УДК 340.132.2+351.751

ДОРОНІН І.М., *кандидат юридичних наук, доцент,*
завідувач наукової лабораторії
НДІ інформатики і права НАПрН України

ПРАВОВІ ПРОБЛЕМИ СУВЕРЕНІЗАЦІЇ ІНТЕРНЕТУ

Анотація. *У статті проаналізовано питання визначеності державного суверенітету стосовно Інтернету, його сегментів. Досліджено практику державного регулювання у сфері телекомунікацій у контексті перспектив централізованого управління мережею Інтернет в межах окремої країни. Визначено, що законодавчі новації в Російській Федерації ухвалено з метою забезпечення стійкості Інтернету на території країни. Водночас суверенізація щодо Інтернету не означає посилення його централізованості. Правове регулювання у цьому контексті є відображенням внутрішньої державної політики.*

Ключові слова: *суверенітет, Інтернет, національна безпека, право телекомунікацій, інформаційне право, державне регулювання.*

Summary. *This paper analyzes problems of state sovereignty for Internet and its segments. Author examined practices of state regulation of telecommunications in the contest of central control for Internet within a specific country. It is defined that legislative innovations were adopted for ensuring the sustainability of Internet within Russian Federation. However, state sovereignty for Internet was not implying a higher degree of centralization. Legal regulation reflects current domestic public policy for Internet.*

Keywords: *sovereignty, Internet, national security, telecommunications law, information law, state regulation.*

Аннотация. *В статье проанализированы вопросы определимости государственного суверенитета относительно Интернета и его сегментов. Исследована практика государственного регулирования в сфере телекоммуникаций в контексте перспектив централизованного управления сетью Интернет в пределах отдельной страны. Определено, что законодательные новеллы в Российской Федерации приняты с целью обеспечения стойкости Интернета на территории страны. Вместе с тем суверенизация в отношении Интернета не должна означать усиления его централизованного управления. Правовое регулирование в этом контексте отображает внутреннюю государственную политику.*

Ключевые слова: *суверенитет, Интернет, национальная безопасность, право телекоммуникаций, информационное право, государственное регулирование.*

Постановка проблеми. Розвиток глобальної комп’ютерної мережі Інтернет невідворотно змінив суспільство та усі соціальні інститути, набувши виняткового соціального значення. Загалом регулювання суспільних відносин у цій сфері здійснюється різними шляхами, у тому числі за допомогою права, як регулятора відносин. Очевидним є і значний багатоаспектний вплив технологій і на розвиток права та його окремих інститутів.

Водночас, існують і залишаються досить дієвими і традиційні види соціальних інститутів, в першу чергу – держава, її органи та механізм державного управління. Прояви активності зазначених інститутів відбуваються у звичний для них спосіб. У галузі правового регулювання мова йде про поняття “суверенного Інтернету”, яке характеризується спробами розповсюдити елементи державного суверенітету на глобальну комп’ютерну мережу, поставивши за мету фактично “деглобалізувати” її.

На цей час загальновідомими є суто технічні способи побудови та використання комп'ютерних мереж закритого типу (у т.ч. умовно закритих), що розповсюджується на певну кількість ідентифікованих абонентів. Водночас, такий тип побудови мережі, що був характерний для другої половини минулого сторіччя, не дозволяє розглядати її як глобальну мережу, а отже у ній не проявляються ті соціальні явища, що характерні для всеохоплюючої глобальної відкритої мережі Інтернет. Тому для органів державного управління в різних державах час від часу характерні намагання здійснити державний вплив за допомогою права на окремі аспекти суспільних відносин, що пов'язані з використанням мережі Інтернет. Найбільш цікавими для наукового дослідження є спроби встановлення контролю (шляхом так званої "суверенізації") певних елементів (сегментів) глобальної мережі Інтернет з боку держави, а також вжиття управлінських заходів під гаслами "суверенізації" Інтернету.

Результати аналізу наукових публікацій. Проблеми управління та державного впливу у сфері використання глобальної мережі Інтернет є предметом досліджень фахівців з соціальної філософії, соціології, економіки, державного управління та технічних наук. У правовій науці проблематика державного впливу розглядається як правило у контексті адміністративного права. Серед комплексних інформаційно-правових досліджень варто виділити монографію О.А. Баранова [1], а також низку робіт монографічного характеру, що стосується окремих напрямів регулювання суспільних відносин у цій сфері [2 – 4]. Останнім часом, з огляду на законодавчі новації у Російській Федерації, питання "суверенного Інтернету" активно розглядається у публіцистичній літературі та політичній полеміці.

