

## МЕТОДОЛОГІЧНІ ЗАСАДИ ДЕРЖАВНОСТІ, ПРАВА І БЕЗПЕКИ

УДК 342.72

**В. О. СЕРЬОГІН,**

*кандидат юридичних наук, доцент,*

*начальник кафедри конституційного та міжнародного права*

*Харківського національного університету внутрішніх справ*

### ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ КОМУНІКАЦІЙНОГО ПРАЙВЕСІ В УКРАЇНІ

Здійснено спробу системної, розгорнутої характеристики законодавчого забезпечення комунікаційного прайвесі в Україні. Зроблено висновок, що українському законодавству бракує системності та єдності підходів до регулювання комунікаційного прайвесі, а відсутність належного інституційного механізму у поєднанні з низьким рівнем загальної правосвідомості суттєво знижує його ефективність.

Науково-технічний прогрес сприяє дедалі більш інтенсивному проникненню держави, інших суспільних інститутів та окремих сторінних осіб у приватне життя громадян. Людина виявляється не захищеною перед потужним механізмом нагляду і шпигування, спорядженим найсучаснішою технікою і технологіями. Сьогодні вже не обов'язково проникати у житло для встановлення звуко- та аудіозаписувальної апаратури. За даних умов особливо страждає комунікаційний аспект недоторканності приватного життя, або, інакше кажучи, комунікаційне прайвесі. Наявні в пострадянській юридичній науці дослідження, що стосуються даної проблематики (зокрема роботи Б. М. Кадникова, І. В. Смолькової, Ю. І. Стецовського, В. М. Тertiшника тощо), здебільшого мають кримінально-правовий чи кримінально-процесуальний характер і майже не стосуються конституційно-правових аспектів теми.

Усе це створює об'єктивні передумови для проведення наукового дослідження усього комплексу проблем щодо забезпечення комунікаційного прайвесі в Україні та приведення національного законодавства в даній сфері у відповідність із кращими зарубіжними аналогами та міжнародно-правовими стандартами. Зазначені обставини зумовлюють актуальність даного дослідження, його теоретичну і практичну значущість.

Метою даного дослідження є з'ясування кількісних і якісних характеристик українського законодавства з питань комунікаційного прайвесі, визначення його позитивних рис і недоліків, формування рекомендацій щодо оптимізації юридичного механізму захисту названого

права з урахуванням міжнародно-правових стандартів і позитивного зарубіжного досвіду. Досягненню означеної мети має сприяти комплексне використання формально-юридичного, порівняльно-правового, системно-структурного та інституційно-функціонального методів дослідження.

Розпочинаючи наше дослідження, передусім відзначимо, що комунікаційний аспект прайвесі (у контексті ст. 31 Конституції України) означає гарантування таємниці приватного спілкування, в тому числі й спілкування шляхом листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки з даного правила можуть бути встановлені лише судом у випадках, передбачених законом, із метою запобігати злочинів чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Найбільш суттєві обмеження комунікаційного аспекту приватності пов'язані зі здійсненням оперативно-розшукових заходів. Пункти 9–11 ст. 8 Закону України «Про оперативно-розшукову діяльність» надають право оперативним підрозділам для виконання завдань оперативно-розшукової діяльності у разі наявності передбачених ст. 6 цього ж Закону підстав вживати таких заходів: а) знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації; б) контролювати шляхом відбору за окремими ознаками телеграфно-поштової відправлення; в) здійснювати візуальне спостереження в громадських місцях із застосуванням фото-, кіно- і відеозйомки, оптичних та радіоприладів, інших технічних засобів [1].

З метою забезпечення конституційних прав громадян на недоторканність житла, таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, невтручання в особисте і сімейне життя під час проведення оперативно-технічних заходів Президентом України 7 листопада 2005 р. було видано Указ «Про додержання прав людини під час проведення оперативно-технічних заходів» [2]. Названим Указом давалася вказівка Кабінету Міністрів України протягом чотирьох місяців затвердити за погодженням із Верховним Судом України і Генеральною прокуратурою України єдину інструкцію про порядок отримання підрозділами, які здійснюють оперативно-розшукову діяльність, дозволів на проведення відповідних заходів та використання одержаних при цьому матеріалів. Проте у встановлений Указом термін відповідна інструкція затверджена не була.

