УДК 1:316.3+340.12

Є. М. Мануйлов, доктор філософії, професор;
Ю. Ю. Калиновський, доктор філософських наук, професор

РОЛЬ І МІСЦЕ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У РОЗБУДОВІ СУЧАСНОЇ УКРАЇНСЬКОЇ ДЕРЖАВИ

Досліджено сутнісні характеристики інформаційної безпеки держави. Визначено особливості взаємозв'язку державотворчого процесу в Україні з необхідністю створення національної системи інформаційної безпеки. Проаналізовано основні інформаційні загрози національній безпеці України. Обґрунтовано необхідність удосконалення правового забезпечення національної інформаційної безпеки з урахуванням закордонного досвіду. Узагальнено існуючі уявлення щодо різновидів і напрямів застосування інформаційної зброї у сучасних інформаційних війнах.

Ключові слова: *інформаційна безпека, державотворення, інформаційні загрози, інформаційна війна, інформаційний суверенітет, інформаційна зброя.*

Актуальність проблеми. В умовах глобальної конкуренції держав за сфери впливу посилилась боротьба між різними суб'єктами міжнародних відносин за панування над свідомістю окремих соціальних груп та цілих народів. Інформаційні війни стали реаліями сучасних міждержавних відносин. Для стабільного державного розвитку важливими стали не тільки економічна, військова, політична безпека, а й інформаційна. Захист інформаційного простору країни у всіх її вимірах став запорукою збереження й розвитку держави. На сьогодні Україна, здійснюючи складні демократичні та соціально-економічні трансформації, перебуває в зоні ризику з точки зору інформаційної безпеки, оскільки цій сфері не приділялась належна увага, що стало однією з причин посилення внутрішніх протиріч та конфліктів, інспірованих ззовні за допомогою в першу чергу інформаційно-комунікаційних засобів.

Окреслені вище проблеми обумовили ***мету*** нашої наукової розвідки, яка полягає у визначенні сутнісних характеристик інформаційної безпеки як важливого чинника державотворчого процесу в сучасній Україні.

Аналіз наукових джерел і публікацій. Узагальнюючи різноманітні підходи до розуміння природи інформаційної безпеки, фахівці виокремлюють її такі сутнісні характеристики: по-перше, це стан захищеності інформаційного простору; по-друге, це стан захищеності національних інтересів України в інформаційному середовищі; по-третє, це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі; по-четверте, це суспільні відносини, пов'язані із захистом життєво важливих інтересів

людини і громадянина, суспільства і держави від реальних та потенційних загроз в інформаційному просторі; по-п'яте, це невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [1, с. 36].

Специфіка інформаційної безпеки полягає в тому, що вона знаходить свій вияв у різноманітних сферах суспільного життя, оскільки збереження та захист інформації є важливою складовою їх функціонування в інформаційному суспільстві.

Як зауважує І. Боднар, головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної і державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні [2, с. 69].

На сучасному етапі вітчизняного державотворення Україна стала об'єктом потужних інформаційних атак, які спрямовані на ураження життєво важливих сфер існування нашої країни. За оцінками вітчизняних експертів з проблем інформаційної безпеки, що сформовані на основі аналізу іноземного впливу на інформаційний медіа- і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

– цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;

– активізація критики вищого державного керівництва України;

– здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах;

– посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;

– дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;

– зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї [3, с. 128].

Указані інформаційні загрози спрямовані на існування держави як цілісного інституційного утворення. У той же час не менш потужними є загрози

суспільній інформаційній безпеці країни, які мають дещо інші вектори впливу, їх руйнівний характер щодо функціонування держави є поліспрямованим та до певної міри латентним, а отже, вкрай небезпечним.

Так, на переконання вітчизняного дослідника О. Дзьобаня, традиційний підхід до визначення загроз інформаційній безпеці суспільства призводить до виділення таких основних їх груп. Перша група загроз пов'язана з бурхливим розвитком нового класу зброї − інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. Друга група інформаційно-технічних загроз для особистості, суспільства й держави − це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Третя група інформаційно-технічних загроз − електронний контроль за життям, настроями, планами громадян, політичних організацій. Четверта група інформаційних загроз − використання нової інформаційної технології у політичних цілях [4, с. 232].

