УДК 323:351; 343:341

ПРОТИДІЯ ЗЛОЧИНАМ У СФЕРІ ІКТ: ДОСВІД ВЕЛИКОЇ БРИТАНІЇ

Покровська Аліса Валеріївна;

Дубов Дмитро Володимирович,
кандидат політичних наук

Розглянуто британське законодавство та практичний досвід у сфері боротьби з інформаційною злочинністю. Досліджено особливості взаємодії безпекових органів Великої Британії та недержавного сектору в умовах протидії поширенню незаконного контенту.

Ключові слова: **інформаційна злочинність, перехоплення комунікації, інформаційна безпека.**

Сучасний стан розвитку суспільства демонструє, що інформація стала критично важливим ресурсом, який дедалі більше впливає на національну та глобальну безпеку. Зростаюча активність злочинних і терористичних угруповань у комунікаційних мережах, поширення кібертероризму, розповсюдження матеріалів загрозливого та аморального характеру, залежність усіх сфер життєдіяльності держави від інформації зумовлюють необхідність активної взаємодії правоохоронних органів із провайдерами інформаційно-комунікативних послуг.

Питання взаємодії держави та ІКТ-провайдерів у сфері протидії інформаційній злочинності нині перебуває у фокусі досліджень вітчизняних і зарубіжних науковців. Поміж теоретично вагомих розробок варто виділити дослідження В. М. Бутузова [1], П. Д. Біленчука [2], Н. С. Козак [3], Б. В. Кузьменко [4]. Також корисними виявилися наукові напрацювання Є. В. Зозулі [5], О. Г. Ширової-Мурараш [6], присвячені розгляду міжнародно-правових заходів боротьби зі злочинністю в інформаційній сфері. Разом з тим у роботах дослідників недостатньо детально розглядається досвід співпраці безпекових огранів провідних держав світу із приватним сектором, що є необхідним для вироблення ефективних стратегій протидії інформаційній злочинності для держав, які таких стратегій не мають.

Саме тому **метою** статті є аналіз діяльності Сполученого Королівства у сфері протидії інформаційній злочинності для можливої адаптації британських досягнень і законодавства до реалій інших держав.

Законодавча база відносин правоохороннних органів Великої Британії з телекомунікаційними провайдерами

Правоохоронні органи Великої Британії наділені широкими повноваженнями для використання даних комунікації під час розслідування. Головним законодавчим документом тут є Акт про регулювання слідчих повноважень 2000 р. (*Regulation of Investigatory Powers Act 2000, RIPA*) [7], а з-поміж інших передусім необхідно назвати окремі кодекси поведінки правоохоронних органів при реалізації положень підрозділів 1 і 2 розділу 1 згаданого Закону (Кодекс поведінки при перехопленні комунікації, *Interception of Communications Code of Practice* [8] і Кодекс поведінки при отриманні доступу та розкритті даних комунікації, *Acquisition and Disclosure of Communications Data Code of Practice* [9]).

Згідно з підрозділом 1 розділу 1 *RIPA* та відповідним Кодексом право на перехоплення має обмежене коло суб'єктів: генеральний директор Служби безпеки (*MI*5), голова Служби зовнішньої розвідки (*MI*6), директор Центру урядового зв'язку (*Government Communications Headquarters, GCHQ*), генеральний директор Національного агентства з розслідування злочинів (*National Crime Agency*), голова Служби столичної поліції (*Metropolitan Police Service, MPS*), голова Служби контррозвідки у складі Міністерства оборони (*Defence Intelligence*), керівник Податкової та митної служби (*Her Majesty's Revenue and Customs*), голови відповідних поліцейських служб Шотландії та Північної Ірландії. Перераховані суб'єкти мають право отримати ордер на перехоплення комунікації, який виписується міністром (*Secretary of State*, а саме маються на увазі такі міністри: міністр внутрішніх справ, міністр зовнішніх справ, міністр оборони, міністр у справах Північної Ірландії, міністр юстиції Шотландії) або, в термінових випадках, іншим вищим посадовцем з відома міністра. Перед тим, як виписувати ордер, міністр має переконатися, що дії з перехоплення необхідні для забезпечення національної безпеки, виявлення чи запобігання тяжким злочинам, забезпечення економічного благополуччя держави. Ордери діють лише на територіях під юрисдикцією Сполученого Королівства протягом трьох місяців з можливістю подовження до трьох (для питань, що стосуються тяжких

злочинів) чи шести місяців (для питань національної та економічної безпеки) [7, 8].

