УДК 342.9

ІНФОРМАЦІЙНІ ІНТЕРВЕНЦІЇ ЯК ЗАГРОЗА КІБЕРНЕТИЧНІЙ БЕЗПЕЦІ

Діордіца І.В., к. ю. н.

У статті автор здійснив етимологічне тлумачення термінів, які становили понятійно-категорійний апарат дослідження. Запропонував звужене та розширене розуміння терміну «інформаційна інтервенція». Акцентував увагу на відсутності законодавчого визначення (діючого), так як і доктринального. Для юриспруденції інформаційна інтервенція була визначена як одне із багатьох ґрунтовно недосліджених феноменів у вітчизняній науці. Зазначено, що кібернетична безпека є частиною національної безпеки.

Ключові слова: *кібернетичний, інформаційний, інформаційна інтервенція, інтервенція, кіберпростір, інформаційне суспільство, кібернетична безпека.*

В статье автор осуществил этимологическое толкование терминов, которые составляли понятийно-категорийный аппарат исследования. Предложил узкое и расширенное понимание термина «информационная интервенция». Акцентировал внимание на отсутствии как законодательного определения (действующего), так и доктринального. Для юриспруденции информационная интервенция была определена как одно из многих основательно неисследованных феноменов в отечественной науке. Отмечено, что кибернетическая безопасность является частью национальной безопасности.

Ключевые слова: *кибернетический, информационный, информационная интервенция, интервенция, киберпространство, информационное общество, кибернетическая безопасность.*

Diorditsa I.V. INFORMATION INTERVENTION AS SECURITY THREAT CYBERSECURITY

It was noted that in narrow and simplified sense information intervention could be understood as a violent intervention of one or more subjects of information relations in someones activities, and in wide sense – it is a set of aggressive in nature actions which are aimed at influencing public opinion and decision making within same or another state and achieving well-defined results. It was also stressed that this phenomenon has always negative manifestation. Information intervention poses a great risk to cyber security, becouse latter is a part of national security and may cause harm to state as a whole and individuals. It was fixed that creation of an effective system for ensuring of cyber security requires from authorities of Ukraine a clear definition of public policy in this area and timely response to dynamic changes occurring in world in area of cyber security with ability to use foreign experience. Thus, the choice of specific means and methods to ensure cyber security of Ukraine is caused by need to take timely measures which are appropriate to scale and nature of actual and potential cyber threats to vital interests of man and citizen, society and state.

Key words: *cyber, informational, informational intervention, intervention, cyberspace, information society, cyber security.*

Постановка проблеми. Україна вступає в нову еру інформаційного суспільства – в еру інформаційних війн. Реалізація національних інтересів щодо забезпечення національної безпеки – один із найважливіших напрямів цієї трансформації. Так, в тексті «Доктрини інформаційної безпеки України», яку було прийнято 28 квітня 2014 року (натомість із незрозумілих нам причин скасовано в 2015 р.), було сказано, що за умов швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної (кібернетичної) безпеки.

Значна низка суспільно небезпечних діянь, спрямованих на заподіяння шкоди державним інтересам, сьогодні може вчинятися як в інформаційному просторі, так і в суто кіберпросторі. З розвитком інформаційного суспільства (далі – ІС) виокремилося певне спрямування злочинних намірів на заподіяння шкоди віддаленим предметам і посягання на об'єкти, які раніше були фактично недосяжні для такої значної кількості осіб. Вчинення посягань на державні політичні та економічні інтереси шляхом втручання в функціонування їх учасників та інститутів, у межах яких вони діють, містять ознаки інтервенції: насильницького втручання в інтереси держав та органів влади держав із боку інших суб'єктів. Оскільки вчинюються подібні дії з використанням комп'ютерних систем і вчинюються у кіберпросторі, вказаний вид інтервенції нами пропонується визначати як «кібернетична інтервенція», характеризуючи її як окрему групу суспільно небезпечних діянь, спрямованих на завдання шкоди інформаційній інфраструктурі держав, життєво важливим сферам існування суспільства. Ці та інші фактори і обумовлюють актуальність нашого дослідження.

Ступінь розробленості проблеми. Окремі аспекти проблематики формування інформаційного суспільства у той чи інший спосіб досліджувались у наукових працях таких вітчизняних учених, як: наукова школа В.А. Ліпкана [1–9], І.В. Арістова [10–11], В.С. Цимбалюк [12–15], І.В. Сопілко [16] та інших, проте незважаючи на те, що теорія інформаційного суспільства є певним чином достатньо розробленою і репрезентованою різноманітними концепціями, але питання інформаційної інтервенції як загрози кібернетичній безпеці є абсолютно новим, що зумовлює потребу у його ретельному дослідженні. Особливо слід зупинитись на тих загрозах, які існують у зв'язку із розвитком інформаційного суспільства в Україні. Окремо зазначимо про викори-

стання праць політологів, а саме: Г.Г. Почепцова [17–19], В.В. Івановського [20].

