УДК 351.746.1

МЕХАНІЗМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ ЗОВНІШНІХ ДЖЕРЕЛ

Ткачук Т. Ю.,
кандидат юридичних наук, доцент,
заступник завідувача кафедри організації захисту інформації
з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки

Стаття присвячена дослідженню механізмів протидії інформаційним загрозам зовнішніх джерел у контексті забезпечення національної безпеки України. Встановлено, що механізми боротьби з інформаційними загрозами з боку зовнішніх джерел, в основному засновані на принципах управління ризиками, дозволяють блокувати деструктивні елементи, властивості, процеси, які руйнують інформаційну безпеку та систему національної безпеки у цілому, і стимулюють конструктивні елементи, властивості, процеси, які сприяли її функціонуванню та розвитку.

Статья посвящена исследованию механизмов противодействия информационным угрозам внешних источников в контексте обеспечения национальной безопасности Украины. Установлено, что механизмы борьбы с информационными угрозами со стороны внешних источников, в основном основанные на принципах управления рисками, позволяют блокировать деструктивные элементы, свойства, процессы, которые разрушают информационную безопасность и систему национальной безопасности в целом, и стимулируют конструктивные элементы, свойства, процессы, которые способствуют ее функционированию и развитию.

The article is devoted to the to research of the mechanisms of counteraction to information threats of external sources in the context of ensuring national security of Ukraine. The mechanisms for countering information threats from external sources, primarily based on risk management principles, allow the blocking of destructive elements, properties, processes that destroy the information security and national security system as a whole, and stimulate constructive elements, properties, processes, which contribute to its functioning and development.

Ключові слова: національна безпека, інформаційна безпека, інформаційні загрози, механізм протидії загрозам.

Постановка проблеми. Основними принципами державного регулювання у сфері забезпечення національної безпеки є орієнтація на державно-правовий механізм забезпечення національної безпеки та реалізація національних інтересів і цілей. Ефективність механізму забезпечення національної безпеки визначається передусім його здатністю сприяти збереженню єдності нації, стабільності суспільних відносин, відтворенню національно-культурних цінностей, подоланню політичних, військових, економічних, соціальних криз, створенню передумов стабільного розвитку, а також здатністю ефективно протидіяти загрозам національній безпеці. Останнє, у свою чергу, викликає до життя власне механізми протидії загрозам національній безпеці, у тому числі інформаційним загрозам, які на сучасному етапі характеризуються підвищеною небезпечністю, адже інформаційне протиборство нарощує свої можливості у результаті стрімкого зростання обсягу та значення інформації у сучасному світі.

Загальні засади протидії загрозам національній безпеці, у тому числі інформаційним загрозам, досліджувались багатьма відомими вітчизняними і зарубіжними науковцями, серед яких О. Довгань, О. Баранов, В. Горбулін, В. Дрьомін, В. Желіховський, Є. Скулиш, І. Івченко, Р. Калюжний, А. Качинський, В. Ліпкан, О. Литвак, В. Пилипчук та інші вчені. Водночас, питання, що стосуються механізмів протидії інформаційним загрозам зовнішніх джерел наразі лишаються вивченими недостатньо, що свідчить про актуальність відповідних спрямувань наукових пошуків.

Мета статті – на основі системного аналізу дослідити механізми протидії інформаційним загрозам, як базового компонента забезпечення національної безпеки України.

Виклад основного матеріалу. У теорії національної безпеки механізм протидії загрозам національній безпеці зазвичай розглядають у широкому або у вузькому сенсі. У вузькому сенсі він виступає як складова частина державного механізму і становить систему державних організацій, органів,

установ, а також недержавних інституцій, спеціально створюваних для забезпечення національної безпеки або таких, що наділяються окремими функціями щодо забезпечення національної безпеки, в їхній взаємодії й практичному функціонуванні (сили забезпечення національної безпеки). У широкому сенсі механізм протидії загрозам національній безпеці охоплює не лише сили, але й систему засобів, за допомогою яких здійснюється протидія відповідним загрозам з метою захисту життєво важливих інтересів суспільства і держави. Такими засобами виступають технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що використовуються з метою збирання, формування, обробки, передачі або приймання інформації щодо стану національної безпеки та щодо заходів, спрямованих на її зміцнення, а також власне методи, способи і прийоми, використовувані суб'єктами забезпечення національної безпеки для вирішення завдань щодо протидії загрозам національній безпеці.

