МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Кафедра правоохоронної діяльності та поліціїстики
Факультет № 6

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни «ІНФОРМАЦІЙНЕ ПРАВО» обов'язкових компонент освітньої програми першого (бакалаврського) рівня вищої освіти

262 Правоохоронна діяльність

на тему :. Правове регулювання телекомунікацій та відносин в сфері віртуальної мережі Інтернет

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30 серпня 2023 року № 7

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 25 серпня 2023 року № 7

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з юридичних дисциплін
Протокол від 29 серпня 2023 року № 7

Розглянуто на засіданні кафедри правоохоронної діяльності та поліціїстики
Протокол від 18 серпня 2023 року № 8

Розробники:
1. Завідувач кафедри правоохоронної діяльності та поліціїстики, кандидат юридичних наук, професор Панова Ірина Вікторівна.

Рецензенти:
1. Заступник начальника відділення поліції №3 Харківського районного управління поліції №1 ГУНП в Харківській області, доктор, снс Прокопенко О.Ю.
2. Професор кафедри адміністративного права та процесу факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор, заслужений діяч науки і техніки України Комзюк А.Т.

План лекції

1. Історія розвитку Інтернет
2. Законодавче регулювання Інтернет в Україні: проблемні питання й перспективи розвитку
3. Правове регулювання інформаційних відносин в інтернет просторі
4. Правопорушення в мережі інтернет
5. Міжнародно-правові аспекти управління Інтернетом
6. Законодавче регулювання телекомунікацій та відносин в сфері віртуальної мережі Інтернет в Україні

Література

1. Конституція України : від 28 черв. 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141. // URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
2. Про захист персональних даних : закон України від 1 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481. // URL: https://zakon.rada.gov.ua/laws/show/2297-17
3. Про захист суспільної моралі : закон України від 20 листоп. 2003 р. № 1296- IV // Відомості Верховної Ради України. – 2004. – № 14. – Ст. 192. // URL: https://zakon.rada.gov.ua/laws/show/1296-15
4. Про інформаційні агентства : закон України від 28 лют. 1995 р. № 74/95-ВР // Відомості Верховної Ради України. – 1995. – № 13. – Ст. 83. // URL: https://zakon.rada.gov.ua/laws/show/74/95-вр
5. Про інформацію : закон України від 2 жовт. 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650. // URL: https://zakon.rada.gov.ua/laws/show/2657-12
6. Про Концепцію Національної програми інформатизації : закон України від 4 лют. 1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 182. // URL: https://zakon.rada.gov.ua/laws/show/75/98-вр
7. Про бібліотеки і бібліотечну справу : закон України від 27 січн. 1995 № 32/95-ВР // Відомості Верховної Ради. – 1995. – № 7. – ст.45. // URL: https://zakon.rada.gov.ua/laws/show/32/95-вр
8. Про Національний архівний фонд і архівні установи : закон України від 24 груд. 1993 № 3814-XII //Відомості Верховної Ради України. – 1994. – № 15. – ст.86. . // URL: https://zakon.rada.gov.ua/laws/show/3814-12
9. Про науково-технічну інформацію: закон України від 25 червн. 1993 № 3322-XII // Відомості Верховної Ради України. – 1993. – № 33. – ст.345. // URL: https://zakon.rada.gov.ua/laws/show/3322-12
10. Про державну таємницю : закон України від 21.01.1994 № 3855-XII // Відомості Верховної Ради України. – 1994. – №16. – С. 93. // URL: https://zakon.rada.gov.ua/laws/show/3855-12
11. Про захист інформації в інформаційно-телекомунікаційних системах :

закон України від 05 лип. 1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – ст.286. // URL: https://zakon.rada.gov.ua/laws/show/80/94-вр

12. Про рекламу : закон України від 3 лип. 1996 р. № 270/96-ВР // Відомості Верховної Ради України. – 1996. – № 39. – Ст. 181. // URL: https://zakon.rada.gov.ua/laws/show/270/96-вр
13. Про доступ до публічної інформації : закон України від 13 січ. 2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314. // URL: https://zakon.rada.gov.ua/laws/show/2939-17
14. Про Доктрину інформаційної безпеки України : Указ Президента України від 25 лютого 2017 року № 47/2017 // Урядовий кур'єр від 28.02.2017. № 38. // URL: https://zakon.rada.gov.ua/laws/show/47/2017

Основна література:

1. Інформаційне насильство та безпека: світоглядно-правові аспекти. Дзьобань О.П., Пилипчук В.Г. / За заг. ред. проф. В.Г. Пилипчука. – Харків: Майдан, 2011. – 244 с.
2. Марущак А. І. Інформаційне право України : підручник / А. І. Марущак. – К. : Дакор, 2011. – 456 с.
3. Інформаційна взаємодія у місцевому самоврядуванні: перспективи правового регулювання Дубняк М.В. : монографія – Київ: Видавничий дім «АртЕк». – 2019. – 190 с.
4. Основи інформаційного права України : навч. посіб. – 2-ге вид., перероб. і доп. Рекомендовано МОН / Цимбалюк В. С., Павловський В. Д. – К., 2009. – 414 с.
5. Інформаційне право та інформаційне законодавство Брижко В.М., Фурашев В.М. : наукове видання. – (НДІІП НАПрН України). Київ: Видавничий дім "АртЕК", 2020. 288 с.
6. Брижко В. М. Методологічні та правові засади упорядкування інформаційних відносин : монографія / Брижко Валерій Михайлович. – К. : ПанТОТ, 2009. – 415 с.
7. Горбулін В. П. Проблеми захисту інформаційного простору України : монографія / В. П. Горбулін, М. М. Биченок. – К. : Інтертехнологія, 2009. – 136 с.
8. Становлення і розвиток системи стратегічних комунікацій сектору безпеки і оборони України Пилипчук В. Г., Компанцева Л. Ф., Кудінов С. С., Доронін І. М., Дзьобань О. П., Акульшин О. В., Заруба О. Г.; за заг. ред. В. Г. Пилипчука: монографія – К. : ТОВ «Видавничий дім «АртЕк», 2018. – 272 с.

Додаткова література:

1. Панова І.В. Фактори, що впливають на утворення системи інформаційного права та формування її змісту // Інформація і право. 2018. № 3 (26). С. 9-15.
2. Панова І.В. Сучасні проблеми цифровізації військового обліку в Україні // Проблеми сучасної поліцеїстики : тези доп. III наук.-практ. конф. (м. Вінниця, 11 трав. 2023 р.) / МВС України, Харків. нац. ун-т внут. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2023. – 208 с. – С.

52-56. https://dspace.univd.edu.ua/items/53e4a11d-7784-47ec-8140-1c250b37af2e

3. Панова І.В., Шевцова А.С. Національна поліція України як суб'єкт формування і реалізації політики інформаційної безпеки України // Проблеми сучасної поліцеїстики : тези доп. ІІ наук.-практ. конф. (м. Харків, 20 квіт. 2022 р.) / МВС України, Харків. нац. ун-т внут. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2022. – 208 с. – С. 281-283. https://dspace.univd.edu.ua/server/api/core/bitstreams/cd87cc48-6e4f-497a-a782-d3a76ce14332/content
4. Панова І.В., Шевцова А.С. Засоби забезпечення інформаційної безпеки України// Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. X Міжнар. наук.-практ. конф., присвяч. 27-й річниці створення Харків. нац. ун-ту внутр. справ (м. Харків, 19 листоп. 2021 р.).–Харків: ХНУВС, 2021.–С. 72-74 https://dspace.univd.edu.ua/items/c216c142-4cdd-427c-927c-f3b9dee6e6c0
5. Щодо окремих питань визначення стандартів кібербезпеки при підготовці працівників для кіберполіції Підготовка охоронців правопорядку в Харкові (1917–2017 рр.): зб. наук. ст. і тез доп. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові (м. Харків, 25 листоп. 2017 р.)/МВС України, Харків. нац. ун-т внутр. справ.–Харків, 2017.–340 с. https://dspace.univd.edu.ua/items/7230016d-744b-497c-8abf-3e2fde902571

Інформаційні ресурси в Інтернеті

1. Офіційний сайт Верховної Ради України https://iportal.rada.gov.ua/
2. Офіційний сайт Кабінету Міністрів України https://www.kmu.gov.ua/
3. Офіційний сайт Судова влада України https://court.gov.ua/
4. Офіційний сайт МВС України www.mvs.gov.ua.
5. Офіційний сайт Верховного Суду України http://www.viaduk.net/clients/vsu/vsu.nsf/
6. Єдиний державний реєстр судових рішень http://www.reyestr.court.gov.ua/
7. Національна бібліотека України ім. В.І. Вернадського http://www.nbuv.gov.ua/
8. Офіційний сайт Харківського національного університету внутрішніх справ http://univd.edu.ua/
9. Харківська державна наукова бібліотека ім. В.Г. Короленко http://korolenko.kharkov.com/
10. Юридична бібліотека http://pravo.biz.ua/
11. сайт Національного інституту стратегічних досліджень. – http://www.niss.gov.ua

1. Історія розвитку Інтернет

Термін "Інтернет" походить відInterconnected Networks (об'єднані мережі). Прообразом сучасної Інтернету прийнято вважати американську військово-промислову територіальну мережу ARPANet (від англійського Advanced ResearchProjectsAgency Network). Розробляли систему вчені Каліфорнійського університету у Лос-Анджелесі, Стендфордського дослідницького центру, Університету штату Юта, Університету штату Каліфорнія в Санта-Барбару. У 1969 року у проекту мережу об'єднала чотири зазначених наукових установи, всі роботи фінансувалися рахунок Міністерства оборони США. Потім мережуARPANET початку активно вона зростатиме і розвиватися.

2 січня 1969 року було прийнято рішення про початок роботи над проектом зі створення мережі комп'ютерів оборонних організацій. Мережа повинна зберігати працездатність за умов ядерної атаки. До 1972 року 40 комп'ютерних центрів могли обмінюватися електронною поштою, здійснювати сеанси роботи з віддаленими сталася на кілька сотень і тисячі кілометрів електронно-обчислювальними автомобілями і передавати файли з цими. Ідеологічною основою проекту стала відсутність загального Центру управління, повна самостійність кожного сегмента. Це було зумовлена необхідністю забезпечити роботу каналів передачі на виході з ладу окремих вузлів. При ієрархічному побудові мережі вихід із ладу центральний елемент приводив до втрати працездатності в усій мережі.

У 1984 році була розроблена система доменних імен. У 1988 року було винайдено протокол InternetRelayChat (IRC), який дозволив спілкуватися у реальному масштабі часу. Встановлюється єдине глобальний інформаційний взаємодія. У 1998 року Папа Римський Іван Павло Другий заснував всесвітній День Інтернету – 30 вересня. Кількість користувачів мережею Інтернет наближається до 1,5 мільярдам чоловік.

Інтернет **–** це організаційно упорядкована сукупність документів і майже інформаційні технології.

2. Законодавче регулювання Інтернет в Україні: проблемні питання й перспективи розвитку

Коли йдеться про інформацію взагалі й про її свободу зокрема, сьогодні перш за все слід говорити про можливості, які надає в цьому плані всесвітня мережа Інтернет. З приводу визначення поняття Інтернет у світі й до сьогодні точаться дискусії, оскільки всесвітню мережу можна розглядати як засіб обміну даними, як комплекс технічних засобів чи взагалі як віртуальний аналог нашого повсякденного життя. Одним з найбільш вичерпних на даний момент є визначення, яке містять Рекомендації парламентських слухань “Росія і Інтернет: вибір майбутнього”:

Інтернет – унікальна сукупність локальних, регіональних і національних комп'ютерних мереж та універсальна технологія обміну даними;

Інтернет – засіб інформаційного спілкування мільйонів людей;

Інтернет – це глобальний інформаційний простір, який не визнає державних кордонів, що робить цю систему якісно новим явищем у світовому співтоваристві;

Інтернет є унікальним за своїми можливостями засобом доступу до інформації щодо будь-яких видів діяльності чи інтересів людини;

Інтернет – один з основних інструментів пізнання світу, навчання, отримання професійних знань;

Інтернет є об'єктом розробки й застосування новітніх програмних та інструментальних технологій, що робить його сферою бурхливого розвитку в майбутньому.

В мережі Інтернет відсутня централізована система управління, Існує тільки координатор системи, роль якого відіграє сьогодні ISOC – Товариство учасників Інтернет. Це громадська організація, що існує за рахунок внесків і пожертвувань спонсорів. Водночас кожна держава створює власні правові й організаційні механізми регулювання використання Інтернет.

У контексті активного використання мережі як глобального інформаційного середовища перед Україною постає питання законодавчого врегулювання нових інформаційних відносин, що виникають у системі людина - Інтернет. Конституційне право людини на інформацію закріплене в основному законі України та інших нормативно-правових актах і, вочевидь, поширюється на інформаційні права людини, що виникають при використанні Інтернет. Однак ні отримання, поширення, пошук, продукування інформації, ні будь-який інший процес, пов'язаний із використанням інформації, ще майже ніяк не відображується в національному законодавстві. Правда, існують декілька нормативно-правових актів у цій галузі, в основному спрямованих на максимальний контроль Інтернет з боку держави (в особі СБУ), серед них – Укази Президента " Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" (від 1 липня 2000 р., № 928) і "Про заходи щодо захисту інформаційних ресурсів держави" (від 10 квітня 2000 р., № 582), Розпорядження Кабінету Міністрів України "Про передачу Державного центру інформаційної безпеки до сфери управління Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ" (від 28 лютого 2001 р., № 63-р) тощо.

В ряді законодавчих актів України, наприклад, у Законі України "Про інформацію", Законі України "Про зберігання науково-технічної інформації" та інших, що регулюють інформаційні відносини, термін "Інтернет" безпосередньо не використовується, однак його мають на увазі при використанні таких термінів, як "інформаційні мережі", "міжнародні мережі передачі даних".

