ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 354.42/44:343.9

Гавловський Владислав Данилович –
начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук, старший науковий співробітник,

Шапочка Сергій Володимирович –
науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

До питання глобального незаконного збору персональних даних з використанням мережі Інтернет

У статті проаналізовано соціально-правові аспекти протиправної діяльності іноземних спеціальних служб із незаконного збору персональних даних з використанням телекомунікаційних мереж, а також запропоновано заходи протидії такій діяльності як у контексті охорони конституційних прав громадян, так і захисту національної безпеки України.

Ключові слова: персональні дані, незаконний збір, спецслужби.

Постановка проблеми. Сьогодні мережа Інтернет є невід'ємною частиною життя будь-якого активного члена суспільства. А можливість швидкого отримання інформації стала визначальним чинником успіхів у бізнесі, політиці, громадській та державницькій діяльності.

Оскільки, згідно із законами ринку, попит завжди породжує пропозицію, збір інформації про користувачів мережі Інтернет уже став звичною справою та системно здійснюється: ІТ-компаніями з метою задоволення маркетингових потреб комерційних структур; іноземними спеціальними службами для отримання оперативно-вагомої інформації

для здійснення як розвідувальної, так і контррозвідувальної діяльності; іншими іноземними урядовими і неурядовими організаціями та окремими особами як з метою задоволення власних інтересів, так і інформаційного забезпечення протиправної діяльності різноманітних злочинних угруповань (терористичних, екстремістських, загально кримінальних тощо).

При цьому, особливу занепокоєність викликає той факт, що, завдячуючи стрімкому розвитку ринку торгівлі технологіями глобального збирання розвідувальних даних, – коло суб'єктів відслідковування стрімко зростає. Придбати спеціальне програмне забезпечення (на кшталт Tempora) для відслідковування, за наявності коштів і потреби, має можливість будь-хто.

Нині новим видом загроз, що виходять з кібернетичного простору, є тотальне відслідковування осіб (індивідів): збирання, накопичення, аналіз й протиправне використання персональних конфіденційних даних користувачів щодо сфери приватного життя, а також фіксація більшості їхніх дій. Із урахуванням масштабів такої діяльності, її розповсюдження на фактично індивідуально невизначене коло наших співгромадян, це не лише порушує їхні конституційні особисті права, а й становить реальну загрозу національній безпеці України. Слід зазначити, що розвідки іноземних держав специфічними розвідувальними методами почали активно впливати на ситуацію в країнах, де здійснюється розвідка, у вигідному для зовнішньополітичного курсу конкретної держави [1, с. 10].

Тут варто зауважити, що збирання спеціальними службами відомостей про фізичних осіб через використання можливостей систем електронного обігу інформації не є новелою. Ще в 1947 році між США та Англією було укладено секретну угоду "UKUSA Agreement", за якою ці держави об'єднували свої технічні й людські ресурси в сфері глобального електронного шпигунства і створили глобальну систему радіоелектронної розвідки Echelon. Пізніше до них долучилися Канада, Австралія і Нова Зеландія. Цю групу країн-партнерів ще називають "п'ять очей". А згодом до альянсу приєдналися Норвегія, Данія, ФРН і Туреччина ("дев'ять очей"). Керівники радіорозвідок держав "п'ятірки" щорічно збиралися разом, щоб обговорити питання планування і координації діяльності за напрямками глобальної розвідки [2].

Сьогодні, завдячуючи викриттям колишнього співробітника Агентства національної безпеки США (далі АНБ) Едварда Сноудена, оприлюднено неспростовну фактичну інформацію про використання АНБ, для відслідковування людей в усьому світі, нових спеціальних надсекретних програм, таких як PRISM і XKeyscore. Отримано докази протиправного використання низкою національних іноземних спецс-

лужб технічних можливостей провідних ІТ-компаній, таких як Google, Facebook, Twitter, Microsoft, Apple, AOL, Yahoo, YouTube, Skype.

