УДК 343.2+340.13+007.51+165.12

РАДУТНИЙ О.Е., *кандидат юридичних наук, доцент,* доцент кафедри кримінального права № 1 Національного юридичного університету імені Ярослава Мудрого, член ВГО “Асоціація кримінального права”

МОЖЛИВІСТЬ ЗАХИСТУ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ КРИМІНАЛЬНО-ПРАВОВИМИ ЗАСОБАМИ

Анотація. *В роботі розглянуто ознаки, що характеризують сучасний стан інформаційного суверенітету України, проаналізовано його нормативне забезпечення в сфері кримінально-правової охорони.*

Ключові слова: *суверенітет, інформаційний суверенітет, злочин, Інтернет, кібервійська, кібератака, нормативне забезпечення, кримінально-правова охорона.*

Аннотация. *В работе рассмотрены признаки, характеризующие современное состояние информационного суверенитета Украины, проанализировано его нормативное обеспечение в сфере уголовно-правовой охраны.*

Ключевые слова: *суверенитет, информационный суверенитет, преступление, интернет, кибервойска, кибератака, нормативное обеспечение, уголовно-правовая охрана.*

Summary. *The article discusses the features that characterize the current state of information sovereignty of Ukraine, analyzes its regulatory support in the field of criminal and law protection.*

Key words*: sovereignty, the sovereignty of information, crime, internet, cyber forces, cyber attack, regulatory support, criminal and law protection.*

Постановка проблеми. Відповідно до положень ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Невід’ємною складовою частиною суверенітету України виступає її інформаційний суверенітет, під яким згідно до положень ст. 1 Закону України “Про Національну програму інформатизації” від 04.02.98 р. № 74/98-ВР розуміють здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави.

Аналіз останніх досліджень. Питанню захисту інформаційної безпеки держави було приділено належну увагу у працях Д.С. Азарова, П.П. Андрушка, Л.В. Багрія-Шахматова, П.С. Берзіна, В.І. Борисова, В.М. Бутузова, В.Б. Вєхова, А.Г. Волєводзі, В.Д. Гавловського, Л.М. Герасіної, В.А. Голубєва, О.П. Горпинюка, В.К. Грищука, В.Д. Гулкевича, М.В. Гуцалюка, Ю.І. Дем’яненко, С.В. Дрьомова, Д.А. Калмикова, М.В. Карчевського, О.М. Костенка, В.В. Крилова, О.В. Красненкова, Є.В. Лащука, С.Я. Лихової, В.О. Меркулової, Т.В. Міхайліної, А.А. Музики, В.О. Навроцького, А.С. Нерсесян, Ю.Ю. Орлова, С.О. Орлова, М.І. Панова, М.В. Плугатир, М.В. Рудика, Н.А. Савінової, К.С. Скоромнікова, В.В. Сташиса, В.Я. Тація, П.Л. Фріса, С.О. Харламової, В.Б. Харченко, А.В. Черних та ін.

Проте, на жаль, ще трапляються випадки сумніву щодо існування інформаційного суверенітету держави і, як наслідок, можливості дослідження форм та засобів його кримінально-правового забезпечення (так, окремі знані вчені – члени редакційної колегії електронного наукового видання “Віснику Асоціації кримінального права України” [1] наполегливо рекомендували автору змінити назву та окремі положення відповідної наукової статті з зазначених міркувань).

© Радутний О.Е., 2014

Втім, проблема інформаційного суверенітету України і сама по собі є малодослідженою, що, безумовно, потребує подальшої розробки.

Метою статті є аналіз сучасного стану інформаційного суверенітету України, можливість його захисту існуючими кримінально-правовими засобами, дослідження необхідності внесення змін у чинне законодавство України.

Виклад основного матеріалу. Наведене вище нормативне визначення інформаційного суверенітету, без сумніву, потребує подальшого вдосконалення. При його розробці слід звернути увагу не тільки на здатність держави контролювати і регулювати потоки інформації з-поза меж держави, але і всередині неї, і, особливо, на її спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним загрозам. Але за механізмом та формами такого регулювання воно має відповідати меті забезпечення та захисту основних та похідних прав і свобод громадян, всього суспільства у цілому, гарантування розвитку культурної та критично мислячої особистості.

