УДК 342.951

Оксана Солдатенко,
докт. юрид. наук, професор,
провідний науковий співробітник
Військового інституту
Київського національного університету імені Тараса Шевченка

ІНФОРМАЦІЙНИЙ ПРОСТІР У МЕРЕЖІ ІНТЕРНЕТ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА КОНТРОЛЬ

Стаття присвячена аналізу окремих законодавчих та нормативно-правових актів, якими регулюються питання вітчизняного інформаційного простору, зокрема, в мережі Інтернет та його контролю. Сформульовано основні висновки щодо сучасного стану законодавчого забезпечення процесу контролю інформаційного простору в мережі Інтернет і пропозиції з його упорядкування в перспективі.

Ключові слова: інформаційний простір у мережі Інтернет, моніторинг інформаційного простору, контроль інформаційного простору в мережі Інтернет, блокування сайтів, заборона доступу до сайтів, Доктрина інформаційної безпеки України.

Постановка проблеми. Починаючи з 2017 року, коли Указами Президента України від 25.02.2017 № 47/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" та від 15.05.2017 № 133/2017 "Про введення в дію рішення Ради національної безпеки і оборони України "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", все частіше йдеться про контроль державою мережі Інтернет. Проте, крім названих указів, питання контролю інформаційного простору в мережі Інтернет натепер не регулюються жодним спеціальним законодавчим актом, так само як і не передбачений він основними законами України у цій сфері: від 02.10.1992 № 2657-XII "Про інформацію" і від 18.11.2003 № 1280-IV "Про телекомунікації", тобто такий контроль фактично здійснюється без належного правового регулювання, що вимагає розроблення відповідних механізмів.

Аналіз останніх досліджень і публікацій. Протягом усього періоду розвитку інформаційного суспільства науковці зверталися до теми інформаційного простору, зокрема, визначення цього поняття наведено у працях А. Манойла [1], Л. Біловус [2], А. Семенова [3], проте, незважаючи на наявність в Україні факту контролю інформаційного простору в мережі Інтернет, натепер відсутні як комплексні наукові праці щодо цього, так і належна нормативно-правова база.

Постановка завдання. У статті поставлено за мету на основі короткого аналізу сучасного стану правового регулювання інформаційного простору в Україні та його контролю виокремити основні проблеми і запропонувати напрями їх вирішення.

Виклад основного матеріалу дослідження.

На думку А. Манойла [1], інформаційний простір – це сукупність суб'єктів інформаційної взаємодії чи впливу; інформації, призначеної для використання суб'єктами інформаційної сфери; інформаційної інфраструктури, що забезпечує можливість обміну між суб'єктами; суспільних відносин, котрі формуються як наслідок утворення, передачі, розповсюдження і зберігання інформації, обміну інформацією всередині суспільства [1, с. 73].

Не можна не погодитися з думкою Л. Біловус [2], що у центрі інформаційного простору стоїть суб'єкт, який створює, накопичує, передає, зберігає інформацію, – всі, хто використовують можливості сучасних інформаційних технологій. Інформаційний простір позбувся усіх обмежень, властивих фізичному простору (державні кордони, океани, велика відстань). Проте він має й певні обмеження, пов'язані з державною чи військовою таємницею, правом на недоторканність приватного життя, – так звані конвенціональні межі [2, с. 189]. У цьому ж джерелі йдеться, що інформаційний простір держави – надзвичайно важлива річ, яка займає друге місце у пріоритеті державної політики після державної незалежності. Україна має забезпечити формування та використання свого інформаційного простору в інтересах держави і своїх громадян [2, с. 190].

З правового погляду, на думку А. Семенова [3], інформаційний простір – це територія поширення інформації за допомогою конкретних компонентів системи інформації та зв'язку, діяльність якої має гарантоване правове забезпечення. Спеціальними вимірами інформаційного простору можуть стати: загальна кількість засобів масової комунікації, загальний обсяг її продукції, що поширюється і приймається на певній території; опосередкована фіксація тих або інших результатів контакту з продукцією засобів масової комунікації реципієнтів [3, с. 91–93].