Метою цієї статті є проведення аналізу впливу традиційних уявлень про державний суверенітет у правовій науці, можливості його розповсюдження на елементи глобальної мережі Інтернет з огляду на існуючі та виникаючі виклики, загрози і небезпеки. Окрім цього, передбачається проведення дослідження стану законотворчості та застосування норм права з огляду на задекларовані цілі правового регулювання (забезпечення національної безпеки) в різних юрисдикціях, проведення порівняння із іншими актами. На підставі зазначеного аналізу будуть зроблені висновки щодо подальших тенденцій у правовому регулюванні.

Виклад основного матеріалу. У контексті цієї статті поняття державного суверенітету буде розглядатись традиційно, тобто він розуміється як верховенство, самостійність, повнота і неподільність державної влади на своїй території та незалежність у міжнародних відносинах [5]. Отже говорячи про "суверенізацію" мова йде насамперед про розповсюдження державної влади. У даному разі така влада поширюватиметься на комп'ютерну мережу, її елементи, або на інші утворення, що можуть бути виділені для розповсюдження на них влади.

У цілому для підтримання функціонування мережі необхідні сервери (тобто технічні пристрої зберігання інформації), лінії зв'язку (які забезпечують зв'язок між ними) та засоби управління (у т.ч. програмне забезпечення). Це спрощене розуміння, але для цілей дослідження правового регулювання воно в цілому відповідає розумінню комп'ютерної мережі на фізичному рівні, що розглядається технічними фахівцями [6, с. 9-13]. Сервери та лінії зв'язку знаходяться в будь-якому разі на території певної держави і на місце їх знаходження і буде розповсюджуватись суверенітет конкретної держави. Але говорячи про суверенізацію Інтернету в контексті державної політики або правового регулювання, мова йде про більш широке коло проблемних питань. Зокрема, серед узагальнених О.А. Барановим підходів до визначення Інтернету для цілей правового регулювання варто зупинитись на розумінні Інтернету як міжнародної

телекомунікаційної мережі загального користування, що призначена для обміну відомостями або як глобальної системи комунікацій, що є засобом інформаційного спілкування та доступу до інформації [1, с. 13].

Якщо відійти від фізичного рівня сприйняття Інтернету, то насамперед мова йде про сегментацію мережі, тобто намагання виокремити певні об'єкти (сегменти), які можливо розглядати як такі, на які розповсюджується державний суверенітет. Зазначена точка зору найбільш яскраво проявляється в дискусіях стосовно "Рунету" (або "Уанету"), тобто російського або українського сегментів Інтернету. Більш-менш зрозумілою є ситуація з доменними іменами, що відповідають національній (державній) приналежності (доменній зоні, у випадку України – це доменна зона "ua"). Адміністрування у цій сфері відповідно до вимог ст. 56 Закону України "Про телекомунікації" покладено на уповноважену організацію [7]. Водночас, адміністрування домену на сьогодні де-факто здійснює юридична особа приватного права, хоча у науковій літературі було звернуто увагу на неврегульованість цього питання ще з 2003 року, незважаючи на наявність розпорядження Кабінету Міністрів України з цього приводу [1, с. 30]. Реєстрація здійснюється цією юридичною особою відповідно до визначених нею Правил [8]. Принаймні адміністрування здійснюється юридичною особою українського права, тому національна приналежність домену конкретній країні не викликає сумнів.

В інших державах існує різна практика. Так, наприклад, Уряд Тувалу (острівної держави в Океанії) передав права адміністрування популярного домену "TV" практично з початку його існування різним компаніям з США [8]. У деяких країнах існує практика прямого адміністрування національного домену верхнього рівня державними органами (Албанія, Бангладеш, Барбадос, Бенін, Габон, Камбоджа, КНР, Малайзія, М'янма, Оман, Пакистан, Саудівська Аравія, Таджикистан та ін.), але в більшості випадків це здійснюється уповноваженими недержавними організаціями, у т.ч. компаніями-нерезидентами або науковими установами. Правила національної належності серверів (ресурсів), а також обмежень (для урядових, військових, освітніх, наукових, медичних тощо) установ встановлюються операторами відповідно до загальних вимог міжнародної організації ICANN. У більшості доменних зон не є обов'язковою належність особи – власника Інтернет-ресурсу (сайту) до резидентів країни, або фізичне знаходження серверів на їх території. Як правило, обмеження та вимоги у цій сфері відповідають загальній державній політиці у сфері телекомунікацій.