Як варіант, можливо запропонувати визначення *інформаційного суверенітету України* як *верховенство та незалежність держави в інформаційній сфері, її здатність у відповідності до прав і свобод людини та громадянина контролювати і регулювати потоки інформації з-поза меж держави та всередині неї, спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним загрозам*.

Згідно до ст.ст. 53, 54 попередньої редакції Закону України “Про інформацію” від 02.10.92 р. № 2657-XII, яка діяла до 10.05.11 р. (Законом України від 13.01.11 р. № 2938-VI “Про внесення змін до Закону України “Про інформацію” вказаний закон було викладено в новій редакції, яка вже не містить нижченаведених положень) основою інформаційного суверенітету України визначались національні інформаційні ресурси, до яких входила вся належна Україні інформація, незалежно від змісту, форм, часу і місця створення. Передбачалося, що Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

З цим визначенням можливо було б погодитися і зберегти його у чинному законодавстві з урахуванням декількох суттєвих зауважень.

Інформаційними ресурсами є весь масив інформації в інформаційних системах – мережі Інтернет, окремих комунікативних пристроях, бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах тощо.

Схоже визначення цього терміну дає згаданий Закон України “Про Національну програму інформатизації” від 04.02.98 р. № 74/98-ВР, який у статті 1 визнає інформаційним ресурсом сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо). Але відповідно до нього не може бути визнана інформаційним ресурсом та інформація, яка не має форми документу, що є суттєвим недоліком наведеного нормативного визначення. Ситуація ще більш ускладниться, якщо у межах кримінально-правового забезпечення пригадати ті роз’яснення з цього питання, які містяться у Законах України “Про інформацію” від 02.10.92 р. № 2657-XII, “Про бібліотеки і бібліотечну справу” від 27.01.95 р. № 32/95-ВР, “Про обов’язковий примірник документів” від 09.04.99 р. № 595-XIV, Рішенні Державної комісії з цінних паперів та фондового ринку “Про затвердження Положення про порядок складання інформації щодо діяльності саморегулівних організацій ринку цінних паперів та подання відповідних документів до Державної комісії з цінних паперів та фондового ринку” від 14.06.05 р. № 316 тощо, або у примітці до ст. 358 КК України, а саме, документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі, або матеріальна форма одержання,

зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві; офіційний документ – документ, що містить зафіксовану на будь-яких матеріальних носіях інформацію, яка підтверджує чи посвідчує певні події, явища або факти, які спричинили чи здатні спричинити наслідки правового характеру, чи може бути використана як документи – докази у правозастосовчій діяльності, що складаються, видаються чи посвідчуються повноважними (компетентними) особами органів державної влади, місцевого самоврядування, об’єднань громадян, юридичних осіб незалежно від форми власності та організаційно-правової форми, а також окремими громадянами, у тому числі самозайнятими особами, яким законом надано право у зв’язку з їх професійною чи службовою діяльністю складати, видавати чи посвідчувати певні види документів, що складені з дотриманням визначених законом форм та містять передбачені законом реквізити.

Оскільки за своїм змістом поняття “інформаційний ресурс” є більшим за обсягом, ніж “документ”, то до інформаційних ресурсів слід віднести і новини у стрічках (on-line-новини), електронні періодичні видання, електронні архіви і бази даних, окремі майданчики для обміну інформацією (Twitter, Facebook, YouTube, ЖЖ, “ВКонтакте”, “Одноклассники” та інші) тощо.

Виникає питання про здатність держави контролювати і регулювати потоки інформації, спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним загрозам, які виникають та мають поширення у цьому середовищі, тобто, питання про сучасний стан інформаційного суверенітету України.

На необхідність участі саме на державному рівні в процесі обігу будь-якої інформації вказують дії найбільш потужних держав сучасності – Сполучених Штатів Америки та Російської Федерації.

Так, починаючи з 2009 року Пентагон оголосив про створення власних кібервійськ – United States Cyber Command [2], а з 2013 року у складі Міністерства оборони РФ створено Силы специальных операций Российской Федерации [3], які за даними аналітиків, опікуються і питаннями інформаційної війни.

