УДК 32.019.5-049.5(477)

Шатун В. Т.,
канд. політ. наук, доцент кафедри державної політики та менеджменту,
Гладун О. В.,
магістрант, Інститут державного управління, Чорноморський державний університет ім. Петра Могили, м. Миколаїв, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА – НЕВІД'ЄМНА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У статті розглядається питання важливості інформаційної безпеки в умовах розвитку інформаційного суспільства та глобальної інформатизації. Акцентовано увагу на сучасному стані захищеності інформаційних ресурсів держави. Здійснено оцінку державної політики у сфері захисту інформації. Проаналізовано основні загрози національній безпеці в інформаційній сфері та заходи державної політики щодо її забезпечення. Окреслено ключові проблеми функціонування та вдосконалення системи захисту інформації на державному рівні. Доведено, що сучасний стан інформаційної захищеності ще не є досить досконалим і потребує свого подальшого розвитку як в технологічному плані, так і на законодавчому рівні.

Ключові слова: *інформація; інформаційні ресурси; інформаційний простір; національна безпека; інформаційна безпека; загроза інформаційній безпеці; інформаційно-психологічна безпека; інформаційні війни.*

Постановка проблеми у загальному вигляді. Розвиток і впровадження практично в усі сфери діяльності інформаційних технологій суттєво змінює структуру суспільства, а також трансформує міжнародні відносини. Одним з найважливіших напрямів цієї трансформації стає реалізація національних інтересів щодо забезпечення національної безпеки.

Такі перетворення призвели до того, що в даний час усе більш актуального характеру набуває забезпечення інформаційної безпеки України як невід'ємного елементу її національної безпеки, а захист інформації перетворюється в одне із пріоритетних державних завдань.

Проблема створення і підтримки захищеного середовища інформаційного обміну, що реалізує певні правила і політику безпеки сучасної держави, є досить актуальною, адже інформація давно вже перестала грати чисто допоміжну роль, перетворившись на вельми важливий і вагомий, мало не матеріал, фактор зі своїми вартісними характеристиками, обумовленими тим реальним прибутком, який можна отримати від її використання. Водночас, цілком можливий сьогодні і варіант збитку, що наноситься власнику інформації шляхом несанкціонованого проникнення в інформаційну структуру і впливу на її компоненти.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми. Окремі питання, пов'язані з дослідженням інформаційної безпеки знайшли відображення в працях вітчизняних вчених: М. Дмитренко висвітлив проблеми інформаційної безпеки України в умовах глобальної інформатизації, М. В. Гуцалюк, який займався вивченням загальних концепцій захисту інформації, А. М. Гуз більш детально розглядав питання історії захисту інформації, А. В. Ліпінська досліджувала інформаційні ресурси в їх загальному розумінні та ступінь їх захищеності на сьогодні.

Формування мети (постановка завдання). Питання інформаційної безпеки як складової національної безпеки України досліджено неповною мірою і потребують подальшого вивчення. Адже нині інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни. Це, в першу чергу, обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, – істотним зростанням впливу інформаційної сфери на життя нашого суспільства.

Виклад основного матеріалу дослідження обґрунтуванням отриманих наукових результатів. Інформація є необхідною складовою функціонування усіх соціальних систем. У приватному житті, для управління складними технологічними системами або для розбудови незалежної держави завжди є нагальна потреба у надійній та оперативній інформації. З метою задоволення інформаційних потреб громадян, юридичних осіб і держави органи державної влади та органи місцевого самоврядування здійснюють інформаційну діяльність та створюють інформаційні служби, системи, мережі, бази і банки даних відповідно до ст. 12 Закону України «Про інформацію».

