УДК 351.86:614:659.3

О. В. Губар
аспірант кафедри глобалістики, євроінтеграції
та управління національною безпекою
Національної академії державного
управління при Президентові України

ІНФОРМАЦІЙНА КОМПОНЕНТА МЕХАНІЗМУ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ БІОЛОГІЧНОЇ БЕЗПЕКИ

Проведено дослідження інформаційної безпеки як інтегрованої складової державного управління у сфері біологічної безпеки, обґрунтовані сучасні підходи до розуміння сутності основних інформаційних загроз національній безпеці, визначено основні форми деструктивних впливів на інформаційний простір, а також основні інструменти сучасної інформаційної боротьби. Визначено основні проблемні аспекти забезпечення інформаційної безпеки суб'єктів біологічної безпеки, зокрема, найбільш вразливі інформаційні та облікові автоматизовані системи суб'єктів забезпечення біологічної безпеки.

Ключові слова: *інформаційна безпека, державне управління, система державного управління у сфері біологічної безпеки, державне управління у сфері біологічної безпеки.*

Постановка проблеми. Доктриною інформаційної безпеки України до життєво важливих інтересів суспільства та держави віднесено формування позитивного іміджу України у світі. Загрозами національним інтересам визнано проведення спеціальних інформаційних операцій в інших державах для створення негативного іміджу України у світі. Пріоритетами державної політики в інформаційній сфері визнано боротьбу з дезінформацією та деструктивною пропагандою, недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дискредитації України на міжнародному рівні [1]. Також до загроз інформаційній безпеці, кібербезпеці і безпеці інформаційних ресурсів віднесено: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [2].

У сучасних умовах підвищення обсягу і швидкості поширення інформації, технологізації інформаційного протиборства для забезпечення геополітичного авторитету держави важливого значення набувають інформаційні фактори. Інформаційний простір стає ареною геополітичної конкуренції та важливим інструментом впливу на свідомість населення. Більшість країн світу визнали інформаційний простір черговим простором суперництва. Рівень розвитку та безпека інформаційного середовища активно впливають на всі складові національної безпеки. Інформаційна безпека є складовою національної безпеки та впливає на захищеність національних інтересів в багатьох сферах життєдіяльності суспільства, включаючи сферу біологічної безпеки, тому деякі науковці розглядають інформаційну безпеку як складову інших сфер національної безпеки. Водночас інформаційна компонента є обов'язковим структурним складником та, одночасно, важливою характеристикою механізму державного управління у сфері біологічної безпеки. За допомогою інформації здійснюється керівний вплив на процеси, що відбуваються в системі державного управління у сфері біологічної безпеки для досягнення бажаних цілей та отримується інформація про стани об'єкта управління системи в цілому [6].

Процес державного управління як сукупність перетворюваної інформації можна розглядати як процес інформаційного обміну. Змістовна характеристика інфор-

маційної компоненти механізму державного управління у сфері біологічної безпеки містить структуру інформації, бази даних, джерела і споживачів інформації, технологічний процес її обробки. Основним продуктом державного управління є використання, передача, аналіз, формування та зберігання інформації. З огляду на викладене виникла необхідність розгляду інформаційної безпеки як інтегрованої складової державного управління у сфері біологічної безпеки.

Вирішення зазначених завдань є комплексною науковою проблемою, тому в межах проведеного дослідження сконцентровано увагу на державно-управлінському аспекті інформаційної безпеки як інтегрованої складової державного управління у сфері біологічної безпеки, а саме – на питаннях забезпечення інформаційної безпеки суб'єктів біологічної безпеки.

Аналіз останніх досліджень і публікацій. Дослідженню питань формування інформаційної політики та забезпечення інформаційної безпеки присвячені роботи В. Антонюка, В. Горбуліна, Р. Марутян, О. Литвиненка, Г. Почепцова та ін. Правові аспекти регулювання процесів захисту інформації та інформатизації розглянуто в роботах Р. Власенка, Р. Калюжного, О. Кохановської, О. Сосніна та ін. Проблемам інформаційної безпеки, інформаційного протиборства та інформаційних війн присвячені праці Г.Грачова, З. Бжезинського, Л. Брауна, Г. Кіссінджера, І. Мельника, Г. Почепцова, В. Петрика, В. Панченко, О. Степка, Х. Френч, Ч. Флавіна та ін. Однак, незважаючи на вагомий науковий доробок зазначених вітчизняних та зарубіжних вчених, у відкритих джерелах відсутні комплексні дослідження інформаційної безпеки як інтегрованої складової державного управління у сфері біологічної безпеки.