Аналіз останніх публікацій за темою дослідження. Проведенням наукових досліджень окремих аспектів незаконного збору персональних даних з використанням специфічних можливостей мережі Інтернет займаються такі вчені, як В. М. Бутузов, В. М. Горовий, О. В. Копан, С. А. Кузьмін, А. І. Марущак, О. О. Поляруш, Є. Д. Скулиш, В. П. Шеломенцев, О. М. Юрченко та інші, а також автори представленої статті. Проте, стрімкий розвиток інформаційних технологій, з використанням яких проводиться глобальне відслідковування громадян, спонукає нас до подальших наукових досліджень.

Мета статті. В попередніх наукових публікаціях вивчалося відслідковування громадян, що здійснювалося ІТ-компаніями. Ця стаття є логічним продовженням здійснюваного нами дослідження соціально-правових аспектів протиправної діяльності іноземних спеціальних служб із незаконного збору персональних даних з використанням телекомунікаційних мереж, а також вироблення заходів протидії такій діяльності як у контексті охорони конституційних прав наших співгромадян, так і захисту національної безпеки України.

Виклад основного матеріалу. Беззаперечним є той факт, що ІТ-компанії мають технологічні можливості відслідковувати інформацію про користувачів з метою отримання вигоди чи передачі цих даних третім особам, у тому числі й іноземним спецслужбам. Хоча представники ІТ-компаній тривалий час намагались спростовувати власну причетність до співпраці зі спеціальними службами у сфері незаконного збору персональних даних громадян, після оприлюднення зібраних секретних документів Е. Сноуденом, установлено, що провідні ІТ-компанії: Google, Facebook, Twitter, Microsoft, Apple, AOL, Yahoo, YouTube, Skype надають свої технологічні можливості АНБ для відслідковування громадян, використовуючи спеціальне програмне забезпечення, таке як PRISM і XKeyscore.

Зокрема, програма PRISM працює з 2007 року після прийняття законів про контроль за діяльністю іноземних розвідок і Акта про захист Америки, що дозволяє вести стеження за агентами іноземних спецслужб та особами, яких є підстави підозрювати у терористичній діяльності, поза територією США без судового рішення, а також за громадянами США лише з дозволу суду.

Зазначена програма надає можливість скачувати закриту інформацію з серверів найбільших Інтернет-компаній США, збирати інформацію з особистого листування в соціальних мережах, аудіо та відео файлів, списків контактів, пошукових запитів користувачів мережі.

В рамках використання цієї програми також відбувається відстежування дзвінків найбільших американських мобільних операторів.

Надсекретне програмне забезпечення XKeyscore (дзеркало) є, по суті, органічним доповненням до PRISM. Воно дозволяє без попереднього дозволу через величезні бази даних, що містять електронну переписку, онлайн-чати, історії Інтернет-пошуку мільйонів людей, здійснювати збирання, накопичення, аналіз і протиправне використання персональних конфіденційних даних користувачів у всьому світі. XKeyscore знаходить цілі за класифікаторами, відстежуючи активність об'єкта в реальному часі. Таку роботу в АНБ називають "цифровою мережевою розвідкою" [3].

Фактично, АНБ за допомогою спеціального програмного забезпечення збирало інформацію через більш ніж 80 посольств і консульств США в різних країнах, прослуховувало 38 іноземних посольств і дипломатичних місій, а також стежило за громадянами різних країн і лідерами 35 держав, що викликало протести [4].

З числа оприлюднених фактів відслідковування набуло резонансу стеження АНБ за штаб-квартирою ООН у м. Нью-Йорку, а також за місією Європейського Союзу при Організації Об'єднаних Націй. Зокрема, влітку 2012 року фахівці спецслужби зламали захист і отримали можливість відслідковувати відеоконференції ООН. Таке стеження порушує положення Розділу 9 Резолюції 169 (II), прийнятої на 101 пленарному засіданні Генеральної Асамблеї ООН 31 жовтня 1947 року, що закріплює Угоду між Організацією Об'єднаних Націй та Урядом Сполучених Штатів Америки з питань місця знаходження Центральних установ ООН та забороняє подібні приховані маніпуляції [5].

