі України, прийнятому ВР України 13. 04. 2012 р. [5]. Відповідно до КПК України, зняття інформації з транспортних телекомунікаційних мереж (ст. 263) та зняття інформації з електронних інформаційних систем (ст. 264) є різновидами втручання в приватне спілкування, яке проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації, якщо при цьому можна встановити обставини, які мають

значення для кримінального провадження. Такі негласні слідчі (розшукові) дії (в частині дій, що проводяться на підставі ухвали слідчого судді) проводяться у кримінальному провадженні щодо тяжких або особливо тяжких злочинів.

Відповідно до ч. 1 ст. 258 КПК України, ніхто не може зазнавати *втручання у приватне спілкування* без ухвали слідчого судді, за винятком випадків проведення негласної слідчої (розшукової) дії до постановлення ухвали слідчого судді, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або особливо тяжкого злочину, передбачених ст. 250 КПК України. *Приватність* такого *спілкування* полягає в тому, що якщо інформація передається та зберігається за таких фізичних чи юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від стороннього втручання.

Відповідно до ч. 4 ст. 258 нового КПК України, *втручанням у приватне спілкування* є доступ до змісту спілкування за умови, коли учасники спілкування мають достатні підстави вважати, що спілкування є приватним. Різновидами такого втручання у новому кодексі визначено *зняття інформації з транспортних телекомунікаційних мереж* та *з електронних інформаційних систем* поряд з аудіо-, відео-контролем особи та арештом, оглядом і виїмкою кореспонденції.

Прокурор, слідчий за погодженням з прокурором зобов'язаний у встановленому порядку звернутися до слідчого судді з клопотанням про отримання дозволу на втручання у приватне спілкування, якщо будь-яка слідча (розшукова) дія включатиме таке втручання.

Зняття інформації з транспортних телекомунікаційних мереж[1] (ТТМ) відповідно до ст. 263 КПК України полягає у проведенні спостереження, відбору та фіксації змісту інформації, яка передається особою та має значення для досудового розслідування із застосуванням відповідних технічних засобів, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку. Таке зняття інформації з ТТМ проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження.

Згідно з ч. 4 ст. 263 нового КПК України, зняття інформації з ТТМ покладається на уповноважені підрозділи органів МВС та СБ України. Керівники та працівники операторів телекомунікаційного зв'язку на виконання положень ст. 263 нового КПК України зобов'язані сприяти виконанню дій із зняття інформації з ТТМ, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її у незмінному вигляді з метою забезпечення подальшого використання у кримінальну судочинстві.

[1] ТТМ - мережі, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу згідно зі ст. 1 Закону України «Про телекомунікації».

Ці положення нового КПК України кореспондуються з ч. 4 ст. 39 Закону України «Про телекомунікації», відповідно до якого оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх ТТМ технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

Окрім того, відповідно до ч. 2 ст. 41 Закону України «Про телекомунікації», персонал оператора, провайдера телекомунікацій несе відповідальність за порушення вимог законодавства щодо збереження таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Адже у ч. 1 ст. 9 вказаного закону зазначено, що охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, яка передається технічними засобами телекомунікацій, та інформаційна безпека ТТМ гарантуються законами України.

В ухвалі слідчого судді про дозвіл на втручання в приватне спілкування в цьому випадку додатково повинні бути зазначені *ідентифікаційні ознаки*, які дозволять унікально ідентифікувати абонента спостереження, ТТМ, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування (ч. 2 ст. 263 КПК України). Такими ознаками можуть бути: номер абонента в телефонній мережі загального користування у форматі «*код країни - код зони або оператора - номер абонента в мережі*»; міжнародний ідентифікаційний номер мобільного терміналу (IMEI); міжнародний ідентифікаційний номер мобільного абонента (IMвI).

Однак ні Закон України «Про оперативно-розшукову діяльність», надаючи оперативним підрозділам право проводити зняття інформації з каналів зв'язку, ні КПК України, не містять норм, що розкривають сутність проваджуваних дій.