Механізм забезпечення національної безпеки – динамічна система, у рамках якої можна виділити наступні стадії: формулювання інтересів, захист яких буде забезпечуватися; виявлення й прогнозування внутрішніх і зовнішніх погроз життєво важливим інтересам; вироблення системи заходів щодо протидії загрозам; нейтралізація загроз; здійснення заходів щодо відновлення нормального функціонування об'єктів безпеки. Множинність засобів протидії інформаційним загрозам та варіативність комбінацій цих засобів залежно від специфіки загроз дозволяють вести мову у множині – про механізми протидії інформаційним загрозам національній безпеці.

Залежно від місцезнаходження джерела можливої загрози, всі загрози національній безпеці, у тому числі – інформаційні, – традиційно поділяються на дві групи: зовнішні й внутрішні. Для інформаційної безпеки того чи іншого об'єкта внутрішніми вважаються ті загрози, що «виникають безпосередньо на об'єкті та зумовлюють взаємодію між його елементами або суб'єктами», тоді як зовнішніми – ті загрози, що «виникають внаслідок його взаємодії із зовнішніми об'єктами» [1, с. 18; 2].

Чинна Стратегія національної безпеки України серед основних загроз національній безпеці, які мають безпосереднє відношення до інформаційної сфери, визначає агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, у тому числі інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, а також ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства, 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 [3]. Необхідно зауважити, що у Стратегії відмежовуються прояви інформаційно-психологічної війни (п. 3.1), загрози кібербезпеці і безпеці інформаційних ресурсів (п. 3.7) від суто загроз інформаційній безпеці (п. 3.6), що не є доцільним.

Доктрини інформаційної безпеки України, як і Стратегія кібербезпеки України, визначають цілий спектр загроз національним інтересам та національній безпеці України в інформаційній сфері.

При розробці стратегій забезпечення національної безпеки також обов'язково враховується сучасний рівень впливу на суспільну свідомість за допомогою інформаційних маніпуляцій. Розвідки й контррозвідки держав використовують в інформаційному протиборстві методи дезінформації й пропаганди, намагаючись добувати секретну інформацію та дезорієнтувати супротивника хибною інформацією. Сучасні інформаційні війни спрямовуються передусім на «мішені» двох класів: по-перше, це технічні засоби супротивника (комп'ютерні мережі, інше устаткування) і, по-друге, це людські ресурси. Якщо метою атак на інформаційні системи супротивника є виведення з ладу критичних секторів життєзабезпечення держави – енергетичного, оборонного, управлінського тощо, то метою другого типу атак є психологічна «обробка» населення [4, с. 9-10]. Зазвичай інформаційна агресія вибудовується у три етапи: створення «ядра» (акумулювання великої кількості людей, незадоволених поточним станом речей); створення середовища (альтернативного інформаційного простору); створення атмосфери (зміна суспільної думки «точковими ударами») [5, с. 51-52; 6]. Інформаційне насильство, використовуване в інформаційному протистоянні, є латентним, прихованим, не завжди розпізнаваним. Тому завданням держави у таких війнах є захист власної інформації, своїх інформаційних систем, захист свідомості населення від маніпуляцій супротивника, а також закриття доступу супротивника (джерела зовнішніх загроз) до інформації, розкриття якої може завдати шкоди обороноздатності країни.

Глобальна мережа Інтернет сьогодні є основним полем протистояння різних сил і засобів, що вимагає нового рівня забезпечення національної безпеки від різнопланових загроз, що мають інформаційне опосередкування. У цей час інформаційна агресивність віртуального простору суттєво впливає на трансформацію діяльності всіх національних, а також міжнародних антитерористичних і антиекстремістських структур. Тому профілактичні заходи, проведені компетентними органами

державної влади в інформаційній сфері, повинні бути спрямовані насамперед на формування стійкості суспільної свідомості населення до впливу деструктивних ідей. Реалізація зовнішніх загроз передбачає пошук уразливості в інформаційній структурі для доступу до основних вузлів інформаційної інфраструктури, сховищ інформації, організаційної мережі, осіб-секретоносіїв тощо. Інструментами реалізації зовнішніх інформаційних загроз виступають різнопланові види так званої інформаційної зброї (не лише віруси, «хробаки», «трояни» та інші форми шкідливого програмного забезпечення, але й інші знаряддя інформаційного впливу).