Особливо великий скандал виник у середині 2013 року, після оприлюднення засекречених даних про глобальне стеження АНБ за Інтернет-користувачами всього світу та відстежування мобільних телефонних дзвінків. Агентство національної безпеки США підтверджує, що збирає дані про дзвінки з мобільних телефонів по всьому світу , однак підкреслює, що ніяких законів, у всякому разі, своєї власної країни – воно при цьому не порушує, а така діяльність здійснюється згідно з указом Президента від 4 грудня 1981 р. № 12333 "Про розвідувальну діяльність США" [6], повідомляє ІТАР-ТАСС з посиланням на офіційного представника АНБ Венса Вайнса [7].

Отже, АНБ займається відслідковуванням більшості соціальних мереж, сервісів електронної пошти, збираючи метадані. В результаті аналізу зазначеної інформації, у поєднанні з відомостями про телефонні дзвінки і трафік електронної пошти, було створено гігантські бази даних з метою побудови складних систем соціальних зв'язків людей, виявлення їх контактів, місцезнаходження на конкретний період часу,

планів на майбутнє та інших персональних відомостей для складання так званих "соціальних карт".

Небезпечно, що такі методи моніторингу дозволяють АНБ відстежувати і знаходити зв'язки між "об'єктами розвідки" усередині США і за межами країни, отримувати величезні бази метаданих без будь-якої формальної звітності [8].

Наслідком оприлюднення зазначених фактів правозахисні організації і значна частина громадян США вважають порушення положень Білю про права (Bill of Rights) і IV поправки до Конституції США (Amendments to the United States Constitution), що гарантують право народу на недоторканість особи, помешкання, особистих паперів і майна від безпідставних обшуків і арештів [9].

Результатом висвітлення в ЗМІ інформації, наданої Е. Сноуденом, стала реакція держав і міжнародних організацій у різних формах: від прийняття нормативно-правових актів, покликаних здійснити спробу врегулювання питань щодо інформаційної безпеки держави та дотримання прав її громадян, аж до створення власних інформаційних мереж, національних сегментів Інтернету.

У контексті захисту наших співгромадян і національної безпеки України повчально-показовими є як фактична діяльність, так і офіційна реакція провідних держав світу на оприлюднені факти виявлення, відслідковування їхніх громадян. Вочевидь, що в ряді випадків офіційна реакції конкретної держави може принципово не збігатися із фактичною діяльністю навіть власних спецслужб.

Зокрема, згідно з даними The New York Times, встановлено, що АНБ мало можливість шпигувати за громадянами Великобританії, незважаючи на існуючий з 1946 року Пакт про заборону шпигунства між цими країнам. У секретних документах 2005 року, оприлюднених Едвардом Сноуденом, вказується, що США залишають за собою право інформувати або питати згоди у країн-партнерів.

В одному з пунктів, позначеному грифом секретності, йдеться про те, що кращим варіантом є отримання дозволу від країни-союзника, за громадянами якої передбачається стеження. Але вже в наступному пункті з тим же грифом і позначкою "NOFORN", яка означає, що з документом заборонено знайомити іноземних громадян, у тому числі союзників США по НАТО, вказується, що АНБ може діяти самостійно, якщо дозвіл не передбачається або якщо США в односторонньому порядку вирішать не питати про це.

У той же час Великобританія з 2007 року дозволила АНБ зберігати у своїх базах номери мобільних телефонів та адреси електронної пошти своїх громадян, які не підозрюються в жодному правопорушенні. До 2007 року, згідно з домовленостями про взаємний обмін розвід-

даними, спецслужби США були зобов'язані видаляти зі своїх баз контакти британських підданих, які в них випадково опинилися. Після внесення змін до документів, АНБ отримало можливість зберігати такі контактні дані з метою встановлення та аналізу зв'язків різних людей між собою [10].