Самі інформаційні війни не є винаходом сучасного інформаційного суспільства (необхідність проведення масових або вузько спрямованих інформаційних заходів була затребуваною на всіх історичних етапах розвитку людства та у всіх його політичних формаціях), проте сьогодні вони вийшли на новий технологічних рівень.

Так, відомий російський виробник антивірусного програмного забезпечення “Лаборатория Касперского” (//www.kaspersky.ru) за останні роки виявив декілька бойових вірусів, які є настільки складними, що їх розробкою, без сумніву, фундаментально і багато часу займалися великі за чисельністю групи фахівців найвищої кваліфікації, а вартість розробки цих шкідливих програм оцінена в 100 мільйонів доларів США. Зрозуміло, що жодним децентралізованим хакерам або їх невеличким об’єднанням, що не підпорядковані потужним державним структурам, такі результати не під силу.

Один з таких вірусів був вже випробуваний в Іраку під час бойових дій для виведення із строю всіх центрифуг супротивника, а тим, хто не має власних технологій протидії і відповідних приладів для цього, залишається переймати досвід героя оповідання Віктора Пелевіна “Зенітні кодекси Аль-Ефесбі” і покладатися на несподівані підходи розв’язання інформаційних проблем.

Концепціями інформаційних війн, які розглядаються як на рівні підтримки державою у вигляді окремих програм (US NSDC (National Security Council) Report

68 “United States Objectives and Programs for National Security” (April 14, 1950) [4], Русская доктрина [5]), так і в публіцистиці (стаття Anne Applebaum під назвою “A need to contain Russia”, опублікована в “The Washington Post” 29 березня 2014 року [6]; книги “New Cold War” та “Spies, Lies and How Russia Dupes the West” британського журналіста Edward Lucas, публікації 2014 року – книги В. Коровина “Третья мировая сетевая война”, М. Старікова та Д. Бєляєва “Россия. Крым. История”, Д. Бєляєва “Разруха в головах. Информационная война против России” тощо), передбачається здійснення кібератак на об’єкти, що мають важливе економічне та(чи) оборонне значення, вплив на населення як власної держави, так і інших суверенних утворювань, за допомогою інформаційного маніпулювання, перекручення фактів, збудження відчуття обурення або прагнення відновлення історичної справедливості, штучного патріотизму тощо.

Вже на сьогодні в мережах Twitter, Facebook, або в “ВКонтакте” існує значна кількість акаунтів (“облікові записи”, від англ. *account*) як засобів вкидання певної інформації у широкі маси користувачів мережі Інтернет. Один найманець (фізична особа як користувач мережі Інтернет) може керувати приблизно 50 – 100 акаунтами. Для того, щоб ввести будь-яку інформацію на перші шпальти новин, треба зробити 4 – 5 тисяч репостів[1] з відповідним тегом (від англ. *tag* – “ярлик”, “етикетка”, “бирка”). Після цього вказана інформація протримається в якості новини впродовж доби. Про неї напишуть ЗМІ, в неї повірять мільйони людей і вона стане загальновідомою і загальнопоширеною.

В інформаційних війнах засоби масової інформації, блогсфери та соціальні мережи виступають в якості збройних засобів. Небезпечною з точки зору інформаційних загроз є також діяльність Інтернет-коментаторів (так званих “тролів”). Явище під назвою “тролінг” полягає у нагнітанні учасником Інтернет-спілкування гніву або конфлікту шляхом відкритого чи таємного перекручення, приниження або образи почуттів іншого співрозмовника. В якості засобів використовуються хвилі виправлень (постмодерація повідомлень, окремих тем або новин) – так званий “флейм” (від англ. *flame* – “полум’я”, “вогонь”), або конфронтація – так званий “холівар” (від англ. *holly war* – “священна війна”)[2]. Найбільшу небезпеку являють оплачувані коментатори, які розміщують свої повідомлення на замовлення за заздалегідь визначеною темою.

Основою здатності держави ефективно протидіяти зовнішнім та внутрішнім інформаційним загрозам є не тільки інформаційні ресурси, але й засоби комунікації (автономні інформаційні системи, незалежне програмне забезпечення, потужності для випуску електронно-обчислювальних машин тощо) і методи певної діяльності (виважені режими доступу, правила обігу певної інформації тощо).