Окремі документи й масиви документів (справи) на будь-яких носіях, у тому числі таких, що забезпечують роботу обчислювальної та організаційної тех-

ніки, створюють інформаційний ресурс – сукупність документів в інформаційних системах (у бібліотеках, архівах, банках даних тощо). Інформаційні ресурси (інформація) є об'єктами відносин фізичних і юридичних осіб між собою та з державою. Разом вони становлять інформаційні ресурси України і захищаються законом поряд з іншими видами ресурсів. Інформаційна діяльність здійснюється в інформаційному просторі України – середовищі, в якому здійснюються продукування, зберігання та поширення інформації і на яке розповсюджується юрисдикція України.

Становлення України як суверенної держави співпало з формуванням у ньому інформаційного суспільства, що потребує розробки принципів інформаційної безпеки людини і громадян, суспільства, держави.

Згідно з Законом України «Про основи національної безпеки України» від 19 червня 2003 року, національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам. Загрози національній безпеці – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України [8].

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві в інформаційній сфері є:

− прояви обмеження свободи слова та доступу громадян до інформації;

− поширення засобами масової інформації культу насильства, жорстокості, порнографії;

− комп'ютерна злочинність та комп'ютерний тероризм;

− розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційну інформацію, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

− намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Отже, інформаційна безпека – стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації, несанкціоноване поширення та використання інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій.

Загроза інформаційній безпеці – це явище, дія негативних чинників або процеси, через які соціальні об'єкти інформаційної безпеки частково або цілком втрачають можливість реалізувати свої інтереси в інформаційній сфері; порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об'єктів інформаційної безпеки [3, с. 16].

Соціальними об'єктами інформаційної безпеки є: особа – її права та свободи в інформаційній сфері; суспільство – його духовні цінності, засади солідарної діяльності; держава – її конституційних лад, суверенітет, ефективне функціонування.

Технічними об'єктами інформаційної безпеки є інформаційні ресурси, інформаційна інфраструктура, інформаційні технології.

Система забезпечення інформаційної безпеки України – це організована державою сукупність суб'єктів (державних органів, посадових осіб, громадських організацій, окремих громадян), об'єднаних цілями та завданнями захисту національних інтересів України в інформаційній сфері, які здійснюють узгоджену діяльність у межах законодавства України.

В Україні політика забезпечення інформаційної безпеки будується на таких засадах:

− обмеження доступу до інформаційного ресурсу є винятком із загального принципу відкритості інформації й реалізується тільки відповідно до чинного законодавства;

− суб'єкти, які збирають, накопичують і обробляють персональні дані й конфіденційну інформацію, несуть відповідальність перед законом за збереження і використання;

− держава забезпечує захист суспільства від хибної, викривленої і недостовірної інформації, що надходить через засоби масової інформації;

− держава реалізує контроль за створенням і використанням засобів захисту інформації шляхом їхньої обов'язкової сертифікації та ліцензування діяльності в галузі захисту інформації;

− держава сприяє всебічному розвитку української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України [4].

Система суб'єктів забезпечення інформаційної безпеки складається з:

− органу законодавчої влади – Верховної Ради України;

− органів судової влади – Конституційний суд, суди загальної юрисдикції;

− органи виконавчої влади – Кабінету Міністрів України та місцевих державних адміністрацій;

− галузевих органів державного управління, що регулюють інформаційні відносини в певних галузях – Державний комітет зв'язку та інформатизації України, Державний комітет телебачення та радіомовлення України, Департамент спеціальних телекомунікаційних систем захисту інформації Служби безпеки України;

− правоохоронних органів – Прокуратура України, Міністерство внутрішніх справ України, Служба безпеки України;

− підприємств, організацій, фірм різних форм власності, діяльність яких пов'язана з наданням послуг зв'язку, із захистом інформації, інформаційних агенцій, суб'єктів видавничої справи.

Указом Президента України «Про заходи щодо забезпечення інформаційної безпеки держави» від 18 вересня 2002 року № 836/2002 з метою підвищення рівня захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, забезпечення інформаційної безпеки держави утворено Державний центр інформаційних та телекомунікаційних систем у складі Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (далі – Департамент), який здійснює методичне керівництво та координує діяльність державних органів, пов'язану із запобіганням, виявленням, реагуванням та усуненням наслідків несанкціо-

нованих дій щодо державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, надає в разі потреби допомогу цим органам у здійсненні заходів із попередження порушення цілісності, доступності та конфіденційності зазначених ресурсів [1, с. 34].