Чинний Порядок отримання дозволу суду на здійснення заходів, які тимчасово обмежують права людини, та використання добутої інформації було затверджено постановою Кабінету Міністрів України від 26 вересня 2007 р. № 1169 [3]. Цей Порядок визначає процедуру отримання дозволу суду на здійснення заходів, які тимчасово обмежують права людини, зокрема на негласне проникнення до житла чи іншого володіння особи, застосування технічних засобів добування інформації, зняття її з каналів зв'язку, установлення контролю за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією особи, а також використання інформації, отриманої під час здійснення таких заходів.

Згідно з названим Порядком, заходи, які тимчасово обмежують права людини, можуть здійснювати тільки ті підрозділи, яким відповідно до закону надано право на провадження оперативно-розшукової діяльності. Виключний перелік таких підрозділів наведено у ст. 5 Закону України «Про оперативно-розшукову діяльність». До цього переліку включено оперативні підрозділи: Міністерства внутрішніх справ України, Служби безпеки України, Служби зовнішньої розвідки України, Державної прикордонної служби України, управління державної охорони, органів державної податкової служби, органів і установ виконання покарань та слідчих ізоляторів Державної кримінально-виконавчої служби України, розвідувального органу Міністерства оборони України.

Для отримання дозволу керівник відповідного підрозділу, у провадженні якого перебуває оперативно-розшукова чи контррозвідува-

льна справа, або його заступник вносить на розгляд суду подання про отримання дозволу, погоджене у визначених законом випадках із прокурором. У цьому поданні зазначаються: 1) гриф секретності, дата та реєстраційний номер; 2) найменування суду, до якого вноситься подання; 3) найменування підрозділу, який вносить подання, та підрозділу, працівники якого залучаються до здійснення заходу; 4) вид, категорія, номер справи та дата її заведення; 5) вид заходу, строки і місце його здійснення (житло чи інше володіння особи, інші приміщення, земельна ділянка, транспортний засіб тощо); 6) обґрунтування необхідності здійснення заходу; 7) дані про особу, стосовно якої передбачається здійснення заходу, місце проживання чи тимчасового перебування такої особи, а також залежно від виду заходу абонентні номери споживача телекомунікаційних послуг і міжнародний ідентифікатор мобільного обладнання; 8) інші відомості, що можуть мати значення для суду. Подання вноситься на розгляд голови апеляційного суду області, міст Київ та Севастополь, Апеляційного суду Автономної Республіки Крим або уповноваженого ним заступника за місцем провадження справи.

За результатами здійснення заходу складається протокол із відповідними додатками. У протоколі зазначаються дата його складення, посада, прізвище та ініціали особи, у провадженні якої перебуває справа, номер справи, за якою здійснювався захід, номер постанови, дата її прийняття та найменування суду, яким видано дозвіл на здійснення заходу, вид заходу та строки його здійснення, найменування підрозділу, працівники якого залучалися до здійснення заходу, дані про особу, стосовно якої здійснювався захід, результати здійснення заходу, відомості про матеріальні носії інформації (матеріали аудіо- чи відеозапису, фото- і кінозйомки, магнітні накопичувачі тощо) та місце їх зберігання. Протокол підписує працівник оперативного підрозділу, у провадженні якого перебуває справа. Забороняється зазначати в протоколі та зберігати в будь-якій іншій формі відомості, що стосуються особистого життя, честі, гідності людини, крім інформації про вчинення заборонених законом дій.