Телекомунікаційні оператори мають сприяти реалізації ордера на перехоплення, однак у межах, що є дійсно розумними та необхідними. Ці межі мають бути визначені домовленістю між урядом та оператором. Якщо такої домовленості досягти не вдалося, міністр вирішує, чи буде притягнений певний оператор до цивільної або кримінальної (після схвалення Генеральним прокурором) відповідальності. Перехоплення може здійснюватися і без ордера в таких випадках: за згодою обох сторін, між якими ведеться комунікація; за згодою однієї зі сторін (тобто з використанням розвідувальних заходів, про які йдеться в частині 2 акта *RIPA* та відповідних кодексів поведінки правоохоронних органів [7]); з ініціативи телекомунікаційного оператора.

Стосовно отримання доступу та розкриття даних комунікації (не самого змісту повідомлення, а того, хто, кому, коли й де це повідомлення передавав), то підрозділ 2 розділу 1 *RIPA* та відповідний Кодекс визначають таких суб'єктів: поліцію, Національне агентство з розслідування злочинів, *MI*5, *MI*6, Податкова та митна служба, *GCHQ*. Крім того, право на отримання доступу також мають державні установи, перераховані в Постанові про регулювання слідчих повноважень, щодо даних комунікації (*Regulation of Investigatory Powers* (*Commu nications Data Order 2010*), а також ті установи, дозвіл яким надано міністром.

Існує два способи отримання доступу до даних комунікації перерахованими суб'єктами: дозвіл уповноваженій особі з відповідного органу на отримання доступу до даних комунікації та попередження, що направляється телекомунікаційному провайдеру з вимогою надати такий доступ. Перший варіант використовується, якщо провайдер не має змоги отримати чи розкрити необхідні дані або якщо між уповноваженим органом і провайдером є домовленість стосовно доцільних механізмів розкриття даних. Попередження направляється провайдеру, якщо він має доступ до даних і сам їх зберігає. Термін дії дозволів та попереджень – один місяць із можливістю подовжити до трьох. Державні органи можуть допомагати провайдерам своєчасно (протягом десяти робочих днів) розкривати необхідні дані у спосіб покриття витрат з боку провайдера [7, 9].

Вимога на надання доступу та розкриття даних комунікації має бути обґрунтована вагомими причинами, поміж яких такі: загроза національній безпеці, запобігання чи виявлення злочинів, загрози економічній стабільності держави, підтримання громадської безпеки, захист здоров'я громадян, збирання податків чи інших платежів державі, запобігання смерті, шкоді фізичному чи моральному здоров'ю особи в надзвичайних ситуаціях, у будь-яких інших ситуаціях за вимогою міністра.

Якщо подібний запит надходить від суду чи іншого правоохоронного органу з-за кордону, міністр згідно з Актом про міжнародне співробітництво в розслідуванні злочинів (*Crime* (*International Co-operation*) *Act* 2003) має розглянути цей запит, передати його до британського суду, який, своєю чергою, може вимагати від провайдера надати необхідну інформацію про комунікаційні дані та передати її відповідній закордонній установі. Подібні запити можуть надходити також від інших закордонних державних установ. У цьому випадку британська установа має розглянути запит, переконатися, що він обґрунтований і не суперечить законодавству про права людини. Якщо такий обмін даними відбувається в межах Європейського Союзу, регулювання відбувається відповідно до Директиви ЄС про захист даних *European Data Protection Directive* (95/#6/ЕС) та законодавства сторони, що надсилає запит [9].