Органи виконавчої влади з метою захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах:

− визначають перелік інформаційних та телекомунікаційних систем, які містять державні інформаційні ресурси, та погоджують його з Департаментом;

− здійснюють згідно з вимогами нормативно-правових актів з питань захисту інформації під методичним керівництвом Департаменту заходи щодо захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, у тому числі підключених до глобальних мереж передавання даних;

− збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків;

− невідкладно (протягом доби) інформують Департамент про спробу вчинення чи власне вчинення несанкціонованих дій;

− надають на запит Департаменту інформацію про технічні та програмні засоби, що використовуються для надання мережних послуг, а також про зміни у способах або видах підключення до глобальних мереж передавання даних;

− здійснюють разом з Департаментом оцінку рівня захищеності державних інформаційних ресурсів на всіх етапах життєвого циклу інформаційних та телекомунікаційних систем під час створення або удосконалення комплексних систем захисту інформації відповідно до вимог нормативно-правових актів з питань захисту інформації;

− оновлюють за рекомендацією Департаменту антивірусні програмні засоби, використовуючи при цьому лише ті з них, які пройшли експертизу в Департаменті.

Координаційним органом з питань національної безпеки, у тому числі й інформаційної є Рада національної безпеки і оборони України, яка координує і контролює діяльність органів виконавчої влади у сфері національної безпеки й оборони. Головою Ради відповідно до ст. 107 Конституції України є Президент України [1, с. 42].

Необхідною складовою інформаційної безпеки є захист інформації від її втрати, витоку або розголошення. Зазвичай зловмисників цікавить передусім виробничо-технологічна інформація та ділова. Іноземні спецслужби може цікавити також стратегічно важлива для України інформація.

Відповідно до інтересів забезпечення національної безпеки і ступеня цінності для держави, а також правових, економічних та інших інтересів користувачів, за режимом доступу інформація поділяється на відкриту інформацію, тобто загальнодоступну, яка використовується в роботі без спеціального дозволу, поширюється через засоби масової інформації, оголошується на конференціях, у виступах та інтерв'ю; та інформацію з обмеженим доступом, яка містить відомості, які становлять той чи інший вид таємниці і підлягають захисту як з боку держави, так і відповідних користувачів.

Порядок обігу інформації з обмеженим доступом регулює ст. 30 Закону України «Про інформацію». Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

До конфіденційної інформації належить медична, тобто свідчення про стан людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я. Конфіденційними є також відомості, що містяться у деклараціях державних службовців. Під комерційно таємницею підприємства розуміють відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення яких може завдати шкоди його інтересам. Склад і обсяг відомостей, що становлять комерційну таємницю та порядок її захисту визначаються керівництвом підприємства. Предметом адвокатської таємниці є питання, з яких громадянин або юридична особа зверталися до адвоката, суть консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні своїх професійних обов'язків.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють до неї систему захисту.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до Закону України «Про державну таємницю» від 21 січня 1994 року [2].

Стаття 8 зазначеного Закону визначає інформацію, що може бути віднесена до державної таємниці. У цій самій статті відзначено, що забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Зазвичай джерела інформації містять інформацію як відкритого, так і обмеженого доступу. Причому інформація того й іншого фонду перебуває в єдиному інформаційному просторі і розділити її без ретельного змістовного аналізу часто не можливо. Наприклад, систематизована сукупність відкритої інформації може у комплексі містити зведення обмеженого доступу.

Особливо складна проблема сьогодення – завчасне створення засобів, необхідних для інформаційного

протиборства, або, якщо користуватися американською термінологією, – «інформаційної війни» [2].