Таким чином, для забезпечення інформаційної безпеки державотворчих процесів в Україні необхідно враховувати як інституційну, так і неінституційну складові. Аналізуючи цю проблему, на нашу думку, варто звернутися до закордонного досвіду. Зокрема, найважливішим аспектом у політиці адміністрації Б. Обами у сфері забезпечення інформаційної безпеки є більш тісне співробітництво держави і бізнесу, що спрямоване в першу чергу на захист державних інформаційних ресурсів, а також усього американського інформаційного простору. Також важливими в забезпеченні інформаційної безпеки є воєнні і розвідувальні аспекти. Досвід США представляє зацікавленість у сфері розвитку воєнних і розвідувальних технологій не тільки всередині ВПК, але й у питаннях державного стимулювання та підтримки інформаційних комерційних технологій. Особливо важливим є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління, а також високоточної зброї [5, с. 285–286].

Для здійснення ефективних, системних безпекових заходів у інформаційній сфері країни необхідно постійно вдосконалювати нормативно-правову базу задля збереження балансу між інтересами держави у сфері інформаційної безпеки та інформаційними правами людини. Так, у Великій Британії, наприклад, функціонує потужна система забезпечення інформаційної безпеки. Законодавство цієї держави передбачає не лише захист інформаційних прав та свобод громадян і громадських організацій, а й встановлює їх суттєве обмеження в інтересах національної безпеки. Функціонують закони «Про захист інформації», «Про збереження державної таємниці», «Про телекомунікації», а також Кодекс практики доступу до урядової інформації. Зокрема, згаданий

вище Кодекс регламентує порядок обмеження доступу до конфіденційної інформації, власником якої є держава, закон «Про захист інформації» адаптовано до вимог Директиви ЄС «Про захист інформації» (1998) [6, с. 92].

У свою чергу, в Німеччині був прийнятий Федеральний закон «Про телекомунікації» (1991), який надає федеральним землям право на ліцензування діяльності, спрямованої на обмеження поширення інформації забороненого змісту (насильство, агресія, порнографія тощо), а закон «Про Інтернет» (1997) накладає обмеження на свободу поглядів та розкриття змісту інформації, що призводить до політичної нестабільності. У лютому 2011 р. Федеративний уряд ухвалив Стратегію кібербезпеки для Німеччини, якою передбачено посилення захисту інфраструктури стратегічного значення. У рамках цього документа наголошувалося, що всі урядові органи, які займаються проблемами кіберзлочинності, мають взаємодіяти не тільки між собою, а й з приватним сектором. Задля забезпечення швидкого виявлення та локалізації небезпечних інцидентів у сфері інформаційних технологій передбачено створення Центру кіберреагування. До завдань цього органу віднесено також вироблення рекомендацій щодо вжиття заходів із забезпечення безпеки в інформаційній сфері. Йдеться також про створення Ради з кібербезпеки – нового органу на рівні державного секретаріату. Заслуговує на увагу, що на саміті ОБСЄ у 2011 р. Німеччина висловила готовність працювати над розробкою міжнародного документа, який би регулював діяльність держав у кіберпросторі та закріплював принципи посилення довіри, прозорості й безпеки [7, с. 24–26].

В Україні також прийнято низку законодавчих актів, які прямо або опосередковано впливають на стан інформаційної безпеки держави, регулюють діяльність суб'єктів інформаційно-комунікативної сфери. Серед законів, спрямованих на регулювання інформаційної сфери, слід виокремити такі: «Про інформацію», «Про доступ до публічної інформації», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про інформаційні агентства», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про науково-технічну інформацію». До інформаційної сфери належать також закони «Про пресу та інші засоби масової інформації», «Про друковані засоби масової інформації (пресу) в Україні», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про посилення захисту майна редакцій засобів масової інформації, видавництв, книгарень, підприємств книгорозповсюдження, твор-

чих спілок», «Про мораторій на відчуження від редакцій державних та комунальних засобів масової інформації приміщень та майна», «Про телебачення і радіомовлення». Водночас, на думку фахівців, норми інформаційного законодавства у значній кількості містяться в інших законах та опосередковано регулюють питання надання, отримання, розкриття, охорони інформації тощо. У зв'язку з цим у науці обґрунтовується доцільність та своєчасність проведення впорядкування інформаційного законодавства, його систематизації, зокрема шляхом прийняття Інформаційного кодексу [8, с. 61].