Окремі положення норм вказаного закону тлумачить постанова Пленуму Верховного Суду України від 28. 03. 08 р. № 2 «Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства» [6], у п. 3 якої зазначається, що 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 переданої інформації. Тобто, отримання оперативними підрозділами інформації про з'єднання абонентів телекомунікацій, навіть без розкриття змісту повідомлень, відповідно до Закону України «Про оперативно-розшукову діяльність» може здійснюватися лише за рішенням суду.

Зняття інформації з ТТМ для контролю та фіксації інформації, що передається через Інтернет й інші мережі передачі даних, може здійснюватися за відповідними ідентифікаційними ознаками: адресою електронної пошти у форматі «ім'я поштової скриньки @домен. домен верхнього рівня» (наприклад, info@ssu.gov.ua); адресою в мережі передання даних із комутацією пакетів, у т. ч. IP-адреса для мережі Інтернету у форматі «xxx.xxx.xxx.xxx» (наприклад, 008.011.015.130); апаратною адресою (MAC-адресою) пристрою, приєднаного до мережевого середовища [7, с. 80].

В результаті зняття інформації з ТТМ можуть бути отримана інформація, що вказує на ознаки кримінального правопорушення в діях підозрюваного, обвинуваченого, а також відомості про протиправну діяльність окремих осіб, котрі контактували з ними через канали мережі під час проведення негласної слідчої (розшукової) дії. Отримані відомості фіксуються на матеріальні носії у форматі, придатному для автоматизованого оброблення на ЕОМ та відтворення слідчим, прокурором або судом із метою проведення інших процесуальних дій. Зміст відомостей з ТТМ, що мають значення для конкретного досудового розслідування, зазначається у протоколі про зняття інформації з ТТМ.

Зняття інформації з ТТМ до постановлення ухвали слідчого судді може бути розпочате на підставі постанови слідчого, прокурора лише у випадку, передбаченому ч. 1 ст. 250 КПК України. При цьому, слідчий за погодженням з прокурором або прокурор зобов'язаний невідкладно звернутися з клопотанням до слідчого судді. Слідчий суддя розглядає таке клопотання згідно з вимогами ст. 248 КПК України. Зняття інформації з ТТМ повинно бути негайно припинено, якщо слідчий суддя постановить ухвалу про відмову в наданні дозволу на його проведення. Отримана внаслідок такої негласної розшукової дії інформація повинна бути знищена відповідно до ст. 255 КПК України.

Порядок зняття інформації з електронних інформаційних систем[2] (ЕІС) закріплено у ст. 264 нового КПК України. Відповідно до ч. 1 ст. 264 кодексу, пошук, виявлення і фіксація відомостей, що містяться в ЕІС або її частині (база даних, система управління базою даних, клієнтське програмне забезпечення тощо), доступ до ЕІС або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в ЕІС (її частині), що має значення для досудового розслідування.

Сутність цієї негласної слідчої (розшукової) дії полягає у пошуку, виявленні й фіксації відомостей, що містяться в ЕІС або її частинах, без відома власника, володільця чи утримувача системи. Зазначена негласна дія проводиться, якщо є відомості про наявність інформації в ЕІС або її частині, що має значення для розслідування [7, с. 84]. Проведення такої негласної слідчої (розшукової) дії забезпечується зняттям інформації, яка оброблялася, зберіга-ється або зберігалася на одній чи кількох ЕІС, об'єднаних у локальну мережу, або ж на зовнішніх накопичувачах інформації, що приєднувалися до ЕІС.

В ухвалі слідчого судді про дозвіл на втручання в приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки ЕІС, в якій може здійснюватися втручання у приватне спілкування (найменування ЕІС, фізична адреса розташування її файлових серверів та робочих станцій або електронна адреса в мережі Інтернет, її власник, володілець чи утримувач) та спосіб обмеження доступу до неї (ч. 3 ст. 264 КПК України). Не потребує дозволу слідчого судді здобуття відомостей з ЕІС або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України).