Метою даної статті є аналіз інформаційної інтервенції як загрози кібернетичній безпеці.

Для досягнення поставленої мети автором було сформульовано завдання здійснити етимологічний аналіз понять, які становлять основу категорійного ряду нашого дослідження, а саме: інформаційний, інтервенції, загроза, кібернетичний та безпека, а потім шляхом їх поєднання і реалізувати ціль наукового доробку.

Виклад основного матеріалу. Вирішуючи поставлені завдання, здійснимо розбір понятійно-категоріального апарату. Перш за все, визначимося із поняттям інформаційний. Використовуючи тлумачний словник української мови, зазначимо, що під «інформаційним» мається на увазі той, що стосується до інформації, який містить інформацію; який опрацьовує та видає інформацію; стосується до інформації як газетно-журнального жанру, що містить інформацію, відомості про що-небудь; стосується до інформації як сукупності відомостей або сигналів, що містяться де-небудь або передаються від одного об'єкта іншому [21, с. 128]. У нашому дослідженні ми будемо використовувати дефініцію «інформаційний», як той, що стосується інформації. Також зауважимо на тому, що згідно з українським законодавством з інформацією можуть бути вчинені різноманітні дії: створення, збирання, одержання, зберігання, використання, поширення, охорона та захист.

Наступною категорією є «інтервенція» – насильне збройне втручання однієї або кількох держав у внутрішні справи іншої держави; агресія [21, с. 129]. Щодо доктринального тлумачення даного терміну, то зазначимо, що під інтервенцією розуміється – насильницьке втручання однієї чи кількох держав у внутрішні справи іншої держави, спрямоване проти її територіальної цілісності або політичної незалежності. У наш час такі цілі означають несумісність з цілями і принципами Статуту ООН [22].

В іншому джерелі знаходимо інше тлумачення: інтервенція (лат. interventio – втручання) – втручання однієї або кількох держав у справи іншої держави або в її взаємозв'язки з третіми державами [23].

Проаналізувавши, консолідувавши та адаптувавши дані дефініції до нашого дослідження, визначаємо інтервенцію як насильницьке втручання одного суб'єкта відносин у діяльність (або справи) іншого.

Також, інкорпоруючи цей та попередній термін, пропонуємо звужене та спрощене авторське розуміння терміну інформаційна інтервенція – насильницьке втручання одного або декількох суб'єктів інформаційних відносин (оскільки всі дії мають місце при використанні інформації) у діяльність іншого чи інших суб'єктів. Нині категорія інформаційна інтервенція досліджується та вживається вченими-політологами, політиками, при написанні різноманітних блогів, але залишається поза межами правового регулювання як на національному, так і на міжнародному рівнях. Тому дане питання є актуальним для здійснення комплексного дослідження в юриспруденції та висунення обґрунтованих пропозицій передусім правового характеру.

Зараз багато дискусій точиться навколо того, що ж таке інформаційна інтервенція і як їй протидіяти.

Для формулювання вичерпнішого визначення «інформаційної інтервенції» здійснимо аналіз існуючих наукових розвідок, в яких дана категорія становила ключовий інтерес.

Так інформаційну інтервенцію визначають як:

– комплекс цілеспрямованих, скоординованих у часі заходів, що забезпечують подання каналами розповсюдження та телекомунікацій масової тенденційної інформації у заздалегідь заданому режимі або її інтерпретацію у потрібному ракурсі з метою впливу на суспільну думку і прийняття рішень в іншій державі, а також інформаційні технології і інформаційна техніка та обладнання іноземного виробництва, споживачами якої є мешканці країни-об'єкта інформаційної інтервенції [20];

– тенденційну інформацію, коли розповсюджуються через системи зв'язку суб'єктивні факти та суб'єктивна інформація, які впливають на суспільну думку і прийняття рішень в іншій державі. В рамках інформаційної інтервенції здійснюють маніпулювання інформацією для досягнення певної мети [24]. З даним визначенням ми не погоджуємося, оскільки, як було зазначено вище, інтервенція – втручання, тобто певні активні дії, які носять протизаконний характер, але не об'єкт;

– під кібернетичною інтервенцією (як видове поняття до родового – інформаційна інтервенція) слід розуміти сукупність агресивних дій у кіберпросторі, спрямованих на втручання шляхом застосування інформаційно-комп'ютерних технологій у внутрішні та зовнішні справи держав із метою заподіяння шкоди їхньому суверенітету або належному функціонуванню їхніх керівних органів або основних сфер життєдіяльності, а отже – аналогічні дії відносно впорядкованої діяльності міждержавних об'єднань та їх керівних органів [25]. На нашу думку, дане трактування є досить обширним та обґрунтованим.