Мета статті – проаналізувати сучасний стан інформаційної компоненти механізму державного управління, її ролі та місця в державному управлінні у сфері біологічної безпеки.

Виклад основного матеріалу. На фоні зростання впливу зовнішніх і внутрішніх деструктивних чинників загрозливих масштабів набуває першості деструктивність зовнішньої залежності України, що може призвести до негативних наслідків та втрати державного суверенітету.

Стан здоров'я населення України оцінюється як незадовільний. Зберігається високий рівень загальної смертності (13,9 на 1000 населення), у 2015 році коефіцієнт смертності залишався одним із найвищих у Європі. В країні відбуваються зміни, що супроводжуються руйнівними процесами, внаслідок чого створюється середовище, сприятливе для поширення соціально обумовлених хвороб – ВІЛ-інфекції, туберкульозу тощо. Внаслідок проведення антитерористичної операції в Донецькій та Луганській областях значно погіршився санітарно-гігієнічний стан населених пунктів та об'єктів життєзабезпечення, погіршується епідемічна ситуація в країні.

Комплекс біохімічних і фізіологічних процесів, що забезпечують життєдіяльність організмів перебуває у тісному взаємозв'язку з навколишнім середовищем. Важливе значення у збереженні живими організмами їх біологічної сутності, біологічних якостей, системоутворюючих зв'язків та характеристик, здатності до ефективного функціонування і прогресивного розвитку відіграє епідемічний процес, що включає в себе не лише біологічні, а й соціальні компоненти. Існування біологічних видів збудників та безперервність епідемічного процесу на території країни забезпечується постійною взаємодією у певних соціальних і природних умовах популяцій збудників-паразитів і хазяїв, а також сукупність абіотичних і біотичних елементів навколишнього природного середовища, що впливають на епідемічний процес. Таким чином, природний фактор відіграє важливу роль в еволюційному становленні паразитарних систем, визначає механізми їх регулюючої ролі та конкретні прояви епідемічного процесу [9, с. 25]. Незважаючи на важливість об'єктивних природних процесів, що впливають на розвиток епідемічного процесу, важливу роль у забезпеченні біологічної безпеки відіграє діяльність суб'єктів забезпечення біологічної безпеки. Використання державою-агресором інструментів сучасної інформаційної боротьби може призвести до протиправ-

ної діяльності або бездіяльності зазначених суб'єктів та створення реальної загрози для національної безпеки, що свідчить про важливість інформаційної компоненти механізму державного управління у сфері біологічної безпеки.

В умовах глобалізації епідемічних процесів, наявності науково- технологічних передумов для розробки біологічних засобів масового ураження, зростання загрози тероризму покращення інформаційної безпеки суб'єктів біологічної безпеки є необхідною передумовою для забезпечення ефективності державного управління в зазначеній сфері.

За даними всесвітнього економічного форуму в рейтингу розвитку інформаційних технологій Україна займає 71 місце, інформаційно-обчислювальні ресурси, задіяні під «хмари», з кожним роком зростають, збільшується рівень довіри до хмарних технологій, близько 90% користувачів вважають їх досить безпечними та надійними, незважаючи на те, що кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом гібридної війни [12]. При цьому майже відсутня достовірна інформація щодо наявних ресурсів та можливостей суб'єктів біологічної безпеки, зокрема, щодо використання ними хмарних технологій та розміщення «хмари» на ресурсах провайдера.

Результати аналізу літературних джерел свідчить про те, що основною інформаційною загрозою національній безпеці можна вважати загрозу інформаційного впливу країни-агресора на свідомість, підсвідомість, інформаційні ресурси, інформаційну сферу машинно-технічних систем та інші об'єкти інформаційної інфраструктури країни з метою нав'язування особистості, суспільству й державі бажаної для країни агресора системи цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної та державної діяльності, управління їх поведінкою і розвитком у напрямку, визначеному країною-агресором [5, с. 2]. До основних форм деструктивних впливів на інформаційний простір відносять: проведення спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії; блокування передачі повідомлень; вплив на форму повідомлень, механізми передачі, зберігання, обробки даних тощо [3].

Важливим інструментом сучасної інформаційної боротьби є інформаційна зброя, здатна: завдавати значної шкоди національним інтересам, підривати основи державності; дискредитувати органи влади та ускладнювати прийняття ними важливих управлінських рішень в життєво важливих сферах життєдіяльності суспільства і держави, блокувати систему державного управління; створювати атмосферу напруженості в суспільстві, дезорганізувати економіку, систему комунікацій; підривати міжнародний авторитет держави тощо [10].