Ситуація з доменом Росії дещо відрізняється двома факторами. Згідно із роз'ясненням Федеральної антимонопольної служби Росії, що обговорювалось у спеціалізованій пресі на початку 2018 року, до так званого "Рунету" (російського сегменту Інтернету) пропонується відносити ресурси з доменними іменами "RU", "SU" та "РФ" [10]. Доменне ім'я "SU" не входить до переліку географічних кодів ISO 3166-1, і тому не розглядається як національне згідно з вимогами ICANN. З початку 1990-х років його адміністрування здійснювалось різними російськими юридичними особами. Ототожнення з "Рунетом" відбувається із врахуванням того фактору, що більшість користувачів ідентифікує таке ім'я з колишнім Радянським Союзом, хоча його реєстрація і відбувалась після розпаду СРСР. Доменне ім'я "РФ" є так званим "кириличним" розширенням, тобто іменем, що засновано не на латинській, а іншій (у даному разі – кирилиці) писемності. На сьогодні в Інтернеті також вживаються домени, що засновані на китайській, корейській, арабській і тамільській писемності. Серед існуючих кириличних імен їх адміністрування здійснюється тими ж національними операторами, що адмініструють відповідний домен латиницею (Білорусь, Казахстан, Монголія, Сербія, Росія (у т.ч. домен "РУС"), Україна).

Але в Росії доволі часто відносять до “Рунету” (тобто російського сегменту Інтернету) фактично необмежене коло Інтернет-ресурсів, що містить контент російською мовою. З 2004 року під патронатом державних органів в Росії здійснюється нагородження “Премією Рунету”. Якщо проаналізувати перелік нагороджених з 2004 року то в основному це державні органи Росії, компанії в галузі телекомунікацій, засоби масової інформації, окремі особи, що є резидентами Росії. Хоча на початку відбувались нагородження міжнародних та іноземних компаній у сфері інформаційних технологій (Microsoft, Intel, Cisco Systems та ін.). За напрямком “Рунет за межами RU” нагороджувались різні організації, які діяли не у Росії. Таким чином, термін “Рунет” є доволі розпливчастим і може мати різні значення.

Позиція державних органів Росії у питаннях регуляції є більш конкретною. Виокремлення “Рунету” вважається недоцільним, а предмет державного впливу конкретизовано тим, що може бути врегульовано на “фізичному” рівні.

Питання “суверенізації” Інтернету (“Рунету”, російського сегменту, тощо) з’явилось останнім часом на порядку денному внаслідок низки законодавчих новацій у Росії.

Спочатку варто узагальнити існуючу в різних країнах практику державного регулювання використання комп’ютерних мереж (у т.ч. Інтернету). Прикладом державних крайнощів у цьому питанні є ситуація у Північній Кореї (КНДР). Вона може бути охарактеризована наступними факторами. Першим є існування загальної внутрішньої мережі користувачів у країні за відсутності її виходу безпосередньо в Інтернет. Тобто від самого початку в країні здійснювалась побудова внутрішньої комп’ютерної ізольованої мережі (Інтранету). Відповідно вона управлялась державними органами шляхами подібними до адміністрування внутрішньодержавної телефонної мережі. Адміністративним шляхом здійснювалась також ідентифікація конкретних абонентів, що використовували комп’ютерні мережі. Зазначені заходи розповсюджувались і на торгівлю індивідуальними засобами зв’язку (мобільні телефони, смартфони, і т.ін.) [11 – 13]. Окрім цього, електронно-обчислювальні машини використовують лише спеціально розроблене і контрольоване державою програмне забезпечення на рівні операційної системи (Red Star OS) [14]. Отже, усі зазначені заходи зумовлені однією метою – отриманням повного контролю за діяльністю особи, що використовує комп’ютерну техніку, за умови повного позбавлення її права на приватність. З точки зору забезпечення кібербезпеки, такі заходи можуть мати певну ефективність лише в умовах глобального контролю телекомунікацій, оскільки, наприклад операційна система Red Star на думку технічних фахівців є слабо захищеною від зовнішнього втручання та інших факторів, що ускладнюють її застосування [15]. Ефективно працювати зазначена система може лише в умовах закритої комп’ютерної мережі (Інтранет). На практиці повної закритості та підконтрольності комп’ютерних мереж не вдалося досягти навіть у КНДР з огляду на контрабанду технічних пристроїв (передусім смартфонів, планшетних комютерів та флеш-накопичувачів) з КНР, що використовуються як засоби для перегляду кінофільмів, прослуховування музики. Окрім цього, в КНДР правоохоронні органи ведуть тривалу боротьбу з намаганнями побудови приватними особами “москітних мереж”, тобто мереж таких пристроїв з використанням не контрольованих державою каналів (wi-fi, Bluetooth, irDa та подібних технологій) [16], а також зі спробами використовувати мережі мобільного зв’язку КНР для доступу до Інтернету через такі пристрої в прикордонних зонах [17].