Для визначення оптимального напряму законодавчого регулювання в сфері Інтернет в ряді країн проведені спеціальні дослідження, створені наукові

центри та громадські організації, прийняті численні законодавчі акти й кодекси поведінки і. Враховуючи, що глобальна комп'ютерна мережа створює єдиний інформаційний простір без державних кордонів і обов'язкових обмежень для всіх її користувачів, проблема законодавчого регулювання Інтернет є ідентичною для в усіх країн. Однак у різних регіонах цей процес має свої особливості. Так, США взяли курс на побудову "інформаційної магістралі" як технологічного засобу, що дозволяє кожному знайти необхідну інформацію. Інформаційна магістраль визначається як сукупність усіх технологій, пов'язаних з продукуванням, обробкою, зберіганням та розповсюдженням інформації, включаючи телебачення, комп'ютерні мережі, супутникове мовлення, комерційні он-лайнові компанії.

В країнах ЄС головну увагу приділяють соціальній стороні чергового етапу світової технологічної революції в контексті розвитку Інтернет. Резолюції й документи Ради Європи присвячені формуванню національної політики в галузі побудови інформаційного суспільства, причому це завдання сприймається не як данина моді, а як необхідна умова розвитку суспільства, недотримання якої призводить до втрати темпів розвитку й відкидання з провідних економічних і технологічних позицій.

В країнах СНД Інтернет розвивається не так швидко, як на Заході, і з традиційним акцентом на забезпеченні інформаційної безпеки з метою підтримки відпрацьованого за роки радянської влади тотального контролю за будь-яким видом інформації. В Україні, крім того, прослідковується й тенденція до "інформаційного суверенітету"2.

Офіційний курс державної політики в галузі інформаційних технологій в Україні окреслює перш за все Закон "Про національну програму інформатизації". Готуються до прийняття такі важливідокументи, як проекти законів "Про захист персональних даних", "Про національні інформаційні ресурси", "Про діяльність у сфері інформатизації", "Про електронний підпис", "Про телекомунікації" та інші. Однак, як і раніше, відсутні законопроектів, які безпосередньо стосуються Інтернет і спрямовані на його розвиток.

Світовими лідерами в галузі Інтернет є, перш за все, США, Японія, Південна Корея, країни ЄС. Серед посттоталітарних держав особливе місце посідає Естонія, яка досягла досить високого рівня розвитку інформаційних технологій і ставить питання про те, чи потрібний взагалі державний контроль за Інтернет. Серед держав СНД особливе місце належить Росії, яка, з одного боку, бурхливими темпами нарощує використання новітніх інформаційних технологій, зокрема Інтернет; а з іншого – намагається цей процес максимально контролювати, чим свідомо його гальмує. На жаль, головний акцент російської державної політики в інформаційній сфері робиться на збереженні "федеративної інформаційної цілісності", що дуже співзвучно з українською концепцією "національного інформаційного суверенітету".

Щоб зрозуміти, яким шляхом потрібно йти Україні для створення національного законодавства в галузі Інтернет, і щоб при цьому право людини на інформацію було реалізовано повною мірою, необхідно ретельно вивчати

міжнародний досвід, і на його основі розробляти власну ефективну законодавчу базу в даній галузі, не відкладаючи це на невизначений термін.

Показово, що в 2000 р. Президент України в своє посланні до Верховної Ради України про внутрішнє й зовнішнє становище України вже нарешті офіційно визначив, що "свобода обігу інформації сьогодні тісно пов'язана з розвитком інформаційних технологій і перш за все Інтернету". На той час, наприклад, в українському сегменті Інтернету розміщувалося понад 320 газет і журналів, причому деякі з них не мали друкованих аналогів. Крім того, на 28 серверах розміщували інформацію політичні партії, на 335 серверах знаходились персональні сторінки окремих політиків і бізнесменів.

Напрями державної політики й заходи Кабінету Міністрів у посланні Президента, що сприяли б розвитку Інтернет і забезпеченню свободи інформації в Україні, наступні:

– активний розвиток мережі Інтернет;

– поширення в Інтернет всебічної інформації про діяльність органів державної влади та місцевого самоврядування;

– швидше впровадження Інтернет у навчальних закладах усіх видів;

– перегляд шкільних програм з інформатики зі значним збільшенням кількості годин на вивчення й практичне освоєння роботи в Інтернеті, випуск відповідного підручника та методичних посібників;

– запровадження на Першому національному каналі телебачення циклу науково-пізнавальних програм, присвячених ознайомленню з можливостями Інтернет.

Однак слід зауважити, що задекларувати розвиток Інтернет в Україні – це одне, а фактично сприяти його розвитку завдяки створенню відповідної законодавчої бази й певним заходам з боку Уряду та інших органів державної влади – зовсім інша справа. Так, наприклад, сьогодні на розгляді Верховної Ради перебуває законопроект "Про телекомунікації" № 2059 від 22 листопада 2002 р., що передбачає введення ліцензування передавання даних. Очевидно, що введення такого ліцензування, зокрема Інтернет-послуг, як і оподаткування при здійсненні електронної комерції, гальмуватиме розвиток українського сегменту мережі. Важливим є й визначення основних термінів у галузі інформаційних технологій при створенні законодавчих актів, які відповідали б сучасному уявленню про Інтернет-технології не тільки пересічного громадянина, а й спеціалістів високої технічної кваліфікації, а також міжнародним стандартам у цій галузі (йдеться про те, що законодавці при створенні Інформаційного кодексу мають бути компетентні в технічних і технологічних питаннях щодо використання комп'ютерних мереж та обміну інформацією в них).

Отже, визначення на державному рівні важливості використання Інтернет, визнання його значення для інформаційного обміну й реалізації права на інформацію громадян України. є надзвичайно важливим моментом для розвитку нашого суспільства І хоча, як правило, в нашій державі відстань між прийняттям певних державних рішень та їх впровадженням у життя може бути

величезною, входження в наше життя Інтернет не викликає жодних сумнівів. Це загальносвітова тенденція, й Україні її не обійти.

3. Правове регулювання інформаційних відносин в інтернет просторі

Проблемними для України питання є пов'язані з можливістю вільного розповсюдження даних в Інтернеті: Це питання: охорони авторських прав, забезпечення інформаційної безпеки, запобігання розповсюдженню недобросовісної або таємної інформації, що створює загрозу для прав і законних інтересів фізичних і юридичних осіб, а також для національних інтересів, державної безпеки, економічного і фінансового розвитку країни.

У зв'язку з розповсюдженням комп'ютерної обробки даних і передачею їх каналами телекомунікаційних мереж, з'явились нові питання щодо захисту персональних даних, забезпечення права громадян на отримання інформації з Інтернету, зокрема правової інформації і інформації про діяльність державних органів, запобігання розповсюдженню відомостей, що не відповідають дійсності, зазіхають на честь, гідність громадян або ділову репутацію юридичних осіб (образливих і наклепницьких відомостей), а також пропаганди, направленої на розпалювання національної, і релігійної ворожнечі, з використанням Інтернету правил електронного документообігу, використання електронного цифрового підпису або зловживання правами, порядок укладення договорів в електронній формі

Однією із головних прогалин законодавства сьогодення, на нашу думку, є відсутність обов'язку особи яка має намір створити веб-сайт надати свої персональні дані (паспортні дані та ін.), для ідентифікації її як власника веб-сайту.

З огляду на простий доступ до мережі Інтернет та швидке зростання кількості її користувачів, на даний момент, актуальним є вирішення питань, пов'язаних із можливостями мережі Інтернет та їх використанням. Такими питаннями, зокрема, щодо вдосконалення організаційно-правового забезпечення поширення інформації мережею Інтернет.

До зазначеної проблеми зверталися провідні вчені - юристи, а саме: В.М. Брижко, В.Д. Гавловський, В.В. Гриценко, М.В. Гуцалюк, В.І. Жуков, Р.А. Калюжний, В.С. Цимбалюк, М.Я. Швець. Ю.А. Агешина, И.Л. Бачило, Ю.М. Батурина, А.Б. Венгерова, А.В. Волокитіна, Е.К. Волчинська, М.М. Ка-реліна, В.А. Копилов, Б.В. Кристальний, А.П. Курило, Дж. Юлел.

У вітчизняній юридичній науці відносини, що пов'язані з використанням інформації в Інтернеті, на нашу думку, досліджені фрагментарно, з огляду на те, що деякі дослідники присвячували наукові пошуки здебільшого окремим проблемам правової охорони об'єктів авторських прав, доступних користувачам Інтернету. Ознайомлення з роботами вчених у цьому напрямку засвідчує, що їх авторами виявлені, в основному, процесуально-правові проблеми з'ясування і доведення фактів порушення авторських прав при розміщенні інформації в Інтернеті.

Світова практика демократичного державотворення переконує в тому, що право на свободу думки і слова, на вільне виявлення своїх поглядів і

переконань є одним з наріжних каменів розбудови демократичної, правової держави і громадянського суспільства. Без свободи слова немає демократії.

У резолюції 59 Генеральної Асамблеї ООН зазначено, що «свобода інформації є основним правом людини і критерієм усіх інших свобод».

Конституція України (ст. 34) гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, на вільне збирання, зберігання, використання і поширення інформації. Це важливе конституційне положення повністю відповідає ст.19 Загальної декларації прав людини та ст.10 Конвенції про захист прав і основних свобод людини.

Україна посідає одне з провідних місць у СНД за кількістю законів, присвячених діяльності мас-медіа і спрямованих на розширення гласності та поінформованості суспільства. За визнанням міжнародних експертів, українське законодавство в галузі інформації дає можливість реалізувати право людини на свободу думки і слова, хоча, звичайно, потребує певних коректив, змін і доповнень.

Основні правила щодо ведення інформаційної діяльності, тобто одержання, використання, поширення та зберігання інформації і захисту прав суб'єктів інформаційних відносин містяться у статтях 32 і 34 Конституції України, а також у Цивільному кодексі України (далі - ЦК), Законах України «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про науково-технічну інформацію», «Про захист від недобросовісної конкуренції», «Про захист інформації в інформаційно - телекомунікаційних системах», «Про державну статистику», «Про бібліотеки і бібліотечну справу», «Про Національний архівний фонд та архівні установи», «Про державну таємницю», «Про Національну систему конфіденційного зв'язку», «Про банки і банківську діяльність», «Про Державну службу спеціального зв'язку та захисту інформації України».

Інтернет як жоден із засобів масової інформації дає можливість реалізувати право вільного збирання, зберігання, використовування і поширення інформації. В Інтернеті можна знайти інформацію на будь-яку тему - від медицини до науки і техніки. Є можливість виявити найдокладніший матеріал про усі види мистецтва, масу корисної інформації для студентів і школярів, дані для тих, хто шукає роботу, довідки про відпочинок, розваги, спорт і різні товари. Об'єднання комп'ютерів у мережі, а мереж - у глобальну міжнародну мережу Інтернет дає практично необмежену можливість вільного доступу до накопиченої людством інформації, незалежно від відстані і місця збереження.

Як показує досвід розвинених країн, за останні роки кількість зафіксованих випадків шахрайства через Інтернет зросла у десятки разів. Водночас законодавче забезпечення Інтернету у тому числі з метою захисту інтересів держави, повинне мати межу, яку не можна було б переступити, аби не зашкодити праву на свободу слова та вільного доступу до інформації. Перш за все Інтернет може бути використаний просто як інструмент для

правопорушень загального характеру - наприклад, якщо зловмисник створює веб-сайт для продажу наркотичних засобів чи розповсюдження порнографії або використовує електронну пошту для шантажу. Тут повинні діяти відповідні загальноправові норми, але специфіка Інтернету зумовлюється тим, що з такими злочинами стає важче боротися з огляду на труднощі з відстеження самого зловмисника та його контактів.

Рішенням Апеляційного суду Сент-Луїса у справі за позовом Американської асоціації індустрії звукозапису RIAA проти корпорації Charter Communication, одного з найбільших інтернет-провайдерів СІЛА представникам індустрії звукозапису заборонено вимагати в інтернет-провайдерів надання персональних даних про користувачів Інтернету, запідозрених у нелегальному поширенні продукції відомих музичних лейблів.

Звукозаписні компанії стверджували, що 93 клієнти Charter Communications протиправно продали через Інтернет близько 100 тис. файлів з музичними записами. Оскільки вся інформація про підозрюваних обмежується їхніми електронними адресами, RIAA спробувала персоналізувати свої судові позови проти Інтернет-піратів, для чого необхідно було одержати особисті відомості про клієнтів Інтернет-провайдера. Компанія відмовилась надати таку інформацію, а суд погодився, що вимоги RIAA до Charter безпідставні, оскільки: «.. .роль Інтернет-провайдера обмежується лише переміщенням файлів по мережі».

Інтернет-комерція - це один з видів бізнесу, і тут повинні діяти всі правові норми, що регулюють господарську діяльність. Зокрема, для електронної комерції характерні такі порушення: ведення комерційної діяльності без належної реєстрації (зокрема, здійснення підприємницької діяльності вимагає обов'язкової реєстрації; для розміщення веб-сайту в Інтернеті реєстрація не є необхідною, але такий сайт цілком може бути використаний для комерційної діяльності, а у випадку виникнення ускладнень - моментально знищений); ухилення від сплати податків; шахрайство, обман замовників та інші порушення прав споживачів; незаконні фінансові та валютні операції (зокрема, інтернаціональний характер Інтернету та підвищений рівень анонімності провокують деяких підприємців на незаконну реєстрацію віртуальних підприємств в офшорних зонах, пов'язані з цим перекази коштів за кордон та їх «відмивання» тощо); незаконне використання чужого товарного знака; недобросовісна конкуренція і реклама.

Недостатньо відпрацьованими є правові методи боротьби з такими специфічними для Інтернету явищами, як спам (Спам Ганга, spam) - масова розсипка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати). Передусім термін «спам» стосується рекламних електронних листів.), хоч останнім часом ситуація починає змінюватися на краще, і такі закони приймаються. У ряді країн спам розглядається як серйозне правопорушення, за яке винуватець має принаймні сплатити штраф і може бути притягнений до кримінальної відповідальності.