У Законі України від 05.10.2017 № 2163-19 "Про основні засади забезпечення кібербезпеки України" відсутнє поняття "інформаційний простір", а наведено тільки визначення поняття "національні електронні інформаційні ресурси" (яке, на нашу думку, є одним з основних складників інформаційного простору) – це систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів [4].

Таким чином, з огляду на наведені вище науково обґрунтовані та законодавчі визначення, вважаємо, що інформаційний простір – це сукупність інформаційних об'єктів, які поширюються його суб'єктами через наявні засоби комунікації, тобто контролю можуть підлягати: об'єкти, суб'єкти та засоби комунікації. При цьому до інформаційних об'єктів належать друкована продукція, радіо, телебачення, супутникове мовлення, яке об'єднує в собі телерадіомовлення й Інтернет.

Розмежуємо адміністративно-правове регулювання порядку використання засобів комунікації – безпосередньої складової частини інформаційного простору, яке передбачає систему контрольних заходів та контроль за суб'єктами й об'єктами інформаційного простору в мережі Інтернет.

Так, адміністративно-правове регулювання використання засобів комунікації включає:

1) державну реєстрацію мереж електрозв'язку, що входять до мережі зв'язку загального користування;

2) реєстрацію засобів зв'язку, інших радіоелектронних засобів і високочастотних пристроїв, що є джерелами електромагнітного випромінювання;

3) реєстрацію державних інформаційних ресурсів та систем;

4) ліцензування та сертифікацію різних видів діяльності у сфері інформаційних технологій;

5) ведення Єдиного державного реєстру сертифікатів ключів підписів, засвідчувальних центрів тощо.

Питання адміністрування адресного простору українського сегмента мережі Інтернет, реєстру домену.UA в координації з міжнародною системою адміністрування мережі Інтернет урегульовано нормами Закону України від 18.11.2003 № 1280-IV "Про телекомунікації" (ст. 56), у якому на Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, покладено функцію контролю за дотриманням умов застосування технічних засобів у телекомунікаційних мережах загального користування (п. 7 ст. 24).

У цьому зв'язку в Україні створені та діють суб'єкти таких адміністративно-правових відносин, пов'язаних із контролем інформаційного простору, зокрема: Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення та радіомовлення України. Діяльність названих органів та виконувані ними функції регулюються численними законодавчими і нормативно-правовими актами.

Детальне ознайомлення з основними функціями цих органів дозволяє переконатися, що ними здійснюється контроль переважно за технічними та програмними засобами на предмет їх відповідності реєстраційним і ліцензійним вимогам, умовам, сертифікатам, тобто за використанням адміністративно-правових методів контролю засобів комунікації, використовуваних в інформаційному просторі, а не за змістовим чи суб'єктним складниками інформаційного простору.

Аналіз інформаційного простору в областях України здійснюється Державним комітетом телебачення та радіомовлення України, його результати оприлюднюються у мережі Інтернет та містять інформацію щодо діяльності обласних державних адміністрацій, які щоденно моніторять місцеві аудіовізуальні засоби масової інформації з метою виявлення матеріалів, що закликають до насильницької зміни та повалення конституційного ладу, посягання на територіальну цілісність, пропаганду війни, сепаратизму і тероризму, та реалізують заходи щодо припинення здійснення ретрансляції заборонених російських

телеканалів на території областей. До функцій Державного комітету телебачення та радіомовлення України також належить моніторинг інформаційного наповнення офіційних веб-сайтів міністерств, інших центральних органів виконавчої влади, обласних, міських державних адміністрацій, результати якого оприлюднюються на офіційній сторінці комітету в мережі Інтернет. Такий регулярний детальний аналіз свідчить про належний контроль за станом інформаційного простору в усіх регіонах України з боку уповноваженого органу.