Загалом громадськими організаціями, що спеціалізуються на дослідженнях стану свободи Інтернету в різних країнах, основними аспектами державного впливу визнано

“перепони для доступу” до Інтернету, “обмеження контенту” та “порушення прав користувачів”. Усі зазначені аспекти взаємопов’язані. Як правило, державний вплив у цій сфері зумовлений метою контролю за діями громадян в інтересах держави. Тому в демократичних суспільствах рівень свободи Інтернету є вищим аніж в авторитарних. Декларовані підстави для обмежень, що зазначаються державними органами, можуть приховувати реальні їх цілі. Як правило, мова йде про боротьбу з тероризмом, злочинністю або ж із необхідністю забезпечення кібербезпеки. Відповідна риторика корелює із політичними гаслами щодо посилення державного впливу, введення обмежень прав і свобод людини для досягнення вищих цілей.

Слід зазначити, що “суверенізація” Інтернету набула досить широкого розповсюдження в аргументації на підтримку низки законодавчих новел у Російській Федерації. Насамперед мова йде про Федеральний Закон Російської Федерації “Про внесення змін до Федерального Закону “Про зв’язок” і Федерального Закону “Про інформацію, інформаційні технології і про захист інформації” від 01.05.2019 року № 90-ФЗ, що набуває чинності з 1 листопада 2019 року [18]. Основними законодавчими новаціями Закону є покладання додаткових обов’язків на операторів зв’язку щодо встановлення спеціального обладнання – технічних засобів протидії загрозам стійкості, безпеки і цілісності функціонування на території Російської Федерації мережі Інтернет. Зазначені технічні засоби є складовою системи централізованого управління мережею зв’язку загального користування. Таким чином законодавчий акт встановлює адміністративно-правові передумови створення та функціонування системи централізованого управління мережею Інтернет в межах Росії відповідним державним органом. Технічна реалізація зазначеного буде регламентована в подальшому на рівні підзаконних актів. Нова глава 7-1 Федерального Закону “Про зв’язок” присвячена відповідним заходам, спрямованим на забезпечення стійкості, безпеки і цілісності функціонування на території Російської Федерації мережі Інтернет. Координація заходів покладається на відповідний федеральний орган. Пряме централізоване управління має здійснюватись зазначеним органом в умовах “надзвичайних обставин”, які визначені вкрай широко – у випадку виникнення загроз стійкості, безпеки і цілісності функціонування мережі Інтернет.

Поняття “суверенітету” щодо Інтернету досить широко використовувалось на етапі підготовки та прийняття зазначеного Закону, оскільки законодавчі новації викликали чималу критику правозахисників. Обґрунтування прийняття Закону містилось в пояснювальній записці до законопроекту. На думку його авторів причиною прийняття Закону є агресивні дії з боку США, що нібито визначені у Стратегії національної кібербезпеки, а також необхідність забезпечення довгострокової та сталої роботи мережі Інтернет на території Росії. Для досягнення цієї мети і пропонується створити інфраструктуру, яка б мала змогу обмежити увесь трафік мережі шляхом контролю усіх точок доступу, а також за необхідності забезпечити використання мережевих ресурсів Росії в умовах відсутності зв’язку із Інтернетом [19]. Зрозуміло, що зазначені складові мети є технічними завданнями, а правовий шлях досягнення мети передбачає адміністративно-правове регулювання діяльності, у т.ч. покладання на суб’єктів господарської діяльності обов’язку встановлювати спеціальне технічне обладнання. Введення за необхідності централізованого управління за таких умов випливає із відповідних заходів, що визначаються цим Законом у межах повноважень державних органів.