На мою думку, повинні повинні бути відрегульовані питання, пов'язані з електронним документообігом та електронним цифровим підписом. В США та

в Європейському Союзі закон про електронний цифровий підпис діє з кінця 90-х років. Для європейських країн важливе значення має директива ЄС 1999/93/ЄС від 13 грудня 1999 р. «Про політику ЄС щодо електронних підписів».

В Україні діє Закон «Про захист інформації в автоматизованих системах» від 5 липня 1994 р., а також положення про технічний захист інформації в Україні, затверджене Указом Президента №1229 від 27 вересня 1999 р. У Кримінальному Кодексі України передбачені статті 361-363, які об'єднані в окремий розділ: «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж».

Інтернаціональний характер Інтернет викликає ряд проблем, пов'язаних з застосуванням національних законодавств. Наприклад, якщо ділові партнери живуть в різних країнах і ведуть бізнес через Інтернет, законодавством якої саме країни повинні регулюватися пов'язані з цим аспекти? Якщо громадянин України живе в Нідерландах, зареєстрував підприємство в Австралії, а веб-сайт - у колумбійській зоні, його партнери знаходяться в Таїланді, а сайт використовується для розповсюдження порнографії - за законодавством якої країни він повинен відповідати за вчинений злочин ?

Для прикладу, у 1999 р. проти Amazon.com був поданий судовий позов, який звинувачував компанію в продажі забороненої літератури на території Німеччини (в цій країні заборонена книга Гітлера «Майн Кампф» та інші нацистські твори). Компанія у запереченні на позов вказала, що клієнти з інших країн, які замовляють книги на її сайті, повинні розглядатися як туристи, які самі відповідають за ввезення книжок до своєї країни.

Таким чином, укладання договору в Інтернеті має транснаціональний характер і потрапляє до сфери міжнародного права. Традиційно для вирішення питання про застосування того чи іншого законодавства береться до уваги місце укладання договору, але в Інтернеті часто не є можливим визначити, на території якої саме країни укладено договір. Тому, якщо в договорі не вказано місце його укладення, таким місцем вважається місце проживання фізичної особи або перебування юридичної особи оферента (того, хто робить пропозицію).

В інформаційному листі Вищого господарського суду України від 28.03.07 №01-8/184 зазначено, що у разі розміщення інформації в мережі Інтернет у вигляді, доступному для публічного ознайомлення, особа, чиї права та законні інтереси порушені її поширенням, може подавати відповідні позовні вимоги до власника веб-сайту, на якому розміщена ця інформація. Дані про власника веб-сайту можуть бути витребувані відповідно до вимог статей 30 та 65 ГПК від товариства з обмеженою відповідальністю «Хостмайстер», яке на даний час адмініструє систему реєстрації та обліку доменних назв і адресу українського сегмента мережі Інтернет. Після здійснення заходів, пов'язаних з переделегуванням прав адміністрування, ці функції має здійснювати об'єднання «Український мережевий інформаційний центр».

Саме тут і постає головна проблема, визначити власника сайту. На сьогодні, при створенні та реєстрації сайту замовник вносить дані на власний

розсуд. Існує сайт, який допомагає визначити дані власника сайту (http://who.is). З 10 спроб встановити власників різних сайтів ми розуміємо, що у разі коли людина має намір займатися цілком дозволеною(легальною) діяльністю вона вказує свої дані при реєстрації сайту (ім'я, прізвище, адресу, контактний телефон), однак спробував перевірити сайти які займаються забороненою діяльністю, наприклад www.radarix.com (на даний час сайт закритий) встановити власника неможливо оскільки будь-які відомості нього відсутні. Вказаний сайт надавав платні інформаційні послуги (бази даних податкової служби, МВС, БТІ та інших) про фізичних та юридичних осіб України та Росії.

Всупереч потужності Інтернету - або саме внаслідок цієї потужності - уряди багатьох країн намагаються обмежити його використання. Спрямована на обмеження свободи висловлювань в Інтернеті діяльність урядів набуває різноманітних форм.

Так, деякі уряди поставили певні типи висловлювань в Інтернеті поза законом. Кримінальна відповідальність передбачається законами, де заявлена мета -захистити неповнолітніх від певних матеріалів, котрі розглядаються як «шкідливі». Однак, як недавно вирішив Верховний Суд СІЛА, вимога, щоб автори Інтернету захистили певну верству населення від своїх матеріалів, у дійсності тотожна тотальній забороні цих матеріалів. Деякі країни вже ввели систему ліцензування, яка вимагає, щоб користувачі Інтернету або провайдери погодились утримуватись від розповсюдження матеріалів певного характеру або блокувати доступ до таких матеріалів; це є необхідною умовою для того, щоб користуватись Інтернетом або надавати до нього доступ. Китай встановив правила, згідно з якими будь-хто, маючий доступ в Інтернет, зобов'язаний утримуватись від розповсюдження заборонених матеріалів. Сингапурське Бюро Інформації вимагає, щоб усі провайдери, згідно з ліцензією, блокували доступ до зарубіжних сайтів та новинних груп, які визнано шкідливими для національних звичаїв. Деякі уряди зобов'язують на примусове використання фільтруючих, рейтингових або маркуючих зміст приладів. Блокування, фільтрування та маркування інформації можуть перешкодити особам користуватись Інтернетом для обміну інформацією, що стосується спірних або небажаних тем, можуть сприяти формуванню глобальної рейтингової системи, що її хочуть створити деякі уряди. При цьому блокується доступ до цілих інформаційних галузей певного змісту, до галузей або сторінок, де є окреслені ключові слова або ланцюжки символів у адресі; можливий також перезапис первісної інформації, яку надають ведучі інформаційних блоків та провайдери.

На Інтернет не можна поширювати правила, що розраховані на вже традиційні засоби поширення інформації, як-то телебачення і радіомовлення, оскільки він дозволяє користувачам самостійно здійснювати вибір, контролювати зміст і відсторонювати себе від небажаної інформації, так само як обирати книги за своїми інтересами у публічній бібліотеці. На дорослих користувачів покладається обов'язок керувати вибором і контролювати зміст, який досягає їх дітей. Такі засоби пропонуються в Інтернет як на платній, так і безоплатній основі.

Таким чином, здійснювати державний контроль у мережі Інтернет необхідно, однак межі цього контролю слід чітко окреслити та не допускати будь-яких порушень прав людини та громадянина на право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, на вільне збирання, зберігання, використання і поширення інформації.

Отже, пропоную при підготовці проекту Інформаційного кодексу України (Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 - 2015 роки») до нього включити розділи, зокрема, про засади електронної торгівлі, правову охорону прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у мережі Інтернет, про охорону баз даних, надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг з використанням мережі Інтернет, правила використання всіх видів інформації і комунікаційних технологій в сфері електронної комерції, а також ввести обов'язкову реєстрацію веб-сайтів подібній реєстрації, визначеній у Законі України «Про державну реєстрацію юридичних осіб та фізичних осіб підприємців».

Враховуючи наведене, вирішення питання правового забезпечення поширення інформації мережею Інтернет має бути комплексним, якому обов'язково мають передувати наукові дослідження та вивчення міжнародного досвіду.

4. Правопорушення в мережі інтернет

Глобальна всесвітня мережа, що об'єднує мільйони комп'ютерів у транснаціональну єдину систему Інтернет відкриває широкі можливості спілкування та обміну інформацією. Незважаючи на те, що темпи розвитку інформаційних технологій в Україні через соціально-економічні проблеми ще відстають від потреб сьогодення, наша держава сміливо входить у світовий інформаційний простір. В Україні налічується понад 500 тис. абонентів мережі Інтернет (1 користувач - на 100 громадян, у США відповідно - 25 користувачів, у Європі - 9). З появою мережі Інтернет виник новий тип суспільних відносин - Інтернет-відносини Діяльність у цій мережі створює крім позитиву значну кількість проблем - етнічних, економічних, соціальних і правових.

Щодня велика частина користувачів мережі свідомо і несвідомо стають правопорушниками. У ряді міжнародних нормативно-правових актів визнано, що кіберзлочинність (у т.ч. злочини, що вчиняються у мережі Інтернет) сьогодні становить загрозу не тільки національній безпеці окремих держав, а й загрожує людству та міжнародному порядку в цілому. За розмірами шкоду, що завдається внаслідок вчинення комп'ютерних злочинів, можна порівняти з перевагами, які отримуються від впровадження сучасних комп'ютерних технологій.

Метою статті є розкриття поняття інтернет-злочинності, визначення специфіки правопорушень, що вчиняються у мережі Інтернет, їх видів та форм,

аналіз негативних наслідків даного виду злочинності та розгляд методів боротьби з нею.

Незважаючи на прийняті національні законодавства щодо боротьби з кіберзлочинністю у ряді країн, у тому числі й в Україні, її «уніфікований» склад досі чітко не визначено, оскільки як можливості технічних засобів, програмного забезпечення, засобів телекомунікації, так і кримінальні хитрування самих кіберзлочинців, безперервно зростають з розвитком науково-технічного прогресу і відсталістю правових норм протидії. За останні кілька років було сформульоване поняття «кіберзлочинність», під якою розуміють злочинність у традиційному сенсі цього слова, але яка наявна в мережі Інтернет.

Сфера вчинення інтернет-злочинів - так званий віртуальний простір, який можна визначити як модельований за допомогою комп'ютера інформаційний простір, де містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що перебувають у процесі руху по локальних і глобальних комп'ютерних мережах, або ж відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі.

Однією з основних характеристик інтернет-злочинності є висока латентність (як природна, так і штучна, що виникає через небажання потерпілих повідомляти про злочини правоохоронним органам). Офіційна статистика правоохоронних органів не відображає вірогідної картини стану правопорушень, що вчиняються у мережі Інтернет, або за її допомогою, як на рівні держави, так і на загальносвітовому рівні. Для оцінювання стану такого виду злочинності необхідно використовувати інші способи одержання даних, такі як інтерв'ювання, фокусні групи, огляди, а також метод «реєстрації звернень» - віктимологічний метод, що полягає у збиранні відомостей про злочини від потерпілих. Використання цих методів поряд з аналізом офіційної статистики дає змогу дослідити масштаби інтернет-злочинності та її тенденції з урахуванням злочинів, що залишилися за рамками зареєстрованих правоохоронними органами антигромадських діянь.

У цілому специфіка злочинності в мережі Інтернет полягає у такому:

- відносній комфортності, тобто готування та скоєння злочину здійснюється практично не відходячи від «робочого місця»;

- доступності - у зв'язку з тенденцією постійного зниження цін на комп'ютерну техніку;

- широкій географії скоєння злочинів, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає «левова частка» злочинності;

- віддаленості об'єкта злочинних посягань - він може перебувати за тисячі кілометрів від місця скоєння злочину;

- складності виявлення, фіксації і вилучення криміналістично-значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її в якості речового доказу і т. ін.;

- широкому використанні злочинцями засобів шифрування інформації.

Для розуміння процесів, що перебігають в такому складному негативному соціальному явищі, як інтернет-злочинність, необхідно розглянути окремі її підвиди. Найбільш часто здійснюються такі: розповсюдження порнографії, шахрайство та ще некриміналізований спам. Крім зазначених, також існують види, які не мають такого широкого поширення в Інтернет, але сприяють вкрай небезпечним видам злочинності не у віртуальному, але реальному світі - наркозлочинність і тероризм.

Наркозлочинність в мережі Інтернет. Нині наркозлочинність і наркоманія набули міжнародного характеру. Революція в галузі інформаційних технологій призвела до того, що в сучасний період проблема розповсюдження наркотиків у світі дедалі частіше перетинається з можливостями сучасних технологій, у тому числі Інтернет, значення якого в даний час величезне. За допомогою мережі Інтернет у будь-яку точку світу можна надіслати інформацію про купівлю-продаж наркотиків, про нові розробки у виготовленні, культивації, їх транспортування і т.д. мережа Інтернет дає можливість встановлювати контакти між виробниками наркотиків, їх продавцями та клієнтами з географічних пунктів значно віддалених один від одного. Глобальна інформаційна мережа дозволяє також особам, зацікавленим у поширенні наркоманії, залучати користувачів Інтернет у вживання наркотиків безпосередньо і популяризувати субкультури, пов'язані з уживанням наркотиків. Зауважимо, що офіційна статистика щодо наркозлочинності в мережі Інтернет просто відсутня, хоча небезпека даного виду злочинності не підлягає сумніву. В даний час найбільш зручним і поширеним способом пошуку інформації про наркотики є запити через пошукові системи. Дослідження посилань, знайдених за допомогою пошукових машин, свідчать про те, що потрапити на пронаркотичні сайти нескладно.

Таким чином, мережа Інтернет сьогодні, на превеликий жаль, є серйозною підмогою наркозлочинності. У зв'язку з чим важливим представляється застосування крім правової боротьби також громадського контролю за поширенням наркотиків у цій мережі. Зокрема, існує необхідність у таких запобіжних заходах, як розробка ресурсів з профілактики наркоманії на противагу пронаркотичним сайтам, а також створення громадських груп, наприклад, журналістів, для введення добровільних обмежувальних правил публікації в мережі Інтернет матеріалу, який пропагує наркоманію. Також, як превентивні заходи можна запропонувати адміністративні та кримінально-правові заходи впливу на комп'ютерні компанії, що надають місце під сайти, де розміщено інформацію про наркотики.