У підсумку зазначимо, що посилення законодавчої бази в інформаційно-комунікаційній сфері спрямовано в першу чергу на захист інформаційного суверенітету сучасних держав. З цього приводу дослідник Є. Кирильчук зауважує, що в науковій літературі, коли ведуть мову про захист національного інформаційного простору як такого, то мають на увазі насамперед державний інформаційний суверенітет, тобто належне володіння й розповсюдження всією спільнотою у державі відповідних національних інформаційних ресурсів. Інформаційний суверенітет − це виключне право держави на формування й використання всіх інформаційних засобів, створених на законодавчих засадах і за державний кошт. Часто, і особливо тепер, зазіхання (порушення) на державний інформаційний суверенітет спричиняє серйозні й складні інформаційні війни [9, с. 61].

Можна стверджувати, що на сучасному етапі вітчизняного державотворення захист інформаційного суверенітету, ефективна стратегія країни щодо існуючих та майбутніх інформаційних війн є одним із найголовніших завдань у сфері національної безпеки України. Визначаючись термінологічно щодо сутності інформаційної війни, варто погодитись з думкою дослідника С. Расторгуєва, який зауважує, що інформаційна війна – це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи систем (держав) одна на одну з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи за допомогою таких засобів, використання яких дозволяє досягати задуманих цілей [10, с. 455–456].

Особлива небезпечність інформаційної війни для існування держави полягає в тому, що вона, як правило, спрямована на «перепрограмування» свідомості населення, окремих соціальних груп: її результатом є ціннісні деформації суспільної свідомості, зміни у настроях та політичних уподобаннях громадян, які є небезпечними для існування країни. Слушно зауважує з цього приводу Р. Чирва, стверджуючи, що головне завдання інформаційних воєн полягає в маніпулюванні масами, дезорієнтації та дезінформації громадян, залякуванні супротивника своєю могутністю [11, с. 9].

Як правило, в інформаційних війнах держави застосовують так звану інформаційну зброю, захист від якої потребує від країни (об'єкта нападу) наявності спеціальних оборонних сил та засобів. Фахівці стверджують, що інформаційна зброя – це інформація (дані), яка є засобом ведення інформаційних воєн і призначення якої полягає у зміні системних якостей об'єкта інформаційного впливу за допомогою прихованих установок на здійснення задуманих користувачем інформаційної зброї дій. Напрями і приклади використання інформаційної зброї є такі:

− порушення, пошкодження або модифікація інформаційних ресурсів і знань людей про самих себе та про середовище, яке їх оточує;

− здійснення впливу на суспільну думку та позицію політичної еліти;

− завдання шкоди протилежній стороні дипломатичними засобами;

− пропагандистські, психологічні та підривні акції у сфері культури й політики;

− дезінформація;

− чутки, створені навмисно;

− упровадження у ЗМІ своїх прибічників для проведення підривних акцій;

− проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне введення різного роду помилок у програмне забезпечення об'єкта;

− інформаційна підтримка дисидентських та опозиційних рухів [12, с. 332].

Необхідно зазначити, що інформаційна зброя особливо ефективно діє проти тієї країни, яка знаходиться у кризовому стані, у суспільній свідомості якої панує ціннісна амбівалентність, соціально-політична невизначеність. Застосування інформаційної зброї стає особливо ефективним, коли у державі спостерігається протистояння між політичними силами, наявною є криза моральної та правової свідомості, є слабкою патріотично налаштована еліта у всіх сферах суспільного життя.

На думку науковців, інформаційна зброя поділяється на два види: інформаційно-технічна та інформаційно-психологічна. Інформаційно-технічна зброя – це зброя, яка впливає на інформаційні ресурси, мережі і системи державного і військового управління. Вона поділяється на:

− алгоритмічну, яка призначена для виведення з ладу або зміни алгоритму функціонування програмного забезпечення інформаційних систем, ресурсів і мереж;

− програмну, яка призначена для руйнування, спотворення (довільним чином) кодів програм, блокування та підміни (фальсифікації) масивів інформації, а також нейтралізації тестових програм і систем захисту інформаційних ресурсів;

– апаратну, яка призначена для тимчасового або повного виведення з ладу окремих компонентів радіоелектронних систем, компонентів радіоелектронного обладнання (у т. ч. систем їх електроживлення), а також дезорганізації функціонування підсистем обміну інформацією та впливу на середовище поширення сигналів [13, с. 143–144].