Інформація використовується виключно для запобігання вчиненню злочину чи встановлення істини під час розслідування кримінальної справи, запобігання, своєчасного виявлення і припинення розвідувальних, терористичних та інших посягань на національну безпеку, в інтересах контррозвідки, для забезпечення безпеки

під час здійснення розвідувальних заходів, захисту сил, засобів та інформаційних систем і облікових даних розвідувальних органів та джерел розвідувальної інформації, а також з метою її доведення до підрозділів, правоохоронних органів, органів державної влади та інших зацікавлених органів у випадках, передбачених законом. У разі коли запобігання вчиненню чи припинення злочину та/або затримання особи, яка перебуває в розшуку, потребує вжиття невідкладних заходів, інформація може негайно передаватися засобами зв'язку з дотриманням правил конспірації.

У випадках порушення прав і свобод людини або юридичних осіб у процесі здійснення оперативно-розшукової діяльності, а також у разі, якщо причетність до правопорушення особи, щодо якої здійснювались оперативно-розшукові заходи, не підтвердилась, відповідні органи зобов'язані невідкладно поновити порушені права і відшкодувати заподіяні матеріальні та моральні збитки в повному обсязі. Громадяни України та інші особи мають право у встановленому законом порядку одержати від органів, на які покладено здійснення оперативно-розшукової діяльності, письмове пояснення з приводу обмеження їхніх прав і свобод та оскаржити ці дії.

Одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, розголошенню не підлягають. Такі відомості, що не містять інформації про вчинення заборонених законом дій, зберігання не підлягають і повинні бути знищені. За передачу і розголошення цих відомостей працівники оперативних підрозділів, а також особи, яким ці відомості були довірені при здійсненні оперативно-розшукової діяльності чи стали відомі у зв'язку зі службою або роботою, підлягають відповідальності згідно з чинним законодавством, крім випадків розголошення інформації про незаконні дії, що порушують права людини.

28 березня 2008 р. Пленум Верховного Суду України прийняв Постанову № 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» [4]. У названій постанові наголошено, що відповідно до ст. 64 Конституції України конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституці-

єю України. Конституцією і законами України передбачається можливість тимчасового обмеження конституційних прав і свобод людини і громадянина, передбачених статтями 30, 31, 32 Конституції України, під час проведення оперативно-розшукової діяльності, дізнання та досудового слідства. Підстави і порядок здійснення заходів, пов'язаних із тимчасовим обмеженням цих конституційних прав і свобод людини і громадянина, визначені Кримінально-процесуальним кодексом України (далі – КПК) [5], законами України «Про оперативно-розшукову діяльність» [1], «Про міліцію» [6], «Про контррозвідувальну діяльність» [7], «Про організаційно-правові основи боротьби з організованою злочинністю» [8].

Обмеження вказаних конституційних прав і свобод людини і громадянина під час проведення оперативно-розшукової діяльності, дізнання та досудового слідства допускається лише за вмотивованим рішенням суду (крім випадку, передбаченого ч. 3 ст. 30 Конституції України) і мають винятковий та тимчасовий характер. До порушення кримінальної справи вони застосовуються з метою запобігання тяжкого чи особливо тяжкого злочину, якщо іншим способом одержати інформацію неможливо. Надання дозволу на проведення оперативно-розшукових заходів після порушення кримінальної справи не залежить від тяжкості злочину.

Розглядаючи подання про тимчасове обмеження конституційних прав і свобод людини і громадянина, суддя перевіряє, чи відображено в ньому всі необхідні дані для їх розгляду, чи підписане воно уповноваженою службовою особою і чи погоджене воно у визначених законом випадках із прокурором, вивчає матеріали оперативно-розшукової, контррозвідувальної або кримінальної справи, за необхідності вислуховує суб'єкта внесення подання і виносить умотивовану постанову про задоволення подання або відмову в такому задоволенні. Обсяги надання матеріалів справи визначаються суддею. Невиконання законних вимог судді може бути підставою для відмови в задоволенні подання.

При розгляді подань суди повинні звертати особливу увагу на строки, протягом яких планується обмежити права людини. У будь-якому разі ці строки не можуть перевищувати строки ведення конкретної оперативно-розшукової справи (ст. 9-1 Закону України «Про оперативно-розшукову діяльність»). Розгляд таких подань здійснюється суддею невідкладно в режимі, що забезпечує нерозголошення даних, які

містяться в них та відповідних матеріалах справи.