Терористична діяльність в мережі Інтернет. Інтернет-тероризм - це один з підвидів комп'ютерного тероризму, де комп'ютерною технологією є всесвітньо поширена, залучена практично у всі світові процеси, загальнодоступна технологія Інтернет. Найбільшу небезпеку тероризм у мережі представляє для країн, де відсоток населення, що користується глобальною мережею, перевищує 50 %, і активно використовується не тільки окремими громадянами, а й державними органами, банківською системою, громадськими

та неформальними об'єднаннями. Незважаючи на те, що поєднання інтернет-тероризм поки звучить незвично, його активне впровадження та розвиток у даний час стає реальною загрозою. Тероризм у мережі Інтернет неоднорідний, його можна поділити на дві складові: по-перше, здійснення терактів за допомогою мережі Інтернет і, по-друге, діяльність, що сприяє тероризму, скажімо, вербування в організації, збирання коштів для терористів або організація взаємодії членів терористичних груп. Оцінити співвідношення поширеності терористичної діяльності в кібер-просторі і в реальному світі досить важко, очевидно, що така мережа дає істотні переваги терористичним організаціям. Зі зростанням впровадження глобальної мережі в життя суспільства та його використання в критичних системах зростає ризик віддаленої терористичної атаки.

Інтернет-шахрайство. Шахрайство - один з видів злочинів проти власності. Це злочинне діяння можна охарактеризувати як одне з найпоширеніших. Розглянемо кілька найбільш поширених та небезпечних з них:

- фальшиві рахунки на оплату з Інтернет-магазинів - підроблені рахунки, що розсилаються по e-mail, містять посилання на шкідливі програми. Одержувач, який відкрив рахунок, негайно стає жертвою зловмисних дій;

- шахрайський інтернет-магазин. Ця схема схожа на схему, за якою діють фірми-однодневки. Шахрай відкриває такий магазин, за вигідними цінами пропонує товар. Приймається передоплата, і все - шахрай ховається, привласнивши гроші;

- фітинг - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів. Шахраї використовують усілякі виверти, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані - наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернет, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів;

- кіберсквотинг - протизаконна діяльність, що полягає у реєстрації, використанні та пропонуванні до продажу доменного імені із несумлінним наміром отримати прибуток від паразитування на гудвілі (нематеріальному активі) або торговельній марці, яка належить іншій особі. Після несумлінної реєстрації, реєстрант (кіберсквотер) зазвичай пропонує продати доменне ім'я законному власнику знака за значно вищою ціною;

- крадіжка послуг - правопорушення з отримання несанкціонованого доступу до будь-якої системи, щоб безкоштовно скористатись її послугами. Прикладом даного виду шахрайства є фоунфрейкинг, тобто використання комп'ютера для проникнення в комунікаційну телефонну систему та незаконне використання послуг з надання міжнародного телефонного зв'язку. Інший приклад даного виду злочинів - «stuffraud», або створення нелегальних копій двійників мобільних телефонів;

- підроблені сайти благодійних фондів. «Подайте Червоному Хресту! Допоможіть жертвам урагану Катріна»! Кіберзлочинці - неперевершені майстри викликати жалість і грати на людських трагедіях. Особливо актуальними такі методи відбирання грошових коштів стають у святковий сезон, коли відвідувачі мережі більш охоче розлучаються з грошима;

- Інтернет-кардинг - використання даних з чужої банківської картки для здійснення всіляких операцій у мережі з метою отримання грошей.

Розповсюдження порнографії. Безконтрольне поширення інформації в мережі сприяло широкому розвитку індустрії порнобізнесу. Щорічний грошовий обіг у цій сфері становить 2-2,5 млрд доларів, зрозуміло, що ця цифра стосується абсолютно законного (у США, Голландії та багатьох інших країнах продаж та виготовлення порнопродукції легальні) розповсюдження. Окрім легального і в установленому порядку поширення у деяких зарубіжних країнах порнографії для осіб, які досягли повноліття, глобальна мережа стала розсадником тіньового порнобізнесу. Величезні доходи від тіньового порнобізнесу стимулюють розвиток іншої кримінальної діяльності в мережі Інтернет. Наприклад, незаконний порнобізнес дає роботу великій кількості хакерів і програмістів, що пишуть вірусні програми, оскільки для втечі від правоохоронних органів організатори нелегальних сайтів часто користуються їх послугами. Поширення порнографії у багатьох випадках є досить складним злочином і тому здійснюється цілими групами співучасників, серед яких є представники інтернет-злочинців різних спеціалізацій. Порноіндустрія глобальної інформаційної мережі та інтернет-злочинність нероздільні, про що свідчить також і те, що за останні 4 роки три випуски популярного серед мережевих злочинців журналу «Хакер» присвячені тому, як організувати свій порнобізнес і свою порностудію. У них докладно описано, як налагодити виробництво порнопродукції, як оминути проблеми з законом і які прибутки крутяться в цій сфері діяльності.

Спам. Практично всім, хто користується електронною поштою, доводиться мати справу зі спамом. Але проблема спаму не обмежується переповненими поштовими скриньками, збільшенням трафіку і неприйнятним змістом листів. Спам також застосовується для доставки шкідливого коду; спам-повідомлення часто використовуються як відправна точка для *drive-by* завантажень шкідливих програм, оскільки в них можна включати посилання на веб-сайти, які кіберзлочинці заразили шкідливим кодом. Крім того, спам - основний інструмент, за допомогою якого фішери заманюють своїх жертв на фальшиві сайти, де у користувачів виманюють конфіденційні дані.

Посилка всупереч волі одержувача, вираженої в конкретних діях, має бути юридично заборонена, оскільки є очевидною байдужість спамера до прав іншої людини. Навіть якщо розсилка здійснюється не всупереч волі користувача, тобто без явного вираження невдоволення (наприклад, в перший раз), масова розсилка, яка уповільнює інтернет-трафік, забирає робочий час або призводить до інших негативних наслідків, також є протизаконною. Спамер повинен нести відповідальність за обсяги інформації, що розсилається, і за шкоду, заподіяну його спамом. Отже, небажаними є як розсилка всупереч явно

вираженої волі, так і будь-яка розсилка, яка веде чи здатна призвести до значних наслідків.

Думки з приводу введення кримінальної відповідальності за спам серед науковців і практиків неоднозначні. Противники ідеї введення кримінальної заборони пов'язують це, насамперед, із обмеженими можливостями засобів і методів збирання доказів, проведення слідства, тому що при здійсненні таких дій може бути порушено право спамерів на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, а це суперечить загальній лібералізації та гуманізації суспільного законодавства.

Організація успішної боротьби з злочинністю на магістралях глобальної мережі вимагає, перш за все, розбудови відповідної законодавчої бази. Перші закони стосовно комп'ютерних злочинів були прийняті Швецією (1973), пізніше - у Німеччині, Австралії, Італії, Франції, Іспанії, Канаді, Сполучених Штатах Америки, які найбільше страждають від злочинів у сфері високих технологій. З кінця 80-х рр. з'явилися перші нормативно-правові акти, що регулюють інформаційні відносини в глобальній мережі. Європейський комітет з проблем злочинності Ради Європи підготував рекомендації із метою визначення правопорушень, пов'язаних з комп'ютерами, для включення їх до законодавства європейських країн.

В Україні кримінальну відповідальність за скоєння комп'ютерних злочинів встановлено XVI розділом КК України - відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. До них відносяться: незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361), викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362), порушення правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363).

Родовим об'єктом цих злочинів є суспільні відносини у сфері безпеки комп'ютерної інформації і нормального функціонування електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

Предмет злочину: 1) електронно-обчислювальна машина (ЕОМ) - комп'ютер - комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних задач; 2) автоматизовані комп'ютерні системи (АКС) - сукупність взаємопов'язаних ЕОМ, периферійного обладнання та програмного забезпечення, призначених для автоматизації прийому, зберігання, обробки, пошуку і видачі інформації споживачам. Комп'ютерні системи можуть бути регіонального та галузевого характеру; 3) комп'ютерні мережі (мережа ЕОМ) - це поєднання декількох комп'ютерів (ЕОМ) та комп'ютерних систем, що взаємопов'язані і розташовані на фіксованій території та орієнтовані на колективне використання загальномережових ресурсів. Комп'ютерні мережі передбачають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, які входять до комп'ютерних систем; 4) носії комп'ютерної інформації - фізичні об'єкти, машинні носії, призначені для

постійного зберігання, перенесення і обробки комп'ютерної інформації. До них відносяться гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти тощо; 5) комп'ютерна інформація - це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному виді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися за допомогою ЕОМ (комп'ютерів).

Об'єктивна сторона цих злочинів може виражатися в активних діях (наприклад, у незаконному втручанні в роботу автоматизованих електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж, у розповсюдженні комп'ютерного вірусу (ст. 361), а також у злочинній бездіяльності, наприклад, при порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж (ст. 363).

Об'єктивна сторона цих злочинів - не тільки вчинення суспільно небезпечного діяння (незаконне втручання в роботу ЕОМ, викрадення, привласнення комп'ютерної інформації тощо), а й настання суспільне небезпечних наслідків (перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, заподіяння істотної шкоди власнику ЕОМ (комп'ютерів), систем та комп'ютерних мереж (ч. 2 ст. 361)). При цьому вимагання комп'ютерної інформації може розглядатися і як злочин з формальним (і усіченим) складом.

Суб'єктивна сторона цих злочинів передбачає, як правило, умисну вину. Хоча можлива і необережність - при порушенні правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363).

Мотиви і цілі можуть бути різними - помста, заздрість, прагнення до володіння інформацією. Якщо ж, наприклад, викрадення інформації, вчиняється з корисливих мотивів і містить ознаки складу шахрайства, вчинене слід кваліфікувати за сукупністю злочинів - за статтями 362 і 190.

Суб'єкт цього злочину - будь-яка особа, а у деяких випадках суб'єкт спеціальний - службова особа (ст. 362), особа, відповідальна за експлуатацію ЕОМ (ст. 363).

Таким чином, законодавство у сфері регулювання комп'ютерних відносин не є досконалим і має значну кількість прогалин. Для чіткого правового регулювання суспільних відносин, що виникають у зв'язку з використанням глобальної мережі Інтернет, є необхідним:

- конкретизація та уніфікація таких правових категорій, як: віртуальний простір, інтернет-суспільство, інтернет-відносини, інтернет-злочинність та перманентна підтримка усіх законодавчих актів, що регулюють інтернет-відносини в актуальному стані, адже сучасні інформаційні технології розвиваються шаленими темпами;

- законодавче визначення класифікації інформаційних прав громадян у мережі Інтернет, з'ясування характеру та особливостей правозастосування

юридичних норм, що регулюють діяльність користувачів цієї мережі в Україні і, насамперед, її UA-сегмента;

- законодавче визначення меж державного втручання у суспільні відносини, пов'язані з використанням мережі Інтернет;

- розширення дій кримінальної відповідальності за протиправне використання можливостей мережі Інтернет (розповсюдження нелегального матеріалу, несанкціоноване перехоплення інформації, комп'ютерний саботаж тощо);

- посилення правового забезпечення безпеки інформаційних систем, а також відповідальність адміністраторів баз даних та інших посадових осіб, які забезпечують експлуатацію комп'ютерних інформаційних систем.

5. Міжнародно-правові аспекти управління Інтернетом

Управління Інтернетом являє собою розробку і застосування урядами, приватним сектором і громадянським суспільством, у своїх відповідних ролях, загальних принципів, норм, правил, процедур прийняття рішень і програм, що регулюють еволюцію і застосування Інтернету

Робоча Група з Управління Інтернетом (WGIG), 2005

Сучасний світ не можна уявити без інформаційно-комунікаційних технологій, що стали невід’ємною складовою частиною повсякденного життя. Серед найбільш вживаних технологій поряд з мобільним зв’язком стоїть Інтернет, що перетворив кожного з його користувачів на мешканця кіберпростору – «умовного середовища, всередині якого відбувається електронний зв'язок, що сприймається як реальний спостерігачем, але породжений комп’ютерною системою та не має реального існування; простору віртуальної реальності».

Відносини між людьми, що існували у реальному світі, знайшли своє відображення у цьому новому віртуальному світі завдячуючи трансляційно-комунікативним властивостям Інтернету, які постійно вдосконалюються та розширюють можливості для спілкування і взаємодії незалежно від фізичних параметрів відстані й часу, усувають соціальні, мовні, культурні та інші розбіжності та перешкоди.

За стрімким розвитком Інтернету та соціальних відносин, глобальним медіумом яких він виступає, ледве встигає правове рулювання як на державному, так і міжнародному рівнях. Взаємозв’язок між технічними, соціальним та політико-правовими аспектами є настільки явним, що політико-правові рішення, що стосуються Інтернету, прийняті на рівні окремих держав зачіпають інтереси всієї міжнародної спільноти. А технічні чи технологічні рішення, що стосуються інфраструктурних питань Інтернету неминуче мають міжнародні політичні наслідки.

Справедливо зазначається, що «атрибути кібер-простору, такі як, транснаціональність, миттєвість і доступність, на національному та інших рівнях ускладнюють регулювання для реалізації та забезпечення дотримання. Соціальне регулювання у сучасному суспільстві розвивалося всередині

фізичних кордонів часу та простору. Розвиток кібер-простору дистанцією його мешканців від місцевого контролю та матеріальних атрибутів громадянства, суверенітету та державності. Це викликає потребу у регуляторних рішеннях, що виходять за межі старих парадигм, та популярність таких функцій як самоорганізація та соціальна взаємодія, аніж інстутиційна влада».

Все це обумовлює необхідність осмислення сучасних глобальних інформаційно-комунікаційних відносин та вирішення актуальних питань їх регулювання за допомогою як правових, так і інших технічних, технологічних, організаційних , саморегулятивних інструментів тощо.

Наявний комплекс питань, викликаних появою та розвитком Інтернет, що потребує вирішення міжнародною спільнотою за допомогою міжнародно-правового регулювання, на нашу думку, можна умовно розділити на дві групи. До першої – належать політико-правові аспекти регулювання функціонування та розвитку інфраструктури Інтернету як глобальної інформаційно-комунікаційної мережі. До другої – спеціальні правові питання, що можна охарактеризувати як цивілізаційні «виклики», що привніс Інтернет по відношенню до вже традиційних комунікаційних та медіа засобів, таких як пошта, телефонний зв'язок і телебачення. Останнє пов’язано, насамперед, з дігіталізацією пристроїв та конвергенцією технологій, що викликає потребу перегляду вже існуючих міжнародно-правових актів з метою приведення їх у відповідність до вимог часу. Ця тема буде нами докладно розглянута нами пізніше.