Спеціальні інформаційні операції та акти зовнішньої інформаційної агресії у сфері біологічної безпеки, як і в інших життєво важливих сферах життєдіяльності суспільства і держави, передбачають завдання шкоди життєво важливим інтересам держави у цій сфері та здійснення вигідного впливу для отримання переваг для держави – ініціатора проведення таких операцій. Як правило, спеціальні інформаційні операції у сфері біологічної безпеки, як і в інших сферах, проводяться спеціальними органами іноземних держав або транснаціональних структур уповноваженими суб'єктом інформаційної війни на здійснення діяльності та передбачають проведення акцій деструктивного впливу для сприяння вчиненню протиправних дій, спрямованих на підрив та ослаблення державного ладу, можуть бути спрямовані проти суб'єктів, що приймають рішення у сфері біологічної безпеки, для компрометації України на міжнародній арені, завдання шкоди опонентам, політичної або економічної дестабілізації тощо. Для здійснення прихованого впливу іноземних держав у сфері біологічної безпеки, як і в інших сферах, використовуються такі загальновідомі методи, як: дезінформування, пропаганда, психологічний тиск тощо. Широко використовується упереджене висвітлення спеціально підібраних правдивих даних, а також подача правдивих даних у спотвореному вигляді. Внаслідок подібних маніпуляцій виникає ситуація, коли суб'єкти забезпечення біологічної безпеки держави фактично знають прав-

диву інформацію про наміри або конкретні дії країни-агресора, однак сприймають їх адекватно і не готові протидіяти негативному впливу.

Інформаційний вплив може здійснюватися на: інформаційні ресурси суб'єктів забезпечення біологічної безпеки, науково-дослідних установ; системи зв'язку і управління та їх інформаційне забезпечення; центри обробки та аналізу інформації; морально-психологічний стан співробітників тощо. Ми поділяємо думку вітчизняних і закордонних дослідників, що найбільш ефективним є використання інформаційної зброї в рамках проведення скоординованих спеціальних інформаційних операцій.

Результати проведених досліджень свідчать про проведення на території держави акцій інформаційного впливу, тобто одноразових акцій інформаційно-психологічного та інформаційно-технічного впливу, що передбачають запланований вплив на свідомість і поведінку людей шляхом поширення упередженої інформації та спеціальних інформаційних операцій – спланованих дій, спрямованих на ворожу, дружню або нейтральну аудиторію, для схилення до прийняття управлінських рішень або вчинення дій, вигідних для суб'єкта інформаційного впливу, включаючи вплив на інформаційно-технічну інфраструктуру. Зокрема, має місце проведення таких акцій у сфері біологічної безпеки та охорони здоров'я населення, про що свідчить наявність таких основних ознак проведення спеціальних інформаційних операцій, як зростання кількості повідомлень негативного змісту певного напряму, збільшення емоційності, тенденційності, сенсаційності при висвітленні певних питань, лавиноподібність. При цьому зазначені операції здійснюються за однаковою схемою. Перша стадія проведення такої операції, як і у інших сферах, передбачає створення інформаційного приводу (існуючої або вигаданої події, що використовується для проведення операції). На другій стадії здійснюється актуалізація інформаційного приводу з поступовим збільшенням кількості повідомлень та їх емоційності та недостовірності. На третій – інформаційний привід використовується для досягнення цілей операції, відбувається закріплення інформаційного приводу. Наступною стадією є поступове завершення спеціальної інформаційної операції після досягнення поставленої мети. До проведення таких операцій залучаються зарубіжні та підконтрольні вітчизняні засоби масової інформації, неурядові організації, ресурси всесвітньої мережі Інтернет, агентура впливу іноземних держав, підконтрольні структури з числа представників законодавчого органу, органів виконавчої влади, органів місцевого самоврядування, політичних партій, релігійних організацій, громадських організацій, відомих діячів науки та культури, представників міжнародних організацій, фармацевтичних компаній і транснаціональних корпорацій. Зазвичай такі операції мають вплив на суспільство з метою переорієнтації на інші цінності, завдання збитків державі, підрив суспільно-політичного ладу. Для проведення спеціальних інформаційних операцій у сфері біологічної безпеки використовуються такі основні методи як дезінформування, пропаганда, диверсифікація громадської думки, поширення чуток тощо. Найчастіше використовується дезінформування, що передбачає введення об'єкту впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій. Як правило, подаються правдиві відомості у перекрученому вигляді, досить поширеним є тенденційне викладення фактів, що полягає в упередженому висвітленні подій та фактів з використанням спеціально підібраних правдивих даних. Крім того, іноді застосовують дезінформування з використанням синтезу правдивої інформації з дезінформацією. Внаслідок низької критичності та навіюваності мас для маніпулювання ними широко використовується негативна пропаганда. Водночас існує ризик проведення акцій дезінформування шляхом імітації витоку закритої інформації, успіху розвідки іноземних партнерів, використання засобів масової інформації тощо.