У межах ЄС також діють акти, спрямовані на сприяння взаємній правовій допомозі при розслідуванні злочинів: Європейська конвенція про взаємну правову допомогу в кримінальних справах 1959, прийнята Радою Європи та ратифікована усіма 47 її членами, та Конвенція про взаємну правову допомогу в кримінальних справах між державами-членами Європейського Союзу 2000 р., а також додаткові протоколи до них. Ці документи регулюють процедури обміну документами, судовими матеріалами, спільні й таємні розслідування та перехоплення комунікацій. Загалом, будь-які дії мають виконуватися з урахуванням національного законодавства обох сторін. Крім того, існує Договір про взаємну правову допомогу між ЄС і США (до 2010 р. був чинним Договір між Великою Британією та США про правову допомогу від 1994 р.), Норвегією, Ісландією, Швейцарією та Японією [10].

Важливу роль для міжнародного співробітництва з питань розкриття та протидії злочинам у комп'ютерних мережах відіграє Конвенція з кіберзлочинності, прийнята Радою Європи 23 листопада 2001 р., яку нині підписали 50 і ратифікували 44 держави світу, зокрема і США [11]. У ній є положення щодо надання сторонами максимальної взаємної допомоги при розслідуванні кримінальних правопорушень, пов'язаних із комп'ютерними системами й даними; обміну між відповідними органами сторін необхідною інформацією; необхідності адаптації внутрішнього законодавства до згаданих вимог [12]. Велика Британія підписала Конвенцію відразу, однак ратифікувала лише у травні 2011 р., після прийняття спільного комюніке зі США з приводу кіберзлочинності. Конвенція набула чинності з 1 вересня того самого року. Таке затягування пояснювалося вже наявним у державі законодавством, зокрема Актом про комп'ютерні злочини 1990 р. (*Computer Misuse Act* 1990), а також суперечностями в парламенті щодо відповідаль-

ності приватного сектору – телекомунікаційних провайдерів [13]. Крім того, Велика Британія не підписала й не ратифікувала Додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28 січня 2003 р. [14].

Варто зазначити, що як і у випадку з антитерористичними актами Великої Британії, якими вводиться посада незалежного оглядача антитерористичного законодавства, аналогічна посада є і для сфери перехоплення комунікацій: стаття 57 *RIPA* передбачає призначення Незалежного комісара з перехоплення комунікацій (*Interception of Communications Commissioner*). Комісар готує щорічний звіт прем'єр-міністру про перехоплення та отримання доступу до комунікації розвідувальними службами, поліцією та державними органами. Згідно зі звітом за 2013 р. усього було видано 2760 ордерів на перехоплення комунікації, що на 19 % менше, ніж у попередньому році. Щодо запитів на одержання доступу та розкриття комунікаційних даних, у 2013 р. усього було надіслано та задоволено 514608 таких запитів; 214 державних органів отримали необхідні дані; 87,7 % запитів було зроблено поліцією, 11,5 % – розвідувальними установами та менше ніж 1 % – іншими державними та місцевими установами; 76,9 % запитів стосувалися питань запобігання та попередження злочинів і безпорядків, 11,4 % – національної безпеки, 11,3 % – запобігання смертей та шкоди в надзвичайних ситуаціях, решта 0,4 % – інших питань (економічна безпека, податки, громадська безпека тощо) [15].

Крім того, законом *RIPA* створюється Трибунал зі слідчих повноважень (*Investigatory Powers Tribunal*), що є незалежним від уряду та складається з провідних діячів юриспруденції, які призначаються Королевою на п'ятирічний термін з можливим подальшим повторним призначенням. Трибунал має право розглядати скарги стосовно перехоплення та отримання доступу до комунікації та проводити самостійні розслідування, а також публікувати звіти [7]. У відкритому доступі, однак, наявний звіт лише за 2010 р., з якого видно, що всього було подано 210 скарг, з яких було задоволено лише 6. На сайті Трибуналу стверджується, що наступний звіт буде доступний на початку 2015 р. та публікуватиметься щорічно [16].