Наразі зупинимось на питаннях, що виникають у зв’язку із функціонуванням та розвитком інфраструктури Інтернету, серед яких ключовим та найбільш актуальним є організаційно-правові засади управління Інтернетом.

У чому полягає актуальність цієї теми, які проблеми в управлінні Інтернет на сьогоднішній день потребують вирішення за допомогою міжнародно-правових інструментів, які шляхи та моделі для цього можуть бути обрані? Спробуємо надати відповіді на зазначені питання. Для аналізу сучасних проблем в управлінні Інтернетом слід повернутися до витоків Інтернету, розглянути його розвиток та зрозуміти зв’язки між ключовими політичними гравцями задіяними в цьому процесі.

Інтернет виник з мережі APRANET (Advanced Research Project Agency Netrwork) Департаменту оборони США, яка була запроваджена у 1969 році з чотирма вузлами зв’язку. Проект мав за мету віднайти метод забезпечення збройних сил та уряду США зв’язком після ядерної війни, під час якої були б зруйновані традиційні телекомунікаційні центри та мережі. За первинною концепцією, система повинна була зв’язати кілька вузлів. Повідомлення розділялися на т.зв. «пакунки», кожний з яких мав адресу призначення та власну позицію у цілому повідомленні, а після досягнення місця призначення відновлювалися в ціле. При цьому маршрут просування окремих «пакунків» через «вузли» визначався випадково та проходив через доступні мережі. Зазначена концепція була втілена в комунікаційний стандарт-протокол

(TCP/IP), що був успішно застосований на основі APRANET 1 січня 1983 року, звідки розпочинається ера Інтернет.

Незважаючи на те, що Інтернет виник як військово-технічний проект США, що обумовило сьогоднішню архітектуру цієї мережі та кодову основу як спадок, його ключові регулятори та політичні захисники залишаються здебільше приватними та неприбутковими структурами, короткий огляд яких подається нижче.

Суттєвий внесок у розбудову структури Інтернет внесла неприбуткова організація Інтернет Суспільство (**ISOC**), що була створена у 1992 році в США. ІС включає в себе представник різних спільнот, технічних спеціалістів, вчених, учасників телекомунікаційного бізнесу, громадського сектору тощо. Частиною ISOC після приєднання у 1992 році стало Правління Архітектурою Інтернет (**IAB-Internet Architecture Board**), організація створена раніше у 1983 році [6]. До компетенції IAB віднесено наглядання за архітектурою протоколів та процедур, що використовуються в Інтернет; процедурою створення стандартів Інтернет; публікацією т.зв. «запитів для коментарів» (Request for Comments); надання консультацій з різних регуляторних, технічних та процедурних питань, пов'язаних з Інтернет та його технологіями. Більшість з членів IAB входить до інших керівних органів, зокрема, до Цільової Групи з Інтернет Проектування (**IETF – Internet Engineering Task Force**).

IETF без перебільшення можна назвати міжнародною спільнотою дизайнерів мереж, операторів, торговців та дослідників, що об'єднані спільним інтересом у функціонуванні та розвитку Інтернет. Робочими групами IETF проводиться кропітка робота з таких питань як маршрутизація, стандарти та транспортування, що оформлюється після опрацювання на вищому рівні керівною групою (**Internet Engineering Steering Group**) та направляється до ISOC як Рекомендовані Стандарти.

Дослідження з таких питань як протоколи, застосування, архітектура та технології Інтернет проводяться Цільовою Групою з Дослідження Інтернет (Internet Research Task Focre), очільник якої призначається IAB. За межами структури ISOC дослідженнями цих питань займається також Консорціум Всесвітньої Мережі (**W3C - World Wide Web Consortium**), заснований у 1994 році.

Ключовою організацією з управління Інтернет, яка також заснована в Сполучених Штатах у 1998 році, є на сьогоднішній день, Інтернет Корпорація Призначених Назв та Номерів (**ICANN – Internet Corporation for Assigned Names and Numbers**). ICANN відповідає за розміщення адрес в кіберпросторі , передачу протокольних параметрів, управління доменними іменами та функціями кореневих серверів.

Дозволимо зробити короткий екскурс в недалеку історію, щоб дати уявлення про генезис цієї організації. Раніше функції адміністрування адресного простору в Інтернет виконувалось за контрактом між Урядом США та організацією **IANA – Internet Assigned Numbers Authority**. Модель регулювання передбачала наявність одного міжнародного провайдера системи доменних імен (DNS), якою являлась корпорація Network Solution Inc. для

gTLD - глобальних доменів верхнього рівня (.com, .net, .gov, .edu, .org). Слід зазначити, що після 1994 року відбувся досі не бачений бум розвитку Інтернет, завдяки поширенню аплікацій кібер-простору – WWW.

Стрімке збільшення чисельності користувачів супроводжувалось лавиною нових доменних імен. Реєстрація нових доменних імен зросла з 300 на місяць у 1992 році до 45.000 щомісячно у 1995 році. З 1995 по 1996 рік кількість зареєстрованих доменних імен зросла з 150.000 до 637.000, з яких 60% становили – «.com». При цьому, реєстраційний збір утримувався приватною неприбутковою корпорацією Network Solutions, Inc (NSI) на підставі 5-річної угоди про співробітництво з Національною Науковою Фундацією (NSF) США.

Комерціалізація адресного простору в Інтернет викликала суттєвий політичний тиск з боку ISOC, Європейської Комісії та міжнародних організацій на Уряд США. Якщо в середовищі технічних спеціалістів ISOC панували економічні мотиви та намагання зберегти контроль на «їхнім» Інтернет, Європейська Комісія намагалась здобути політичний вплив на регулювання Інтернет та покласти ці функції на міжнародну організацію, зменшивши регуляторну монополію Сполучених Штатів.

Саморегулювання приватного сектору як концепція регулювання Інтернет активно просувається адміністрацією президента Клінтона у цей період. Її втілення в адміністрування адресного простору Інтернет знайшло в т.зв. «Білому документі з управління Інтернет».

Хоча політичні мотиви обрання саме такого підходу знаходяться в іншій площині. Як зазначає M. Mueller, «галузева саморегуляція» була ширмою для процесу, що може бути точніше описаний як «закулісна» гра між двома основними гравцями – приватним та державним, обидва з яких представляли інтереси США.

Тим самим, було відкинуто пропозиції Європейської Комісії покласти функції регулювання Інтернет на міжнародну організацію. Покладення цієї функції на організацію «приватного сектора» - ICANN технічно позбавляло Європейську Комісію можливості брати безпосередню участь та впливати на рішення, проте за Сполученими Штатами залишилися важелі впливу на будь-яку організацію «приватного сектора», що до цього часу опікувалася проблема регулювання Інтернет та знаходиться під їх юрисдикцією.

У 2009 році між ICANN та Департаментом торгівлі США було підписано т.зв. «Підтвердження Зобов'язань» (**Affirmation of Commitments**), згідно з яким сторони підтвердили незалежний статус ICANN та прагнення сприяти міжнародній участі в технічній координації системи доменних імен (**DNS**).

Білий документ з управління Інтернет закликав ICANN та ВОІВ створити механізм вирішення спорів, щоб система доменних імен не створювала можливостей для порушення прав власників товарних знаків. Таким чином, на ICANN було покладено суттєві регуляторні та право-забезпечувальні функції, пов'язані із інтелектуальної власністю, що споконвічно належали до урядових повноважень; а до вироблення політики щодо управління Інтернетом долучились представники індустрії інтелектуальної власності.

ICANN затвердив політику щодо вирішення спорів стосовно доменних імен (**UDRP**) у жовтні 1999 року. Тим самим було запроваджено глобальний, єдиний процес вирішення спорів між власниками товарних знаків та реєстрантами доменних імен. Вирішенням спорів займаються призначені ICANN організації, серед яких значиться також Центр арбітражу та посередництва ВОІВ.

Під впливом лобіювання з боку індустрії інтелектуальної власності Конгресом США у 1999 році було прийнято законодавчі зміни, якими запроваджувалось покарання за т.зв. «кібер-сквотинг» (навмисну, недобросовісну та оманливу реєстрацію доменних імен) та поширювався правовий захист товарних знаків на сферу присвоєння доменних імен, що легітимізувало політику, запроваджену ICANN.

Політика UDRP, на думку багатьох дослідників, вже давно потребує перегляду. У документі, нещодавно підготовленому спільнотою некомерційних користувачів (NCUC), що входить до правління ICANN в складі GNSO, наголошується на необхідності розгляду цього питання не у вузькому колі експертів, а в рамках існуючих процедур GNSO.

Під впливом міжнародної громадськості та інших політичних гравців, зокрема ЄС, відбувається активне обговорення необхідності передачі важелів контролю, що історично були в руках Уряду Сполучених Штатів, до ширшого кола керманичів , що колективно представлятимуть глобальні спільноти технічних спеціалістів та користувачів Інтернет. Наразі триває активна міжнародна дискусія щодо реформування управління ICANN, яке залишається недостатньо прозорим та представницьким з точки зору досягнення глобальних цілей розвитку Інтернет.

Існуючим станом справ з регулюванням Інтернет незадоволена Європейська Комісія. У зверненні до Європарламенту та Ради про організацію та управління Інтернет та резолюції Ради у 2000 році зазначалось про необхідність досягнення збалансованого та рівного наглядання за з боку публічної влади, визначення правил управління діяльністю ICANN загальними доменами та розділення діяльності реєстрів та реєстраторів, а також передачі адміністрування системою кореневих серверів від Департаменту торгівлі США до ICANN під належним наглядом публічної влади.

У червні 2009 року вимоги Європейської Комісії стають більш чіткими та системними. У зверненні «Інтернет урядування: подальші кроки» зазначається, що Інтернет став критично важливим ресурсом для усього світу та особливо для ЄС, з огляду на повсякденне користування його послугами звичайними користувачами, бізнесом та урядами. А тому надійність Інтернет має забезпечуватися не тільки Інтернет організаціями, що відповідальні за координацію ресурсів.

Не відкидаючи важливість участі приватного сектору у конструюванні та щоденному адмініструванні Інтернет, з чим, на думку Європейської Комісії, приватний сектор справляється добре, наголошується на очікуванні користувачами від їх держав правових гарантій забезпечення дотримання загальносуспільних інтересів, що не будуть знехтуванні на користь

комерційним або регіональним інтересам під час визначення майбутнього управління Інтернет.

Ключовими принципами управління Інтернет визначено: безпеку та стабільність, повагу до прав людини, свободи вираження поглядів, приватності, захист персональних даних та сприяння культурній та мовній різноманітності. До цього додаються ключові принципи, що забезпечують розвиток Інтернет:

- відкрита, сумісна та сітьова (‘end-to-end’) фундаментальна основа архітектури Інтернет повинна поважатися;

- участь приватного сектора у– повсякденному адмініструванні Інтернет повинна підтримуватися приватними організаціями відповідальним за координацію Інтернет ресурсів, що мають бути підзвітними міжнародній спільності за свою діяльність. Роль держав повинна в основному сфокусуватися на принципах вироблення політики та не опікування повсякденною діяльністю Інтернет;

- багатосторонній процес управління Інтернетом продовжує забезпечувати ефективний та недискримінаційний механізм глобальної кооперації та заслуговує на подальшу підтримку;

держави потребують повної взаємодії з– цим багатостороннім процесом, а зацікавлені сторони мають визнавати, що держави, в кінцевому рахунку, відповідальні за вироблення та впровадження державної політики;

- домовленості з управління Інтернетом повинні бути на недискримінаційній основі, адресувати нагальну потребу покращення участі країн, що розвиваються, у ключових форумах з прийняття управлінських рішень

Нарікання Європейської Комісії викликає той факт, що ICANN до цього часу є зовнішньо підзвітним лише уряду Сполучених Штатів на підставі Угоди про Спільний Проект (Joint Project Agreement) та контракту про технічне адміністрування IANA, в той час як адміністрування файлів кореневих серверів є питанням надзвичайної важливості не лише для уряду США, але й для усіх країн світу.

Відзначаючи відсутність міжнародного консенсусу щодо створення нової міжнародної організації для виконання наглядових функцій або покладення такої відповідальності на будь-яку існуючу організацію, Європейська Комісія не виключає можливості використання альтернативного підходу, щоб зробити ICANN зовнішньо підзвітною таким чином, що кожний уряд (держава) зможе у своїх власних інтересах здійснювати обов’язки відповідно до свого рівня компетенції. Існуючий механізм, коли Урядовий Дорадчій Комітет (GAK) дає пораду приватній корпорації, на думку Європейської Комісії, не є ефективним засобом здійснення державної політики. А односторонній нагляд стосовно ICANN та IANA з боку Сполучених Штатів має бути замінений на інший механізм для забезпечення багатосторонньої підзвітності ICANN.

За концепцією Лессіга, порядок та контроль в Інтернет забезпечується завдяки технічному дизайну (архітектурі) системи, ненормативному регулюванню та національному законодавству. На його думку, Інтернет не тільки формується через «код», на якому він побудований, але також розвиток

«коду» дозволить комерційному сектору опанувати «досконалим засобом контролю» за «підтримки держави».

Проте, такий підхід, що покладає функціональний детермінізм в основу розвитку регулювання Інтернет, входить у протиріччя з такими властивостями сучасних глобальних комунікацій як децентралізоване функціонування, відкритість і свобода вибору, без яких неможливий соціальний розвиток. У тоталітарних суспільствах обмеження вільного руху інформації через глобальні комунікації є поширеною практикою, що втілює цензуру за допомогою технічних засобів та співпраці з лояльним бізнесом.

Необхідність підпорядкування технічних регуляторів визначеним політичним цілям та пріоритетам, що повинні закладатися в архітектуру мережі та код (протоколи, стандарти, процедури), вимагає впровадження механізмів політичного контролю за технічною складовою розвитку Інтернет. Як зазначає Курбалія, «всякий раз, коли це можливо, принципи, такі як свобода комунікацій, повинні чітко проголошуватися на політичному рівні, а не мовчазно припускатися на технічному рівні. Технологічні рішення повинні посилювати політичні принципи, а не залишатися лише єдиним шляхом їх просування».