Щодо контролю інформаційного простору в мережі Інтернет, то детальне вивчення наукових джерел і зарубіжного досвіду дозволяє зробити висновки щодо методів контролю інформаційного простору в мережі Інтернет, до яких належать:

1) блокування або заборона доступу до сайтів, що містять інформацію, яка порушує чинне в тій чи іншій країні законодавство (застосовується в Австралії, Азербайджані, Алжирі, Бахрейні, Білорусі, Бельгії, Бірмі, В'єтнамі, Німеччині, Данії, Єгипті, Зімбабве, Індії, Йорданії, Іраку (під контролем США), Ірані, Італії, Казахстані, Канаді, Киргизії, Китаї, Кубі, Малайзії, ОАЕ, Пакистані, Саудівській Аравії, Південній Кореї, Північній Кореї, Сінгапурі, Сирії, Таїланді, Тунісі, Туркменістані, Туреччині, Узбекистані) [5];

2) фільтрування інформаційного потоку в місцях загального користування (інтернет-кафе, навчальні заклади, підприємства) – передбачає обмеження доступу до інформації на основі "чорних списків" – заборони доступу до адрес, що містяться в списку (Китай, Російська Федерація) чи "білих списків" – дозволу доступу тільки до конкретних адрес (Північна Корея), а також за ключовими словами [5];

3) відстеження активності інтернет-користувачів (Російська Федерація), перлюстрація повідомлень;

4) авторизація користувачів при доступі в інтернет із застосуванням провайдерами програмних чи апаратних засобів (Білорусь, Алжир, Іран).

Найжорсткіша система контролю мережі Інтернет діє в Північній Кореї (КНДР), де створено замкнену (що не має виходу в глобальну) мережу Інтернет. Пошук інформації та її публікація у внутрішній мережі КНДР здійснюються спеціальними державними органами. Доступ до глобальної мережі Інтернет є тільки у деяких співробітників наукових і виробничих установ, список яких затверджується органами державної безпеки, а список установ – особисто керівником держави [5].

Одну з найдосконаліших систем контролю мережі Інтернет має Китай, яка включає як законодавчу базу, що формувалася поступово та у логічній послідовності, так і систему фільтрування трафіку. У цій країні жорсткіше здійснюється політична цензура, ніж блокування сайтів аморальної спрямованості.

Регулятивна політика КНР здійснюється в трьох основних напрямах [6]:

1) регулювання всіх видів потокових відеосайтів (а деяких із них – у режимі реального часу), що можуть розміщувати контент, який би ніколи не вийшов на державному телебаченні;

2) регулювання поширення відео у пірінгових (торент) мережах, що стосується порнографічних матеріалів;

3) регулювання сайтів, які функціонують у межах філософії Веб 2.0 ("контент, що створюється користувачами"), – китайські YouTube-клони (www.tudou.com, www.youku.com, www.56.com, www.ouou.com).

Тут ідеться про системи The Golden Shield Project (Проект "Золотий щит" спрямований на стеження за громадянами в мережі Інтернет і контроль за розміщеним там контентом) та Green Dam ("Зелена дамба" – цензурне програмне забезпечення, спрямоване на захист китайців від згубного впливу порнографічних ресурсів). В основі системи – блокування картинок, тексту та веб-адрес за певними значеннями, що передбачає обов'язкове функціонування програмного забезпечення на комп'ютерах.

Корисним у контексті цього наукового дослідження є досвід Великої Британії. О. Бусол, посилаючись у своїй статті [7] на першоджерела, стверджує, що однією з важливих структур у системі взаємодії державних органів Великої Британії та ІКТ-провайдерів є Internet Watch Foundation (IWF) – незалежна неурядова благодійна саморегульована організація, утворена у 1996 р. для виявлення та ліквідації незаконних матеріалів у мережі Інтернет, якою спільно керують ІКТ-провайдери, представники уряду та правоохоронні установи, представники благодійних організацій, громадського сектору. Видаленню підлягають матеріали, пов'язані з дитячою порнографією, а також інший контент, розміщення якого порушує чинне законодавство країни. IWF як самостійно шукає заборонений матеріал, так і розглядає скарги від користувачів та надсилає провайдерам попередження з вимогою видалити матеріал, що не підлягає транслюванню, чи закрити до нього доступ. Якщо провайдер відмовляється задовольнити вимогу, IWF має право передати справу на розгляд до правоохоронних органів. Натепер членами IWF є більшість ІКТ-провайдерів, що діють у Великобританії, а також провідні інтернет-компанії, такі як Google, Facebook, Twitter,

Yahoo!, на яких поширюється дія Кодексу поведінки членів IWF [7].