Більше того, за даними німецького видавництва Spiegel Online, британська спецслужба "Центр урядового зв'язку" (Government Communications Headquarters, GCHQ) здійснювала проникнення до ділової соціальної мережі LinkedIn та, з використанням фальшивих профілів LinkedIn співробітників, отримувала доступ до комп'ютерів компаній, що їх зацікавили [11].

Завдячуючи матеріалам викриття діяльності служб розвідки стало відомо про те, що GCHQ активно співпрацює з АНБ і бере участь у глобальному проекті відслідковування з використанням таємного програмного забезпечення комп'ютерного стеження Tempora. Програма складається з двох компонентів "Mastering the Internet" і "Global Telecoms Exploitation", кожен з яких здійснює збір особистих даних, перехоплення телефонних розмов та Інтернет-трафіка, інформації соціальних мереж у величезних обсягах [12].

Показовою є ситуація із слідкуванням за власними громадянами у Канаді. Зокрема, за даними канадських ЗМІ, відстежування громадян цієї країни проводилося так само, як у США. Але, на відміну від американської програми, яку підтримала більша кількість членів Конгресу, прослуховування в Канаді було ініційовано низкою внутрішніх директив, які не були розглянуті парламентом країни.

Спецслужби Канади проводили й проводять операції у тісній співпраці з американськими колегами. Так, вони спільно стежили за учасниками саммітів G8 і G20, що проводилися на території Канади [13].

Також спецслужби Канади за запитом АНБ розгорнули стеження за Інтернет-каналами більш ніж у 20 розвинених країнах світу, недоступних для спецслужб США [14].

Також не нехтують відслідковуванням громадян і спецслужби Австралії. Зокрема, за даними видання Sydney Morning Herald, спецслужби Австралії використовують для шпигунської діяльності австралійські дипломатичні місії в країнах Азії, координуючи свою роботу в сфері розвідки з колегами із США.

При цьому, генеральний прокурор Австралії М. Дрейфус безпосередньо вказав, що діяльність спецслужб контролюється відповідними урядовими органами, в них не було виявлено правопорушень, а розвіддіяльність Австралії здійснюється з метою захисту її демократичних цінностей. Він додав, що доступ спецслужб до телекомунікацій спричинив порушення 5928 судових справ і винесення 2267 вироків, що ґрунтувалися

на "законним чином перехоплених матеріалах" у 2011–2012 роках, і більшість із них – це серйозні кримінальні злочини [15].

Використання австралійських посольств для перехоплення електронних даних в азіатських країнах у співпраці із США і без відома більшості австралійських дипломатів, а також спроби австралійських спецслужб прослуховувати телефони президента Індонезії Сусіло Бамбанга Юдойоно (Susilo Bambang Yudhoyono), його дружини та низки відомих політиків призвело до того, що Міністр закордонних справ країни Марті Наталегава (Marty Natalegawa) зажадав вибачень і назвав це "недружнім актом, який суттєво впливає на двосторонні відносини".

Достатньо активно АНБ відстежувало телефонні дзвінки, смс-повідомлення, електронні листи громадян Іспанії, а також членів уряду, в тому числі прем'єр-міністра Маріано Рахоя, в минулому – Міністра внутрішніх справ Іспанії.

Виправдовуючись, посол США в Іспанії Дж. Костос повідомив, що АНБ в Іспанії здійснює свою діяльність виключно з метою забезпечення безпеки та протидії тероризму, в співпраці з іспанським розвідувальним відомством, не порушуючи законодавства Іспанії, за яким перехоплення дзвінків, листування і доступ до даних про дзвінки без санкції суду вважаються злочином. Своєю чергою, генеральна прокуратура Іспанії оголосила про початок попереднього розслідування з метою встановлення фактів стеження за громадянами країни співробітниками АНБ. Проте, ніяких суттєвих юридичних чи політичних рішень до даного часу керівництвом держави прийнято так і не було [16].