Протиправне порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, тягне за собою кримінальну відповідальність згідно зі ст. 163 Кримінального кодексу України.

На жаль, чинне законодавство України не встановлює чітких підстав для зняття інформації з каналів зв'язку (прослуховування телефонів, мобільних телефонів, відстеження електронних повідомлень, контроль за переглядом інформації в мережі інтернет), чіткий строк, протягом якого здійснюється зняття такої інформації, а також обставини, за яких така інформація повинна знищуватися, і як вона може бути використана. Гарантії законності при здійсненні зняття інформації з каналів зв'язку явно недостатні. Внаслідок цього ніхто не може контролювати кількість дозволів та необхідність здійснення прослуховування, а особи, щодо яких здійснювалися такі заходи, не знають про це і, відповідно, не можуть оскаржити такі дії в суді чи іншим чином захистити своє право на приватність. На ці недоліки законодавства, що стосується захисту комунікаційного аспекту приватності, вперше було вказано ще у 2005 р. [11, с. 92], проте і сьогодні вони не усунуті [12, с. 82–83].

У справі «Волохи проти України» [13] Європейський суд із прав людини зазначив, що вимоги пропорційності втручання та їх виключна й тимчасова природа викладені в ст. 31 Конституції України і ст. 9 Закону України «Про оперативно-розшукову діяльність». Проте ні ст. 187 КПК, ні жодна інша норма українського права не містять механізму, який би дав гарантію того, що вищезазначені принципи були дотримані на практиці. Норма, про яку йдеться, не містить жодних указівок стосовно осіб, до котрих застосовуються такі заходи, обставин, за яких вони можуть використовуватися, часових обмежень, що мають бути встановлені й дотримані. Отже, ця норма не може вважатися достатньо чіткою та детальною для того, щоб забезпечити відповідний захист від неналежного втручання державних органів у право заявників на повагу до їхнього приватного життя та кореспонденції.

Крім того, Суд мав переконатись у тому, що існують відповідні ефективні гарантії проти зловживань, оскільки система таємного нагляду, створена для захисту національної безпеки та громадського порядку, включає ризик під-

риву чи навіть руйнування демократії на підставі її захисту. Такі гарантії мають бути так само передбачені законодавством в однозначному вигляді та застосовуватися для нагляду за відповідними діями державних органів. Процедури нагляду мають узгоджуватися із цінностями демократичного суспільства, зокрема із принципом верховенства права, який чітко викладений у преамбулі Конвенції. Принцип верховенства права вказує, зокрема, що втручання органів виконавчої влади в права людей має піддаватися ефективному наглядові, який зазвичай має виконуватися судовою владою, принаймні як останньою інстанцією, оскільки судовий контроль найкраще гарантує незалежність, неупередженість та належне провадження.

Слід відзначити, що на сьогодні єдиною країною, чинні норми про прослуховування телефонних розмов були схвалені Європейським судом з прав людини, є ФРН [14]. Тож у процесі удосконалення українського законодавства у сфері забезпечення комунікаційного прайвесі доцільно не «винаходити велосипед», а використати німецький досвід.

Точні дані про обсяги прослуховування телефонних розмов в Україні невідомі, оскільки офіційна статистика державними органами не надається. Так, відомо, що у 2002 р. судами було надано понад 40 000 санкцій. Офіційно підтверджено, що у 2003 р. Апеляційний Суд найменшої в Україні Чернівецької області надав 823 дозволи на зняття інформації з каналів зв'язку [15, с. 45–60]. Певні дані про кількість таких санкцій можна було б отримати з Єдиного державного реєстру судових рішень, оскільки судові рішення про надання дозволів на проведення окремих слідчих дій або оперативно-розшукових заходів у кримінальних справах включаються до Реєстру після винесення постанови (ухвали) про закриття справи чи постановлення вироку. Проте на сьогодні цей Реєстр має значущі недоліки – суттєву неповноту і низький рівень контекстного пошуку.