Головною структурою, що взаємодіє з комунікаційними операторами у питаннях дозволеного контенту та фільтрування інформації, є Офіс із комунікацій (Office of Communications), створений у 2003 р. Актом про комунікації – Communications Act 2003, установа зі статусом державної корпорації, підзвітна парламенту, яка фінансується за рахунок надходжень від учасників телекомунікаційного ринку та урядових грантів [7]. В Україні схожі функції розділено між відомствами, про які йшлося вище (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна рада України з питань телебачення і радіомовлення), що свідчить про розпорошення регулюючого впливу на сферу інформатизації. Крім того, ці структури керуються у своїй діяльності одними і тими ж нормативно-правовими актами, що підтверджує дублювання виконуваних ними функцій та не переконує у високій ефективності їхньої діяльності. У цьому контексті досвід Великої Британії є корисним для України в частині об'єднання згаданих структур в єдиний орган з прозорими функціями.

В Україні, на відміну від Великої Британії, відсутні законодавчі акти, якими передбачався б контроль інформаційного простору в мережі Інтернет та обмежувалося право на інформацію в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, захисту репутації або прав інших людей, як про це зазначено у п. 2 ст. 6 Закону України від 02.10.1992 р. № 2657-XII "Про інформацію".

Незважаючи на відсутність чіткого правового регулювання як самого поняття, так і процедури контролю інформаційного простору (особливо в мережі Інтернет), у ст. 11 Закону України від 06.12.1991 № 1932-XII "Про оборону України" серед основних функцій Генерального штабу Збройних Сил України визначено участь в організації використання та контролю за повітряним, водним і інформаційним простором держави, який здійснюється в особливий період.

Указом Президента України "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" передбачалося визначення механізму реалізації повноважень Генерального штабу Збройних Сил України щодо участі в організації і контролі за інформаційним простором держави та його здійснення в особливий період. Доцільно зазначити, що більшість положень цього Указу Президента України до сьогодні залишилися невиконаними.

Застосування в Україні класичних методів контролю інформаційного простору в мережі Інтернет, про які йшлося вище, розпочалося у 2017 році відповідно до Доктрини інформаційної безпеки України, введеної в дію Указом Президента України від 25.02.2017 № 47/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»" (далі – Доктрина). У ній зазначено: застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на головну арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресії, війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Серед основних пріоритетів державної політики в інформаційній сфері визначено: законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету; пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку. Ця норма свідчить про використання в Україні такого методу контролю інформаційного простору в мережі Інтернет, як блокування або заборона доступу до сайтів, що містять інформацію, яка порушує чинне законодавство. Такий підхід також можна розцінювати і як заходи щодо мінімізації збитків від здійснення як іноземними державами, так і внутрішніми організаціями підривних психологічних операцій, про що писала О. Бусол [7].

При цьому доцільно зазначити, що у Доктрині жодного разу не згадується поняття "контроль" (який ми розглядаємо як одну з основних функцій системи управління – системи спостереження і перевірки процесу функціонування і фактичного стану керованого об'єкта з метою перевірки відповідності поточного стану об'єкта бажаному та необхідному стану, передбаченому законами, інструк-

ціями, іншими нормативними актами, а також програмами, планами, договорами, проектами, угодами тощо), а йдеться тільки про: моніторинг засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні (Міністерство інформаційної політики України); моніторинг загроз національним інтересам і національній безпеці в інформаційній сфері (Міністерство інформаційної політики України); моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері (Служба безпеки України); протидію спеціальним інформаційним операціям, спрямованим проти Збройних Сил України та інших військових формувань (Міністерство оборони України).

Моніторинг традиційно розуміється як процес постійного ознайомлення із загальним станом об'єкта контролю чи окремими напрямами його діяльності [8, с. 254], він не є тотожним поняттям чи синонімом до поняття "контроль" та передбачає систематичне збирання інформації, яка може бути використана для поліпшення процесу управління об'єктом, прийняття рішення та як інструмент зворотного зв'язку.