Між тим, Україна не має своєї незалежної бази з випуску електронно-обчислювальних та комунікативних пристроїв, не підтримує паростки своїх національних виробників, не задіє державних програм заохочення щодо них. Поодинокі суб’єкти господарювання, такі як ТМ Impression (//www.impression.ua) повністю

[1] “Репост” – засіб поширення інформації в мережі Інтернет, що полягає у її передачі в соціальних мережах від одного користувача до іншого шляхом збереження на власній сторінці (від англ. *repost* – “визначення”, “зв’язок”, “образ” тощо).

[2] Див. додатково: Семенов Д.И., Шушарина Г.А. Сетевой троллинг как вид коммуникативной деятельности // Международный журнал экспериментального образования : научный журнал. – М., 2011. – Вып. 8. – С. 135-136; Внебрачных Р.А. Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник Удмуртского университета. – 2012. – Вып. 1. – С. 48-51. – Режим доступу : http://vestnik.udsu.ru/2012/2012-031/vuu_12_031_08.pdf

залежать від іноземних комплектуючих та програмного забезпечення. Відсутні також і власні національні майданчики для обміну інформацією (на кшталт Twitter, Facebook, YouTube, ЖЖ, “ВКонтакте”, “Одноклассники” тощо).

Відсутність технологічного циклу з виготовлення сучасного пристрою, в т.ч. його процесору та мікросхем, або програм, які забезпечують роботу цього пристрою, не дозволяє державі почувати себе у безпеці в інформаційній сфері як на рівні фізичних пристроїв, так і на рівні їх змістового наповнення.

Структура всесвітньої мережі Інтернет побудована таким чином, що її основні базові центри, вузли та магістралі знаходяться за межами території України. Національний уряд України не має як впливу, так і відношення до таких транснаціональних корпорацій, як ICANN (https://www.icann.org/ru – некомерційна організація з розподілу адрес та номерів, яка відповідає за глобальну координацію системи унікальних елементів Інтернету, стабільність роботи та безпечну організацію), IANA (//www.internetassignednumbersauthority.org – “Адміністрація адресного простору Інтернет” – організація, що управляє просторами IP-адрес, доменів верхнього рівня, а також реєструє типи даних MIME і параметри інших протоколів Інтернету, працює під контролем ICANN), ISOC (//www.internetsociety.org – міжнародна професійна організація, що здійснює розвиток та забезпечення доступу у мережі Інтернет) та інших, які насправді її контролюють.

Відсутність власної інформаційної інфраструктури, складовими якої виступають незалежні Інтернет, телебачення, засоби масової інформації тощо, не дозволяє державі вести інформаційні війни або боронитися від інформаційних атак як на своїй території, так і на території інших учасників інформаційних відносин.

Україна не має державних структур, які б цілеспрямовано здійснювали захист від кібератак та негативного інформаційного впливу як на загальнонаціональному, так і локальному рівнях. На рівні урядових організацій відсутні адекватні план та методи протидії зазначеним явищам.

З огляду на вищезазначене можливо прийти до висновку про критично низький рівень інформаційного суверенітету України або відсутність такого взагалі.

У зв’язку з цим виникає питання, чи можливо охороняти кримінально-правовими засобами те, що не існує, або знаходиться на доволі низькому етапі розвитку.

Відповідь на це питання полягає у наступному. Не виникає сумніву щодо необхідності охорони життя, навіть якщо його рівень неухльно спадає, або охорони відносин статевої свободи чи недоторканності незалежно від моральних якостей потерпілої особи. Так само не виникає сумнівів у необхідності кримінально-правової охорони інформаційного суверенітету України навіть на тому рівні, який зараз існує. Завданням інших фундаментальних юридичних дисциплін є підвищення стандартів інформаційного суверенітету, розробка його ідеології та меж у співвідношенні з загальнолюдськими цінностями й міжнародними зобов’язаннями, а заходи кримінально-правового впливу виконуватимуть функції охорони та забезпечення розвитку вказаних суспільних відносин.

Під час розгляду актуальної проблеми завжди виникає питання про дослідження рівня нормативного забезпечення інформаційного суверенітету України в галузі кримінально-правової охорони.