За даними експертів, найбільші порушення права на недоторканність приватного життя в Україні пов'язані саме з комунікаційним прайвесі. Законодавство не передбачає чітких підстав для зняття інформації з каналів зв'язку (прослуховування телефонів, мобільних телефонів чи відстеження повідомлень електронної пошти та інтернет-серфінгу), певного періоду такого пошуку інформації, а також обставин, за яких така інформація має бути знищена та як вона може бути використана. Гарантії законності отримання інформації з каналів зв'язку

є недостатніми. Таким чином, ніхто не може контролювати кількість дозволів на прослуховування, тоді як особи, на яких ці заходи спрямовані, не оповіщені про них і, відповідно, не можуть оскаржити такі дії в суді чи в інший спосіб захистити своє право на прайвесі.

Як зазначалося вище, Президент України ще восени 2005 р. видав Указ «Про додержання прав людини під час проведення оперативно-технічних заходів», проте його дотримання надалі пов'язано здебільшого з інституційними змінами в правоохоронних органах, а не із встановленням процесуальних гарантій від зловживань. Багатьом експертам у галузі прав людини такі заходи видаються поверховими. Передача «прослуховування» громадян одному органу, у даному випадку СБУ, сама по собі не може вирішити проблему. Жоден із наведених в Указі заходів, на нашу думку, не приведе до поліпшення ситуації, оскільки не враховує позитивну практику зарубіжних (передусім європейських) країн та стандарти, визначені Європейським судом із прав людини.

Вищезазначений Указ Президента України визначає необхідність створення в державі єдиного державного органу, що мав би право здійснювати зняття інформації з каналів зв'язку – служби спеціального зв'язку та захисту інформації України як центрального органу виконавчої влади зі спеціальним статусом, визначивши її основними завданнями реалізацію державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації. Необхідно відзначити й позитивний аспект – ця служба повністю формально відділена від СБУ, хоча фактично складається з її колишніх працівників.

Першим завданням після створення цього державного органу стало питання передачі в його відання усього обладнання для зняття інформації з каналів зв'язку, яким володіли правоохоронні органи. І тут з'явилися цікаві факти. Як виявилось, правоохоронні органи не змогли порухувати, скільки в них комплексів, призначених для зняття інформації з каналів зв'язку. СБУ довелося декілька разів просила здати все обладнання до новоутвореної служби, що отримала ексклюзивне право на зняття інформації з каналів зв'язку в країні.

Верховна Рада України ще 26 листопада 2006 р. прийняла проект Закону України «Про

внесення змін до деяких законодавчих актів України щодо попередження зняття інформації з телекомунікаційних мереж» [16]. Незважаючи на певні позитивні риси, даний законопроект насправді істотно нічого не змінював, оскільки не встановлював жодних додаткових гарантій від зловживань, визначених міжнародним правом (зокрема у рішеннях Європейського суду з прав людини), а лише розширював межі кримінальної відповідальності за порушення таємниці кореспонденції. Уже в березні 2007 р. проект був готовий до другого читання, проте й досі не прийнятий. Натомість у серпні 2010 р. у Парламенті був зареєстрований проект Закону України про внесення змін до ст. 39 Закону України «Про телекомунікації» (щодо основи національної безпеки у сфері телекомунікацій) [17], а у вересні того ж року альтернативний законопроект вніс депутат Ю. А. Кармазін [18]. Тож питання про законодавче врегулювання відносин, пов'язаних зі зняттям інформації з телекомунікаційних мереж в Україні, зберігає свою актуальність і залишатиметься предметом розгляду в парламенті протягом найближчого часу.

Однією з проблем, що дедалі загострюється, є забезпечення прайвесі у комп'ютерних мережах. СБУ з метою протидії так званому «комп'ютерному тероризму», здійснює заходи з контролю за користувачами мережі інтернет, регулюванню українського сегмента мережі. Незважаючи на відсутність правового визначення законом повноважень СБУ в цій сфері, вона й надалі впроваджує технічні можливості для контролю за користувачами мережі інтернет.