Поміж законодавчих ініціатив щодо розширення можливостей держави отримувати доступ до комунікації однією з найсуперечливіших була спроба прийняття Законопроекту про дані комунікації (*Communications Data Bill* 2012), який намагалася просувати в парламенті міністр внутрішніх справ, консерватор Тереза Мей і який не був підтриманий частиною урядової коаліції, представленої ліберальними демократами. Законопроектом мали бути внесені зміни до *RIPA* стосовно збирання та зберігання телекомунікаційними провайдерами інформації про користувачів на вимогу державних органів, навіть якщо це не є доцільним для діяльності провайдера; також передбачалося обов'язкове використання провайдерами технології *Deep Packet Inspection* (технології накопичення статистичних даних, перевірки та фільтрації мережевих пакетів за їх вмістом: аналізуються не лише заголовки, а й повний вміст трафіку; за допомогою *DPI* можна виявляти і блокувати віруси, фільтрувати інформацію, що не відповідає заданим критеріям [17]); значно розширювалися повноваження поліції стосовно запитів на отримання даних про комунікацію: вона могла раз на місяць отримувати дозвіл від вищих державних службовців на надсилання таких запитів провайдерам) [18].

Необхідність таких широких повноважень для правоохоронних і розвідувальних органів була обґрунтована в доповіді «Доступ розвідувальних і безпекових органів до даних комунікації» парламентської Комісії з розвідки та безпеки (*Intelligence and Security Committee*). У доповіді зазначалося, що останнім часом взаємодія з телекомунікаційними провайдерами на добровільній основі значно ускладнилася, що стало причиною 25-відсоткової «прірви» між необхідним і фактичним доступом державних органів до потрібних даних. Комісія дійшла висновку про необхідність більш жорсткого законодавчого регулювання відносин із провайдерами [19].

Оскільки зазначений законопроект не отримав необхідної підтримки в парламенті й викликав неоднозначну реакцію у британському суспільстві та світового інтернет-співтовариства, державі довелося шукати інші способи закріплення більш широких повноважень.

Так, важливою подією, що стосується розширення державою доступу до комунікації, стало прийняття 17 липня 2014 р. Акта про утримання даних та слідчі повноваження (*Data Retention and Investigatory Powers Act* 2014, *DRIPA* [20]). Згідно із цим законом міністр (той самий *Secretary of State*) може своїм запитом (*retention notice*) вимагати утримання телекомунікаційним оператором(ами) даних про комунікацію (знову ж таки, без доступу до змісту повідомлень), стосовно зазначених у *RIPA* питань, на строк до 12 місяців. Оператор має надавати доступ на підставі підрозділу 2 розділу 1 *RIPA*, або в іншому випадку – за судовим ордером. Деякі положення *RIPA* підлягають доповненню, насамперед ті, що стосуються його екстериторіальної дії – комунікаційні оператори, розташовані поза межами Великої Британії, але надають британським користувачам послуги, також мають відповідати на запити.

Цей закон діятиме до 31 грудня 2016 р., тобто політичній силі, що прийде на зміну консервативно-ліберальній коаліції у 2015 р., необхідно буде розробляти новий закон чи продовжувати дію чинного [20].