У цій сфері розвитку озброєнь розглядаються два типи дій і, відповідно, дві групи засобів. Перша сукупність засобів зв'язку, що пов'язана з «інформаційною війною» як специфічним видом протиборства, можливо не пов'язаного з традиційними військовими діями, в особливій сфері, що називається «інфосферою». При цьому зачіпаються усі компоненти інформаційного потенціалу держав: інформація і її інформаційні носії, центри зосередження інформації; наукові і всі інші кадри – творці та споживачі інформації; технічні засоби збору, переробки, накопичення, збереження і передачі інформації; програмно-математичні засоби; інфраструктура всебічних систем управління; органи управління інформаційними ресурсами держави. Хоча така війна буде вестись спеціальними структурами, у ній є суттєвий військовий аспект, оскільки можливі наслідки, що знизять бойові можливості збройних сил, а саме: блокування системи управління ракетно-ядерною зброєю та іншими стратегічними системами військового призначення; порушення роботи систем управління військово-транспортними перевезеннями та іншими системами забезпечення військових формувань (матеріалами, енергією, тощо); різке погіршення морально-політичної обстановки у військових формуваннях, серед їх резерву і зниження бойового духу особового складу внаслідок дезінформації, порушення систем забезпечення життєдіяльності, дезорганізації систем управління тощо.

Серед нових найбільш важливих засобів «інформаційної війни» сьогодні називають різні математичні, програмні засоби типу «вірусів» і «закладок», засоби дистанційного витирання інформації, що записана на магнітних носіях, генераторами електромагнітних імпульсів, засоби неконтрольованого включення у закриті інформаційні мережі та ін.

У більш вузькому розумінні словосполучення «інформаційна війна» стає одним із різновидів бойових дій – інформаційних, або важливою фазою безпосередньої підготовки до них.

Найважливішими складовими концепції «Інформаційна війна» є: оперативна безпека, введення супротивника в оману, психологічні операції, електронна війна і вогневе знищення, які проводяться в комплексі з глибокою і всебічною розвідкою як для дезорганізації системи управління противника, так і для захисту власної системи управління в ході бойових дій. При цьому інформація, що циркулює в системі управління, розглядається як високопріорітетний об'єкт впливу і захисту, зниження або підвищення достовірності.

Якісно новий рівень сучасних інформаційних технологій дозволяє ефективно проводити інформаційні операції, які є складовими інформаційних війн, у глобальних масштабах з метою формування в потрібному руслі та контролю над масовою свідомістю населення. За допомогою інформаційної зброї вирішуються типові завдання:

− маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни супротивника з метою створення політичної напруженості та хаосу;

− дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби, провокації репресій проти опозиції, провокація взаємознищення;

− зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;

− дезінформація населення про роботу державних органів, підрив їх авторитету, дискредитація органів управління;

− провокація соціальних, політичних, національних і релігійних заворушень;

− ініціація страйків, масового безладдя й інших акцій економічного протесту;

− підрив міжнародного авторитету держави, його співробітництва з іншими країнами;

− завдання збитків життєво важливим інтересам держави в політичній, економічній, оборонній і в інших сферах [4].

Важливим заходом у сучасних умовах є забезпечення інформаційно-психологічної безпеки України. Основними заходами щодо реалізації державної політики в цьому напрямі мають стати:

– оцінка стану інформаційно-психологічної безпеки в країні, виявлення джерел внутрішніх і зовнішніх загроз інформаційно-психологічної безпеки громадян, визначення пріоритетних напрямів відвертання, парирування і нейтралізації цих загроз;

– удосконалення нормативно-правової бази забезпечення інформаційно-психологічної безпеки громадян України;

– координація діяльності органів державної влади і інших органів, на яких покладено завдання забезпечення інформаційно-психологічної безпеки громадян України;

– контроль діяльності органів державної влади і органів місцевого самоврядування, що беруть участь у вирішенні завдань забезпечення інформаційно-психологічної безпеки громадян України;

– попередження, виявлення і припинення правопорушень, що зазіхають на безпеку законних інтересів громадян, суспільства і держави в сфері забезпечення інформаційно-психологічної безпеки громадян;

– організація розробки державних і регіональних програм забезпечення інформаційно-психологічної безпеки громадян і координація робіт щодо їх реалізації;

– здійснення міжнародної співпраці у сфері забезпечення інформаційно-психологічної безпеки громадян, представлення інтересів України у відповідних міжнародних організаціях.