Водночас детальний аналіз Доктрини дозволяє зробити висновок, що у ній: відсутній механізм виявлення, фіксації, блокування та видалення з інформаційного простору держави вказаної вище інформації; відсутній точний перелік тем, які можуть нести інформаційну загрозу безпеці чи підриву конституційного ладу в Україні; не сформульовано загрози в інформаційній сфері, які би співвідносилося з положеннями Закону України від 19.06.2003 № 964-IV "Про основи національної безпеки України", а також напрями нейтралізації таких загроз.

Контроль інформаційного простору (у т.ч. в мережі Інтернет) пов'язується з цензурою – системою державного нагляду [9, с. 1580] за змістом і розповсюдженням інформації, творів, передач радіо і телебачення, веб-ресурсів з метою обмеження або недопущення поширення ідей і відомостей, визнаних владою шкідливими, небажаними для неї або суспільства в цілому, як методу захисту і контролю інформаційного простору з боку певних структур.

Цензура як контроль держави публічного вияву думок і творчості громадян неодноразово мала місце на території України. І хоча сьогодні в Україні вона заборонена законодавством – Конституцією України (ст. 15) та іншими законами (ст. 24 "Про інформацію", ст. 2 "Про друковані засоби масової інформації", ст. 5 "Про телебачення і радіомовлення", ст. 2 "Про інформаційні агентства", ст. 309 Цивільного кодексу України), владні суб'єкти періодично використовують приховану цензуру (адміністративні заходи з обмеження ефірного часу, тиск на редакції друкованих та Інтернет-видань тощо).

Одним із вітчизняних нормативно-правових актів, який безпосередньо пов'язують із цензурою, є Указ Президента України від 15 травня 2017 року № 133/2017 "Про рішення Ради Національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", яким передбачено блокування ресурсів Mail.ru, Яндекс, соціальних мереж "ВКонтакте", "Одноклассники" та суттєво розширено коло російських телерадіокомпаній, ІТ-компаній і виробників програмного забезпечення, які потрапили під обмеження, згідно з яким провайдери телекомунікацій зобов'язані обмежувати доступ користувачів до вказаних ресурсів, що ще раз підтверджує застосування в Україні такого методу контролю, як блокування або заборона доступу до інтернет сайтів.

Серед недоліків цього рішення відзначимо відсутність документів, які б регламентували конкретні технології та порядок їх використання для онлайн-захисту країни. Крім того, оскільки згідно із Законом України від 05.03.1998 № 183/98-ВР "Про Раду національної безпеки і оборони" рішення Ради є обов'язковими тільки для органів виконавчої влади (ст. 10), то вони не можуть поширюватися на приватних провайдерів телекомунікацій. Департаментом кіберзлочинності Національної поліції до цього часу не розроблено процедуру блокування доступу до вказаних ресурсів. У Законі України від 18.11.2003 № 1280-IV "Про телекомунікації" відсутнє поняття "інтернет-провайдери", які, згідно з Рішенням Ради національної безпеки і оборони, мають припинити надання послуг і доступу користувачам мережі Інтернет до ресурсів російських сервісів. Законом визначено тільки поняття "провайдер телекомунікацій" та "оператор телекомунікацій", що зумовлює наявність колізії щодо того, хто повинен виконувати відповідне рішення, що вимагає внесення змін до названого вище Закону.

Водночас передбачені ним санкції є неефективними з огляду на можливості використання анонімайзерів, VPN та проксі, про що свідчить той факт, що жодна з відповідальних служб не продемонструвала жорсткого контролю за виконанням Указу Президента та не запропонувала чіткого плану

дій для інтернет-провайдерів. Насамкінець: заходи, передбачені Указом Президента України № 133/2017, не відповідають принципам, передбаченим Законом України від 14.08.2014 № 1644-VII "Про санкції", та створюють прецедент Інтернет-цензури.