Але слід зазначити, що “суверенізація” не означає встановлення централізованого управління Інтернетом. Загалом в міжнародному праві кібервійни зазначено наступне

ставлення до суверенітету в кіберпросторі. Перше правило Талліннського статуту (Tallinn Manual) щодо міжнародного права, яке може бути застосовано до кібервійни, визначає загальні підходи до суверенітету в кіберпросторі. Зокрема визначено, що держава може здійснювати контроль над кібер-інфраструктурою і діяльністю в межах своєї суверенної території [20, с. 25]. Тобто суверенітет держави щодо об'єктів, на які він розповсюджується, є похідним від суверенітету держави щодо певної території. Зазначене стосується і об'єктів кібер-інфраструктури. За таких умов держава дійсно має суверенні права щодо встановлення обмежень, у тому числі і у питанні доступу до мережі Інтернет на власній території. Питання можливого порушення суверенітету внаслідок проведення операцій в кіберпросторі (кібервійна), а також пріоритету прав людини у цьому контексті, що визначені міжнародно-правовими актами, є досить складними і комплексними, їх однозначне трактування є справою майбутнього, про що свідчить характер наукової дискусії в цьому напрямку [21, с. 211-212].

Таким чином, суверенне право держави мати контроль над об'єктами кібер-інфраструктури на своїй території під сумнів не ставиться. Але суверенітет не означає наявності права власності або необхідності розповсюдження на ці об'єкти прямого державного управління. Отже, зазначені законодавчі новели ніякої суверенізації не встановлюють. Мова йде лише про посилення державного регулювання певної сфери. Причини для такого посилення можуть бути різні, але у випадку Росії вони скоріше за все є політичними. Ефективність обраних заходів щодо протидії військовим операціям, які проводяться у кіберпросторі, зможуть оцінити відповідні технічні фахівці. Слід лише зазначити, що у Стратегії національної кібербезпеки США не передбачено проведення операцій в кіберпросторі, спрямованих на обмеження доступу до Інтернету будь-якої держави, але цілий розділ присвячений просуванню "американського впливу". До числа цілей такого впливу Стратегія відносить забезпечення стійкості Інтернету та свободи Інтернету [22, с. 24]. Саме реалізації таких завдань фактично і протидіють заходи по встановленню централізованого управління використанням мережі Інтернет та його перетворення на територіально замкнену мережу (Інтранет). І саме такими вірогідно і були справжні цілі ухвалення в Росії законопроекту 608767-7.

Висновки.

1. "Суверенізація Інтернету" загалом є політичним терміном, який відображає певні тенденції у державній політиці окремих країн. Зазначені тенденції, як правило, мають внутрішній характер, тісно пов'язані із існуючим в державі політичним режимом і відображають його характер. У правовому значенні поняття суверенітету може використовуватись як термін міжнародного права.

2. Загальне розуміння суверенітету передбачає суверенітет держави над об'єктами (у тому числі кібер-інфраструктури) за принципом території, на яку розповсюджується суверенітет. При цьому держава має право контролювати доступ до мережі та діяльність у ній відповідно до вимог законодавства, у тому числі міжнародно-правових актів щодо захисту прав людини.

3. Адміністративна діяльність щодо державного регулювання у сфері телекомунікацій регламентується національним законодавством відповідної держави. Технічні вимоги стосовно організації доступу та використання мережі Інтернет забезпечуються державою шляхом встановлення нормативно-правових вимог. Водночас питання розповсюдження суверенітету та сприйняття суверенітету (національної приналежності) щодо певних ресурсів може бути значно ускладнено з огляду на глобальний характер мережі Інтернет.

4. Перспективними у цьому контексті є подальші наукові дослідження стосовно визначення підстав для державних обмежень, що реалізовуються у кіберпросторі, визначення гарантій забезпечення прав і свобод людини, які пов'язані з використанням мережі Інтернет та пошуку балансу між необхідністю реалізації цілей держави і правами людини.

Використана література

1. Баранов А.А. Интернет: объект правоотношений и предмет регулирования: монография. Київ: Ред.журн. "Право України"; Харків: Право, 2013. 144 с.

2. Динис Г.Г. Міжнародно-правові концепції глобального права, права Інтернету або кіберправа та трансформації міжнародного права. *Часопис Київського університету права.* 2011. № 2. С. 279-285.

3. Рассолов И.М. Право и Интернет: теоретические проблемы. 2-е изд. Москва: Норма, 2009. 383 с.