Поспішне прийняття *DRIPA* (перше слухання відбулося 14 липня 2014 р.) було, зокрема, обґрунтоване тим, що Директива Європейського парламенту та Ради ЄС 2006/24/ЕС від 15 березня 2006 р. «Про збереження даних, створених або оброблених при наданні загальнодоступних засобів комунікації чи комунікаційних мереж і доповнення Директиви 2002/58/ЕС» [21] 08 квітня 2014 р. була визнана Судом Європейського Союзу недійсною через те, що вона, за висновком суду, порушує фундаментальні права на особисте життя й захист персональних даних. Ініціатива прийняття Директиви була подана Великою Британією під час її головування в Європейській Раді в липні-грудні 2005 р. та прийнята в березні 2006 р. під головуванням Австрії. У національне британське законодавство вона була імплементована в 2009 р. відповідною Постановою (*Data Retention (EC Directive) Regulations* 2009). У ній період утримання даних був фіксованим – 12 місяців і стосувався лише операторів у межах Великої Британії, крім того, не передбачав судового ордеру на доступ до даних [22]. Тобто на сьогодні *DRIPA*, по суті, суперечить законодавству ЄС. А вимога Великої Британії до закордонних провайдерів надавати доступ до даних комунікації виглядає доволі зухвало, з огляду на те, що такі провайдери діють передусім відповідно до національного законодавства.

Взаємодія держави, приватного сектору та неурядових організацій

Державні структури, попри суворі законодавчі заходи, намагаються взаємодіяти з провайдерами за можливості на основі добровільних домовленостей. Головною структурою, що взаємодіє з комунікаційними операторами, насамперед з питань дозволеного контенту й фільтрації інформації, є Офіс з комунікацій (*Ofcom*, утворений у 2003 р. Актом про комунікації – *Communications Act* 2003), установа, що формально має статус державної корпорації, підзвітна парламенту, фінансується з надходжень від учасників телекомунікаційного ринку та урядових грантів [23].

Ofcom визначає перелік фільтрів, які провайдери мають «добровільно» встановлювати для забезпечення онлайн-безпеки користувачів, а саме фільтрів, що блокують матеріали порнографічного характеру, матеріалів, що зображують жорстокість, наркотики, ненависть, суїцид, сприяють поширенню шкідливих звичок, заохочують хакерство й незаконний обмін файлами. Згідно зі щорічною доповіддю *Ofcom* на кінець 2013 р. чотири головні ІКТ-провайдери (*British Telecom, TalkTalk, Sky, Virgin Media*), що покривають 95 % британських домогосподарств, встановили фільтрування за замовчуванням, тобто користувачі не можуть відключити його за бажанням [24]. Звичайно, це не забезпечує цілковитої ліквідації в інтернеті небажаних матеріалів, оскільки є чимало способів обходити такі фільтри. Крім того, наразі у Великій Британії існує проблема надмірного або помилкового блокування матеріалів веб-сайтів, що є причиною зростаючої активності організацій, які борються за свободу слова та відкритість інтернету, зокрема *Open Rights Group* [25].

Однією з важливих структур для взаємодії державних органів та ІКТ-провайдерів є *Internet Watch Foundation* – незалежна неурядова благодійна саморегульована організація, створена в 1996 р. для виявлення та ліквідації законних матеріалів в інтернеті. Вона керується спільно ІКТ-провайдерами, представниками уряду та правоохоронних установ, представниками благодійних організацій, громадського сектору. Найбільша увага приділяється видаленню матеріалів, пов'язаних із дитячою порнографією, але також розглядаються випадки ліквідації іншого злочинного контенту, що порушує чинне законодавство.

IWF самостійно шукає неправомірний матеріал, а також розглядає скарги від користувачів. У разі оцінки матеріалу як неправомірного *IWF* з'ясовує, хто є провайдером, що надає доступ до такого матеріалу. Якщо провайдер діє на території Великої Британії, фонд надсилає йому попередження з вимогою видалити матеріал чи закрити до нього доступ; якщо провайдер відмовляється задовольнити вимогу, *IWF* має право передати справу на розгляд правоохоронних органів [26]. Так, у 2010 р. між *IWF* та Асоціацією начальників поліції (*Association of Chief Police Officers, ACPO*) було підписано спеціальну Угоду про співробітництво з метою сприяння обміну інформацією та пришвидшення процедур виявлення й видалення контенту [27]). Нині членами *IWF* є більшість ІКТ-провайдерів, що діють у Великій Британії, а також провідні інтернет-компанії, зокрема такі, як *Google, Facebook, Twitter, Yahoo!*, на які поширюється дія Кодексу поведінки членів *IWF* [26].