У свою чергу, інформаційно-психологічна зброя – це зброя, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан людини, соціальних груп та суспільства в цілому. Вона поділяється на:

– пропагандистську, яка призначена для здійснення інформаційно-психологічного впливу, спрямованого на закріплення бажаних уявлень, звичок, переконань у людини (соціальної групи), або, навпаки, – руйнування небажаних уявлень, звичок та переконань;

– психофізичну, яка призначена для здійснення інформаційного й (або) енергетичного впливу на психічні функції та на роботу фізіологічних органів і систем людини;

– нейролінгвістичну, яка призначена для управління людською свідомістю та поведінкою за допомогою лінгвістичних конструкцій, набору певних символів, кольорів, звуків, архетипів, візуальних зображень тощо;

– психотропну, яка призначена для впливу на мозок людини, збудження або зниження процесів мислення і сприйняття інформації за рахунок використання механізму зміни біохімічних характеристик процесів, що відбуваються у нервовій системі людини;

– психотронну, яка призначена для впливу спеціальними технічними засобами на свідомість та підсвідомість людини з метою зниження її волі, пригнічення, тимчасового виведення з ладу, зомбування тощо;

– психогенну, яка призначена для внесення змін у нервово-психічну діяльність мозку людини;

– психоаналітичну, яка призначена для впливу на підсвідомість людини терапевтичними засобами, зокрема у стані гіпнозу та глибокого сну з навіюванням їй необхідних установок тощо [13, с. 144].

Як інформаційно-технічна, так й інформаційно-психологічна зброя негативно впливають на державотворчий процес у будь-якій країні, руйнуючи комунікативні системи в різних сферах життєдіяльності суспільства, розмиваючи культурно-історичні коди існування нації, підриваючи «інформаційно-культурний імунітет» народу.

Виходячи з наведеного вище, можна констатувати, що подальша розбудова Української держави потребує створення системи інформаційної (зокрема, кібернетичної) безпеки України, яка повинна мати наступальну спрямованість як з питань захисту, так і просування національних інтересів. Реалізація такої системи, на думку фахівців, передбачає такі напрями:

– розробка й удосконалення нормативно-правової бази у сфері інформаційної безпеки, яка на сьогодні є фрагментарною та не повною мірою відповідає існуючим потребам;

– створення (визначення) керівного та координаційного органу системи інформаційної безпеки України у структурі державних органів виконавчої влади;

– визначення (уточнення) переліку суб'єктів підтримання інформаційної безпеки, їхніх функцій, завдань і повноважень, для чого необхідно внести відповідні зміни до чинного законодавства України;

– проведення досліджень та визначення потреб у технічному, фінансовому й кадровому забезпеченні функціонування системи з метою прийняття рішення стосовно розробки відповідної цільової державної програми або внесення змін до чинних цільових державних програм;

– активізація заходів у Міністерстві оборони України та Генеральному штабі Збройних Сил України зі створення власної системи інформаційної безпеки, яка має стати складовою національної системи інформаційної безпеки, а також розробки відповідної нормативно-правової бази в рамках реалізації Концепції забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України [14, с. 41].

Висновки. Таким чином, захист державних інтересів у інформаційній сфері передбачає реалізацію низки програм гуманітарного, економічного та військово-технічного характеру. Необхідно зазначити, що важливими засобами протидії інформаційній експансії щодо України є розвиток та оптимізація системи освіти й виховання населення, проведення активної інформаційної політики держави, економічна підтримка наукових досліджень у сфері інформаційних технологій тощо.

ЛІТЕРАТУРА

1. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навч. посіб.] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.
2. Боднар І. Р. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Механізм регулювання економіки. – 2014. – № 1. – С. 68–75.
3. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О. М. Косогов // Зб. наук. пр. Харк. ун-ту Повітр. Сил. – 2014. – Вип. 3. – С. 127–130.
4. Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності : монографія / О. П. Дзьобань. – Х. : Майдан, 2010. – 260 с.
5. Олійник О. В. Інформаційна безпека США / О. В. Олійник // Боротьба з організ. злочинністю і корупцією (теорія і практика). – 2012. – № 1 (27). – С. 280–288.