Таким чином, здійснивши контент-аналіз даних та інших дефініцій, зазначимо, що під «інформаційною інтервенцією» в широкому сенсі варто розуміти певний комплекс дій агресивного характеру (агресія знаходиться за межами закону), які спрямовані на здійснення впливу на суспільну думку і прийняття рішень всередині однієї або іншої держави, та досягнення чітко визначених результатів. Також наголошуємо на тому, що дане явище завжди має негативний прояв.

Проаналізувавши та синтезувавши ситуацію в інформаційному просторі України, сформульовано твердження про те, що інформаційну інтервенцію можна поділити на:

– духовну (комплекс цілеспрямованих, скоординованих у часі заходів, що забезпечують подання каналами розповсюдження та телекомунікацій масової тенденційної інформації у заздалегідь заданому режимі або її інтерпретацію у потрібному ракурсі з метою

впливу на суспільну думку і прийняття рішень в іншій державі);

– матеріальну (інформаційні технології і інформаційну техніку та обладнання іноземного виробництва, споживачами якої є мешканці країни-об'єкта інформаційної інтервенції) [20].

На сьогоднішній день повністю відсутній механізм протидії цьому явищу, і в результаті цього наш національний інформаційний простір залишився відкритим і беззахисним, чим і скористалися інші країни, використовуючи це у власних інтересах. Як приклад, можемо зауважити про присутність зарубіжних телеканалів, таких як Euronews, BBC World News, Белсат ТВ та ін. [26]. Значною є присутність зарубіжних мовників і в радіопросторі України. Відомі українському слухачеві «Русское радио» и «Маяк» (Росія), радіостанції «Голос Америки» та «Свобода» (США), BBC (Великобританія) тощо [27]. Як теле– так і радіостанції досить часто транслюють українські та зарубіжні новини (інформацію), але з певним «викривленням» і, як результат, помилкове її застосування чи підроблення, спотворення й перекручування призводять до великих втрат.

Цьому сприяє відсутність Інформаційного кодексу, в якому було б систематизовано сукупність норм права, що регулюють увесь спектр суспільних інформаційних правовідносин.

Зокрема, канал «Інтер», який належав проурядовим особам, під час Євромайдану необ'єктивно подавав інформацію, часто спотворюючи окремі факти.

Зважаючи на приналежність кожного телеканалу, видавництва та інших засобів розповсюдження інформації певній особі, то за даного випадку абсолютно відсутня можливість об'єктивності та всебічності висвітлення подій.

На сьогоднішній день, окрім вищезазначених прикладів, можна також говорити про «спіраль мовчання», коли мас-медіа можуть маніпулювати громадською думкою за рахунок надання слова представникам меншості й замовчування думок більшості, а також за допомогою якої аналізуються процеси формування та функціонування громадської думки. Саме на перетині впливу масової комунікації й зворотної реакції індивідів народжується та взаємодія, яка змінює громадську думку.

Оскільки доведення інформації споживачам через ЗМІ відбувається дозовано та з «чітко визначеною метою», не з ціллю ознайомлення, а з уже сформованими та нав'язаними висновками, то, в даному випадку, відбувається певне маніпулювання суспільною думкою громадськості та формування передумов для унеможливлення вироблення самостійного бачення та формування власної думки щодо тих чи інших подій. Така ситуація є сприятливою для масового залякування або виділення «негативних» і «зайвих» персонажів як у політиці, так і в інших сферах суспільного життя [9, с. 134].

Прикладом внутрішніх ще радянських інтервенцій слід вважати телесеанси Кашпировського і Чумака, які «відключали» населення від проблем сьогодення. Внутрішня інформаційна інтервенція – це і програма «Погляд» часів перебудови. Тобто спочатку програма «Погляд» створювалася для одних цілей, а вже потім почала функціонувати для інших. Але на той час вона вже була розкручена як найцікавіший інформаційний продукт [18].

Сьогодні досить часто такі інформаційні інтервенції супроводжують виборчі кампанії, намагаючись принципово змінити їх хід за рахунок реінтерпретації дій свого опонента [19].

Варто зауважити, що присутність іноземних ЗМІ, особливо електронних, в інформаційному просторі України є досить високою. З одного боку, це сприяє диверсифікації джерел отримання інформації, розвитку конкурентного середовища на ринку ЗМІ, підвищенню якості телерадіопрограм, а з іншого – створює можливості для формування суспільної думки в Україні в інтересах зарубіжних держав і «сліпе» слідування нав'язаним ідеалам та абсолютне небажання чи невміння здійснення аналізу.