Хоча у сучасному світі обмеження доступу до сайтів, як зазначено вище, є неефективним рішенням з технологічного погляду, 19.06.2017 Міністерством інформаційної політики оприлюднено додатковий перелік сайтів, переданий до СБУ для блокування, серед яких: rusvesna.su, rusnext.ru, news-front.info, novorosinform.org, nahnews.org, antifashist.com, antimaydan.info, lug-info.com, novorossia.today, comitet.su, novoross.info, freedom.kiev.ua, politnavigator.net, odnarodyna.org, zasssr.info, ruspravda.info, on-line.lg.ua, ruscrimea.ru, c-pravda.ru, 1tvcrimea.ru.

У лютому 2018 року Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, погоджено проект Постанови Кабінету Міністрів України "Про реалізацію і моніторинг ефективності персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" [10], підготовлений Адміністрацією Державної служби спеціального зв'язку та захисту інформації України на виконання Плану організації виконання Указу Президента України від 15.05.2017 № 133/2017, схваленого на засіданні Кабінету Міністрів України 24.05.2017 (протокол № 36), якою врегульовується технічна перевірка блокувань сайтів із санкційного списку. У проекті передбачено: забезпечити придбання технічних засобів для моніторингу стану припинення надання послуг із доступу до інформаційних ресурсів. Державній службі спеціального зв'язку та захисту інформації спільно зі Службою безпеки України "встановити технічні засоби на телекомунікаційних мережах", які мають з'єднання з мережами інших держав для блокування сайтів по доменних іменах і відповідних їм IP-адресах. Реалізація на практиці норм цієї постанови призведе до надмірного контролю та втручання у роботу мережі Інтернет з боку правоохоронних і контролюючих органів та до можливості зловживань і недотримання прав людини при перехопленні інформації силовими структурами. Міжнародною неурядовою правозахисною організацією Freedom House вже висловлено думку, що такий крок розцінюється як посилення цензури [11].

Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, 27.01.2018 також погоджено законопроект, розроблений Національною поліцією, пов'язаний з імплементацією в українське законодавство Конвенції про кіберзлочинність, яким передбачено дозвіл блокування сайтів на термін від трьох місяців до трьох років за рішенням суду. У ньому також передбачена можливість для правоохоронців блокувати інтернет-ресурси без судової постанови, "якщо потрібно запобігти тяжкі злочини" [12], тобто положення законопроекту зобов'язують провайдерів формувати списки своїх клієнтів "для однозначної і миттєвої ідентифікації особистості кожного кінцевого споживача" [12], що свідчить про упровадження в Україні таких методів контролю, як відстеження активності інтернет-користувачів (за досвідом Російської Федерації) та авторизація користувачів при доступі в мережу Інтернет із застосуванням провайдерами відповідних програмних чи апаратних засобів (за зразком систем, що діють у Білорусі, Алжирі, Ірані), – це свідчить про упровадження в Україні трьох із чотирьох можливих методів контролю інформаційного простору в мережі Інтернет. Для цього планується використовувати дорогу технологію перевірки і фільтрації інтернет-трафіку (Deep Packet Inspection, DPI), що можна розцінювати не тільки як цензуру в мережі Інтернет, а й як фільтрацію інформаційного потоку, стеження та маніпулювання інформацією в мережі Інтернет, що суперечить свободі слова та вільному розвитку інформаційного суспільства в цілому й інформаційного простору зокрема.

Доцільно особливо зазначити, що згідно зі ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених законодавством. Ст. 34 гарантовано всім громадянам право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Вільне збирання і поширення інформації може бути обмежене тільки у випадках, передбачених законом і з легітимною метою.

Україна, безперечно, зобов'язана захищати свої інформаційні кордони, проте важливо забезпечити наявність такого громадянського суспільства, яке б не дозволило вчиняти такі дії без рішення суду. Прагнення держави не повинні суперечити правам громадян на особисту свободу, свободу слова, базові людські цінності.

Висновки з дослідження і перспективи подальших розвідок у даному науковому напрямі.