4. Серго А. Интернет и право. Москва: Бестселлер, 2003. 272 с.

5. Декларація про державний суверенітет України: Закон України від 16.07.90 р. URL: https://zakon.rada.gov.ua/laws/show/55-12 (дата звернення 21.04.2019).

6. Комагоров В.П. Архитектура сетей и систем телекоммуникаций: учебное пособие. Томск: Изд-во Томского политехн. ун-та, 2011. 154 с.

7. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV. Дата оновлення: 04.11.2018. URL: https://zakon.rada.gov.ua/laws/show/1280-15/stru (дата звернення: 01.05.2019).

8. Правила домену UA. URL: http://www.domenua.com.ua/uapolicy-ukr.php (дата звернення: 01.05.2019).

9. Berkens M. Verisign Renews Contract With Tuvalu To Run.TV Registry Through 2021. *The Domains.com.* February, 25, 2015. URL: https://www.thedomains.com/2012/02/25 (дата звернення: 01.05.2019).

10. Соболев С., Истомина М. Не наш YouTube: почему ФАС отказалась считать видеосервис частью Рунета? *РБК: Технологии*. 16.05.2018. URL:https://www.rbc.ru/technology _and_media/ 16/05/2018/5afae6119a794735ac623eab (дата звернення: 01.05.2019).

11. Mansourov A. North Korea on the Cusp of Digital Transformation: Nautilus Institute Special Report. October, 2011. URL: http://www.nautilus.org/wp-content/uploads/2011/12/DPRK_ Digital_Transformation.pdf (дата звернення: 01.05.2019).

12. Komiyama K. The Information Technology Industry in North Korea. *Keio University Global Research Institute Working Papers*. 2019. Vol. 4. URL: http://www.kgri.keio.ac.jp/en/docs/ S180620190226.pdf (дата звернення: 01.05.2019).

13. Гогилашвили Е. Как сидят в Интернете в Северной Корее? *BIT.UA.* 10.09.2018. URL: https://lab.bit.ua/2018/09/north-korea-intranet/ (дата звернення: 01.05.2019).

14. Schiess N. Governmental Control of Digital Media Distribution in North Korea: Surveillance and Censorship on Modern Consumer Devices. *DPRK Tech Info*. 2017. May. URL: https://dprktech.info/media/governmental_control_of_digital_media_distribution_in_north_korea-nschiess.pdf (дата звернення: 01.05.2019).

15. Tushar S.D. Now The Super-Secure Red Star OS Can Be Hacked With Just A Link. *TechViral*. December, 6.2016. URL: https://techviral.net/now-red-star-os-can-be-hacked (дата звернення: 01.05.2019).

16. Choe Sang-Hun. North Koreans Rely On Smuggled Cellphones to Connect to the Outside World. *The New York Times*. March, 26, 2016. URL: https://www.nytimes.com/2016/03/27/world/ asia/north-korea-china-mobile-phones.html (дата звернення: 01.05.2019).

17. Kim Joon-Ho, Lee Jiin-Jun, Lipes J. North Korea Shuts Down Illegal Cell Phone Access to Chinese Networks. RFA. 20.09.2018. URL: https://www.rfa.org/english/news/korea/cellphones-0920 2018161614.html (дата звернення: 01.05.2019).

18. О внесении изменений в Федеральный Закон “О связи” и Федеральный Закон “Об информации, информационных технологиях и защите информации”: Федеральный Закон Российской Федерации от 01.05.19 г. № 90-ФЗ. URL: http://publication.pravo.gov.ru/File/GetFile/0001201905010025?type=pdf (дата звернення: 01.05.2019).

19. О внесении изменений в Федеральный Закон “О связи” и Федеральный Закон “Об информации, информационных технологиях и защите информации”: пояснительная записка к законопроекту № 608767-7 от 14.12.18 г. URL: https://sozd.duma.gov.ru/bill/608767-7 (дата звернення: 01.05.2019).

20. Tallinn Manual on The International Law applicable to Cyber Warfare/ Ed. Michael N. Schmitt. N.Y.: Cambridge University Press, 2013. 215 p.

21. Corn Gary, Taylor Robert. Sovereignty in the Age of Cyber. *AJIL Unbound*. 2017. Vol. 111. P. 207-212.

22. National Cyber Strategy of the USA. September, 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата звернення: 01.05.2019).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~