Агентство національної безпеки США перехоплювало телефонні дзвінки громадян Франції, крім того, стеження велося за представниками ділових кіл, політиками та представниками французької влади. Так, Держсекретар США Джон Форбс Керрі (John Forbes Kerry) заявив, що прослуховування телефонних дзвінків у Франції – це частина операції із забезпечення безпеки американських громадян.

Прокуратурою розпочато перевірку за вказаним фактом. Заява Французької ліги прав людини була подана "проти невстановлених осіб", проте в тексті документа в якості можливих відповідачів були перераховані АНБ і ФБР, а також великі Інтернет-компанії, такі як Microsoft, Yahoo, Google, Facebook, AOL та Apple [17].

У Нідерландах група адвокатів і журналістів подала позовну заяву до суду Гааги щодо протидії використанню національними спецслужбами телефонних даних, наданих їм АНБ. Показово, що Міністр внутрішніх справ Р. Пластерк, чиє міністерство виступає в суді відповідачем, підтвердив, що АНБ перехоплювала дані телефонних дзвінків. Позивачі вважають, що уряд Нідерландів вчиняв протизаконно, отримую-

чи дані від іноземних розвідслужб, що були зібрані через програми стеження на зразок PRISM [18].

За повідомленнями норвезької газети Dagbladet, АНБ здійснювало збір метаданих про мільйони дзвінків норвежців.

Спочатку норвезькі спецслужби, коментуючи зазначену інформацію, заперечували свою участь у масштабній програмі стеження американських колег.

У національному ж поштовому і телекомунікаційному управлінні вказали, що моніторинг телефонних переговорів норвезьких громадян будь-ким, окрім телефонних компаній, є порушенням законів країни.

Але, несподівано Глава Норвезької служби розвідки Челлі Грандхаген (Kjell Grandhagen) визнав, що норвезька розвідслужба збирала інформацію з метою допомогти проведенню військових операцій норвезьких військ у конфліктних зонах за кордоном, а також для боротьби з тероризмом, таким чином намагаючись спростувати інформацію, згідно з якою за цим стеженням стояло АНБ. Хоча і визнав, що потім зібраною інформацією ділилися із США й іншими своїми партнерами у сфері розвідки [2].

Новий витік інформації продемонстрував, що Індія є однією з головних цілей АНБ, яке давно стежить за націями, що входять до BRICS (Brazil, Russia, India, China, South Africa) – групи найбільших за площею та населенням країн, що швидко розвиваються. Тут США використали дві основні програми для збору даних: Boundless Informant – система обробки, аналізу і візуалізації великих масивів даних у глобальному масштабі, та PRISM. Перша використовувалася для моніторингу телефонних розмов і доступу до Інтернет-мереж Індії, в той час, як PRISM збирала інформацію, використовуючи можливості різних технологічних гігантів США [19].

На протязі декількох років АНБ систематично прослуховувало комунікації уряду та Президента Мексики. Ще в травні 2010 року спеціалісти спецпідрозділу АНБ Tailored Access Operations зламали поштовий сервер у президентському домені у внутрішній мережі мексиканського уряду та отримали доступ до вмісту поштової скриньки президента Феліпе Кальдерона (Felipe Calderon). За інформацією АНБ, цей поштовий домен використовували також члени кабінету міністрів для дипломатичних і економічних комунікацій [20].

На жаль, спільна діяльність національних спецслужб різних держав у відслідковуванні громадян "третіх" країн, також набуває все більшого розвитку. Зокрема, Агентство національної безпеки США спільно зі спецслужбами Канади відстежувало телефонні дзвінки та електронне листування не лише громадян Бразилії, а й їх президента

Ділми Вана Руссефф (Dilma Vana Rousseff), яка у вересні навіть скасувала запланований візит до США.