Держава в процесі реалізації своїх функцій із забезпечення інформаційно-психологічної безпеки громадян України повинна:

– організовувати і проводити об'єктивний та всебічний аналіз і прогнозування загроз інформаційно-психологічної безпеки України, розробляти заходи та механізми забезпечення інформаційно-психологічної безпеки громадян України;

– організовувати роботу органів державної влади щодо реалізації комплексу заходів, спрямованих на запобігання, парирування і нейтралізацію загроз інформаційно-психологічної безпеки України, локалізації та ліквідації наслідків їх прояву;

– організовувати взаємодію органів законодавчої та виконавчої влади з громадськими організаціями та громадянами в процесі виявлення загроз інформаційно-психологічної безпеки громадян України і визначення правових механізмів протидії цим загрозам;

– підтримувати законну діяльність громадських об'єднань у галузі протидії загрозам інформаційно-психологічної безпеки громадян України, а також забезпечення у встановлюваних законодавством рамках громадського та державного контролю діяльності засобів масової інформації;

– організовувати розробку вимог з безпеки сучасних інформаційних технологій для психічного здоров'я громадян та інформувати про них суспільство;

– здійснювати контроль діяльності органів державної влади щодо реалізації державної політики забезпечення інформаційно-психологічної безпеки України;

– здійснювати необхідну протекціоністську політику щодо організацій, що беруть участь у формуванні відкритих інформаційних ресурсів загального користування та надають інформаційні послуги громадянам на основі цих ресурсів;

– забезпечувати захист психіки дітей та молоді від впливу інформації, здатної завдати шкоди їх психічному здоров'ю;

– забороняти протиправну діяльність громадських організацій і релігійних об'єднань, що завдає шкоди психічному здоров'ю людини і суспільства.

Недосконалість чинного інформаційного законодавства та фінансова слабкість більшості українських ЗМІ використовують закордонні неурядові організації, фінансово-політичні клани, радикальні та екстремістські налаштовані політичні сили для проникнення в інформаційний простір держави для використання його на свою користь. Зокрема, використовуючи можливості Українського медіапростору, іноземні держави здійснюють інформаційну політику у вигідному для них руслі (проведення широкомасштабних PR – акцій, стажування українських журналістів, поширення друкованої продукції тощо). Фіксуються непоодинокі спроби використати окремих радикально настроєних осіб з метою дестабілізації суспільно-політичної обстановки, розпалювання сепаратистських настроїв, національної та релігійної ворожнечі.

Відсутність механізмів державного контролю за розповсюдженням інформації через Інтернет сайти спричиняє стрімке збільшення обсягу повідомлень суспільно-політичного змісту (анонімних, достовірність яких викликає сумніви, провокативного і відверто протиправного характеру), які дублюються традиційними вітчизняними ЗМІ з посиланням на Інтернет.

До основних загроз інформаційній безпеці держави слід віднести посилення технологічної залежності від іноземних країн в інформаційній сфері України та витіснення з національного ринку засобів інформатизації і телекомунікації вітчизняного виробництва.

Використовуючи впливові політичні та бізнесові зв'язки, представники закордонних компаній впроваджують у державні установи телекомунікаційні і комп'ютерні обладнання іноземного виробництва з недокументованими функціями, чим створюють умови для віддаленого несанкціонованого доступу до інформації, що циркулює в інформаційно-телекомунікаційних системах та комп'ютерних мережах органів державної влади й місцевого самоврядування. В основному, цей процес відбувається за рахунок кредитів міжнародних фінансових організацій та в рамках міжнародної технічної допомоги, що супроводжується усуненням від участі у тендерах на постачання комп'ютерного й телекомунікаційного обладнання конкурентоспроможних вітчизняних компаній. Таким чином, створюються реальні передумови для технічного проникнення до державних інформаційних ресурсів.