Протидія зовнішнім загрозам інформаційній безпеці України відбувається в умовах прогресування тенденції до переформатування сфер впливу у світовому просторі на тлі глобалізації політичних, соціально-економічних, культурних відносин. Виявлення та аналіз відповідних загроз ускладнюється низкою факторів: наявність відчуття у частини населення відсутності зовнішніх загроз країні; у Військовій доктрині та Доктрині інформаційної безпеки чітко не визначені потенційні зовнішні загрози країні, що призводить до відсутності чіткої класифікації й ранжування загроз за ступенем важливості й порівняльній динаміці їх наростання; відсутність ясного розуміння причин і джерел появи цих загроз тощо.

Забезпечення безпеки в умовах внутрішніх і зовнішніх динамічних змін вимагає наявності дієвого механізму забезпечення безпеки, у тому числі – механізмів протидії загрозам, що виконує функції підтримки системної інваріантності. Механізм протидії інформаційним загрозам зовнішніх джерел може бути визначений як інтегрована цілісна сукупність необхідних і достатніх функціональних і правових елементів, за допомогою яких суб'єкт формує раціональну систему впливу на загрози інформаційній безпеці та зумовлені ними ризики, забезпечуючи таким чином результативне виконання завдань і функцій, покладених на систему забезпечення інформаційної безпеки та національної безпеки у цілому.

Механізми протидії інформаційним загрозам зовнішніх джерел, як частина загального механізму забезпечення інформаційної безпеки держави та національної безпеки у цілому, мають передбачати:

– мету забезпечення безпеки, що полягає у збереженні цілісності й захищеності інформаційної сфери у процесі її функціонування й розвитку;

– рівень безпеки, що диференціює структурні складові системи, які можуть стикатися з потенційними і реальними небезпеками;

– сфери безпеки, що визначають можливості функціонування й розвитку інформаційної сфери;

– параметри безпеки, що встановлюють припустимі межі відхилень у потенціалі системи інформаційної безпеки, кількості її елементів, їх якості, властивостях, зв'язках;

– перелік загроз, наслідки їх реалізації й механізм запобігання, обумовлені: внутрішніми закономірностями функціонування системи інформаційної безпеки й впливом на неї зовнішнього середовища, що веде до небажаних і незворотних порушень в її відтворенні й розвиткові; змінами, що наступають у випадку реалізації загроз (такі, що компенсуються або не компенсуються; оборотні та необоротні; такі, що зачіпають або не зачіпають життєздатність системи); організаційно оформленою сукупністю стратегічних і тактичних дій, що забезпечують підтримку функціонування системи інформаційної безпеки та її здатність до самовідтворення.

З-поміж інформаційних загроз зовнішніх джерел наразі найбільшу небезпеку для національної безпеки України становлять:

– спроби несанкціонованого доступу до інформації й впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню та внутрішню політику України, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях.

– недостатня поінформованість населення зарубіжних країн (передусім тих, що межують з Україною) про зовнішньополітичну та внутрішньополітичну діяльність України;

– поширення за кордоном дезінформації про зовнішню та внутрішню політику України;

– інформаційний вплив іноземних політичних, економічних, військових і інформаційних структур на розробку й реалізацію стратегії зовнішньої та внутрішньої політики України;

– порушення прав українських громадян і юридичних осіб в інформаційній сфері за кордоном.

Механізми протидії інформаційним загрозам зовнішніх джерел передбачають необхідність організації багаторівневої й різноспрямованої системи заходів, які повинні враховувати передусім особливості зовнішніх факторів – конфігурації геополітичної, регіональної кон'юнктури і структурно-функціональної ролі країни, а також впливу транснаціональної організованої злочинності.

Отже, своєчасний моніторинг характеру, особливостей, масштабів загроз та їх наступне прогнозування мають особливе значення. Прогнозування є важливим і самостійним елементом профілактики інформаційних загроз зовнішніх джерел, та, відповідно, забезпечення національної безпеки. Основним методом прогнозування є моделювання, головними принципами якого є: встановлення мети моделі; виділення обмеженої кількості ключових факторів, які привносять істотні зміни у досліджувану систему; встановлення характеру взаємозв'язків між виділеними факторами; встановлення

принципу множинності зв'язків між факторами й виділення сутнісних зв'язків, які й визначають характер розвитку й зміни системи.