Ділма Вана Руссефф на засіданні Генеральної асамблеї ООН звинуватила США у шпигунстві проти своєї країни і запропонувала ООН створити правову основу для запобігання використанню спецслужбами кіберпростору в своїх цілях. А також, з метою забезпечення захисту національної безпеки, вона підписала декрет, в якому йдеться про те, що комунікації між органами державної влади Бразилії з березня 2014 року будуть здійснюватися виключно телекомунікаційними мережами інформаційних служб організацій і відомств Федеральної державної служби обробки даних Бразилії (Serpro), використовуючи власні розробки. Сьогодні бразильські державні відомства використовують електронну пошту, розроблену американською компанією Microsoft [21].

Агентство національної безпеки США займалося прослуховуванням телефонних розмов папи Римського Франциска (Franciscus PP.) і кардиналів Католицької церкви. Журналісти вважають, що реакція понтифікату була самою гідною. "Нам про це нічого не відомо; у будь-якому випадку, нам нічого приховувати" [22].

Наприкінці жовтня 2013 року офіційний представник уряду ФРН Штеффен Зайберт повідомив, що Німеччина має інформацію щодо можливого прослуховування мобільного телефону Федерального канцлера Ангели Доротеї Меркель (Angela Dorothea Merkel) спецслужбами США [23].

Незабаром після цього, А. Меркель у телефонній розмові з президентом США Бараком Обамою (Barack Hussein Obama) зажадала пояснень, на що Президент США, за даними німецьких джерел, заявив, що стеження велося без його відома і було припинене в 2010 році.

А прес-секретар Білого дому Джеймс "Джей" Карні (James "Jay" Carney) взагалі заперечив факт прослуховування американськими спецслужбами, в тому числі й АНБ, телефонних розмов Федерального канцлера Німеччини.

Після цього скандалу Німеччина запропонувала підписати нову угоду зі спецслужбами США щодо заборони взаємного шпигунства. Проте американська сторона вважає вже існуючі домовленості цілком прийнятними, а укладення нової угоди – недоречним [24].

Варто відзначити, що раніше, коли тільки спалахнув скандал, пов'язаний з викриттями діяльності АНБ, німецький лідер вважала стеження за громадянами цілком виправданим заходом для протидії тероризму. При цьому канцлер ФРН підкреслила, що без можливості контролю за телекомунікаціями забезпечити ефективну протидію терористичній загрозі було б неможливо [25].

Німеччина також була ініціатором підготовки резолюції ООН "Право на недоторканність особистого життя в цифровому столітті" проти стеження за Інтернет-користувачами, проект якої було схвалено 26 листопада делегатами Третього комітету Генеральної Асамблеї ООН.

Резолюція засуджує подібні дії та окремо підкреслює небезпеку, яку несе масовий збір особистої інформації користувачів.

Вказаний документ покликаний поширити на користувачів Інтернету право на захист приватного життя та особистого листування, гарантоване всім людям Міжнародним пактом про політичні та громадянські права від 1966 року. Генеральна Асамблея ООН підтверджує, що ті ж права, які людина має в реальному середовищі, повинні також діяти та захищатися і у віртуальному середовищі, особливо право на недоторканність особистого життя.

У резолюції міститься заклик Генеральної Асамблеї ООН до держав, що схвалять резолюцію, провести огляд процедур, практики та законодавства, що стосуються стеження за повідомленнями, їх перехоплення та збору особистих даних і створити на національному рівні незалежні механізми контролю, здатні забезпечити прозорість й підзвітність державного стеження за засобами зв'язку, перехоплення повідомлень і збору особистої інформації [26].