Саморегуляція приватного сектору здійснюється, як правило, шляхом складання кодексів поведінки або сумлінної бізнес-практики. Попри те, що саморегуляція є корисним засобом для регулювання поведінки учасників всередині ринку, застосування її до чутливих публічних питань, зокрема, регулювання змісту інформації (контенту) в кіберпросторі (WWW) та інших питань, що стосуються фундаментальних прав та свобод користувачів, на нашу думку, без належного контролю з боку держави не є виправданим. Ця сфера має прямий зв'язок з публічними функціями держави, а тому якщо держава делегує певні регуляторні функції приватному сектору, така діяльність має бути настільки прозорою та підзвітною, щоб не викликати жодних сумнівів у її відповідності публічним інтересам.

Покладання регуляторної функції на комерційний сектор, що здебільше орієнтований на прибутковість інвестицій в телекомунікаційному секторі, на нашу думку, не відповідатиме у повній мірі інтересам розвитку Інтернету як глобального медіуму. Його цінність (*vs* «ціна») вимірюється не капіталізацією інвестицій у телекомунікаційну інфраструктуру, а доданою вартістю, що створюється в його середині, у т.зв. кіберпросторі, соціальними комунікаціями. Орієнтація саме на ціннісний підхід, на наш погляд, дозволить визначити оптимальну «формулу» для регулювання Інтернет.

Робочою групою з управління Інтернетом (WGIG) , що була створена під час роботи ВСІС, було запропоновано чотири моделі управління інфраструктурою. За першою моделлю, при ООН створюється Глобальна Рада Інтернет (GIC), в якій держави є членами, а представники приватного сектора та громадського сектору входять з правом дорадчого голосу. ICANN стає підзвітним GIC. За другою моделлю, взагалі не створюється спеціальної організації для контролю за ICANN. При цьому, посилюються дорадчі функції GAC, а міжнародна дискусія щодо розвитку Інтернет ведеться в рамках

форуму, в якому беруть участь державний, приватний та громадський сектори. За третьою моделлю створюється Міжнародна Рада Інтернет, в якій беруть участь держави на правах членів, а приватний та громадський сектор виступають лише з дорадчим голосом. Цій організації стає підзвітним ICANN, проте його роль залишається незмінною.

Нарешті за четвертою із запропонованих моделей, пропонується розділити функції політичні , управлінські та контрольні. Модель передбачає наявність глобального форуму з учасниками з трьох секторів, Глобальної Ради з Політики Інтернет (GIPC), в якій членами є держави, а приватний та громадський сектор є спостерігачами; а також Наглядового Комітету, який призначається GIPC та уповноважується наглядати за ICANN.

Як вбачається із запропонованих моделей, жодна з них не змінює функції ICANN, не трансформує його в багатосторонній орган та не посилює вплив держав на прийняття ним рішень. Запропоновану участь приватного та громадського сектору на правах дорадчого голосу або спостереження в керівному органі (GIC, IIC або GIPC) також не можна вважати ефективною формою збалансованого представництва.

13 вересня 2011 року уряди трьох країн - Індії, Бразилії та Південної Африки (IBSA) зробили спільну заяву, у якій закликали до створення «нового глобального органу» з управління Інтернетом. Цей орган, на їхню думку, повинен:

«i) бути розташованим в рамках системи ООН; ii) виконувати завдання з розробки і запровадження міжнародної публічної політики з метою забезпечення координації та узгодження наскрізних глобальних питань, пов’язаних з Інтернетом; iii) інтегрувати та контролювати органи відповідальні за технічне та операційне функціонування Інтернету, включаючи запровадження глобальних стандартів; iv) вирішувати питання розвитку, що стосуються Інтернету; v. здійснювати арбітраж та вирішувати спори, якщо необхідно, та vi) нести відповідальність за кризове управління».

Проте, незважаючи на проголошену спрямованість на багатосторонність управління Інтернетом, рекомендація не містить жодного натяку на участь в цьому процесі громадянського суспільства та приватного сектора, що не дозволяє її сприймати як дійсно демократичну ініціативу, а не чергову спробу взяти Інтернет під державний контроль.

Слід наголосити, що в Женевських принципах інформаційного суспільства (ВСІС) питання повної і дієвої участі усіх зацікавлених сторін в управлінні Інтернетом, з урахуванням їх компетенції та повноважень у відповідних сферах впливу, є ключовим:

«49. Управління Інтернетом охоплює як технічні питання, так і питання державної політики, та повинно залучати всі зацікавлені сторони і відповідні міжурядові і міжнародні організації. У зв'язку з цим визнається, що:

а) політичні повноваження з пов'язаних з Інтернет питань державної політики є суверенним правом держав. У них є права і обов'язки щодо пов'язаних з Інтернет питань міжнародної політики;

б) приватний сектор відіграє і повинен продовжувати відігравати важливу роль у розвитку Інтернет, як в технічній, так і в економічній сферах;

с) громадянське суспільство також відіграє важливу роль в питаннях Інтернету, особливо на рівні громад, і повинно продовжувати грати таку роль;

г) міжурядові організації відіграють і повинні продовжувати грати роль, сприяючи міждержавній координації з питань, пов'язаних з Інтернет;

е) міжнародні організації також відіграють і повинні продовжувати грати важливу роль у розвитку технічних стандартів і відповідної політики стосовно Інтернету».

Альтернативною моделлю управління Інтернетом може бути багаторівнева система, що включає такі складові: верхній рівень – багатосторонній політичний представницький орган, що включає основних політичних учасників (держави, регіональні організації, представників ІКТ-індустрії, громадянське суспільство - спільноти користувачів); виконавчий орган – секретаріат, до якого делегуються представники багатостороннього представницького органу та входять представники технічного органу. Виконавчий орган укладає контракти з регіональними реєстраторами, технічними виконавцями – адміністраторами адресного простору і є підзвітним представницькому органу; технічний орган (на основі ICANN), до складу якого входять представники регіональних реєстраторів, технічні спеціалісти, що координують технічні питання, які виносяться на розгляд та затвердження виконавчому органу, а у разі необхідності прийняття політичного рішення, - на розгляд та прийняття представницьким органом.

Таким чином, забезпечується багатосторонність, пропорційність представництва, прозорість і підзвітність діяльності та оперативність вирішення організаційно-технічних питань. Принципи та пріоритети розвитку інфраструктури Інтернету повинні бути закріплені в міжнародно-правовій угоді. В загальній частині міжнародно-правової угоди мають знайти закріплення принципи розвитку інформаційного суспільства, зокрема, ті, що містяться в документах ВСІС. До компетенції цієї організації слід також віднести розробку нових міжнародно-правових угод в інформаційно-комунікаційній сфері, координацію діяльності з розробки та внесення змін до існуючих міжнародно-правових актів. Серед можливих варіантів для «інтернаціоналізації» ICANN розглядається також структура Міжнародного союзу електрозв’язку.

Питання розвитку комунікацій є ключовим у діяльності Міжнародного союзу електрозв’язку, основною метою, якого є підтримання та розширення співробітництва між учасниками з метою удосконалення та раціонального використання усіх видів електрозв’язку.

Регламент межнародного електрозв’язку (International Telecommunication Regulations) Міжнародного союзу електрозв’язку дополнює його Статут та Конвенцію адміністративними положеннями. Регламент міжнародного електрозв’язку був підписаний понад 20 років тому, 9 грудня 1988 року у Мельбурні на Всесвітній адміністративній конференції з питань телефонного та телеграфного зв’язку (WATTC-88) та вступив у силу з 1 липня 1990 року.

Метою Регламенту є спрощення «глобального взаємозв’язку та сумісності» транскордонного телекомунікаційного трафіку. Регламент встановлює правила з усіх аспектів обміну телекомунікаційним трафіком, обліку та розрахунків, безпеки, відповідальності та оподаткування. Крім того, були досягнуті так звані «Спеціальні угоди». Цей документ відіграв важливу роль у забезпеченні швидкого зростання обміну трафіком по Інтернет-протоколу (IP), використанні віртуальних приватних мереж, а також надання додаткових послуг.

На той час ринок телекомунікацій не був лібералізований, і у більшості країн існувала монополія держави у цьому секторі. Міжнародна угода у цій сфері була корисною і необхідною для того, щоб телекомунікаційні оператори могли здійснювати зв’язок з усім світом. Як приклад, що показує масштаб проблеми, можна навести той факт, що під час узгодження договору в 1988 р. тільки американські телекомунікаційні компанії щорічно обмінювалися трафіком на суму 12 млрд. дол стаціонарними мережами. Наявність чітких правил, що гарантують доступ на ринок, було дуже важливим для роботи глобальних телекомунікаційних мереж. Цей договір надав приватним телекомунікаційним операторам фундаментальну глобальну основу, що гарантує сумісність (без необхідності отримання погоджень або ліцензій в кожній країні), а також гарантував спрямування доходів до національних бюджетів за допомогою платежів по врегулюванню розрахунків. Незважаючи на те, що Регламент міжнародного електрозв'язку (Регламент МЕЗ) був узгоджений в епоху державних телекомунікаційних монополій, існують деякі положення, які підтвердили свою важливість для зростання глобального Інтернету, зокрема, позарегламентний юридичний механізм, передбачений у «Спеціальних угодах», що визначає спосіб передачі Інтернет-трафіку глобальними мережевими операторами.

Обсяг міжнародного трафіку (голосового по стаціонарним лініях), за якого укладався Регламент у 1988 році, одразу почав різко скорочуватися, що негативно відбилося на доходах телефонних компаній, як державних, так і приватних.

Перегляд Регламенту МЕЗ запланований під час проведення Всесвітньої конференції міжнародного електрозвязку (WCIT-2013), що відбудеться у м. Дубаї в грудні 2013 року, організацією якої займається робоча группа Ради МСЕ, що є відповідальною за проведення низки глобальних та регіональних підготовчих засідань для узгодження пропозицій. Серед пропозицій, внесених окремими державами-членами МСЕ для розгляду та включення до оновленого Регламенту МЕЗ такі:

- обов’язкова імплементація положень Рекомендацій у внутрішньодержавне законодавство з метою їх дотримання приватними операторами;
- контрзаходи проти спаму (включаючи боротьбу зі спамом), а також інших пов'язаних з цим проблем, таких як фішинг, шкідливі програми і коди і т. д.;
- врегулювання спорів;

- домовленість щодо обміну даними та вплив на вартість міжнародного Інтернет-трафіку;
- неправильна виділення ресурсів номерів, найменувань і адрес, а також ідентифікація абонентів;
- якість обслуговування;
- кібербезпека, включаючи безпеку даних, переданих сигналів, даних про трафік, а також даних про рахунки;
- правильне використання моделей виставлення рахунків та оплати;
- захист персональних даних;
- управління «новими технологіями»;
- захист дітей в Інтернеті, а також
- виділення та розподіл Інтернет-адрес.

Наразі триває обговорення цих пропозицій у робочому порядку, у тому числі на європейському регіональному рівні. Зокрема, у цій роботі бере участь така спеціалізована організація як Європейська конференція адміністрацій пошт і електрозв'язку (СЕРТ).

Діяльність СЕРТ, що була заснована у 1959 році, включає співробітництво у промислових, експлуатаційних, регулюючих питаннях, а також у технічних питаннях стандартизації сектора зв'язку. На цей час СЕРТ об'єднує 48 регулюючих органів країн європейського регіону (Адміністрація зв'язку України є членом СЕПР), що займаються стратегічним плануванням у цій сфері.

СЕПТ, зокрема, підготовлено 5 критеріїв, за якими оцінюються пропозиції, для їх подальшої рекомендації для прийняття або відхилення під час WCIT-2013:

Критерій 1. Загальна відповідність ключовим принципам щодо змісту Регламенту МЕЗ

- містити стратегічні та політичні питання високого рівня, що стосуються міжнародних телекомунікаційних послуг та засобів;
- забезпечувати права телекомунікаційних операторів та постачальників послуг здійснювати комерційний вибір та їх операційна на технічна свобода брати участь у міжнародному електрозв'язку.

Крітерій 2. Відповідність положенням Преамбули та Статті 1 Конституції Союзу. У цьому критерії наголошується, що Конституція Союзу не надає Рекомендаціям МСЕ обов'язкової сили, Рекомендації МСЕ за своєю природою не є обов'язковими, а мають застосовуватися на добровільній основі. У зв'язку з цим робоча група (СЕРТ) вважає, що перегляд Регламенту МЕЗ не повинен змінювати природу Рекомендацій МСЕ.

Критерій 3. Відповідність міжнародним угодам / законодавству, прийнятому членами СЕПТ, зокрема:

- відповідати Четвертому Протоколу Угоди СОТ;
- оцінюватися з урахуванням положень законодавства Європейського Союзу про електрозв'язок

Критерій 4. Не зачіпати сфери, у який застосовуються правові та політичні принципи, що перебувають виключно у межах суверенних прав

Держав-учасниць. СЕПТ оцінює пропозиції, що стосуються національної безпеки, оборони, контенту та кіберзлочинності в контексті Резолюції 130, в редакції ухваленій на Повноважній конференції МСЕ у Гвадалахарі у 2010 р.: «МСЕ повинен зосередити ресурси і програми на тих галузях кібербезпеки, які відповідають його основному мандату та досвіду, особливо у технічній сфері і сфері розвитку, та не включати галузі, що відносяться до застосування Державами-членами правових та політичних принципів, повязаних з національною обороною, національною безпекою, контентом та кіберзлочинністю, які відносяться до їхніх суверенних прав».

Критерій 5. Виключення сфер, що не відносяться до цілі та предмету Регламенту МЗЕ. За цим критерієм, пропозиції щодо внутрішньодержавних (національних) послуг електрозв'язку або транспортування не повинні міститися у Регламенті. Це пов'язано із положеннями Преамбул як Статуту МСЕ, так і Регламенту, які повністю визнають «суверенне право кожної Держави регулювати свій електрозв'язок».