Стратегічні знання, отримані за результатами прогнозування, дозволяють ілюструвати модель розвитку досліджуваного середовища, а також обґрунтовувати змістовні особливості її структурних елементів. Для моніторингу, прогнозування і профілактики загроз при цьому є придатним будь-яке середовище, яке характеризується наявністю зовнішніх джерел, з яких можуть продуціюватися та відтворюватися загрози інформаційній безпеці особистості, суспільства й держави.

Слід враховувати, що в умовах стрімкого розвитку інформаційного суспільства, якій також зумовлює вдосконалення методів ведення інформаційних воєн, звичні технології й механізми протидії зовнішнім загрозам національній безпеці застаріли, і на передній план виходять нові способи стримування розгортання загроз та мінімізації ризиків, що ними зумовлені. Методи протидії інформаційним загрозам зовнішніх джерел можна умовно розділити на дві групи:

– профілактичні, або превентивні, методи, які використовуються для недопущення розгортання відповідних загроз або для запобігання появі подальших ризиків на початковому етапі розгортання таких загроз;

– оперативні методи, які використовуються безпосередньо у відповідь на агресивні кроки, що виходять від зовнішніх джерел інформаційних загроз та пов'язані з їх розгортанням та реалізацією.

Серед заходів превентивної протидії інформаційним загрозам зовнішніх джерел вирізняють чотири основні групи: нормативно-правові, адміністративні, інформаційні і економічні заходи.

Оперативна протидія повинна здійснюватися тільки після виявлення достовірної інформації щодо структур, груп або осіб, що є рушійними силами, оцінки ступеня загрози і наявних ресурсів для її нейтралізації. Зокрема, механізм протидії інформаційним загрозам зовнішніх джерел, розгортання яких відбувається у ході гібридної війни, має включати: постійний контроль інформаційного простору (преса, телебачення, радіо, Інтернет); обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією; посилення авторитету своєї влади та уряду, армії серед населення країни, аби перешкодити переходу на бік ворога та підтримці дій, які він нав'язує; ефективна інформаційна політика: стратегічна спрямованість та зворотний зв'язок із суспільством [7, с. 394].

Окрім того, можуть бути виокремлені політичні, економічні та інші механізми протидії інформаційним загрозам зовнішніх джерел. Зокрема, враховуючи політичні цілі, що випливають з єдиної стратегічної мети забезпечення національної безпеки України, можна виділити деякі політичні механізми протидії інформаційним загрозам зовнішніх джерел:

– механізми розробки й прийняття рішень у Раді безпеки ООН, взаємодія у рамках ОБСЄ, механізми зміцнення й розвитку у рамках інших міждержавних утворень, які є засобом політичної, економічної й військової євроінтеграції України;

– механізми державного й військового управління, впливу політичних партій, уведення адміністративно-правових режимів тощо, пов'язані з управлінням внутрішньополітичними процесами, що прямо впливають на забезпечення інформаційної безпеки країни;

– механізми просування інтересів держави у міжнародній інформаційній сфері, інформаційне забезпечення державної політики України, пов'язане з доведенням до вітчизняної й міжнародної громадськості достовірної інформації про державну політику країни, розвиток сучасних інформаційних технологій, захист інформаційних ресурсів тощо;

– механізми протидії зовнішнім загрозам політичної, економічної безпеки України тощо.

Зрозуміло, що механізми протидії інформаційним загрозам зовнішніх джерел можуть видозмінюватися, тому що конкретний механізм створюється відразу зі з'ясуванням наявності певної загрози й формулюванням стратегічної мети щодо її нейтралізації. Слід також враховувати, що за сучасних умов розподіл інформаційних загроз на внутрішні й зовнішні мають умовний характер. Оскільки інформаційні загрози завжди мають комплексний характер, замахи на зовнішню безпеку країни формують загрози внутрішньої безпеки, а внутрішня дестабілізація веде до зовнішньої уразливості держави.