Висновки. Посилення протиріч між державами, які пов'язані з контролем за міжнародними телекомунікаціями та діяльністю національних спецслужб (у першу чергу, США) щодо глобального відслідковування громадян й окремих лідерів країн є детермінантами фрагментації та можуть призвести до розпаду мережі Інтернет. Як приклад фрагментації мережі Інтернет може розглядатися Китай, що відмежувався від глобальної мережі Інтернет, повністю заборонивши використання соціальних мереж, сервери яких перебувають за межами країни (замість Facebook в Китаї використовують XiaoNei, а замість Twitter – Weibo), уряд також змусив китайські технологічні компанії і глобальні сервіси розробити національні версії програмних продуктів, що забезпечують можливість повного контролю мережі з боку спецслужб.

З великою вірогідністю можна констатувати, що спецслужби іноземних держав, особливо після відмови України від підписання угод про асоціацію із Євросоюзом, намагатимуться ще більш системно відслідковувати керівників держав пострадянських країн, у тому числі й України, здійснюючи моніторинг їх особистих блогів, акаунтів, переписки з використанням мережі Інтернет та телефонних дзвінків.

У зв'язку з активністю силових структур, що здійснюють відслідковування злочинців у кіберпросторі, ускладнилося використання традиційної мережі Інтернет для вчинення злочинів, а тому вони почали користуватися альтернативним Інтернетом – DarkNet або DarkWeb,

розробленим на основі системи TOR (The Onion Router), спрямованої на забезпечення анонімності в мережі Інтернет, з можливістю приховування місцезнаходження користувача, його активності від будь-кого, хто здійснює моніторинг мережі чи аналіз трафіку.

Перспективи подальшого використання. На переконання авторів, застосування у ході правотворчої та правозастосовної практики вказаних вище висновків має сприяти не тільки підвищенню ефективності правової охорони конституційних прав і свобод громадян України, а й захисту життєво важливих інтересів нашої держави від зовнішніх загроз, які виходять із протиправного використання іноземними спецслужбами та організаціями сучасних інформаційних технологій.

Список використаних джерел

1. Поляруш А. А. Информационная война против Украины: причины и социально-политические технологии : науч.-популяр. изд. / А. А. Поляруш, А. М. Юрченко. – К. : Изд-во "Кий", 2011. – 199 с.

2. Норвежские спецслужбы признались в телефонном шпионаже / [Электронный ресурс]. – Режим доступа :
http://world.lb.ua/news/2013/11/19/241968_norvezhskie_spetssluzhbi_priznalis.html.

3. XKeyscore: NSA tool collects 'nearly everything a user does on the internet' / [Electronic resourse]. – Mode of access :
http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

4. Эдвард Сноуден: АНБ следило за штаб-квартирой ООН / [Электронный ресурс]. – Режим доступа :
http://telegraf.com.ua/mir/usa/736150-edvard-snouden-anb-sledilo-za-shtab-kvartiroy-oon.html.

5. Соглашение между Организацией Объединенных Наций и Соединенными Штатами Америки по вопросу о месторасположении Центральных учреждений Организации Объединенных Наций / [Электронный ресурс]. – Режим доступа :
http://www.un.org/ru/ga/2/docs/2res.shtml.

6. Executive Order 12333 United States Intelligence Activities / [Electronic resourse]. – Mode of access :
http://www.tscm.com/EO12333.html.

7. АНБ США подтвердило, что собирает данные о звонках с мобильных телефонов по всему миру / [Электронный ресурс]. – Режим доступа :
http://itar-tass.com/mezhdunarodnaya-panorama/817484.

8. АНБ США шпионит через социальные сети / [Электронный ресурс]. – Режим доступа :
http://cybersecurity.ru/crypto/182126.html.

9. Bill of Rights and Later Amendments / [Electronic resourse]. – Mode of access :
http://www.ushistory.org/documents/amendments.htm.