Одним з аспектів інформаційної боротьби в зазначеній сфері є інформаційно-технічна боротьба. Інформаційна зброя може бути ефективним засобом знищення, змі-

ни або викрадення інформаційних масивів; здобування необхідної інформації внаслідок подолання систем захисту, обмеження або заборони доступу до них для законних користувачів; дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних та комп'ютерних мереж, високотехнологічного обладнання, що забезпечує життєдіяльність суспільства і функціонування органів державного управління. Інформація, що циркулює в автоматизованих системах державного управління та зв'язку, які є невід'ємними компонентами структури державного управління у сфері біологічної безпеки, стає критично важливим державним ресурсом, що впливає на національну безпеку. Використання засобів реалізації програмно-технічних методів збирання, спотворення, знищення інформації та впливу на функціонування інформаційних систем дозволяє здійснювати несанкціонований доступ до комп'ютерних систем, визначати коди доступу, інформацію про зашифровані дані та передавати отримані відомості каналами обміну зацікавленим країнам. Крім того, можливе використання біологічних засобів, здатних знищувати електронні схеми та радіоізоляційні матеріали, а також мультимедійних та програмних засобів, здатних впливати на підсвідомість операторів інформаційних систем та погіршувати стан їх здоров'я. Найбільш вразливими до такого впливу у сфері біологічної безпеки є інформаційні та облікові автоматизовані системи обробки облікової інформації суб'єктів забезпечення біологічної безпеки та електронні інтегровані системи спостереження за захворюваннями [10]. Тому відсутність належного контролю за діяльністю зі створення та захисту систем збору, обробки, зберігання і передачі інформації у сфері біологічної безпеки, особливо у разі залучення до зазначеної діяльності іноземних агентів, створює сприятливі умови для несанкціонованого доступу до конфіденційної інформації, здійснення контролю за процесом її передачі та обробки іноземними спецслужбами, а також виникнення технологічної залежності від іноземних держав, що є реальною загрозою для національної безпеки.

Висновки і пропозиції. Інформаційна компонента є однією з найважливіших складових механізму державного управління у сфері біологічної безпеки. В сучасних умовах технологізації інформаційного протиборства діяльність відповідних органів сектору безпеки та існуюче нормативно-правове регулювання є недостатньо ефективними, що ускладнює забезпечення інформаційної безпеки суб'єктів біологічної безпеки. Тому завдання щодо наукового пошуку пріоритетних напрямів підвищення ефективності інформаційної безпеки суб'єктів біологічної безпеки набувають стратегічного значення. Вирішення цих завдань ускладнюється укоріненням корупції, діяльністю державних органів в інтересах міжнародних організацій, транснаціональних корпорацій, в корпоративних та особистих інтересах.

Результати проведених емпіричних досліджень свідчать про збільшення ймовірності використання посадовими особами суб'єктів забезпечення біологічної безпеки міжнародного інформаційного простору в деструктивних цілях, про підвищення активності неурядових структур, які можуть бути залучені до проведення спеціальних інформаційних операцій у сфері біологічної безпеки та здійснення психологічного впливу, а також збільшення активності організацій та окремих осіб, які беруть участь в міжнародних гуманітарних програмах та можуть під виглядом просвітницьких акцій проводити спеціальні інформаційні операції з метою дискредитації України на міжнародному рівні та завдавати шкоди життєво важливим інтересам держави у цій сфері.

Враховуючи зростання кількості повідомлень про співробітництво органів безпеки іноземних держав з хакерськими угрупуваннями, до першочергових заходів, спрямованих на забезпечення інформаційної безпеки суб'єктів біологічної безпеки, можна віднести:

– удосконалення нормативно-правового регулювання в зазначеній сфері;

– обмеження поширення таємної і конфіденційної інформації, боротьба з дезінформацією, пропагандою і спробами підірвати державний лад;

– забезпечення цілісності суспільства, підтримка правопорядку, запобігання маніпуляціям свідомістю осіб, уповноважених на виконання завдань і функцій держави та громадян через інформаційні канали;

– моніторинг інформаційно-технологічних факторів ризику;

– розробку засобів захисту суб'єктів забезпечення біологічної безпеки від небезпечних інформаційних впливів;

– контроль над виробництвом і впровадженням інформаційних технологій, що можуть використовуватися з протиправною метою.