Представляти й просувати інтереси провайдерів перед британським урядом має Асоціація провайдерів інтернет-послуг (*Internet Service Providers Association, ISPA*), створена у 1995 р., яка наразі нараховує 200 членів. Асоціація не займається переслідуванням і вилученням незаконного контенту поміж своїх членів, однак зобов'язує їх діяти відповідно до Кодексу поведінки – законно, пристойно та чесно. У жовтні 2014 р. *ISPA* представила принципи, які, за її висновком, мають ураховуватися під час реформування законодавства у сфері перехоплення, отримання доступу та використання інформації: мінімізація даних (зберігатися має обмежений та обґрунтовано необхідний обсяг даних); максимальна відкритість діяльності державних органів; прозорість (правоохоронні органи мають надавати громадськості регулярні звіти про

кількість запитів до провайдерів); повага юрисдикції (зберігання даних не має суперечити реалізації повноважень обох сторін); конкурентоспроможність (будь-які заходи, пов'язані зі збереженням даних комунікації, не мають шкодити ІКТ-бізнесу) [28].

ІКТ-провайдери позиціонують себе як досить незалежні й відкриті до взаємодії з урядом суб'єкти. Про це можуть свідчити нещодавні заяви з боку провідних британських провайдерів на брифінгу *BBC* про готовність встановлення фільтрів для екстремістських і терористичних матеріалів, а також розміщення на сайтах спеціальної кнопки для повідомлення користувачами про виявлення таких матеріалів (на зразок застосовуваної для матеріалів порнографічного характеру) [29].

Щодо провайдерів і компаній поза межами Великої Британії, насамперед *Facebook, Google* і *Twitter*, то процедура отримання доступу та вилучення незаконних матеріалів тут значно складніша. Так, *Facebook* на своєму сайті зазначає, що дані користувачів надаються урядовим органам інших держав на основі договорів між США та цією державою про правову взаємодопомогу. Кожен запит перевіряється на правову обґрунтованість і відповідність правилам діяльності компанії. Якщо уповноважений орган у США надасть *Facebook* (відповідно до Закону США про збереження повідомлень, *Stored Communications Act*) судовий запит (надає право розкривати основні дані користувача – ім'я, адресу електронної пошти, *IP*-адресу, дані кредитних карток), судове рішення (дозволяє отримати доступ до певних записів та іншої інформації з аккаунта) або судовий ордер (можна розкрити матеріали включно з повідомленнями, фотографіями, відеозаписами, записами на стіні, інформацію про місцезнаходження), такі дані можуть бути передані за рішенням Міністерства юстиції США іншій державі [30].

Подібні можливості перераховує на своєму сайті й *Google*, додаючи, що у випадку, якщо певне розпорядження видається безпосередньо закордонним органом, то йому можуть бути надані лише реєстраційні дані аккаунта *Google* чи *YouTube* (ім'я, адреса електронної пошти, *IP*-адреса, позначки часу) [31]. Аналогічно діє і *Twitter* [32].

Кожна із цих провідних компаній щороку публікує відповідний звіт (*transparency report*). За 2013 р. *Facebook* отримав 2619 запитів від Великої Британії на отримання інформації про користувачів та аккаунти, 71,68 % запитів було задоволено; також було обмежено доступ до 9 матеріалів [33]. *Google* у 2013 р. отримав 46 запитів від судів на видалення контенту, 63 % яких було задоволено, та 71 запит від інших органів, задоволено 52 % запитів; 1535 запитів було здійснено на отримання інформації про користувачів, 72 % частково задоволено [34]. До *Twitter* із січня по червень 2014 р. було надіслано 78 запитів на отримання інформації стосовно 220 аккаунтів, 46 % задоволено; також було надіслано 17 запитів на видалення контенту (3 – від судів, 14 – від поліції й інших державних установ), з яких задоволено 6 % (видалено усього 2 твіти) [32].