10. Великобритания в 2007 году разрешила АНБ следить за жителями страны / [Электронный ресурс]. – Режим доступа :
http://www.kp.ru/online/news/1591752.
11. Спецслужбы внедрились в деловую соцсеть LinkedIn / [Электронный ресурс]. – Режим доступа :
http://www.companion.ua/articles/content?id=262736.
12. За последние три года АНБ перечислило британским спецслужбам $160 млн / [Электронный ресурс]. – Режим доступа :
http://inagist.com/all/402319166759108608/.
13. Спецслужбы Канады тоже прослушивают граждан / [Электронный ресурс]. – Режим доступа :
https://translate.google.com.ua/?hl=ru&tab=wT.
14. АНБ сотрудничает со спецслужбами Канады из-за возможности получить легкий доступ к странам мира / [Электронный ресурс]. – Режим доступа :
http://www.securitylab.ru/news/448453.php.
15. Австралийский генпрокурор: Сноуден и Мэннинг разоблачителями не являются / [Электронный ресурс]. – Режим доступа :
http://inosmi.ru/world/20130816/211960475.html.
16. АНБ отследило 60 млн телефонных звонков в Испании за месяц / [Электронный ресурс]. – Режим доступа :
http://www.inopressa.ru/article/28oct2013/elpais/nsa_1.html.
17. Сноуден рассекретил данные о слежке АНБ за гражданами Франции / [Электронный ресурс]. – Режим доступа :
http://proit.com.ua/news/internet/2013/10/21/122228.html.
18. На правительство Нидерландов подали в суд из-за шпионажа / [Электронный ресурс]. – Режим доступа :
http://internetua.com/na-pravitelstvo-niderlandov-podali-v-sud-iz-za-shpionaja-anb.
19. Индия – главный объект, исследуемый АНБ США / [Электронный ресурс]. – Режим доступа :
http://it-site.net/news-222/indiya-glavnyj-obekt-issleduemyj-anb-usa.
20. АНБ три года читало почту президента Мексики / [Электронный ресурс]. – Режим доступа :
http://www.xakep.ru/post/61455/.
21. В Бразилии решили защититься от шпионажа со стороны США, отказавшись от почты Microsoft / [Электронный ресурс]. – Режим доступа :
http://internetua.com/v-brazilii-reshili-zasxititsya-ot-shpionaja-so-storoni-ssha--otkazavshis-ot-pocsti-Microsoft.
22. Итальянские СМИ: АНБ США осуществляло слежку за Ватиканом / [Электронный ресурс]. – Режим доступа :
http://www.securitylab.ru/news/447162.php.
23. АНБ могло прослушивать телефон Меркель / [Электронный ресурс]. – Режим доступа :
http://www.dni.ru/polit/2013/10/23/262536.html.
24. Der Spiegel: американцы и немцы не договорились о взаимном шпионаже / [Электронный ресурс]. – Режим доступа :

http://rus.ruvr.ru/news/2013_11_11/SHpigel-Amerikanci-i-nemci-ne-dogovorilis-o-vzaimnom-shpionazhe-8655/.

25. Меркель оправдала спецслужбы за прослушку / [Электронный ресурс]. – Режим доступа :
http://www.dni.ru/polit/2013/7/10/255935.html.

26. Делегаты Третьего комитета Генассамблеи приняли резолюцию о неприкосновенности личной жизни в цифровой век / [Электронный ресурс]. – Режим доступа :
http://www.un.org/russian/news/story.asp?NewsID=20669&Kw1=%D1%80%D0%B5%D0%B7%D0%BE%D0%BB%D1%8E%D1%86%D0%B8%D0%B8#.UrLjdUCDtV9.

В статье проанализированы социально-правовые аспекты противоправной деятельности иностранных специальных служб по незаконному сбору персональных данных с использованием телекоммуникационных сетей, а также предложены меры противодействия такой деятельности как в контексте охраны конституционных прав граждан, так и защиты национальной безопасности Украины.

In the article the socially-legal aspects of the illegal activity of the foreign special services on the illegal collection of the personal data with the use of TCNS are analyzed, and also the measures of counteraction of such activity are offered, both in the context of guard of constitutional rights of the citizens and defense of the national security of Ukraine.

Стаття надійшла до редакції журналу 3 грудня 2013 року.