Відповідно до наказу Державного комітету зв'язку від 17 червня 2002 р. № 122, надавати послуги з доступу до глобальних мереж передачі даних установам та організаціям, що одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності, можуть лише інтернет-провайдери, які встановили державну систему моніторингу (аналог російського СОРМ) і отримали відповідний сертифікат СБУ. Особливо негативно інтернет-провайдери поставилися до вимоги СБУ встановлювати обладнання для моніторингу за власні кошти. Відділити трафік державного і недержавного користувача послуг і зробити його недоступним для моніторингу неможливо, тож автоматично всі клієнти компаній, що погодилися на встановлення обладнання, стають об'єктами постійного моніторингу з боку СБУ.

Згідно з Висновком Міністерства юстиції України від 4 серпня 2006 р. № 13/71 наказ

№ 122 було виключено з Державного реєстру нормативно-правових актів 21 серпня 2006 р. Незважаючи на це, вся діяльність, що здійснювалася на його підставі, здійснюється й надалі. Жодне обладнання не демонтовано й перелік провайдерів фактично й надалі функціонує. За даними експертів, на сьогодні СБУ незаконно перехоплює повідомлення та здійснює постійне стеження вже близько 50 % українського трафіку. При цьому рівень стеження зростає на регіональному рівні до 90 %, оскільки регіональним провайдерам важче сперечатися із СБУ.

Українська Гельсінська спілка захисту прав людини звернулася до Служби безпеки України з вимогою роз'яснити, на якій підставі здійснюється подальший моніторинг інтернету, коли наказ № 122 втратив свою чинність. У відповіді СБУ було зазначено, що ця діяльність здійснюється на підставі закону про оперативно-розшукову діяльність. Проте з огляду на функціонування системи моніторингу, виникають значні сумніви, що постійний моніторинг здійснюється виключно в межах порушених оперативно-розшукових справ. Справа в тому, що специфіка моніторингу вимагає постійного стеження за трафіком, а не вибіркового й переважно щодо конкретної особи.

Проведене дослідження дає підстави для висновку, що, на жаль, конституційні норми, які формулюють вичерпний перелік підстав для втручання в комунікаційне прайвесе та умови для такого втручання, не отримали достатнього розвитку в законах і підзаконних актах. Доволі нечітке формулювання або взагалі відсутність регламентування дозволених випадків втручання у комунікаційні аспекти приватного життя особи, обсягу та способів такого втручання, – є найбільш не вирішеною проблемою в законодавчому регулюванні прайвесе в Україні, що породжує численні порушення цього права на практиці. Відповідальність за порушення права на комунікаційне прайвесе передбачена як у кримінальному, так і в цивільному й адміністративному законодавстві, проте через нечіткість формулювань застосувати норми про цю відповідальність практично неможливо. Удосконалення процедур, пов'язаних з обмеженням комунікаційного прайвесе, слід проводити з урахуванням передового зарубіжного досвіду, передусім досвіду ФРН. Тому дослідження німецького законодавства у сфері прайвесе є одним з **пріоритетних напрямків подальших досліджень** у даній сфері.