Наразі триває активне обговорення в робочих групах зазначених пропозицій щодо можливого поширення компетенції Міжнародного союзу електрозв'язку на низку політико-правових питань управління Інтернетом. Однак можна прогнозувати, що відсутність консенсусу між ключовими політичними силами не сприятиме досягненню остаточної домовленості з вищезазначених питань.

6. Законодавче регулювання телекомунікацій та відносин в сфері віртуальної мережі Інтернет в Україні

Закон України «Про телекомунікації» від 18 листопада 2003 року визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами.

Стаття 1. Визначення основних термінів

1. У цьому Законі терміни вживаються в такому значенні: абонент — споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі;

адреса мережі Інтернет — визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;

адресний простор мережі Інтернет — сукупність адрес мережі Інтернет;

дані — інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

домен — частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;

домен.иЛ — домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет;

домен другого рівня — частина ієрархічного адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі;

Інтернет — всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

інформаційна система загального доступу — сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та

передавання даних;

інформація — відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

кінцеве обладнання — обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг;

передавання даних — передавання інформації у вигляді даних з

використанням телекомунікаційних мереж;

провайдер телекомунікацій — суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і

надання в користування каналів електрозв'язку;

рухомий (мобільний) зв'язок — електрозв'язок із застосуванням радіо технологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдний унікальний ідентифікаційний номер мобільної станції;

споживач телекомунікаційних послуг (споживач) — юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб; [•]

суб'єкти ринку телекомунікацій — оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або

постачальники технічних засобів комунікацій; [•]

Стаття 3. **Призначення телекомунікацій**

1. Сфера телекомунікацій є складовою частиною галузі зв'язку України.

2. Телекомунікації є невід'ємною частиною виробничої та соціальної інфраструктури України і призначені для задоволення потреб юридичних і фізичних осіб, органів державної влади в телекомунікаційних послугах.

Стаття 5. Сфера дії Закону

1. Дія цього Закону поширюється на відносини суб'єктів рнку телекомунікацій щодо надання та отримання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування.

2. Дія цього Закону не поширюється на телекомунікаційні мережі, що не взаємодіють з телекомунікаційними мережами загального користування, за

винятком їх використання в умовах надзвичайної ситуації, надзвичайного стану та воєнного стану.

Стаття 6. **Принципи діяльності у сфері телекомунікацій**

1. Основиними принципами діяльності у сфері телекомунікацій є:

1) доступ споживачів до загальнодоступних телекомунікаційних послуг, які необхідні їм для задоволення потреб, участі в політичному, економічному та громадському житті;

2) взаємодія та взаємозв'язаність телекомунікаційних мереж для забезпечення можливості зв'язку між споживачами всіх мереж;

3) забезпечення сталості телекомунікаційних мереж і управління цими мережами з урахуванням їх технологічних особливостей на основі єдиних стандартів, норм і правил;

4) державна підтримка розвитку вітчизняного виробництва технічних засобів комунікацій;

5) заохочення конкуренції в інтересах споживачів телекомунікаційних послуг;

6) збільшення обсягів телекомунікаційних послуг, їх переліку та утворення нових робочих місць;

7) впровадження світових досягнень у сфері телекомунікацій, залучення, використання вітчизняних та іноземних матеріальних та фінансових ресурсів, новітніх технологій, управлінського досвіду;

8) сприяння розширенню міжнародного співробітництва у сфері телекомунікацій та розвитку глобальної телекомунікаційної мережі;

9) забезпечення доступу споживачів до інформації про порядок отримання та якість телекомунікаційних послуг;

10) ефективність, прозорість регулювання у сфері телекомунікацій;

11) створення сприятливих умов діяльності у сфері телекомунікацій з урахуванням особливостей технологій та ринку телекомунікацій.

2. Надання телекомунікаційних послуг на території України є виключним правом юридичних осіб з місцезнаходженням на території України, які зареєстровані відповідно до законодавства України, та/або фізичних осіб — суб'єктів підприємницької діяльності з постійним місцем проживанням на території України.

Стаття 7**. Вживання мов у сфері телекомунікацій**

1. У сфері надання телекомунікаційних послуг в Україні вживаються українська мова, мови інших національностей відповідно до законодавства України.

2. Адреси відправника та одержувача телеграм, що пересилаються в межах України, повинні зазначатись українською або російською мовою.

3. Текст телеграми може бути написаний будь-якою мовою з використанням літер кирилиці або латинської абетки.

4. Міжнародні повідомлення, які передаються через телекомунікаційні мережі загального користування, обробляються з використанням мов, передбачених міжнародними договорами України.

Стаття 9. **Охорона таємниці телефонних розмов, телеграфної та іншої кореспонденції, безпека телекомунікацій**

2. Зняття інформації з телекомунікаційних мереж заборонене, крім винятків, передбачених законом.

3. Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що надається цими мережами.

Стаття 13. **Органи управління у сфері телекомунікацій**

1. Державне управління у сфері телекомунікацій здійснюють: Кабінет Міністрів України; центральний орган виконавчої влади в галузі зв'язку; інші органи виконавчої влади відповідно до закону.

Стаття 14. **Компетенція Кабінету Міністрів України у сфері телекомунікацій**

1. Кабінет Міністрів України: 1) забезпечує проведення державної політики у сфері телекомунікацій; 2) забезпечує рівні умови розвитку всіх форм власності у сфері телекомунікацій; 3) здійснює управління об'єктами державної власності у сфері телекомунікацій; 4) спрямовує і координує діяльність міністерств, інших центральних органів виконавчої влади у сфері телекомунікацій.

Стаття 15. **Повноваження центрального органу виконавчої влади в галузі зв'язку**

1. Центральний орган виконавчої влади в галузі зв'язку (ЦОВЗ): 1) розробляє пропозиції щодо державної політики у сфері телекомунікацій і реалізує її у межах своїх повноважень; 2) розробляє проекти законів, інших нормативно-правових актів; 3) розробляє та затверджує нормативно-правові акти з питань, віднесених до його компетенції; 4) визначає вимоги щодо рівня якості телекомунікаційних послуг; 5) впроваджує технічну політику у сфері надання телекомунікаційних послуг, стандартизації, підтвердження відповідності технічних засобів телекомунікацій; 7) організовує та відповідає за розроблення стандартів у сфері телекомунікацій; 8) затверджує технічні вимоги до телекомунікаційних мереж, засобів і об'єктів телекомунікацій; 9) розробляє та реалізує технічну політику у формуванні номерного ресурсу; 10) розробляє за участю національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, міністерств та інших центральних органів виконавчої влади Концепцію розвитку телекомунікацій України, спрямовану на досягнення стратегічних інтересів та міжнародної конкурентоздатності України; 11) розробляє прогнози розвитку телекомунікаційних мереж та послуг; 12) організовує наукове забезпечення функціонування і розвитку сфери телекомунікацій; 13) організовує проведення досліджень та розробку рекомендацій щодо конвергенції комп'ютерних та телекомунікаційних технологій; 14) інформує суб'єктів ринку телекомунікацій про політику та стратегію розвитку телекомунікаційних мереж загального користування; 15) вирішує в межах компетенції питання щодо забезпечення зв'язку для потреб

державної системи урядового зв'язку, національної системи конфіденційного зв'язку, органів безпеки, оборони, охорони правопорядку; 16) вирішує в межах компетенції питання щодо готовності функціонування телекомунікаційних мереж загального користування в умовах надзвичайних ситуацій та надзвичайного стану; 17) здійснює співробітництво з міжнародними організаціями та відповідними органами інших держав; 18) виконує обов'язки Адміністрації зв'язку та радіочастот України; 19) здійснює інші повноваження відповідно до законодавства.

Стаття 17. **Орган державного регулювання у сфері телекомунікацій**

1. Органом державного регулювання у сфері телекомунікацій є національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації.

2. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, є державним колегіальним органом, підпорядкованим Президенту України, підзвітним Верховній Раді України.

3. Положення про національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації (1067/2011), затверджується Президентом України.

4. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, для здійснення своїх повноважень може створювати та ліквідовувати свої територіальні органи у випадках, передбачених у положенні про національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації. Територіальні органи діють на підставі положення, що затверджується національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Стаття 18. **Повноваження національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації**

1. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації: 1) вносить пропозиції до органів державної влади щодо проектів законів та інших нормативно-правових актів, стандартів у сфері телекомунікацій; 2) видає нормативні акти з питань, що належать до компетенції національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, та контролює їх виконання; 3) забезпечує державний нагляд за додержанням суб'єктами ринку законодавства про телекомунікації; 4) здійснює ліцензування та реєстрацію у сфері надання телекомунікаційних послуг; 4-1) встановлює Правила здійснення діяльності у сфері телекомунікацій; 5) здійснює розподіл, присвоєння, облік номерного ресурсу, видачу та скасування дозволів, нагляд за використанням номерного ресурсу; 5-1) встановлює порядок надання послуг із перенесення абонентських номерів та порядок надання послуг національного роумінгу; 5-2) відповідно до закону встановлює порядок відкриття номерного ресурсу, в якому забезпечується утворення персональних номерів абонентів, та порядок адміністрування, присвоєння абонентам і обслуговування персональних номерів, визначає організацію, яка здійснює централізоване технічне адміністрування персональних номерів та перенесених абонентських номерів; 6) забезпечує

контроль за якістю телекомунікаційних послуг та задоволенням попиту споживачів; від 01.06.2010 } 7) здійснює відповідно до закону тарифне регулювання у сфері телекомунікацій та встановлює порядок взаєморозрахунків між операторами телекомунікацій; 8) дає дозвіл операторам, провайдерам телекомунікацій на встановлення спеціальних тарифів для інвалідів та соціально незахищених осіб на загальнодоступні телекомунікаційні послуги; 9) здійснює організаційно-правове забезпечення загальнодоступних телекомунікаційних послуг та послуг пропуску трафіка; 10) отримує безоплатно від операторів, провайдерів телекомунікацій необхідну для виконання своїх повноважень звітність та інформацію, у тому числі таку, що містить фінансово-економічні показники, у визначених національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, обсягах, формах і порядку; визначає ринки телекомунікаційних послуг, здійснює їх аналіз та визначає операторів телекомунікацій з істотною ринковою перевагою у порядку, затвердженому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації; 11) отримує безоплатно від центральних та місцевих органів виконавчої влади, органів виконавчої влади Автономної Республіки Крим, органів місцевого самоврядування документи, матеріали, статистичну та іншу інформацію, визначену законодавством; 12) приймає в межах своєї компетенції рішення, які є обов'язковими для виконання суб'єктами ринку телекомунікацій; 13) застосовує у межах своїх повноважень в установленому законодавством порядку адміністративні стягнення до суб'єктів ринку телекомунікацій; 14) передає до Антимонопольного комітету України матеріали в разі виявлення порушень законодавства про захист економічної конкуренції; 15) звертається до суду з відповідними позовними заявами в разі порушення суб'єктами господарювання, що здійснюють діяльність на ринку телекомунікацій, законодавства про телекомунікації; 16) регулює взаємодію операторів телекомунікацій при взаємоз'єднанні телекомунікаційних мереж, у тому числі щодо послуг пропуску трафіка, встановлює порядок маршрутизації трафіка; 17) створює сприятливі організаційні та економічні умови для залучення інвестицій у сферу телекомунікацій; 18) забезпечує рівні умови діяльності у сфері телекомунікацій; 19) забезпечує досудове вирішення спорів між суб'єктами ринку телекомунікацій щодо взаємоз'єднання телекомунікаційних мереж, у тому числі щодо послуг пропуску трафіка, надання послуг національного роумінгу, перенесення абонентських номерів та використання персональних номерів; 20) встановлює порядок ведення і веде реєстр операторів, провайдерів телекомунікацій; 21) розробляє та затверджує в межах своєї компетенції Регламент національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, а також інші нормативно-правові акти; 22) здійснює співробітництво з відповідними органами регулювання у сфері телекомунікацій інших держав; 23) видає офіційний друкований бюлетень і публікує в ньому нормативно-правові акти, відомості, передбачені цим Законом, та іншу інформацію; 24) здійснює інші повноваження, передбачені цим Законом, іншими законами та нормативно-правовими актами.

Стаття 19. **Нагляд за ринком телекомунікацій**

1. Державний нагляд за ринком телекомунікацій здійснюється шляхом: 1) контролю за якістю телекомунікаційних послуг; 2) контролю за наявністю передбачених законом ліцензій, інших дозвільних документів у сфері телекомунікацій; 3) перевірки додержання ліцензійних умов, особливих умов ліцензій операторами, провайдерами телекомунікацій; 4) контролю за додержанням суб'єктами ринку телекомунікацій законодавства, стандартів та інших нормативних документів у сфері телекомунікацій; 5) вимірювання в порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, параметрів телекомунікаційних мереж, контролю за дотриманням операторами телекомунікацій порядку маршрутизації трафіку на телекомунікаційних мережах. 3. Для здійснення державного нагляду за ринком телекомунікацій уповноважені національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, посадові особи мають право: 1) доступу у встановленому законодавством порядку на територію і до приміщень операторів, провайдерів телекомунікацій, виробників та постачальників технічних засобів телекомунікацій; 2) перевіряти дотримання вимог законодавства про телекомунікації суб'єктами ринку телекомунікацій, їх відокремленими підрозділами; від 01.06.2010 } 3) давати в межах своїх повноважень суб'єктам ринку телекомунікацій обов'язкові для виконання приписи щодо усунення порушень нормативно-правових актів; 4) застосовувати в установленому законодавством порядку санкції за порушення законодавства про телекомунікації до суб'єктів ринку телекомунікацій; 5) безоплатно отримувати від суб'єктів ринку телекомунікацій необхідні для виконання завдань, покладених на національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, цим Законом, інформацію, пояснення та інші матеріали; 6) безоплатно отримувати від центральних та місцевих органів виконавчої влади, органів виконавчої влади Автономної Республіки Крим, органів місцевого самоврядування документи, матеріали, статистичну та іншу інформацію, необхідну для виконання функцій, покладених на національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації; 7) з метою розгляду звернень фізичних та юридичних осіб, що надходять до національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, отримувати від операторів, провайдерів телекомунікацій необхідні документи та інформацію, а також видавати в установленому порядку приписи за результатами розгляду звернень; 8) інші права, визначені законодавством.