6. Алямкін Р. В. Правове забезпечення національної інформаційної безпеки / Р. В. Алямкін, М. П. Федорін // Наук. зап. Ін-ту законодавства Верхов. Ради України. – 2013. – № 4. – С. 91–96.
7. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201) / Нью-Йорк, Организация Объединенных Наций. – 2012. – 57 с.
8. Пастушенко В. М. Проблеми правового регулювання державного управління інформаційною сферою України / В. М. Пастушенко // Наук. зап. Ін-ту законодавства Верхов. Ради України. – 2015. – № 1. – С. 59–64.
9. Кирильчук Є. М. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції / Є. О. Кирильчук // Наук. пр. МАУП. – 2013. – Вип. 1 (36). – С. 60–63.
10. Расторгуев С. П. Философия информационной войны / С. П. Расторгуев. – М. : Моск. психол.-соц. ин-т, 2003. – 496 с.
11. Чирва Р. Інформаційна війна – зброя, страшніша за ядерну / Раїса Чирва // Профспілк. вісті. – 2014. – № 13. – С. 8–9.
12. Шпига П. С. Основні технології та закономірності інформаційної війни / П. С. Шпига, Р. М. Рудник // Проблеми міжнар. відносин. – 2014. – Вип. 8. – С. 326–339.
13. Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби / О. В. Левченко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2014. – № 2 (20). – С. 142–146.
14. Радковець Ю. І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України / Ю. І. Радковець // Наука і оборона. – 2014. – № 3. – С. 36–42.

РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРОИТЕЛЬСТВЕ СОВРЕМЕННОГО УКРАИНСКОГО ГОСУДАРСТВА

Мануйлов Е. Н., Калиновский Ю. Ю.

Исследованы сущностные характеристики информационной безопасности государства. Определены особенности взаимосвязи процесса государственного строительства в Украине с необходимостью создания национальной системы информационной безопасности. Проанализированы основные информационные угрозы национальной безопасности Украины. Обоснована необходимость совершенствования правового обеспечения национальной информационной безопасности с учетом зарубежного опыта. Обобщены существующие представления о разновидностях и направлениях применения информационного оружия в современных информационных войнах.

Ключевые слова: *информационная безопасность, государственное строительство, информационные угрозы, информационная война, информационный суверенитет, информационное оружие.*

ROLE AND PLACE OF INFORMATION SECURITY IN MODERN UKRAINIAN STATE BUILDING

Manuylov E. M., Kalinovsky Y. Y.

Studied intrinsic characteristics of state information security. Determined features of the state building process interrelation in Ukraine with the need of creating a national information security system. It is noted that the specific of information security is that it is manifested in various spheres of public life as the preservation and protection of information is an important part of their operation. In turn, procuring the information security strengthens the state, allowing it to withstand dangers in this area. Analyzed the basic informational threats to national security of Ukraine. At the present domestic state building stage Ukraine became the object of powerful information attacks aimed at the destruction vital areas of our country. According to national experts on information security issues that formed based on the analysis of foreign influence on the informational media – and cyberspace Ukraine, there are signs of real threats to our country. Grounded the necessity of improving the legal provision of national information security, taking into account the international experience. For implementing effective security measures in system information area of country, we need to continuously improve the regulatory framework for preserving the balance between the interests of the state in the field of information security and information rights. It is noted that the strengthening of the legal framework in the field of information and communication aimed, primarily, to protect information sovereignty of modern states. Generalized the existing ideas about the varieties and areas of information weapon application in modern information wars. Determined that a particular danger of information war for the existence of the state is that it is usually aimed at the awareness «reprogramming» for the individual social groups: the result is the value deformation of social consciousness, changes in attitudes and policy preferences of citizens who are threatening the existence of countries. Typically, in the state information wars use the so-called information weapons, which can be stopped with the defense capabilities. It should be noted that the information weapon particularly effectively acts against the country, which is in crisis in which public mind dominates ambivalence of values, socio-political uncertainty. The use of information weapon is particularly effective there is a confrontation between the political forces, the crisis of moral and legal consciousness is weak patriotic elite in all spheres of public life in the country. It is noted that further development of the Ukrainian state needs to create a system of information (including cyber) security of Ukraine, which should be aggressively focused on the protection and promotion of national interests.

Key words: *information security, state, information threats, information warfare, information sovereignty, information weapons.*