#### Список використаної літератури

1. Про оперативно-розшукову діяльність [Електронний ресурс] : закон України від 18 лют. 1992 р. № 2135-ХІІ. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2135-12>.
2. Про додержання прав людини під час проведення оперативно-технічних заходів : указ Президента України від 7 листоп. 2005 р. № 1556/2005 // Офіційний вісник України. – 2005. – № 45. – Ст. 2834.
3. Про затвердження Порядку отримання дозволу суду на здійснення заходів, які тимчасово обмежують права людини, та використання добутої інформації : постанова Кабінету Міністрів України від 26 верес. 2007 р. № 1169 // Офіційний вісник України. – 2007. – № 73. – Ст. 2725.
4. 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 : постанова Пленуму Верховного Суду України від 28 берез. 2008 р. № 2 // Вісник Верховного Суду України. – 2008. – № 4. – Ст. 4.
5. Кримінально-процесуальний кодекс України [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1001-05>.
6. Про міліцію [Електронний ресурс] : закон України від 20 груд. 1990 р. № 565-ХІІ. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=565-12>.
7. Про контррозвідувальну діяльність [Електронний ресурс] : закон України від 26 груд. 2002 р. № 374-ІV. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=374-15>.
8. Про організаційно-правові основи боротьби з організованою злочинністю [Електронний ресурс] : закон України від 30 черв. 1993 р. № 3341-ХІІ. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3341-1>.
9. Про телекомунікації [Електронний ресурс] : закон України від 18 листоп. 2003 р. № 1280-ІV. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1280-15>.
10. Про поштовий зв'язок [Електронний ресурс] : закон України від 4 жовт. 2001 р. № 2759-ІІІ. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2759-14>.
11. Права людини в Україні – 2004. Доповідь правозахисних організацій / за ред. Є. Захарова, І. Рапп, В. Яворського. – Х. : Фоліо, 2005. – 92 с.
12. Права людини в Україні – 2007. Доповідь правозахисних організацій / за ред. Є. Захарова, І. Рапп, В. Яворського. – Х. : Права людини, 2008. – С. 82–83.

13. Справа «Волохи проти України» [Електронний ресурс]. – Режим доступу: <http://www.minjust.gov.ua/0/19619>.

14. *Klass and others v. Federal Republic of Germany* // European Court of Human Rights. – Series A. – № 28 (1979-80) 2 EHRR 214. – September 6, 1978.

15. Захаров Є. Оперативно-розшукова діяльність та приватність комунікацій / Є. Захаров // Свобода інформації та право на приватність в Україні. Т. 2. – Х. : Фоліо, 2004 – С. 45–60.

16. Проект Закону від 6 жовт. 2006 р. № 2288 [Електронний ресурс]. – Режим доступу: [http://search.ligazakon.ua/l\\_doc2.nsf/link1/JE1RK001.html](http://search.ligazakon.ua/l_doc2.nsf/link1/JE1RK001.html).

17. Проект Закону про внесення змін до статті 39 Закону України «Про телекомунікації» (щодо основи національної безпеки у сфері телекомунікацій) [Електронний ресурс]. – Режим доступу: [http://w1.c1.rada.gov.ua/pls/zweb\\_n/webproc4\\_1?id=&pf3511=38362](http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=38362).

18. Проект Закону про внесення змін до частини четвертої статті 39 Закону України «Про телекомунікації» (щодо встановлення на телекомунікаційних мережах технічних засобів для перехоплення комунікацій і оплати цього уповноваженими органами) від 2 верес. 2010 р. № 7023-1 [Електронний ресурс]. – Режим доступу: [http://w1.c1.rada.gov.ua/pls/zweb\\_n/webproc4\\_1?id=&pf3511=38444](http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=38444).

*Надійшла до редколегії 07.02.2011*

### **СЕРЁГИН В. А. ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ КОММУНИКАЦИОННОГО ПРАЙВЕСИ В УКРАИНЕ**

Осуществлена попытка системной, развёрнутой характеристики законодательного обеспечения коммуникационного прайвеси в Украине. Сделан вывод, что украинскому законодательству не хватает системности и единства подходов к регулированию коммуникационного прайвеси, а отсутствие должного институционального механизма в сочетании с низким уровнем общего правосознания существенно снижает его эффективность.

### **SERIOGIN V. LEGAL GUARANTYING OF COMMUNICATION PRIVACY IN UKRAINE**

An attempt of systematic, detailed characteristic of communication privacy legislation in Ukraine is made. It was concluded that Ukrainian legislation lacks consistency and cohesion of similar approaches to the regulation of communication privacy, and lack of proper institutional mechanism, coupled with low level of legal consciousness, substantially reduces its effectiveness.