Зняття інформації з ЕІС або їх частин може здійснюватися як з безпосереднім фізичним доступом до них правоохоронних органів, так і шляхом віддаленого доступу (програмного проникнення). Негласне зняття інформації із ЕІС полягає в застосуванні засобів спецтехніки із великим ресурсом оперативної та постійної пам'яті, яка забезпечує повне копіювання інформації з жорсткого диску та інших електронних носіїв інформації підозрюваного (обвинуваченого), що можуть містити інформацію, яка має значення у кримінальному провадженні. Програмне проникнення до ЕІС (їх частин) здійснюється шляхом застосування спеціальних програм, які забезпечують копіювання інформації, оброблюваної на ПЕОМ підозрюваного (обвинуваченого), на віддалений комп'ютер уповноваже-ного органу, який проводить цю негласну слідчу (розшукову) дію [7, с. 86].

Зміст інформації, одержаної в ході зняття відомостей з ЕІС або їх частин, фіксується на відповідному носієві особою, яка здійснювала зняття та забезпечує обробку, збереження або передавання інформації (ч. 2. ст. 265 КПК України).

Проведення зняття інформації з ТТМ й ЕІС (або їх частин) має на меті пошук та фіксацію інформації, що може бути використана у кримінальному провадженні для розкриття та розслідування злочинів. Така інформація також може бути використана для планування та проведення слідчих дій, здійснення заходів запобігання й припинення інших правопорушень. При цьому можна отримати інформацію, яка має доказове значення у кримінальному провадженні та може вказувати на ознаки вчинення злочину окремими особами, місця зберігання документів і предметів, що мають доказове значення.

Окрім того, правоохоронні органи в процесі моніторингу й фіксації інформації, що має значення для кримінального провадження, можуть проводити цілеспрямований пошук відкритої інформації з метою виявлення відомостей, необхідних у справі. Зокрема, у мережі Інтернет може здійснюватися пошук інформації стосовно осіб, підозрюваних у підготовці й вчиненні злочинів, їх зв'язків та інших відомостей, необхідних для вирішення завдань досудового розслідування. Отримання дозволу слідчого судді на пошук та фіксацію цієї інформації КПК не вимагає, оскільки вона є загальнодоступною й не відбувається обмеження приватності спілкування окремих осіб [7, с. 87].

Разом з тим, окрім законодавчого врегулювання визначеного вище кола питань діяльності правоохоронних органів в інформаційній сфері, потребують також остаточного приведення у відповідність до положень Конвенції про кіберзлочинність норми вітчизняного законодавства, наявною є потреба створення умов, які б покращували можливості цих органів в реалізації правозастосовної функції у сфері протидії комп'ютерній злочинності [8, с. 41-42]:

---

[2] Відповідно до ст. 1 Закону України «Про захист інформації в автоматизованих системах» від 5. 07. 1994 р. (зі змінами і доповненнями від 31. 05. 2005 р.), ЕІС – це організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів. Власником інформації слід уважати фізичну або юридичну особу, якій належить право власності на цю інформацію. Крім того, під власником ЕІС слід розуміти фізичну або юридичну особу, якій належить право власності на саму систему. Володілець - фізична або юридична особа, яка має законне право фактично використовувати річ згідно з призначенням. Утримувач - фізична чи юридична особа, яка постійно або тимчасово володіє, застосовує та несе відповідальність за використання предмета утримання та його збереження.

- по-перше, необхідно прийняти розроблений СБ України законопроект «Про моніторинг телекомунікацій» на виконання Резолюції Ради ЄС «Про законне перехоплення телекомунікацій» (96/С 329/01) від 17. 01. 1995 р. Суб'єктами перехоплення телекомунікацій неодмінно повинні бути визначені як правоохоронні органи, оператори (провайдери) телекомунікацій, ДССЗЗІ України, так і Уповноважений ВР України з прав людини, прокуратура та судові органи;

-по-друге, прийняти необхідні зміни до Закону України «Про телекомунікації» щодо врегулювання сфери надання та використання Інтернет-послуг в Україні за наступними основними моментами:

− вдосконалення нормативного регулювання відносин між операторами телекомунікаційних послуг, Інтернет-провайдерами, споживачами їх послуг та правоохоронними органами в існуючих правових межах;