Таким чином, натепер в Україні відсутній комплексний закон та відповідні підзаконні нормативно-правові акти щодо правового регулювання контролю інформаційного простору в мережі Інтернет, де чітко б визначалися: правовий статус суб'єктів контролю; зміст контрольних відносин; використання

встановлених законом способів і методів контролю; правові норми щодо юридичної відповідальності контролюючих та підконтрольних суб'єктів. У такому аспекті доцільно розробити відповідні акти, якими б регулювалися види контролю інформаційного простору в мережі Інтернет, розмежовані за: контролюючими суб'єктами, об'єктами контролю, змістом та методами контролю, етапами (стадіями) контролю, а також за результатами і наслідками контрольної діяльності. Проте, як свідчить досвід Китаю, застосування державою методів контролю мережі Інтернет серйозно шкодить економіці країни, а технологічний сектор залишається без інновацій, такі самі наслідки можливі й в Україні.

Список використаних джерел:

1. Манойло А. Государственная информационная политика в особых условиях: монография / А. Манойло. – М. : МИФИ, 2003. – 388 с.

2. Біловус Л. Український інформаційний простір: сьогодення та перспективи / Л. Біловус [Електронний ресурс]. – Режим доступу : http://ijimv.knukim.edu.ua/zbirnyk/1_1/bilovus_l_i_ukrayinskyy_informatsiynyy_prostir.pdf.

3. Семенов А. Захист національного інформаційного простору Великої Британії / А. Семенов // Матеріали міжнародної конференції «Політична праксеологія: безпека, технології, комунікації» / за ред. В. Бебика. – Київ : ВАПН, 2016. – 117 с.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-19 [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/2163-viii.

5. Лихтман Б. Правительства берут интернет под контроль / Б. Лихтман, А. Сидельников [Електронний ресурс]. – Режим доступу : http://www.infosecurity.ru/_gazeta/content/091225/art2.shtml.

6. China's new online video regulation: reading the tea leaves [Electronic resource] / Rebecca MacKinnon. – Access mode: http://rconversation.blogs.com/rconversation/2008/01/chinas-new-onli.html.

7. Бусол О. Основні риси контролю за національним інформаційним простором Королівства Велика Британія / О. Бусол [Електронний ресурс]. – Режим доступу : http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2961:osnovni-risi-kontrolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya&catid=8&Itemid=350.

8. Фінансова енциклопедія / О. П. Орлюк, Л. К. Воронова, І. Б. Заверуха [та ін.] ; за заг. ред. О. П. Орлюк. – К. : Юрінком Інтер, 2008. – 472 с.

9. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. – К.; Ірпінь : ВТФ "Перун", 2005. – 1728 с.

10. Про реалізацію і моніторинг ефективності персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : Проект Постанови Кабінету Міністрів України [Електронний ресурс]. – Режим доступу : http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=280657&cat_id=38837&ctime=1503913672346.

11. Freedom House опасается, что в Украине может усилиться цензура в интернете [Електронний ресурс]. – Режим доступу : https://strana.ua/news/127317-freedom-house-opasaetsja-chto-v-ukraine-mozhet-usilitsja-tsenzura-v-internete.html.

12. Російський сценарій. Усе, що потрібно знати про тотальне стеження за інтернет-користувачами в Україні [Електронний ресурс]. – Режим доступу : https://nv.ua/ukr/techno/it-industry/rosijskij-stsenarij-use-shcho-potribno-znati-pro-totalne-stezhennja-za-internet-koristuvachami-v-ukrajini-2454611.html.

Статья посвящена анализу отдельных законодательных и нормативно-правовых актов, регулирующих вопросы отечественного информационного пространства, в частности в сети Интернет, и его контроля. Сформулированы основные выводы о современном состоянии законодательного обеспечения процесса контроля информационного пространства в сети Интернет и предложения по его усовершенствованию в перспективе.

Ключевые слова: информационное пространство в сети Интернет, мониторинг информационного пространства, контроль информационного пространства в сети Интернет, блокировка сайтов, запрет доступа к сайтам, Доктрина информационной безопасности Украины.

The article is devoted to the analysis of separate legislative and regulatory acts, which regulate questions of the domestic information space, in particular in the Internet, and its control. The main conclusions about the current state of legislative provision of the information space control process on the Internet and proposals for its streamlining in the future are formulated.

Key words: information space on the Internet, monitoring of information space, control of information space on the Internet, blocking of sites, prohibition of access to sites, Doctrine of Information Security of Ukraine.