Питання відповідальності безпосередньо компаній, що надають послуги соціальних мереж, є досить складним, оскільки ці провідні компанії не підпорядковані британському законодавству (*Google, Facebook* і *Twitter* не мають дата-центрів на території Великої Британії). До того ж, вони схильні позиціонувати себе не як суб'єкти, що мають поставати перед законом, а як спільноти, що діють за власними правилами та процедурами, зокрема щодо усунення забороненого контенту [35]. Тому не дивною видається нещодавня опальна стаття голови *GCHQ* Роберта Ханнігана у *Financial Times*, де він стверджує про те, що американські ІКТ-гіганти створюють для терористів «мережу для командування та управління» [36]. Однак, з огляду на те, що, крім взаємовигідного співробітництва з цими компаніями, у Великої Британії особливих альтернатив немає, такий підхід не можна назвати продуктивним.

Висновки

Законодавство Великої Британії у сфері перехоплення, отримання доступу та використання даних є ретельно розробленим, всеохопним і надає державним органам широкі повноваження, зумовлені необхідністю швидкого й ефективного розкриття злочинів і ліквідації загроз безпеці держави та її громадян. Прогресивною можна назвати наявність незалежного оглядача діяльності держави у цій сфері. Однак питання межі, до якої держава може втручатися в особисті дані користувачів, а також проблема строку утримання провайдерами даних комунікації й досі залишаються недостатньо доопрацьованими. Вочевидь, уже в найближчій перспективі Велика Британія може постати і перед проблемою урегулювання прірви, що виникла між національним законодавством і законами ЄС після прийняття нею Акта про утримання даних і слідчі повноваження.

Незважаючи на досить розгалужену нормативно-правову базу, держава активно взаємодіє з ІКТ-провайдерами через неурядові організації та об'єднання на засадах співробітництва. Хоча повноцінні «добровільність» та «рівноправність» такого співробітництва іноді викликають обґрунтовані сумніви, останнє слово, зокрема з питання розумних меж застосування фільтрів для веб-сайтів, залишається за державою.

Відкритим залишається питання застосування санкцій до закордонних ІКТ-компаній, що надають послуги соціальних медіа, які нині по-

ліпшують координацію дій усіх без винятку осіб, включно зі злочинцями й терористами. Ця проблема вже стала інтернаціональною та потребує реальної міжнародної співпраці. Це змушує звернутися до ідей створення окремих міжнародних договорів для регулювання взаємодії держав з питання відповідальності соціальних медіа, що доповнюватиме чинні договори про міжнародно-правову допомогу та Європейську конвенцію з кіберзлочинності.