Новою тенденцією, яка створює передумови до реалізації загроз інформаційній безпеці держави, є активізація діяльності іноземних суб'єктів господарювання щодо запровадження програмного забезпечення для систем електронного документообігу, за наявності достатньої кількості вітчизняних підприємств-розробників та постачальників аналогічної продукції. Окремі властивості зазначених програмних продуктів свідчать про можливу наявність недокументованих функцій.

Аналіз процесів, що відбуваються в інформаційній сфері, свідчить про існування передумов до порушення сталого функціонування системи управління державою та збройними силами в особливий період.

Стабільно високий інтерес закордонних бізнесових кіл щодо придбання контрольних пакетів акцій провідних вітчизняних компаній у сфері мобільного зв'язку, інформаційно-телекомунікаційних послуг та національних мереж передачі даних. Унаслідок цього може виникнути ситуація, при якій іноземні держави зможуть використовувати їх мережевий простір на шкоду інтересам України. Адже з розвитком засобів інформації й комунікацій, що оперують інформацією, трансформують, дозують її, створюється можливість певного інформаційного управління суспільством, у якому влада заснована й здійснюється шляхом панування над управлінням інформаційними потоками. Питання влади все частіше висувається як питання інформації: хто управляє її організацією, розподілом її потоків та її дозуванням, той реально управляє й самим суспільством [4].

Глобалізація відкритих комп'ютерних і телекомунікаційних мереж, швидке зростання світового ринку інформаційних технологій, продуктів і послуг, формування міжнародного інформаційного простору створюють передумови для порушення традиційних механізмів забезпечення геополітичної цілісності держав, роблять серйозний вплив на багато елементів державності та національних правових систем. Саме тому зростає значення міжнародно-правових механізмів регулювання інформаційної сфери. Нові тенденції необхідно враховувати під час визначення напрямів реалізації державної політики в частині розвитку інформаційного законодавства та його окремих напрямків.

Також Україні варто ініціювати міжнародні переговори з проблем забезпечення безпеки в інформаційній сфері. Зокрема, повинні бути досягнуті угоди між максимальною кількістю країн з координації діяльності у сфері боротьби з інформаційним тероризмом і інформаційним криміналом, із запобігання цих загроз і узгодження дій та в мінімізації їх наслідків. Предметом переговорів повинен також стати міжнародно-

правовий захист національних інформаційних ресурсів та інтелектуальної власності, а також авторських прав на матеріали, поширювані світовими відкритими мережами, в першу чергу через Інтернет. Повинні бути вироблені узгоджені національні та міжнародні правові норми, що встановлюють відповідальність за хакерство та інші комп'ютерні злочини, зловмисне проникнення в державні та корпоративні інформаційні мережі, порушення прав і законних інтересів громадян у процесі інформаційного обміну. Необхідно розглянути можливості контролю за поширенням у мережі Інтернет непристойної і такої, що наносить шкоду суспільній моралі, інформації, недобросовісну рекламу, розпалювання війни, шахрайські операції тощо, які чинять негативний вплив на масову свідомість, фізичне, психічне і соціальне здоров'я людей.

Державна інформаційна політика сьогодні спрямована на забезпечення належних правових, економічних, внутрішньо- і зовнішньополітичних, організаційних та інших умов. Усі ці умови необхідні для:

– створення розвиненої та захищеної інформаційної інфраструктури України;

– розвитку міжнародного співробітництва в інформаційній сфері та утвердження України як країни з інформаційним суспільством;

– забезпечення безпеки інформаційної діяльності, життєво важливих інтересів особи, суспільства та держави в інформаційній сфері.

Суттєвим для інформаційної політики будь-якої держави є дотримання балансу інтересів особистості, суспільства і держави. Держава повинна забезпечувати відкритість та поінформованість суспільства про діяльність її органів і суспільних інститутів в інформаційній сфері [4].