Слід також враховувати, що загрози, передусім – зовнішні, – належать до сторонніх щодо системи забезпечення безпеки факторів, а відтак, неможливо не лише досягти стану їх абсолютної відсутності, але і скласти вичерпний перелік, адже вони змінюються в умовах мінливого середовища. То ж у сучасному світі відбувається зміщення акцентів із загроз на ризики, оскільки такий підхід дозволяє відходити від розуміння загроз як констант та застосовувати різнопланові підходи для унеможливлення їх розгортання, особливо за умов невизначеності [8]. Відповідно, механізми протидії інформаційним загрозам зовнішніх джерел, які базуються на принципах управління ризиками, і передбачають процес прийняття та виконання управлінських рішень, спрямованих на зниження вірогідності виникнення несприятливих наслідків та мінімізацію можливої шкоди, викликаної реалізацією загроз, за сучасних умов є найбільш перспективними і результативними. Відповідні механізми дозволяють впливати передусім на керовані елементи (ризики), досягаючи значних для забезпечення її

прийнятного стану результатів шляхом застосування відносно незначних зусиль [9, с. 30-39; 10, 11, 12, 13, с. 69-83], а також успішно поєднувати профілактичні та оперативні методи протидії інформаційним загрозам зовнішніх джерел.

Висновки. Механізми протидії інформаційним загрозам зовнішніх джерел – це сукупність різноманітних видів діяльності органів державного й військового управління, громадських організацій і політичних інститутів тощо, а також способів їх взаємин, які дозволяють оперативно впливати на зовнішні загрози інформаційній безпеці або управляти ризиками, що ними зумовлені, з метою їх локалізації й нейтралізації. Конкретні механізми протидії інформаційним загрозам зовнішніх джерел вибудовуються виходячи з системи потенційних і реальних небезпек, імовірності їх настання, з урахуванням циклу розвитку системи (зародження, становлення, зрілість, трансформація) і її конкретного стану (криза, депресія, підйом), виходячи з наявних фінансових, матеріальних, кадрових можливостей країни, на основі балансу інтересів суспільства, держави, груп, окремих особистостей. Оцінка відповідних механізмів базується на: інформаційній політиці держави, її впливі на параметри безпеки; виявленні ступеня ризику відхилень параметрів для стійкості системи інформаційної безпеки; визначенні зовнішніх обставин, в яких відбуваються відхилення: збільшення (при несприятливому зовнішньоекономічному середовищі) або зниження (при сприятливому зовнішньому середовищі) ризиків. Таким чином, механізми протидії інформаційним загрозам зовнішніх джерел, передусім такі, що базуються на принципах управління ризиками, дозволяють здійснювати блокування деструктивних елементів, властивостей, процесів, що руйнують систему інформаційної безпеки та національної безпеки у цілому, і стимулювати конструктивні елементи, властивості, процеси, що сприяють її функціонуванню й розвитку.

Література:

1. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С. 16-22.
2. Хілько О. Л. Визначення загроз національній безпеці в українській теоретико-політичній думці. URL: sevntu.com.ua/jspui/bitstream/123456789/ 1835/politolog.52.2003.48-56.pdf
3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015. URL: www.president.gov.ua/documents/2872015-1907
4. Григор'єв В. І. Технології сучасної інформаційно-психологічної війни. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 48-52.
5. Благодарний А. М., Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С. 6-15.
6. Пилипчук В. Г., Дзьобань О. П. Проблема агресії і насильства: світоглядно-інформаційний вимір. URL: social-science.com.ua/article/806
7. Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Актуальні проблеми управління державною безпекою: зб. матер. наук.-практ. конф (Київ, 19 березня 2015). К.: Центр навч., наук. та період. видань НА СБ України, 2015. С. 393-396.
8. Гриненко І. М., Ковальчук А. Ю., Прокоф'єва-Янчиленко Д. М., Сокрут Б. В. Управління ризиками організованої злочинності в Україні. К.: ВАІТЕ, 2013. 380 с.
9. Гриненко І. М., Прокоф'єва-Янчиленко Д. М., Сокрут Б. В. Ризики та загрози організованої злочинності в Україні: стан та перспективи. Київ: ВАІЕУ, 2014. 194 с.
10. Recommendation of the Council on the Governance of Critical Risks. Paris, 6-7 May 2014: [Online tool]. URL: http://www.oecd.org/mcm/C-MIN%282014%298-ENG.pdf (Accessed 13.11.2017).
11. National Security Strategy of the United States, The White House, February, 2015: [Online tool]. URL: https://www.whitehouse.gov/sites/default/ files/docs/2015_national_security_strategy.pdf
12. Andrews and Bonta (2006-2007). Risk-need-responsivity model for offender assessment and rehabilitation. Public Safety Canada, Ottowa, Ontario: [Online tool]. URL: http://www.publicsafety.gc.ca/res/cor/rep/risk_need_200706-eng.aspx.
13. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень. К.: НІСД, 2013. 104 с.