Стаття 32. **Права споживачів телекомунікаційних послуг**

1. Споживачі під час замовлення та/або отримання телекомунікаційних послуг мають право на: 1) державний захист своїх прав; 2) вільний доступ до телекомунікаційних послуг; 3) безпеку телекомунікаційних послуг; 4) вибір оператора, провайдера телекомунікацій; 5) вибір виду та кількості телекомунікаційних послуг; 6) безоплатне отримання від оператора, провайдера телекомунікацій вичерпної інформації щодо змісту, якості, вартості та порядку надання телекомунікаційних послуг; 7) своєчасне і якісне одержання

телекомунікаційних послуг; 8) отримання від оператора, провайдера телекомунікацій наявних відомостей щодо наданих телекомунікаційних послуг; 9) обмеження оператором, провайдером телекомунікацій доступу споживача до окремих видів послуг на підставі його власної письмової заяви; 10) повернення від оператора, провайдера телекомунікацій невикористаної частки коштів у разі відмови від передплачених телекомунікаційних послуг у випадках і в порядку, визначених правилами надання і отримання цих послуг; 11) відмову від телекомунікаційних послуг у порядку, встановленому договором про надання телекомунікаційних послуг; 12) відшкодування збитків, заподіяних унаслідок невиконання чи неналежного виконання оператором, провайдером телекомунікацій обов'язків, передбачених договором із споживачем чи законодавством; 13) оскарження неправомірних дій операторів, провайдерів телекомунікацій шляхом звернення до суду та уповноважених державних органів; 14) відмову від оплати телекомунікаційної послуги, яку вони не замовляли; 15) отримання відомостей щодо можливості та порядку відмови від замовленої телекомунікаційної послуги; 16) безоплатне отримання від оператора, провайдера телекомунікацій рахунків за надані телекомунікаційні послуги. За особистим зверненням споживача з урахуванням технічної можливості обладнання телекомунікаційної мережі нарахована до оплати сума за надані послуги повинна бути розшифрована тільки за той розрахунковий період, до якого споживач має претензії, із зазначенням номера абонента, якого викликав споживач, виду послуги, часу початку і закінчення кожного сеансу зв'язку, обсягу наданих послуг, суми коштів до сплати за кожний сеанс зв'язку. Телекомунікаційні послуги, які надаються знеособлено (анонімно), розшифровці не підлягають; 16-1) перенесення абонентського номера, користування персональним номером та отримання послуг національного роумінгу; 17) інші права, визначені законодавством України та договором про надання телекомунікаційних послуг. 2. Абонент, який отримує телекомунікаційні послуги без укладення договору в письмовій формі, може зареєструватися в оператора, надавши йому персональні дані відповідно до закону в порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Стаття 33**. Обов'язки споживачів телекомунікаційних послуг**

1. Споживачі телекомунікаційних послуг зобов'язані дотримуватися Правил надання та отримання телекомунікаційних послуг, що затверджує Кабінет Міністрів України, зокрема: 1) використовувати кінцеве обладнання, що має документ про підтвердження відповідності; 2) не допускати використання кінцевого обладнання споживача для вчинення протиправних дій або дій, що суперечать інтересам національної безпеки, оборони та охорони правопорядку; 3) не допускати дій, що можуть створювати загрозу для безпеки експлуатації мереж телекомунікацій, підтримки цілісності та взаємодії мереж телекомунікацій, захисту інформаційної безпеки мереж телекомунікацій, електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможливлювати надання послуг іншим споживачам; 4) не допускати використання на комерційній основі кінцевого обладнання та абонентських

ліній для надання телекомунікаційних послуг третім особам; 5) виконувати умови договору про надання телекомунікаційних послуг у разі його укладення, у тому числі своєчасно оплачувати отримані ними телекомунікаційні послуги; 6) виконувати інші обов'язки відповідно до законодавства. 2. У разі використання абонентами лічильників обліку тривалості телекомунікаційних послуг, що встановлюються на кінцевому обладнанні для перевірки правильності нарахування плати за отримані послуги, абоненти зобов'язані: 1) використовувати лічильники, що мають документ про підтвердження відповідності згідно із законодавством України; 2) періодично здійснювати метрологічну повірку лічильників як засобів вимірювальної техніки в порядку, визначеному законодавством України. 3. Споживачі телекомунікаційних послуг зобов'язані виконувати інші обов'язки відповідно до цього Закону та законодавства України.

Стаття 34. **Захист інформації про споживача**

1. Оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо. 2. Призначені для оприлюднення телефонні довідники, у тому числі електронні версії та бази даних інформаційно-довідкових служб, можуть містити інформацію про прізвище, ім'я, по батькові, найменування, адресу та номер телефону абонента в разі, якщо в договорі про надання телекомунікаційних послуг міститься згода споживача на опублікування такої інформації. Під час автоматизованої обробки інформації про абонентів оператор телекомунікацій забезпечує її захист відповідно до закону. Споживач має право на безоплатне вилучення відомостей про нього повністю або частково з електронних версій баз даних інформаційно-довідкових служб. 3. Інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватись у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача.

Стаття 35. **Захист інтересів споживачів у разі припинення діяльності оператором, провайдером телекомунікацій з надання телекомунікаційних послуг** 1. Оператор, провайдер телекомунікацій, який припиняє діяльність з надання телекомунікаційних послуг, зобов'язаний попередити споживачів не пізніше ніж за три місяці до припинення надання телекомунікаційних послуг. 2. У разі анулювання чи визнання недійсною ліцензії, вилучення номерного та/або радіочастотного ресурсу внаслідок порушення оператором, провайдером телекомунікацій законодавства такий оператор, провайдер зобов'язаний відшкодувати абоненту витрати, пов'язані з припиненням надання телекомунікаційних послуг, у встановленому законом порядку.

Стаття 36. **Відповідальність споживачів телекомунікаційних послуг**

1. Споживачі телекомунікаційних послуг несуть відповідальність за порушення норм цього Закону, Правил надання та отримання телекомунікаційних послуг відповідно до закону. 2. У разі затримки плати за надані оператором, провайдером телекомунікаційні послуги споживачі

сплачують пеню, яка обчислюється від вартості неоплачених послуг у розмірі облікової ставки Національного банку України, що діяла в період, за який нараховується пеня. 3. Сплата споживачем пені, правомірне припинення чи скорочення оператором, провайдером переліку телекомунікаційних послуг не звільняє споживача від обов'язку оплатити надані йому телекомунікаційні послуги. 4. У разі виявлення пошкодження телекомунікаційної мережі, що сталося з вини споживача, усі витрати оператора телекомунікацій на усунення пошкодження, а також відшкодування інших збитків (у тому числі неотриманий прибуток) покладаються на споживача.

Стаття 38. **Права операторів, провайдерів телекомунікацій**

1. Оператори телекомунікацій мають право на: 1) здійснення діяльності у сфері телекомунікацій відповідно до законодавства; 2) отримання ліцензій відповідно до цього Закону; 3) отримання номерного ресурсу; 4) планування та розвиток власних мереж; 5) установлення тарифів на телекомунікаційні послуги, що ними надаються, крім тих послуг, тарифи на які регулюються державою відповідно до цього Закону; 6) присвоєння телефонних номерів споживачам у межах виділеного оператору номерного ресурсу та задіяння персональних номерів у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації; 7) з'єднання телекомунікаційних мереж, що знаходяться в його власності або користуванні, з телекомунікаційними мережами, що знаходяться у власності або користуванні інших операторів, відповідно до цього Закону; 8) скорочення переліку або припинення надання телекомунікаційних послуг споживачам, які порушують правила надання і отримання телекомунікаційних послуг, або на відключення кінцевого обладнання споживача, якщо воно не має виданого в установленому законодавством порядку документа про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій, у порядку, визначеному цими правилами; 9) відключення на підставі рішення суду кінцевого обладнання, якщо воно використовується абонентом для вчинення протиправних дій або дій, що загрожують інтересам державної безпеки; 10) зупинення діяльності у сфері телекомунікацій відповідно до цього Закону і в порядку, встановленому ЦОВЗ та узгодженому з національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації; 11) установлення телекомунікаційного обладнання в приміщеннях, що належать їм на правах найму, з дозволу власника приміщення; 12) інші права, передбачені законодавством України та договорами про надання телекомунікаційних послуг.

2. Відключення кінцевого обладнання підрозділам Міністерства оборони України, Служби безпеки України, Служби зовнішньої розвідки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України, спеціально уповноваженого центрального органу виконавчої влади з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, спеціально уповноваженого центрального органу виконавчої влади з питань охорони державного кордону, центрального органу виконавчої влади в галузі

митної справи, з'єднувальних ліній служб екстреного виклику здійснюється в порядку, встановленому Кабінетом Міністрів України.

3. Провайдер телекомунікацій користується правами, передбаченими частиною першою цієї статті, за винятком прав, передбачених пунктами 2, 3, 6, 7 частини першої цієї статті, а також має право на підключення технічних засобів до телекомунікаційної мережі оператора відповідно до законодавства.

4. Провайдери телекомунікацій здійснюють діяльність у сфері телекомунікацій на підставі договору з оператором телекомунікацій - резидентом України та копії ліцензії цього оператора на відповідний вид діяльності у випадках, передбачених законом.

Стаття 39. **Обов'язки операторів і провайдерів телекомунікацій** 1. Оператори телекомунікацій зобов'язані: 1) здійснювати діяльність у сфері телекомунікацій відповідно до законодавства за умови включення до реєстру операторів, провайдерів телекомунікацій, а у визначених законом випадках також за наявності відповідних ліцензій та/або дозволів; 2) надавати безоплатний доступ споживачам до телекомунікаційних мереж загального користування для виклику пожежної охорони, міліції, швидкої допомоги, аварійних служб газу та підрозділів екстреної допомоги населенню за єдиним телефонним номером 112; 3) надавати телекомунікаційні послуги за встановленими показниками якості; 4) надавати споживачам вичерпну інформацію, необхідну для укладення договору, а також щодо телекомунікаційних послуг, які вони надають; 4-1) надавати абонентам послугу перенесення абонентського номера, користування персональним номером у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації; 5) вести достовірний облік телекомунікаційних послуг, що надаються споживачеві; 6) забезпечувати правильність застосування тарифів; 7) зберігати записи про надані телекомунікаційні послуги протягом строку позовної давності, визначеного законом, та надавати інформацію про надані телекомунікаційні послуги в порядку, встановленому законом; 8) не допускати порушень правил добросовісної конкуренції на ринку телекомунікацій; 9) першочергово надавати телекомунікаційні послуги підрозділам Міністерства оборони України, Служби безпеки України, Служби зовнішньої розвідки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України, спеціально уповноваженого центрального органу виконавчої влади з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, спеціально уповноваженого центрального органу виконавчої влади з питань охорони державного кордону, центрального органу виконавчої влади в галузі митної справи; 10) забезпечувати готовність своїх телекомунікаційних мереж до роботи в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, в тому числі можливість оповіщення своїх споживачів у цих умовах; 11) надавати щорічно до ЦОВЗ інформацію про свої телекомунікаційні мережі для відпрацювання мобілізаційних планів у межах, визначених Кабінетом Міністрів України; 12) вести облікову та іншу, визначену законодавством, документацію щодо своїх

телекомунікаційних мереж та взаємоз'єднання з іншими телекомунікаційними мережами; 13) своєчасно надавати ЦОВЗ та національній комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, звіти та інформацію в обсягах, порядку і строки, визначені законодавством; 14) оприлюднювати тарифи на телекомунікаційні послуги, що встановлюються самим оператором, не пізніше ніж за сім календарних днів до їх введення; 15) забезпечувати використання наданого номерного ресурсу в терміни, визначені національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації; 16) попереджувати споживачів про можливе скорочення переліку телекомунікаційних послуг чи відключення їх кінцевого обладнання у випадках і порядку, передбачених правилами надання і отримання цих послуг; 17) вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами; 18) на підставі рішення суду обмежувати доступ своїх абонентів до ресурсів, через які здійснюється розповсюдження дитячої порнографії; 18-1) подавати до центрів системи екстреної допомоги населенню за єдиним телефонним номером 112: невідкладно після отримання екстреного виклику від абонента рухомого (мобільного) зв'язку - дані про його номер і місцезнаходження; щомісяця - інформацію про абонентські номери фіксованого телефонного зв'язку, прізвища, імена, по батькові, найменування та адреси, що містяться в базі даних; 19) виконувати інші обов'язки відповідно до законодавства України.

2. Усі пункти частини першої цієї статті, крім пунктів 1, 2, 10, 11, 12, 15, 17, 18-1, поширюються також на провайдерів телекомунікацій. Оператори, провайдери телекомунікацій зберігають та надають інформацію про з'єднання свого абонента у порядку, встановленому законом.

3. У разі якщо оператор, провайдер телекомунікацій встановлює плату за телекомунікаційні послуги згідно з почасовими тарифами, то при розрахунках із споживачами він зобов'язаний враховувати лише повні тарифні одиниці часу.

4. Оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

5. Оператори, провайдери телекомунікацій не мають права відмовляти в подальшому наданні загальнодоступних послуг інвалідам I та II груп усіх категорій, поточна заборгованість яких за отримані послуги не перевищує трьох мінімальних пенсій за віком. 6. Оператори телекомунікацій, що надають послуги рухомого (мобільного) зв'язку на території України, за умови укладення відповідної письмової угоди між собою зобов'язані надавати можливість абонентам отримувати послугу національного роумінгу.