Список використаної літератури:

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25.02.2017 р. № 47/2017: [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/472017-21374.
2. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26.05.2015 р. № 287/2015 : [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/2872015-19070.
3. Петрик В.М. Информационно-психологическая безопасность в епоху глобализации: [учеб. пособ.] / [В.М Петрик, В.В. Остроухов, А.А. Штоквиш и др.]; под ред. В.В. Остроухова. – К., 2008. – 544 с.
4. Жарков Я.М. Інформаційно-психологічне протиборство (еволюція та сучасність): [монографія] / Я.М.Жарков, В.М.Петрик, М.М.Присяжнюк та ін. –К.: ПАТ «Віпол», 2013. – 248 с.
5. Домбровська С.М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. Теорія та практика державного управління / С.М. Домбровська. – 2015. – Вип. 1(48). – С. 1-5.
6. Приходченко Л. Структура механізму державного управління: взаємозв'язок компонентів та фактори впливу на ефективність / Л. Приходченко // Вісник Національної академії державного управління при Президентові України. – 2009. – № 2. – С. 105-133.
7. Зозуля О.С. Інформаційна зброя як геополітичний чинник та інструмент силової політики / О.С. Зозуля // Державне управління: теорія та практика. – 2013. – № 2. – С. 82-89 [Електронний ресурс]. – Режим доступу: http://www.nbuv. gov.ua/j- pdf/Dutp_2013_2_12.pdf.
8. Михальчук В.Ф. Спеціальні інформаційні операції в контексті інформаційних війн / В.Ф. Михальчук // Науковий часопис НПУ імені М.П.Драгоманова. Серія № 2. Комп'ютерно-оріентовані системи навчання: зб. наукових праць / Редрада. – К. : НПУ імені М.П.Драгоманова, 2009. – № 7(14). – С. 207-210.
9. Епідеміологія: [підручник для студ. вищих мед. навч. закладів] / [А.М. Андрейчин, З.П. Василишин, Н.О. Виноград]; за ред. І.П. Колеснікової. – Вінниця: Нова Книга, 2012. – 576 с.
10. Пєвцов Г.В. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: [монографія] / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський. – Х. : Цифрова друкарня № 1, 2013. – 272 с.
11. Степко О.М. Аналіз головних складових інформаційної безпеки держави / Степко О.М. // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 1(18).
12. Рівень розвитку інформаційно-комунікаційних технологій в Україні та світі [Електронний ресурс]. – Режим доступу: http://edclub.com.ua/analityka/riven-rozvytku-informaciyno-komunikaciynyh-tehnologiy-v-ukrayini-ta-sviti.
13. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: автореф. дис. … канд. наук з держ. управління: спец. 25.00.02 / В.В. Антонюк; Національна академія держ. управління при Президентові України. – Київ, 2017. – 20 с.

Губарь О. В. Информационная компонента механизма государственного управления в сфере биологической безопасности

В статье рассматриваются вопросы информационной безопасности как интегрированной составляющей государственного управления в сфере биологической безопасности, обоснованы современные подходы к пониманию сущности основных информационных угроз национальной безопасности, определены основные формы деструктивных воздействий на информационное пространство, а также основные инструменты современной информационной борьбы. Проанализированы проблемные моменты обеспечения информационной безопасности субъектов биологической безопасности.

Ключевые слова: *информационная безопасность, государственное управление, государственное управление в сфере биологической безопасности.*

Gubar O. Data component of the government control mechanism in biosecurity sector

The study of information security as an integral component of the government control of biosecurity sector structure is conducted, the modern approaches to understanding the essence of the main cyber threats to state security are justified, the main forms of destructive influences on the informational space are identified, as well as the basic tools of the modern information warfare. The main challenges of biosecurity subjects information security are determined, particularly the most vulnerable information and accounting automated systems of biosecurity ensuring subjects.

The research of information security as an integrated component of state management in the field of biological safety was conducted, modern approaches to understanding the essence of the main information threats to national security were substantiated, the main forms of destructive influences on the information space and the main tools of modern information struggle were determined. The main problem points of ensuring information security of biological safety agents are determined, in particular, the most vulnerable information and accounting automated systems of subjects of providing biological safety.

Key words*: information security, public management, national biological security management, system of state control in the sphere of biological security.*