Слід звернути увагу на те, що якщо кримінальна інтервенція може відбуватися лише за умови посягання з перетином фізичних державних кордонів. Інформаційна інтервенція – інтервенція у інформаційне середовище, яке не має фізичних кордонів, що відокремлюють держави одну від одної, може бути як зовнішньою (здійснюватися з території іншої держави чи міждержавного об'єднання), так і внутрішньою (здійснюватися з території власної держави чи міждержавного об'єднання). За умови вчинення інформаційної інтервенції у співучасті різних держав вона має характеризуватися як змішана.

Також наголосимо на тому, що інформаційну інтервенцію можна визначити, як початок інформаційної війни. Як відомо, інформаційні війни – це дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації та процесам, що базуються на інформації та інформаційних системах ворога при одночасному захисті власної інформації та процесів, що базуються на інформації та інформаційних системах [16].

Українські експерти перераховують такі інформаційні війни, під обстріл яких потрапила Україна:

– просування ідеї расизму в Україні перед початком футбольного чемпіонату Євро-2012;

– героїзація російського президента Володимира Путіна в Україні;

– дискредитація європейського вибору шляхом акцентуації на питаннях гомосексуалізму;

– залякування сценаріями війни з Росією;

– підтримання антиукраїнської тези про крах Української держави, розповсюдження концепції failed state щодо України;

– інформаційна протидія Росії в галузі торгівлі зброєю.

Можна додати й просування ідеї антисемітизму в Україні у зв'язку з виступами представників «Свободи», які завжди чомусь за дивним збігом обставин супроводжувались присутністю російських ЗМІ, котрі одразу ж тиражували інформацію про антисемітизм в Україні [17].

Наступним поняттям є безпосередньо «загроза» – груба, зухвала обіцянка заподіяти яке-небудь зло, неприємність; погрожування, нахваляння; можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь; те, що може заподіювати яке-небудь зло, якусь неприємність [21, с. 268]. Саме останнє трактування ми і будемо використовувати.

Окремими категоріями є «кібернетичний» та «безпека». «Кібернетичний» – той, що стосується до кібернетики [21, с. 300]. «Безпека» – стан, коли кому-, чому-небудь ніщо не загрожує [21, с. 68]. Тобто під «кібернетичною безпекою», у спрощеному вигляді, можна розуміти стан, коли ніщо не загрожує кібернетиці.

Враховуючи різні наукові підходи до визначення безпеки, під кібернетичною безпекою пропонується розуміти стан захищеності життєво важливих інтересів і громадянина, суспільства і держави від зовнішніх та внутрішніх загроз, пов'язаних із використанням ресурсів кіберпростору (іншими словами ресурсами інформаційно-телекомунікаційних систем), за якого в державі забезпечуються гарантовані умови для реалізації державної інформаційної політики.

Водночас кібернетичну безпеку слід розглядати як складову інформаційної безпеки [28]. Кібернетична безпека охоплює лише ту частину інформаційної сфери, в якій для обробки інформації застосовуються інформаційно-телекомунікаційні системи.

Акцентуємо увагу й на існуванні проекту Закону України «Про кібернетичну безпеку України», в якому кібернетична безпека (кібербезпека) визначена, як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [29].

А в проекті Стратегії забезпечення кібернетичної безпеки України кібернетична безпека (кібербезпека) визначена як стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави [30].

Крім того, не зважаючи на те, що на даний час дію даного документа скасовано, відповідно до Доктрини інформаційної безпеки України, інформаційна (кібернетична) складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційна безпека розглядається і як невід'ємна складова кожної зі сфер національної безпеки, і як важлива самостійна сфера забезпечення національної безпеки.

У загальному основними загрозами кібернетичній безпеці України є:

– використання кіберпростору у воєнних цілях, створення іншими державами кібервійськ, кіберпідрозділів у традиційних родах військ;

– розроблення іноземними державами нових видів зброї кібернетичного характеру;

– існування в інших країнах планів наступальних та розвідувальних військових операцій у кіберпросторі;

– освоєння іноземними спеціальними службами методів розвідувально-підривної діяльності у кіберпросторі, методів маніпулювання суспільною свідомістю за допомогою кіберпростору;

– можливість втягування України у збройні конфлікти чи у протистояння з іншими державами через використання національного сегменту кіберпростору;

– спроби втручання у внутрішні справи держави (інформаційна інтервенція – авт.) з використанням соціальних мереж, поширення у національному сегменті кіберпростору культу насильства, жорстокості, порнографії;

– активізація проявів кібертероризму;

– поширення кіберзлочинності;

– критична залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції, поширення фактів включення у програмно-технічні засоби прихованих шкідливих функцій;

– зростання ризиків виникнення надзвичайних ситуацій техногенного характеру через зниження рівня захищеності об'єктів критичної інформаційної інфраструктури держави [29].

Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як зсередини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури, як «транзитного майданчика» для приховування атаки на інформаційну інфраструктуру третьої сторони [30].

Також як загрози в сфері кібернетичної безпеки можна виділити: кіберзлочинність, кібертероризм та кібершпигунство, кібервійна, а самі інформаційні інтервенції і можуть бути складовими перерахованих дій. Злочини із використанням сучасних інформаційно-телекомунікаційних технологій стають все звичнішою практикою в житті українських громадян.

Найбільше увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів.

Інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах, є стійким об'єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп активістів (хактивістів), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків.

З урахуванням широкої інформатизації сектора безпеки і оборони, зокрема, ство-

рення ЄАСУ ЗС України, оборонний потенціал нашої держави стає більш чутливим до кіберзагроз. Впровадження провідними країнами сучасних кіберозброєнь перетворює кіберпростір на окрему, поряд із традиційними «Земля», «Повітря», «Море», «Космос», сферу ведення бойових дій, а у найближчому майбутньому рівень обороноздатності країни буде визначатись у т. ч. наявністю у неї ефективних підрозділів для ведення бойових дій в кіберпросторі та здатність протистояти кіберзагрозам у сфері оборони [30]. Таким чином, нагальною є проблема створення інформаційних військ України.

У глобальному відкритому суспільстві, яким є інформаційне суспільство, кібернетична (інформаційна – авт.) інтервенція може мати не лише глобальні наслідки, як і безпосередньо полягати у діях, що характеризуватимуться глобальними ознаками: можливістю спільної участі в інтервенції необмеженої кількості суб'єктів, які значно віддалені один від одного щодо одного об'єкта, або щодо необмеженої кількості об'єктів одночасно. Аналогічно, можливе одночасне вчинення кіберзлочинів із метою інтервенції до великої кількості об'єктів або одного надважливого, у т. ч. стратегічного об'єкта. З урахуванням можливостей робити це поза межами кордонів на будь-якій відстані, тож підвищена загроза кібернетичній безпеці стає безперечною. На жаль, існують прямі докази наявних фактів вчинення кібернетичної інтервенції, що дозволяють констатувати факт існування такої.

Найпростішим прикладом кібернетичної інтервенції є триденна безперервна кібернетична атака на сайт Президента України В.А. Ющенка, яка розпочалася 30 жовтня 2007 року і нараховувала близько 18 тис. точкових атак, які вчинювалися з території РФ, Казахстану, України, США, Ізраїлю та Великобританії. Проте у служб безпеки такі дії не викликають особливого здивування, адже сайти президентів різних країн світу постійно піддаються подібним хакерським атакам. Хакери з ЄСМ заявляють, що слідом за сайтом Ющенка «положать» сайт СБУ [31].

Загроза кібернетичній безпеці у вигляді інформаційної інтервенції може бути не лише зовнішньою. Беруть участь у кібервійнах і українські хакери. Так, після подій навколо акту вандалізму на Говерлі [32] сайти Євразійського союзу молоді, який взяв відповідальність за їхнє проведення, були атаковані з України. У відповідь зазнали атак сайти Президента України та СБУ.

Більш сучасним прикладом є хакерська активність 2014–2015 р.р.: сайт Минрегиона был взломан хакерами – пресс-служба ведомства 27.12.2014 [33], хакеры взломали Twitter Администрации Президента Украины 14.07.2015 р. [34], сайт Президента Украины прекратил работу и выдает ошибку 20.07.2015 р. [35] та ін.

Кібернетичні атаки на офіційні сайти вищих керівних органів держав не обмежуються прикладами стосовно атак на сайти президентів, наведені вище. Атакуються комп'ютерні системи всіх гілок влади у всьому світі: атаки здійснюються з метою перешкоджання діяльності прокуратури; з метою фальсифікації списків виборців і фальсифікації підрахунку голосів на виборах, посягаючи, відповідно, на функції державного обвинувачення або на волевиявлення народу, яке є складовою суверенітету держави.

Не можна не приділити окремої уваги можливості спрямування кібернетичної інтервенції в мілітаристичну сферу. Сучасна мілітаристична війна неможлива без використання інформаційно-комп'ютерних технологій – ІКТ.