Привабливим кроком виглядала би пропозиція якнайшвидшого внесення змін у чинний КК України у зв’язку з відсутністю статті, яка передбачає кримінальну відповідальність саме за порушення інформаційного суверенітету України. Така стаття і мала би диспозицію на кшталт “порушення інформаційного суверенітету України” або

описувала більш ранню поведінку особи як “дії, спрямовані на порушення інформаційного суверенітету України”. Але порушення навіть інформаційного суверенітету завжди виявлятиметься в конкретних формах. Наприклад, це можуть бути заклики до дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, надання інформаційної допомоги іноземній державі, збирання з метою передачі або передача відомостей, що становлять державну, банківську, комерційну таємницю, відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, розголошення державної таємниці тощо. Проте, відповідальність за такі дії вже передбачена ст.ст. 109, 111, 114, 231, 328, 330 КК України.

Крім того, Особлива частина КК України містить цілий розділ XVI “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку”, що в ст.ст. 361 – 3631 передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут, несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації, несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється, перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку КК України тощо.

Формами та способами порушення інформаційного суверенітету України також можуть бути і перешкоджання здійсненню виборчого права або права брати участь у референдумі, роботі виборчої комісії або комісії з референдуму чи діяльності офіційного спостерігача (ст. 157 КК України), надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (ст. 158 КК України), порушення таємниці голосування (ст. 159 КК України), порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер (ст. 163 КК України), перешкоджання законній діяльності професійних спілок, політичних партій, громадських організацій (ст. 170 КК України), посягання на здоров’я людей під приводом проповідування релігійних віровчень чи виконання релігійних обрядів (ст. 181 КК України), приховування або перекручення відомостей про екологічний стан або захворюваність населення (ст. 238 КК України), публічні заклики до вчинення терористичного акту (ст. 2582 КК України), завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об’єктів власності (ст. 259 КК України), погроза вчинити викрадання або використати радіоактивні матеріали (ст. 266 КК України), заклики до вчинення дій, що загрожують громадському порядку (ст. 295 КК України), ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та

дискримінацію (ст. 300 КК України), ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України), схиляння до вживання наркотичних засобів, психотропних речовин або їх аналогів (ст. 315 КК України), спонукання неповнолітніх до застосування допінгу (ст. 323 КК України), схиляння неповнолітніх до вживання одурманюючих засобів (ст. 324 КК України), незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359 КК України), умисне пошкодження ліній зв’язку (ст. 360 КК України) тощо.

Висновки.

Україна має критично низький рівень власного інформаційного суверенітету, що потребує наполегливого підвищення останнього та його захист кримінально-правовими засобами. Чинний КК України містить достатню кількість норм, які здатні здійснювати охоронну та превентивну функції щодо інформаційного суверенітету України. У зв’язку з цим відсутня необхідність його доповнення нормою з формулюванням “порушення інформаційного суверенітету України” у назві та(або) диспозиції.

Перспективи подальших досліджень. Зазначене не відкидає необхідності пошуку інших форм реагувань на новітні виклики сучасності, дослідження щодо яких передбачається здійснювати у напрямі вдосконалення організаційних механізмів державного управління в інформаційній сфері та розвитку заходів кримінально-правового забезпечення.

Використана література

1. – Режим доступу : //www.nauka.jur-academy.kharkov.ua

2. United States Cyber Command. – (Wikipedia). – Режим доступу : //www.en.wikipedia.org/wiki/United_States_Cyber_Command

3. Силы специальных операций Российской Федерации. – (Википедия). – Режим доступу : https://ru.wikipedia.org/wiki/Силы_специальных_операций_Российской_Федерации

4. NSC 68: United States Objectives and Programs for National Security. – Режим доступу : https://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm

5. Русская доктрина. – Режим доступу : //www.rusdoctrina.ru/page95507.html

6. Applebaum A. A need to contain Russia / The Washington Post. – 29.03.2014. – Режим доступу : //www.washingtonpost.com/opinions/anne-applebaum-a-need-to-contain-russia/2014/03/20/8f2991dc-b06b-11e3-9627-c65021d6d572_story.html

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