− покладення на Інтернет-провайдерів зобов'язання щодо зберігання даних про реєстрацію користувачів Інтернет протягом 90 днів відповідно до положень ч. 2 ст. 16 Конвенції про кіберзлочинність 2001 р. з метою формування необхідної доказової бази для викриття та розслідування комп'ютерних злочинів,

вчинених з використанням мережі Інтернет;

- по-третє, вкрай важливо передбачити у чинному Кримінальному кодексі України відповідальність за навмисне перехоплення технічними засобами, без права на це, інформації шляхом фіксації електромагнітних випромінювань комп'ютерної системи, яка містить в собі такі дані (ст. 3 Конвенції);

- по-четверте, для реалізації зазначених кримінально-правових норм у протидії кіберзлочинності необхідно внести зміни та доповнення до КПК України та законів України «Про оперативно-розшукову діяльність», «Про контр-розвідувальну діяльність», «Про телекомунікації» у частині, що стосується процесуальних прав органів досудового розслідування та прокурора, фіксації доказів в електронній формі, проведення обшуків і вилучення ЕОМ, систем та мереж або їх складових, а також інформації, яку вони містять.

При цьому повинні знайти відображення положення про:

– повноваження слідчого та прокурора видавати накази або інші обов'язкові до виконання приписи про термінове збереження комп'ютерних даних, необхідних для розкриття злочинів (ч. 1 ст. 16, ст. 17 Конвенції);

– обов'язковість збереження провайдерами даних про трафік інформації на термін до 90 днів з можливістю його продовження (ч. 2 ст. 16 Конвенції);

– обов'язок суб'єкта, який зберігає комп'ютерні дані, не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом визначеного періоду (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21 Конвенції);

– запровадження спрощеного порядку (за потреби проведення невідклад-них оперативно-розшукових заходів чи слідчих дій) розкриття провайдером органу розслідування обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг, і трафік інформації (ч.1 ст. 17 Конвенції);

– надання слідчому та прокурору права терміново поширити проведення обшуку (огляду, виїмки чи інших слідчих дій) на будь-яку іншу систему, коли вони здійснюють вказані дії щодо конкретної комп'ютерної системи або її частини й мають обґрунтовані підстави вважати, що дані, які розшукуються, можуть зберігатися в цій системі чи її частині, і до таких даних можна здійснити законний доступ чи вони доступні першій системі (ч. 2 ст. 19 Конвенції).

ІІІ Висновок

Таким чином, ефективній реалізації положень КПК України щодо зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем, безсумнівно, сприятиме прийняття Закону України «Про моніторинг телекомунікацій», а також внесення змін до законів України «Про телекомунікації», «Про оперативно-розшукову діяльність» та «Про контррозві-дувальну діяльність» у частині створення умов, які б покращували можливості уповноважених органів в реалізації правозастосовної функції з протидії комп'ютерній злочинності.

Література: ***1.*** *Серьогін В.С. Проблеми створення системи моніторингу інформаційного простору України /В.С. Серьогін // Інформаційна безпека держави у світлі розвитку сучасних інформаційних технологій: Матеріали наук.-практ. конф. (м. Київ, 30 червня 2006р.). – К.: Наук.-вид. відділ НА СБ України, 2007. – С. 99-103.* ***2.*** *Конвенція Ради Європи про кіберзлочинність / Додаток до Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 р. // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71.* ***3.*** *Коцюба О.А. Щодо оптимізації законодавчого регулювання окремих напрямів протидії розвідувальній діяльності /О.А.Коцюба // Проблеми законодавчого регулювання діяльності СБ України у контексті положень Конституції України та побудови демократичного суспільства // Матеріали науково-практичної конференції (9 лютого 2006 р.). Київ. - НКЦ «Інститут оперативної діяльності та державної безпеки». - 2006. – С. 196 -199.* ***4.*** *Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28.01.1981 р. / Додаток до Закону України «Про ратифікацію Конвенції про про*

захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» від 6.07.2010 р. №2438-VI // Відомості Верховної Ради України. – 2010. - №46. - Ст. 542. ***5.*** *Кримінальний процесуальний кодекс України. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України»: (відповідає офіційному текстові). – К.: Алерта, 2012. - 304с.* ***6.*** *Постанова Пленуму Верховного Суду України «Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства» від 28.03.2008 р. №2 //http://www.scourt.gov.ua/clients/vs.nsf.* ***7.*** *Негласні слідчі (розшукові) дії. Коментар до глави 21 Кримінального процесуального кодексу України / [кол. авт.; за заг. ред. Є.Д. Скулиша]. - К. : Наук.- вид. центр НА СБУ, 2012. - 132 с.* ***8.*** *Климчик О., Мельник Д. Реалізація положень конвенції про кіберзлочинність в законодавстві України / О. Климчук, Д. Мельник // Інформаційна безпека людини, суспільства, держави. – 2009. – № 1(1). – С. 39-43.*

УДК 004.056.5; 338.516.2

МОДЕЛЬ ЦІНОУТВОРЮЮЧИХ ЧИННИКІВ НАДАННЯ ПОСЛУГ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Володимир Кононович, Юрій Копитін*, Марина Копитіна

*Одеська національна академія зв'язку ім. О. С. Попова, *КП «Обласний інформаційно-аналітичний центр» Одеської обласної ради*

Анотація: **Розкрито основні засади ведення в Україні господарської діяльності у сфері забезпечення інформаційної безпеки (СЗІБ). Побудовано модель витрат на впровадження СЗІБ у формі спіралі Архімеда. Запропоновано класифікацію послуг у СЗІБ. Відображено основні чинники, що впливають на процес ціноутворення надання послуг у СЗІБ у вигляді моделі.**

Summary: **The basic principles of doing business in Ukraine in the sector of information security (SIS) is showed. The model of the costs of implementation SIS is build. The classification of services SIS is proposed. A model of the main factors that affect the pricing of services SIS is displayed.**

Ключові слова: **Послуги у сфері забезпечення інформаційної безпеки, ціна, якість.**

І Вступ

Сучасний світ характеризується тенденціями глобалізації та інтеграції світової економіки, широким використанням інформаційно-комунікаційних технологій (ІКТ), формуванням нового типу економіки – економіки знань або інноваційної економіки, в якій основними чинниками розвитку і джерелами зростання якості життя людей є знання, високі технології та людський капітал. Генерування і впровадження ідей та інновацій, виробництво високоякісних конкурентоспроможних товарів та послуг у всіх сферах діяльності та їх споживання є сьогодні ключовою сферою економіки та фундаментом, на якому будується інформаційне суспільство.

Стрімке використання новітніх ІКТ несе в собі не лише позитивний розвиток, а й загрози інформаційної безпеки (ІБ), що створює передумови для витоку, розкрадання, втрати, спотворення, підробки, знищення, копіювання і блокування інформації і, як наслідок, веде до заподіяння шкоди. З підвищенням значущості і цінності ІКТ зростає важливість надання якісно нових послуг у сфері забезпечення інформаційної безпеки (СЗІБ).

Окремі складові даної тематики висвітлені в публікаціях Доморева В. В., Загинайлов Ю. М., Малюк А. О., Ткаченко В. В., Соколової А. О., Філіппової І. А, Баталової Н. В., Анісімова О. О. та інших. Однак, будь-яких комплексних досліджень ринку ІБ та надання послуг в СЗІБ, в тому числі процесу їх ціноутворення, в Україні та СНД не проводилося.

В зв'язку з цим, *метою статті* є висвітлення проблематики та пошук відповідей на проблемні питання процесу ціноутворення надання послуг у СЗІБ, а також представлення основних його чинників у вигляді моделі.

Для реалізації даної мети використано чинне національне законодавство, нормативно-правові акти, міжнародні та державні стандарти, світові практики щодо забезпечення ІБ та надання послуг, думки експертів, результати спеціалізованих досліджень, рекламні матеріали компаній та інші відкриті джерела інформації.