Слід наголосити на тому, що в разі цілеспрямованої кібернетичної інтервенції з метою захоплення керування подібним арсеналом, а це в умовах динаміки розвитку ІКТ та ІТ не виключено, подібна атака або певні її елементи зможуть бути застосовані злочинцями за їхнім волевиявленням проти внутрішніх і зовнішніх інтересів держави чи кібернетичної безпеки, зокрема, або міждержавного об'єднання на розсуд злочинців. Окремі злочини, що можуть бути вчинені у складі інформаційної інтервенції, можуть призвести, щонайменше, до втрати високоточною зброєю орієнтації або втрати зв'язку з пунктами керування.

Можливість здійснення інформаційної інтервенції обумовлюється станом розвитку саме ІКТ і їх запровадженням у всі сфери життєдіяльності сучасного суспільства.

Інформаційна інтервенція першочергово спрямовується на інформаційні комп'ютерні технології, що забезпечують належне функціонування систем життєзабезпечення суспільства, і це, структурно, є визначальною ознакою інформаційної інтервенції, як специфічної групи злочинів, що створюють загрози розвитку інформаційного суспільства.

Особливу небезпеку становлять соціальні ризики, здатні створити об'єктивну загрозу національній безпеці так званих країн-донорів, тобто країн, що підлягають інформаційній інтервенції. В умовах поширення світових глобалізаційних процесів інформаційні простори різних держав взаємодіють, проникають один в інший, взаємоперетворюються. Зворотною стороною цього є небезпеки, пов'язані зі складнощами державного контролю і впорядковування цих власне самоорганізаційних процесів, від яких найбільше потерпають так звані слабкі держави.

По-перше, ці держави мають значно менші технічні й технологічні можливості та ресурси порівняно з добре розвиненими. По-друге, їх державна інформаційна політика, як правило, недосконала і належно не сформульована. По-третє, рівень загальної й інформаційної культури не тільки населення відповідних країн, а й соціуму загалом, надто низький.

Відтак їх інформаційний простір майже не захищений від інформаційної інтервенції, поширення несанкціонованої, чужинної медіапродукції, виробленої технологічно потужнішими державами-агресорами, а вони самі і їх населення надміру вразливі до медіавпливу. Інформаційна інтервенція спричинює вкрай небезпечні наслідки: обмежує державний суверенітет країн-донорів; узалежнює їх від світової, міжнародної ситуації; уніфікує їх культуру,

тобто підводить її під нав'язані маніпуляторами стандарти; робить їх заручниками світових політичних, економічних, фінансових подій і криз (цін на енергоносії і пальне, екологічних проблем тощо); примушує до невигідної міжнародної співпраці; нав'язує неякісну, чужинну медіапродукцію (чужинні ідеї, стандарти, норми життя, медіанасильство, порнографію і т. ін.). У результаті з національного інформаційного простору витісняється своє, національне, те, що зміцнює націю, гарантує її національну ідентичність [36].

Поява нових медіа полегшила процес міжнародних інформаційних інтервенцій, бо вони створюють інформаційно-комунікативний простір, в якому пришвидшено всі процеси обміну. Державний апарат не в змозі реагувати і прогнозувати можливі наслідки таких інтервенцій. І майже на кожному кроці він програє [18].

І відкриті, й закриті системи можуть наражатися на інформаційні інтервенції. Закриті системи більше їх бояться, оскільки блокують альтернативні смисли, тож коли ті потрапляють у їхнє інформаційне поле, закриті системи не можуть витримати удару. Адже блокуються саме ті смисли, до яких ця система має найбільшу чутливість. Багато в чому саме так впав і Радянський Союз, коли його почали бомбардувати шкідливими для нього смислами. Але перебудова відрізнялася ще й тим, що це смислове бомбардування робила сама влада, лише частково йшлося про зовнішні інформаційні інтервенції. Інформаційні інтервенції в закриту систему, як це продемонструвала перебудова, намагаються поєднати з тими суб'єктами та об'єктами, які в цій системі були забороненими. Це створює механізми самопоширення такої інформації, після того як її було введено із зовні [17].

Унаслідок неналежного правового регулювання в національному інформаційному просторі України спостерігається низка негативних явищ, які створюють реальні та потенційні загрози кібернетичній безпеці. У 2014 році на території Автономної Республіки Крим та південно-східних регіонах України здійснювався інформаційно-психологічний тиск на населення України з боку засобів масової інформації Російської Федерації, спостерігалася інформаційна експансія (чи інтервенція – авт.) у національний інформаційний простір України, захоплювались стратегічні об'єкти української телекомунікаційної інфраструктури.