У нинішніх умовах для забезпечення безпеки національних інтересів в інформаційній сфері особливо важливою стає активізація діяльності суб'єктів стосовно інформаційної безпеки. Насамперед це стосується діяльності з питань захисту конституційних прав і свобод громадян, розвитку регіональних інформаційно-телекомунікаційних систем та забезпечення їх безпечного функціонування, формування регіональних відкритих інформаційних ресурсів та їх ефективного використання. Проблема забезпечення інформаційної безпеки України багато в чому обумовлена прогалинами в правовому регулюванні взаємодії органів виконавчої влади при вирішенні завдань забезпечення інформаційної безпеки.

Для вирішення цієї проблеми вважається доцільним здійснити наступні заходи:

– створити ефективну багаторівневу державну систему забезпечення інформаційної безпеки, у якій будуть діяти єдині правові норми і механізми захисту інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури й інформаційних прав громадян, здійснюватиметься ефективна координація діяльності органів державної влади й управління.

– розробити механізм узгодження діяльності органів державної і місцевої влади в забезпеченні інформаційної безпеки;

– активізувати діяльність із формування державної політики в забезпеченні інформаційної безпеки регіонів, створенні необхідних для реалізації цієї політики організаційних структур і нормативної правової бази;

– зміцнювати взаємодію регіональних структур із державними органами виконавчої влади при вирішенні питань забезпечення інформаційної безпеки.

Ще одна проблема, що пов'язана з функціонуванням державної системи інформаційної безпеки України, – це забезпечення прозорості діяльності державних органів, що беруть участь у формуванні відкритих державних інформаційних ресурсів і здійсненні доступу до них громадян. У даний час відсутність даної інформації стає перешкодою для залучення внутрішніх і закордонних інвестицій, оскільки комерційні структури готові вкладати свої гроші в розвиток відкритих державних інформаційних ресурсів за умови, що ці гроші будуть використані за призначенням.

Висновки. Сучасний глобальний інформаційний простір не має меж і володіє надшвидкісними можливостями. В той же час він також потерпає від стрімко зростаючої кількості незаконних втручань, які спрямовуються проти безпеки особистості, держави в цілому, міжнародної стабільності. Активізація інформаційного обміну між країнами формує ставлення до захисту комунікаційних систем, як до невід'ємної складової національної безпеки кожного учасника такого процесу, спонукає об'єднувати зусилля для вироблення єдиних, узгоджених підходів до забезпечення конфіденційності інформаційних ресурсів, що є власністю держави.

Ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає, в умовах науково-технічного прогресу та переходу до постіндустріального суспільства, загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до непоправних збитків суспільству й державі. Все це визначає проблему формування організаційно-правових засад системи управління і захисту інформаційних ресурсів, як найактуальнішу і невідкладну.

Стратегічно важливою залишається проблема координації правотворчого процесу щодо формування правових засад побудови, забезпечення функціонування і розвитку системи управління інформаційними ресурсами України, а також розвитку інформаційної інфраструктури країни.

Щодо перспектив подальших розвідок. Останні події в нашій державі показали, наскільки влада є неготовою протистояти інформаційним війнам, оскільки питання інформаційної політики не розглядаються на достатньому рівні. Необхідно звернути увагу на здобутки в цій сфері зарубіжних країн і налагодити законодавчий процес в системі захисту стратегічних інформаційних ресурсів.