Список використаних джерел

1. *Бутузов В. М.* Співвідношення понять «комп'ютерна злочинність» і «злочинність у сфері високих інформаційних технологій» / М. Бутузов [Електронний ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exeC21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2009_20_31.pdf
2. *Біленчук П. Д.* Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк. – Київ : Атіка, 2002. — 240 с.
3. *Козак Н. С.* Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку / Н. С. Козак [Електронний ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/znpifyua_2013_2_26.pdf
4. *Кузьменко Б. В.* Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти / Б. В. Кузьменко, О. Ю. Заїка [Електронний ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/jnn_2013_7_6.pdf
5. *Зозуля* Є. В. Міжнародне співробітництво МВС України щодо протидії злочинності у сфері високих технологій / Є. В. Зозуля [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/Nvdduvs_2011_4_7.pdf
6. *Широкова-Мурараш О. Г.* Міжнародно-правові заходи щодо упередження злочинності у сфері інформаційної безпеки / О. Г. Широкова-Мурараш [Електронний ресурс]. – Режим доступу: http://jrnl.nau.edu.ua/index.php/IMV/article/view/3122
7. *Regulation* of Investigatory Powers Act 2000 [Електронний ресурс]. – Режим доступу: http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf
8. *Interception* of Communications Code of Practice Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000 [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf
9. *Acquisition* and Disclosure of Communications Data Code of Practice Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000 [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97961/code-of-practice-acquisition.pdf
10. *Obtaining* Evidence and Information from Abroad [Електронний ресурс]. – Режим доступу: http://www.cps.gov.uk/legal/l_to_o/obtaining_evidence_and_information_from_abroad/
11. *Convention* on Cybercrime status [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG
12. *Європейська* конвенція з кіберзлочинності [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575/page2
13. *Cybercrime* and the law: a review of UK computer crime legislation [Електронний ресурс]. – Режим доступу: http://securelist.com/analysis/publications/36253/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/
14. *Додатковий* протокол до Конвенції, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28 січня 2003 року [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_687
15. *2013* Annual Report of the Interception of Communications Commissioner. The Rt Hon. Sir Anthony May [Електронний ресурс]. – Режим доступу: http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf
16. *Investigatory* Powers Tribunal Report 2010 [Електронний ресурс]. – Режим доступу: http://www.ipt-uk.com/section.aspx?pageid=28
17. *Deep* packet inspection [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Deep_packet_inspection
18. *Draft* Communications Data Bill [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf
19. *Intelligence* and Security Committee : Access to communications data by the intelligence and security Agencies [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf
20. *Data* Retention and Investigatory Powers Act 2014 [Електронний ресурс]. – Режим доступу: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

21. *Directive* 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

22. *The Data* Retention (EC Directive) Regulations 2009 [Електронний ресурс]. – Режим доступу: http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksi_20090859_en.pdf

23. *What* is Ofcom? [Електронний ресурс]. – Режим доступу: http://www.ofcom.org.uk/about/what-is-ofcom/

24. *Ofcom* Report on Internet safety measures Internet Service Providers: Network level filtering measures [Електронний ресурс]. – Режим доступу: http://stakeholders.ofcom.org.uk/binaries/internet/internet_safety_measures_2.pdf

25. *Open* Rights Group Campaigns [Електронний ресурс]. – Режим доступу: https://www.openrightsgroup.org/campaigns/censorship

26. *Internet* Watch Foundation [Електронний ресурс]. – Режим доступу: https://www.iwf.org.uk/

27. *Service* Level Agreement between the Association of Chief Police Officers (ACPO) and the Internet Watch Foundation (IWF) [Електронний ресурс]. – Режим доступу: https://www.iwf.org.uk/assets/media/hotline/SLA %20ACPO %20IWF %20FINAL %20OCT %202010.pdf

28. *Industry* body ISPA sets out five principles for future surveillance law reform [Електронний ресурс]. – Режим доступу: http://www.ispa.org.uk/industry-body-ispa-sets-five-principles-future-surveillance-law-reform/

29. *Downing* Street presses ISPs over 'jihad reporting' button [Електронний ресурс]. – Режим доступу: http://www.bbc.com/news/technology-30052211

30. *Информация* для правоохранительных органов [Електронний ресурс]. – Режим доступу: https://www.facebook.com/safety/groups/law/guidelines/

31. *Юридические* процедуры [Електронний ресурс]. – Режим доступу: http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_does_google_do

32. *Twitter* Transparency Report [Електронний ресурс]. – Режим доступу: https://transparency.twitter.com/

33. *Отчет* огосударственных запросах [Електронний ресурс]. – Режим доступу: https://govtrequests.facebook.com/country/United %20Kingdom/2014-H1/

34. *Отчет* о доступности сервисов и данных [Електронний ресурс]. – Режим доступу: http://www.google.com/transparencyreport/userdatarequests/GB/

35. *House* of Lords Select Committee on Communications 1st Report of Session 2014–15 [Електронний ресурс]. – Режим доступу: http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/37.pdf

36. *Hannigan R.* The web is a terrorist's command-and-control network of choice / R. Hannigan [Електронний ресурс]. – Режим доступу: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3JDkLi0bx