Поділяємо наукову позицію про те, що з метою попередження зловживання інформацією та для захисту інформаційних прав сучасний стан забезпечення національної та кібернетичної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз та реалізації права на отримання достовірної інформації. Паралельно все вищевикладене свідчить про потребу прийняття нормативно-правових актів, в яких був би передбачений механізм захисту інформаційних прав від протиправних дій третіх осіб щодо інформації [16].

Продовжуючи ідею загроз кібернетичній безпеці, можна зауважити, що є залежність країни і в інформаційному, і смисловому вимірах. Це коли країні не вистачає власних новин чи власних фільмів, і вона заповнює ці прогалини чужим продуктом. Україна є чітким прикладом цієї ситуації.

У той же час, у широкому сенсі, ідеологія кібернетичної інтервенції у ІС характеризується іншою ідеєю, виокремленою від ідеї звичайної кіберзлочинності, що направлена, як і загальнокримінальна злочинність, на, переважно, отримання певної матеріальної вигоди.

Очевидно, що в умовах розвитку інформаційного суспільства питання криміналізації інформаційної інтервенції мають порушуватися на міжнародному рівні за ініціативи й окремих держав. Однак ініціатива запровадження відповідних заходів кримінально-правової політики має носити здебільшого міжнародний характер: на рівні модельних конвенцій, і, очевидно, спільних стратегій між країнами кооперативних об'єднань (НАТО, ЄС) [37].

Висновки. Таким чином, здійснивши дослідження, ми дійшли наступних висновків.

У звуженому та спрощеному сенсі інформаційна інтервенція – насильницьке втручання одного або декількох суб'єктів інформаційних відносин у діяльність іншого чи інших, а в широкому – певний комплекс дій агресивного характеру, які спрямовані на здійснення впливу на суспільну думку і прийняття рішень всередині однієї або іншої держави, та досягнення чітко визначених результатів.

Акцентуємо, що дане явище завжди має негативний прояв.

Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці, оскільки остання є частиною національної безпеки, та може завдавати школи як державі в цілому, так і окремим фізичним особам. Створення дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення правових засад державної політики у цій сфері та своєчасного реагування на динамічні зміни, що відбуваються у світі в сфері забезпечення кібернетичної безпеки із можливістю застосування міжнародного досвіду.

При цьому, вибір конкретних засобів і способів забезпечення кібернетичної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави.

ЛІТЕРАТУРА:

1. Ліпкан В.А. Інкорпорація інформаційного законодавства України: [монографія] / В.А. Ліпкан, К.П. Череповський / за заг. ред. В.А. Ліпкана. – К.: ФОП О.С. Ліпкан, 2014. – 408 с.

2. Ліпкан В.А. Теорія управління в органах внутрішніх справ: [навчальний посібник] / За ред. В.А. Ліпкана. – К.: КНТ, 2007. – 884 с.

3. Баскаков В.Ю. Інформація з обмеженим доступом: поняття та ознаки / В.Ю. Баскаков // Актуальні проблеми державотворення: матеріали науково-практичної конференції (Київ, 28 червня 2011 р.). – К. : ФОП О.С. Ліпкан, 2011. – С. 47–49.

4. Залізняк В.А. Міжнародно-правове регулювання права на інформацію / В.А. Залізняк // Підприємництво, господарство і право. – 2010. – № 8. – С. 69–72.

5. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Логінов; Нац. акад. внутр. справ України. – К., 2005. – 20 с.

6. Череповський К.П. Інкорпорація інформаційного законодавства України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / К.П. Череповський; Запоріз. нац. ун-т. – Запоріжжя, 2013. – 19 с.

7. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 280 с.

8. Ліпкан В.А. Теоретична концепція Білої книги / В.А. Ліпкан // Підприємництво, господарство і право. – 2010. – № 9. – С. 80–83.

9. Рудник Л.І. Право на доступ до інформації: дис. ... канд. юрид. наук : 12.00.07 / Національний університет біоресурсів і природокористування України / Л.І. Рудник. – К., 2015. – 247 с.

10. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : ... дис. д-ра. юр. наук : 12.00.07 / І.В. Арістова. – Х., 2002. – 476 с.

11. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: [монографія] / за заг. ред. О.М. Бандурки – Харків: вид-во Ун-ту внутр. справ, 2000. – 368 с.

12. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : [монографія] / В.С. Цимбалюк. – К.: «Освіта України» 2010. – 388 с.

13. Цимбалюк В.С. Основи інформаційного права України: [навч. посібн.] / [В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.]; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К.: Знання, 2004. – 274 с.

14. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства / В.С. Цимбалюк – К. : Освіта України, 2011. – 426 с.