ЛІТЕРАТУРА

1. Виноградова, Г. В. Інформаційне право : [навч. посібн.] / Г. В. Виноградова. – К. : МАУП, 2011.– 144 с.
2. Галамба М. Інформаційна безпека України: поняття, сутність та загрози [Електронний ресурс]. – Режим доступу : http://www.justinian.com.ua/article.php?id=2463.
3. Гуцалюк М. В. Організація захисту інформації : [навч. посібн.] / М. В. Гуцалюк. – К. : Альтерпрес, 2012. – 224 с.
4. Дмитренко М. Проблеми інформаційної безпеки України [Електронний ресурс]. – Режим доступу : http://social-science.com.ua/article/807.
5. Василенко Д. П. Законодавство провідних країн світу в сфері захисту інформації [Електронний ресурс] – Режим доступу : http://www.kdu.edu.ua/statti/2010-2-1(61)/128.PDF.
6. Про захист інформації в автоматизованих інформаційних системах: Закон України [Електронний ресурс] : офіц. вид. станом на 5.07.94 р.; № 80. – Режим доступу : URL: http://rada.gov.ua.
7. Про інформацію: Закон України [Текст] : офіц. вид. станом на 2 жовтня 1992 р. // Відом. Верховної Ради України. – 1992. – № 48. [Зміни внесено Законами України № 1642-III від 06.04.2000 р. // Відом. Верховної Ради України. – 2000. – №27; №304–III від 07.02.2002 р.]
8. Про основи національної безпеки України: Закон України [Електронний ресурс] : офіц. вид. станом на 19.06.2003 р.; № 964-IV. – Режим доступу : URL: http://rada.gov.ua.
9. Черненко Т. В. Пріоритети державної інформаційної політики в умовах гібридної війни / Т. В. Черненко // Стратегічні пріоритети. – № 4 (37), 2015. – С. 83–92.

В. Т. Шатун, А. В. Гладун,
Черноморский государственный университет им. Петра Могилы, г. Николаев, Украина

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – НЕОТЪЕМЛЕМАЯ СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ

В статье рассматривается вопрос важности информационной безопасности в условиях развития информационного общества и глобальной информатизации. Акцентировано внимание на современном состоянии защищённости информационных ресурсов государства. Осуществлена оценка государственной политики в сфере защиты информации, поскольку именно через информационную среду чаще всего осуществляются угрозы национальной безопасности в различных сферах деятельности государства. Проанализированы основные угрозы национальной безопасности в информационной сфере и меры государственной политики по ее обеспечению. Определены ключевые проблемы функционирования и совершенствования системы защиты информации на государственном уровне.

Предметом исследования является современное состояние, проблемы и перспективы развития системы защиты государственных информационных ресурсов.

Цель статьи заключается в исследовании современного состояния информационной безопасности государства, поскольку в условиях развития информационного общества и глобального внедрения информационных технологий, данный вопрос стал неотъемлемым элементом национальной безопасности страны.

Доказано, что современное состояние информационной защищённости еще не достаточно совершенным и требует своего дальнейшего развития, как в технологическом плане, так и на законодательном уровне.

Ключевые слова: *информация; информационные ресурсы; информационное пространство; национальная безопасность; информационная безопасность; угроза информационной безопасности; информационно-психологическая безопасность; информационные войны.*

V. Shatoon, O. Gladun,
Petro Mohyla Black Sea State University, Mykolayiv, Ukraine

INFORMATION SECURITY – THE MAIN COMPONENT OF NATIONAL SECURITY OF UKRAINE

The article discusses the importance of information security in the conditions of development of the information society and global information. The attention is focused on the current state of protection of information resources of the state. The estimation of the state policy in the sphere of protection of the information, since it is through the information environment is most often carried out threats to national security in various areas of the state. The analysis of the major threats to national security in the information sector and public policy measures to ensure it. Identified key issues and improving the functioning of the protection system at the state level information.

The subject of study is the current state, problems and prospects of development of system of protection of state information resources.

The purpose of the article is to study the modern state of information security of the state, as in the conditions of development of the information society and the global implementation of information technology, the issue has become an integral element of national security of the country.

It is proved that the current state of information security is still not perfect enough and requires further development, both in terms of technology and at the legislative level.

Key words: *information; information resources; information environment; national security; information security; information security threats; information and psychological security; information warfare.*

Рецензенти: **Багмет М. О.,** д-р іст. наук, професор;
Шевчук О. В., д-р політ. наук, професор.

Дата надходження статті до редколегії 26.04.2016