15. Цимбалюк В.С. Концепція кодифікації законодавства України про інформацію / В.С. Цимбалюк // Інформаційні технології в глобальному управління: матеріали міжнародної науково-практичної конференції (м. Київ, 29.10.2011 р.). – К.: ФОП О.С. Ліпкан – С. 73–91.

16. Сопілко І.В. Інформаційні загрози та безпека сучасного українського суспільства. – [Електронний ресурс]. – Режим доступу : http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/8181/9770.

17. Почецов Г.Г. Інформаційні війни в закритих і відкритих системах. – [Електронний ресурс]. – Режим доступу : http://www.academy.gov.ua/doc/zmi_pro_nas/publ/publ_2013_06_30.pdf.

18. Почепцов Г.Г. Нові медіа як засіб міжнародних інформаційних інтервенцій. – [Електронний ресурс]. – Режим доступу: http://osvita.mediasapiens.ua/material/13955.

19. Почепцов Г.Г. Внутрішні інформаційні інтервенції. – [Електронний ресурс]. – Режим доступу : http://osvita.mediasapiens.ua/ethics/manipulation/vnutrishni_informatsiyni_interventsii/.

20. Івановський В.В. Структура інформаційної інтервенції в українське суспільство. – [Електронний ресурс]. – Режим доступу : http://eprints.zu.edu.ua/2444/1/37-40.pdf.

21. Великий тлумачний словник сучасної української мови / [укл. О. Єрошенко]. – Донецьк: ТОВ «Глорія Трейд», 2012. – 864 с.

22. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду

ООН від 26 червня 1945 р. – [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/995_010.

23. Танцюра В.І. Політична історія України: навчальний посібник / За ред. В.І. Танцюри. – 2-ге вид., доповн.. – К., 2008. – 552 с.

24. Інформаційні війни: теорія, PR, зв'язки із громадськістю, дипломатія. – [Електронний ресурс]. – Режим доступу : http://politiko.ua/blogpost82707.

25. Савінова Н.А. Кібернетична інтервенція: до питань походження та потреби криміналізації в умовах формування та розвитку інформаційного суспільства. – [Електронний ресурс]. – Режим доступу : http://justinian.ua/article.php?id=3912.

26. Канали незалежних операторів. – [Електронний ресурс]. – Режим доступу : http://xtratv.com.ua/uk/kanali-nezalezhnih-operatoriv.

27. Світ радіо. – [Електронний ресурс]. – Режим доступу : http://www.proradio.org.ua/wire/.

28. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2. – С. 299–309.

29. Проект Закону України «Про кібернетичну безпеку України» від 04 червня 2013 р. – [Електронний ресурс]. – Режим доступу : pw1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=47240...

30. Проект Стратегії забезпечення кібернетичної безпеки України. – [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf.

31. Хакери з ЄСМ заявляють, що слідом за сайтом Ющенка «положать» сайт СБУ. –

[Електронний ресурс]. – Режим доступу : http://www.unian.ua/politics/73946-hakeri-z-esm-zayavlyayut-scho-slidom-za-saytom-yuschenka-polojat-sayt-sbu.html.

32. Евразийский союз молодежи уничтожил Герб Украины на вершине Говерлы, 18.10.07 р. – [Електронний ресурс]. – Режим доступу : http://korrespondent.net/ukraine/events/212658-evrazijskij-soyuz-molodezhi-unichtozhil-gerb-ukrainy-na-vershine-goverly.

33. Сайт Минрегиона был взломан хакерами – пресс-служба ведомства, 27.12.2014 г. – [Електронний ресурс]. – Режим доступу : http://korrespondent.net/ukraine/3461338-sait-mynrehyona-byl-vzloman-khakeramy-press-sluzhba-vedomstva.

34. Хакеры взломали Twitter Администрации Президента Украины 14.07.2015 г. – [Електронний ресурс]. – Режим доступу : http://ru.tsn.ua/ukrayina/hakery-vzlomali-twitter-administracii-prezidenta-ukrainy-451401.html.

35. Сайт Президента Украины прекратил работу и выдает ошибку 20.07.2015 г. – [Електронний ресурс]. – Режим доступу : http://rian.com.ua/politics/20150720/370831489.html.

36. Петрунько О.В. Соціалізувальні ресурси і ризики агресивного медіа середовища. – [Електронний ресурс]. – Режим доступу : http://elibrary.kubg.edu.ua/2638/1/O._Petunko_%20RMOVLP_17_SRRAM.pdf.

37. Савінова Н.А. Кібернетична інтервенція: до питань походження та потреби криміналізації в умовах формування та розвитку інформаційного суспільства. – [Електронний ресурс]. – Режим доступу : http://justinian.ua/article.php?id=3912.